РЕГЛАМЕНТ

электронного взаимодействия Регистратора с Эмитентами и Акционерами

(Приложение № 5 к Правилам ведения реестров владельцев ценных бумаг от 07.07.2017 г.)

1. Термины и определения

В настоящем Регламенте используются следующие термины и определения:

Администратор безопасности – уполномоченное лицо Организатора СЭД, отвечающее за эксплуатацию следующих сервисов электронного взаимодействия и документооборота Регистратора с Эмитентами и акционерами - Личный кабинет эмитента, Личный кабинет акционера, системы электронного документооборота «ЭмитентИнформСервис», средств криптографической защиты информации и электронной подписи (далее «ЭП») и использование криптографических ключей.

Авторизация – санкционирование доступа пользователя ЛКЭ или ЛКА к их функциям и данным в объеме имеющихся у Пользователя прав и полномочий после успешного прохождения Аутентификации.

Акционер – зарегистрированное в реестре ценных бумаг Эмитента физическое или юридическое лицо, а также акционер акционерного инвестиционного фонда, владелец инвестиционного пая.

Аутентификация – проверка, осуществляемая ЛКЭ и ЛКА при входе Пользователя в систему. В ЛКЭ используется однофакторная аутентификация по паролю, полученному Пользователем при регистрации. В ЛКА используется двухфакторная аутентификация по установленному Пользователем паролю и одноразовому коду, получаемому Пользователем в виде смс-сообщения на свой контактный телефон при каждом входе в систему.

Владелец сертификата ключа проверки электронной подписи – Пользователь сервиса ЛКЭ и/или СЭД «ЭмитентИнформСервис» и/или ЛКА, которому в установленном настоящим Регламентом порядке выдан сертификат ключа проверки электронной подписи.

Доставка электронного сообщения/ документа – процесс перемещения электронного сообщения или документа от отправителя к получателю.

ЕСИА, Единая система идентификации и аутентификации — информационная система в Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных информационных системах и иных информационных системах (подробности по ссылке https://esia.gosuslugi.ru).

Заявление – заявление о подключении к сервису электронного взаимодействия, совершенное в письменном виде по форме, установленной Регистратором (Приложение № __к настоящему Регламенту).

Идентификация – определение пользователя ЛКЭ или ЛКА по присвоенному ему персональному идентификатору. Идентификатор присваивается Пользователю при его регистрации в ЛКЭ или ЛКА.

Информационная система – упоминаемые совместно или по отдельности ЛКЭ, ЛКА, СЭД «ЭмитентИнформСервис» и Система ведения реестров «Вереком-2».

Ключевой носитель – электронный информационный носитель, содержащий средства усиленной электронной подписи, в том числе криптографические ключи и сертификат ключа проверки электронной подписи.

Ключ электронной подписи – уникальная последовательность символов, известная только Владельцу сертификата ключа и предназначенная для создания усиленной электронной подписи.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Кодовое слово – секретное слово, указанное Пользователем в Заявлении о подключении к электронному сервису ЛКА и используемое для авторизации Пользователя ЛКА при его обращении по телефону к Регистратору.

Контактный телефон – номер мобильного телефона, указанный в Заявлении о подключении к электронному сервису ЛКА, либо в регистрационных данных Пользователя в ЕСИА.

Контактный e-mail – адрес электронной почты Пользователя, указанный в Заявлении о подключении к электронному сервису ЛКА, либо в регистрационных данных Пользователя в ЕСИА.

Компрометация ключа - констатация Пользователем сервиса ЛКЭ и/или ЛКА и/или СЭД «ЭмитентИнформСервис» обстоятельств, при которых возможно несанкционированное использование неуполномоченными лицами регистрационных данных, предоставляющих доступ и/или Ключ электронной подписи.

Конфиденциальная информация – документированная информация, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, при отсутствии к ней свободного доступа на законном основании и/или если обладатель информации принимает меры к ее охране.

Конфликтная ситуация - ситуация, при которой у Сторон возникает необходимость разрешить вопросы признания или непризнания авторства и/или целостности электронного запроса и/или сообщения, обработанных средствами криптографической защиты информации.

Криптографическая защита - защита данных при помощи их криптографического преобразования.

Криптографический ключ (Ключ) - общее название ключа усиленной электронной подписи и ключа проверки электронной подписи.

ЛКЭ, Личный кабинет эмитента – сервис электронного взаимодействия Регистратора с Эмитентами, интегрированный на интернет-сайте Регистратора в разделе «Личный кабинет эмитента», позволяющий Сторонам обмениваться информацией и документами в электронном виде.

ЛКА, Личный кабинет акционера – сервис электронного взаимодействия Регистратора с Акционерами, интегрированный на интернет-сайте Регистратора в разделе «Личный кабинет акционера», позволяющий Сторонам обмениваться информацией и документами в электронном виде, а также предоставляющий возможность Пользователю реализовывать корпоративные права посредством совершения юридически значимых действий, в частности - направленных на обеспечение возможности голосования на общем собрании акционеров Эмитента.

Логин – уникальная последовательность символов, позволяющая однозначно идентифицировать Пользователя ЛКЭ или Пользователя ЛКА.

Обработка информации– создание, хранение, передача, прием, преобразование и отображение информации.

Код – уникальная последовательность символов, действительная ограниченное время, однократно передаваемая Пользователю соответствующего электронного сервиса Регистратора, в целях подтверждения конкретных действий Пользователя в электронном сервисе.

Организатор системы электронного документооборота, Организатор СЭД – лицо, которое своими действиями создает организационно-технические предпосылки для электронного документооборота, в настоящем Регламенте под Организатором СЭД понимается Акционерное общество «Реестр» (лицензия ФСБ РФ на предоставление услуг в области шифрования информации №0013282 от 29.12.2014, лицензия ФСТЭК РФ на деятельность по

технической защите конфиденциальной информации №3040 от 27.09.2016).

Отправитель – лицо, которое направляет электронное сообщение и/или электронный документ через электронные сервисы ЛКЭ и/или ЛКА и/или СЭД «ЭмитентИнформСервис».

Пароль – известная только Пользователю ЛКА или ЛКЭ последовательность символов, используемая для аутентификации Пользователя.

Подписант электронного документа – уполномоченное лицо Эмитента или Регистратора, наделенное правом подписания электронного документа своей электронной подписью.

Получатель – лицо, которому адресовано электронное сообщение и/или документ, отправленные самим Отправителем или от имени и по поручению Отправителя.

Пользователь ЛКЭ и/или СЭД «ЭмитентИнформСервис» – Уполномоченное лицо Эмитента – владелец сертификата ключа проверки электронной подписи и/или простой электронной подписи, прошедший у Организатора СЭД этапы регистрации и допуска к работе с электронным сервисом ЛКЭ и/или СЭД «ЭмитентИнформСервис».

Пользователь ЛКА - физическое лицо, являющееся зарегистрированным лицом в реестре акционеров Эмитента или физическое лицо, являющееся представителем юридического лица, зарегистрированного в реестре акционеров Эмитента, и которому предоставлен доступ в ЛКА в соответствии с настоящим Регламентом.

Простая электронная подпись - электронная подпись, которая посредством использования логинов, паролей и/или иных средств подтверждает факт формирования электронной подписи Пользователем. Электронные документы и электронные сообщения, сформированные в ЛКА и/или ЛКЭ Пользователем, авторизованным с помощью его Логина и Пароля, и/или дополнительно подтвержденные Кодом, считаются подписанными простой электронной подписью.

Расшифровка - процесс криптографического преобразования зашифрованных данных в расшифрованные**.**

Регистрация – процедура создания в Информационной системе Регистратора записи о Пользователе сервиса.

Регламент электронного взаимодействия Регистратора с Эмитентами и Акционерами – настоящий Регламент, далее «Регламент», определяет условия и порядок электронного взаимодействия Регистратора с Эмитентами и Акционерами через сервисы электронного взаимодействия ЛКЭ, ЛКА и СЭД «ЭмитентИнформСервис». Регламент является приложением к Правилам ведения реестров владельцев ценных бумаг, размещенным на сайте Регистратора http://www.aoreestr.ru/, утвержденным Регистратором и согласованным в законодательно установленном порядке. Регистратор вправе вносить изменения и дополнения в Регламент в одностороннем порядке. Регламент в новой редакции вступает в силу по истечении тридцати рабочих дней с момента его опубликования на сайте Регистратора. Изменения и дополнения, внесенные Регистратором в настоящий Регламент, не имеют обратной силы и не изменяет правоотношений с Пользователями ЛКЭ, ЛКА и СЭД «ЭмитентИнформСервис», возникших до вступления в силу таких изменений и дополнений.

Регистрационный Центр (РЦ) – элемент инфраструктуры криптографических ключей, отвечающий за идентификацию и аутентификацию Пользователей при изготовлении сертификатов, и обладающий необходимым комплексом программно-технических средств усиленной ЭП и СКЗИ для организации защищенного канала связи, обеспечивающего достоверную передачу запросов сертификатов в УЦ.

Секретный ключ шифрования – уникальная последовательность данных, используемая для формирования электронной подписи и расшифровки запроса и/или электронного документа (см. также Ключ электронной подписи).

Сертификат ключа проверки электронной подписи (Сертификат ключа) – электронный документ и/или документ на бумажном носителе, выданные для усиленной электронной подписи Удостоверяющим центром или Администратором безопасности Организатора СЭД, и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа.

СЭД «ЭмитентИнформСервис», Система электронного документооборота «ЭмитентИнформСервис» – корпоративная информационная система, обеспечивающая в режиме удаленного доступа оперативное и конфиденциальное получение отчетов из электронной системы ведения реестров. Доступ осуществляется по каналам сети Internet в защищенном режиме с использованием криптографических ключей усиленной электронной подписи, выданных Удостоверяющим центром.

Система ведения реестров «Вереком-2», СВР – сертифицированное программное обеспечение ведения реестров акционеров (сертификат ПАРТАД №73 от 19.09.2003), используемое Регистратором в своей деятельности.

Системный журнал – электронный журнал информационной системы, автоматически формируемый соответствующей Информационной системой Организатора СЭД, в котором содержится информация о действиях и лицах, выполнивших эти действия (Пользователи и сотрудники Организатора СЭД) в Информационной системе.

СКЗИ, Средства криптографической защиты информации - совокупность программно-технических средств, обеспечивающих применение шифрования при организации запросов (электронных сообщений). СКЗИ могут применяться как в виде самостоятельных программных модулей, запускаемых в ручном или автоматическом режиме, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

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

Стороны электронного обмена информацией и документами, Стороны – Регистратор и Эмитент, Регистратор и Пользователь ЛКА

УЦ, Удостоверяющий центр УЦ – юридическое лицо, осуществляющее функции по созданию и выдаче Сертификатов ключей проверки электронной подписи, а также иных функций, предусмотренных действующим законодательством РФ.

Уполномоченное лицо Эмитента – физическое лицо – единоличный исполнительный орган Эмитента или лицо, включенное в Список уполномоченных лиц эмитента, имеющих право на получение информации.

Усиленная электронная подпись – неквалифицированная электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

В ходе взаимодействия Сторон, применяются следующие разновидности Усиленной электронной подписи:

УЦ «Сигнал-КОМ» - публичный Удостоверяющий Центр компании «Сигнал-КОМ» (Лицензия ФСБ РФ **ЛСЗ №0000089, рег. № 12291Н** от 22.06.2012 г. на осуществление работ и оказание услуг в области защиты информации), обладающий необходимым комплексом

программно-технических средств ЭП, обеспечивающих изготовление и обслуживание сертификатов ключей проверки электронной подписи (www.signal-com.ru).

Шифрование - процесс криптографического преобразования данных, позволяющий предотвратить доступ неуполномоченных лиц к зашифрованному содержимому электронного документа.

Электронное сообщение – сообщение, (информация) в электронном виде, отправляемое и получаемое Сторонами через электронные сервисы ЛКЭ и ЛКА, не скрепленное электронной подписью отправителя.

Электронный документ – документ, информация которого представлена в электронной форме и подписана тем видом электронной подписи, который предусмотрен настоящим Регламентом для подписания электронных документов определенного вида.

Эмитент (Эмитенты) – акционерное общество, держателем реестра владельцев ценных бумаг которого является Регистратор.

Одинаковые по наименованию термины, определенные в настоящем Регламенте, и используемые в законодательстве РФ, понимаются в значении, указанном в настоящем Регламенте. Остальные термины и определения, используемые в настоящем Регламенте, должны пониматься в соответствии с действующим законодательством Российской Федерации.

2. **Общие положения.**

2.1. Настоящий Регламент определяет порядок и условия обмена информацией и документами в электронном виде, подписанными электронной подписью посредством электронных сервисов ЛКА, ЛКЭ и/или СЭД «ЭмитентИнформСервис». Регламент также определяет порядок использования электронных подписей, виды подлежащих использованию электронных подписей, пределы компетенций используемых видов электронных подписей, условия регистрации, замены и аннулирования сертификатов ключей, правила работы с ключевыми носителями, а также порядок урегулирования споров, возникающих из электронного документооборота.

2.2. Авторизация Пользователя в ЛКА, ЛКЭ и/или СЭД «ЭмитентИнформСервис» означает согласие Пользователя с действующей редакцией Регламента.

2.3. Настоящий Регламент в соответствии со ст. 428 Гражданского кодекса Российской Федерации является договором присоединения. Договор присоединения считается заключенным с Пользователем с момента, когда Пользователь первый раз успешно авторизуется в ЛКА, ЛКЭ и/или СЭД «ЭмитентИнформСервис».

2.4. Присоединяясь к настоящему Регламенту в порядке, установленном ст. 437 и ст. 438 Гражданского кодекса Российской Федерации Пользователи ЛКЭ, ЛКА и/или СЭД соглашаются, что действие настоящего Регламента являются для них обязательными, а ввод Логина и Пароля перед началом работы в ЛКА или ЛКЭ является достаточным условием для идентификации и аутентификации Пользователя, и подтверждает его право пользоваться ЛКА или ЛКЭ в соответствии с условиями, закрепленными настоящим Регламентом.

2.5. Эмитент и Акционер обязуются не разглашать третьим лицам Логин и Пароль, предоставленные им для доступа к ЛКА или ЛКЭ, и в связи с этим принимают на себя все риски, связанные с их разглашением или утратой. Регистратор полностью освобождается от ответственности, связанной с разглашением или утратой Логина или Пароля. В отношении пользователей, Эмитент и Акционер подтверждают и гарантируют, что они получили от уполномоченных ими Пользователей ЛКА и ЛКЭ документальное подтверждение принятия на себя Пользователями аналогичных обязательств.

2.6. Эмитент и Акционер проинформированы и согласны с тем, что при использовании ими/их уполномоченными Пользователями ЛКА, ЛКЭ или СЭД «ЭмитентИнформСервис»

Эмитент и Акционер принимают на себя все риски, связанные с нарушением конфиденциальности, в том числе связанные с неправомерными действиями третьих лиц, направленными на причинение вреда (убытков) Пользователям, Эмитенту, Акционеру или Регистратору.

2.7. Право пользования ЛКА и ЛКЭ предоставляется Регистратором безвозмездно. Услуги Регистратора, оказываемые с помощью ЛКА и ЛКЭ, тарифицируются в соответствии с Прейскурантом дополнительных услуг Регистратора, либо их стоимость определяется договорами с Регистратором.

2.8. Электронные документы, созданные/пересылаемые Регистратором или Пользователями с использованием ЛКА и ЛКЭ, и подписанные одним из предусмотренных настоящим Регламентом видом электронной подписи, в соответствии с п. 2 ст. 6 Федерального закона от. 06.04.2011 г. № 63-ФЗ «Об электронной подписи» признаются равнозначными документам на бумажных носителе, подписанным собственноручной подписью и вступают в силу для подписавшей их стороны с момента подписания, а для противоположной Стороны – с момента направления ей такого документа в порядке, предусмотренном настоящим Регламентом.

2.9. В предусмотренных настоящим Регламентом случаях, при направлении Регистратором и Пользователями в адрес друг друга электронных документов, подписанных простой электронной подписью, такие документы признаются равнозначными документам на бумажном носителе, подписанным собственноручными подписями Пользователя ил уполномоченных представителей Регистратора.

2.10. ЛКА и ЛКЭ обеспечивают автоматическую авторизацию Пользователя для определения его полномочий на формирование и отправку юридически значимых электронных документов.

2.11. Стороны не вправе оспаривать признание электронной подписи и (или) подписанного ею электронному документа, как не имеющего юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в сервисе ЛКА, ЛКЭ и СЭД «ЭмитентИнформСервис».

2.12. Для работы с ЛКА, ЛКЭ или СЭД «ЭмитентИнформСервис» на компьютере Пользователя необходимо обеспечить доступ к информационно-коммуникационной сети Internet, установить Web-браузер с включенным Java Script.

2.13. Для работы с ЛКА через мобильное приложение на мобильном устройстве Пользователя необходимо установить приложение «Реестр-Онлайн» из магазина мобильных приложений для операционных систем Android или iOS.

2.14. Электронные документы, которыми обмениваются стороны в СЭД «ЭмитентИнформСервис» , ЛКЭ и/или ЛКА являются для сторон юридически значимыми и признаются электронными документами, равнозначными документам на бумажном носителе, подписанным собственноручной подписью уполномоченного представителя Стороны-Отправителя и влекут правовые последствия, предусмотренные для соответствующих типов документов.

2.15. Стороны соглашаются, что используемые ими организационные и технические средства осуществления электронного документооборота обеспечивают необходимый уровень конфиденциальности и защиты информации от неправомерных действий третьих лиц, и являются достаточными для обеспечения достоверности, целостности и однозначного определения подлинности электронного документа, владельца сертификата ключа проверки электронной подписи.

2.16. Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов).

2.17. Замена ключей электронной подписи не влияет на юридическую силу электронного

документа, если он был подписан электронной подписью, действительной на момент подписания.

2.18. При выдаче, внеплановой смене ключей электронной подписи, а также в случае их компрометации Стороны руководствуются настоящим Регламентом.

2.19. Сертификаты ключей действительны до момента истечения установленного срока их действия или аннулирования.

2.20. Любой Пользователь вправе получить консультацию по всем вопросам, связанным с работой ЛКА и ЛКЭ, обратившись к уполномоченным сотрудникам Регистратора в порядке, указанном на официальном сайте по адресу http://www.aoreestr.ru/.

2.21. Пользователь уведомляется о том, что при обращении по телефону к Регистратору по вопросам, связанным с работой ЛКА, ЛКЭ или СЭД «ЭмитентИнформСервис» Регистратор вправе осуществлять запись телефонных разговоров, запросить кодовое слово для дополнительной идентификации обратившегося лица.

2.22. Сервис ЛКА, ЛКЭ и СЭД «ЭмитентИнформСервис» предоставляется Пользователям круглосуточно. Ограничение доступа к указанным сервисам может осуществляться Регистратором в одностороннем порядке для проведения технических работ. Информация об ограничении доступа размещается на официальном сайте Регистратора по адресу: http://www.aoreestr.ru/.

3. **Сервис ЛКЭ**

3.1. Условия получения доступа к сервису ЛКЭ

3.1.1. Для осуществления электронного обмена электронными сообщениями и электронными документами между Сторонами, а также направления Эмитентом Регистратору online запросов на получение информации из реестра в виде бумажного документа, Стороны используют сервис ЛКЭ, доступ к которому осуществляется с сайта АО «Реестр» по защищенному internet-соединению.

3.1.2. Для получения доступа к сервису ЛКЭ, Организатор СЭД, на основании Заявления Уполномоченного лица Эмитента о подключении к электронному сервису ЛКЭ (далее – Заявление о подключении), предоставляет заявителю запечатанный конверт, содержащий простую электронную подпись – Логин и Пароль. Заявление о подключении подлежит подписанию со стороны Эмитента только в случае, если конверт, содержащий логин и пароль не поврежден и не вскрыт.

3.1.3. Подписание Заявления о подключении, подтверждает согласие Эмитента с условиями настоящего Регламента, а также подтверждает, что Эмитента полностью удовлетворяет предоставляемая Организатором СЭД степень защиты информации, обмен которой предполагается в рамках сервиса ЛКЭ.

3.1.4. Доступ Пользователя к электронному сервису ЛКЭ предоставляется в течение 1 (одного) рабочего дня после получения Организатором СЭД оригинала Заявления о подключении, подписанного Уполномоченным лицом Эмитента и при условии идентификации его подписи.

3.1.5. Организатор СЭД, выполняет процедуру активации выданной Пользователю простой электронной подписи в сервисе ЛКЭ и высылает соответствующее уведомление по адресу электронной почты, указанному в Заявлении о подключении.

3.1.6. Предоставление доступа каждому следующему Уполномоченному представителю Эмитента осуществляется Организатором СЭД по процедуре, предусмотренной п.п. 3.2 - 3.4 настоящего Регламента.

3.1.7. Пользователь системы ЛКЭ может выступать в качестве Уполномоченного лица от нескольких Эмитентов, в этом случае он может получить один комплект простой и усиленной

электронной подписи для всех представляемых им Эмитентов.

4. **Работа в ЛКЭ и СЭД «ЭмитентИнформСервис»**

4.1. С целью обеспечения авторства, юридической значимости, достоверности, целостности и конфиденциальности электронных документов, запросов и электронных сообщений при информационном взаимодействии Стороны используют простую электронную подпись, Средства криптографической защиты информации и усиленную электронную подпись.

4.2. При успешном входе в электронный сервис ЛКЭ с использованием простой электронной подписи, Пользователь получает доступ ко всем возможностям, электронного сервиса ЛКЭ, включая право создания ключа усиленной ЭП.

4.3. После создания сертификата ключа усиленной ЭП, Пользователь получает возможность подписания ЭП и направления Регистратору: распоряжений на предоставление информации из реестра, заявлений, договоров/соглашений на оказание услуг Регистратора, сообщений и иной информации (материалов), подлежащей предоставлению лицам, имеющим право на участие в общем собрании акционеров, а также номинальным держателям.

4.4. После получения доступа к СЭД «ЭмитентИнформСервис» и создания ключа усиленной ЭП, Пользователь получает возможность подписания такой ЭП и направления Регистратору распоряжений на предоставление информации из реестра, а также получения подписанных усиленной ЭП Регистратора ответов, содержащих информацию из реестра, подготовленную по распоряжениям Эмитента.

4.5. Сформированные в электронном сервисе ЛКЭ и СЭД «ЭмитентИнформСервис» электронные документы, подписанные электронной подписью Отправителя, автоматически (без участия оператора) регистрируются в системе ведения реестра и являются безотзывными.

4.6. Обмен иной информацией, предусмотренной возможностями электронного сервиса ЛКЭ и СЭД «ЭмитентИнформСервис», не указанной в настоящем разделе Регламента, осуществляется Сторонами в виде электронных сообщений.

5. **Сервис ЛКА**

5.1. Функциональные возможности Пользователя сервиса ЛКА.

Сервис ЛКА предоставляет Пользователям следующие возможности:

- получать сведения о ценных бумагах, учитываемых на лицевых счетах Акционера, открытых в реестрах владельцев ценных бумаг Эмитентов, ведение которых осуществляется Регистратором;
- голосовать на общем собрании акционеров путем заполнения на сайте в сети Internet электронной формы бюллетеней не позднее двух дней до даты проведения общего собрания акционеров или до даты окончания приема бюллетеней при проведении общего собрания акционеров в форме заочного голосования в случае, если у Регистратора заключен договор с Эмитентом, предполагающий такую возможность;
- регистрироваться и голосовать на общем собрании акционеров путем заполнения электронной формой бюллетеней в день проведения общего собрания в случае если у Регистратора заключен договор с Эмитентом, предполагающий такую возможность;
- получать сведения о корпоративных действиях, проводимых Эмитентом - общих собраниях акционеров, выкупах ценных бумаг и прочих действиях в случае, если Регистратор получил соответствующее поручение от Эмитента;
- получать сообщения от Регистратора и от Эмитентов;

5.2. Условия получения доступа к сервису ЛКА

5.2.1. Доступ к сервису ЛКА предоставляется Регистратором лицам, зарегистрированным в

реестре владельцев ценных бумаг. Доступ к сервису ЛКА может быть предоставлен владельцам ценных бумаг, сведения о которых были переданы Регистратору номинальным держателем в процессе подготовки к проведению собрания акционеров. Регистрация новых пользователей в ЛКА осуществляется одним из двух способов – путем личной подачи Заявления Регистратору или путем авторизации через ЕСИА.

5.2.2. Регистрация Пользователя путем подачи Заявления происходит в следующем порядке:

- Пользователь обращается в офис регистратора, заполняет и предоставляет Заявление на подключения сервиса ЛКА.
- Регистратор регистрирует Пользователя в ЛКА и выдает Пользователю запечатанный конверт, содержащий Логин и Пароль Пользователя. Для замены ранее указанных Пользователем в Заявлении номера контактного телефона, а также адреса электронной почты, необходимо личное обращение Пользователя в офис Регистратора и подача Заявления для внесения изменений в учетные данные Пользователя.
- Доступ к сервису ЛКА открывается Пользователю не позднее следующего рабочего дня после регистрации.
- При первом входе в ЛКА Пользователь должен сменить полученный в запечатанном конверте временный Пароль на постоянный.

5.2.3. Регистрация Пользователя с авторизацией через ЕСИА осуществляется в следующем порядке:

- Пользователь заходит в ЛКА по ссылке на сайте Регистратора или устанавливает мобильное приложение и входит в него;
- Незарегистрированный Пользователь нажимает на кнопку регистрации через сайт Государственных услуг – систему ЕСИА;
- После прохождения авторизации Пользователь подтверждает свое согласие на передачу своих данных в АО «Реестр», после чего автоматически возвращается в ЛКА;
- В экранной форма ЛКА Пользователь вносит Пароль, который он будет использовать в дальнейшем при авторизации в ЛКА;
- ЛКА направляет на контактный телефон Пользователя код для подтверждения регистрации, после ввода которого автоматически регистрирует нового Пользователя;
- Замена используемого Пользователем номера контактного телефона, а также адреса электронной почты осуществляется только через сайт Государственных услуг;
- Доступ к сервису ЛКА открывается Пользователю не позднее следующего рабочего дня после регистрации.

5.2.4. Успешно прошедший аутентификацию Пользователь авторизуется системой и получает полный доступ к ее функционалу и данным.

6. **Документы ЭДО**

6.1. Подлинник электронного документа (порядок признания).

Все экземпляры Электронного документа, имеющиеся у Организатора СЭД и Эмитента, являются подлинниками данного Электронного документа. Подлинник электронного документа может иметь неограниченное количество экземпляров. Подлинником Электронного документа считается документ с воспроизведенным содержанием и Электронной подписью. Подлинник Электронного документа не существует, если:

- нет ни одного учтенного Организатором СЭД или Эмитентом экземпляра данного Электронного документа;
- получение или восстановление экземпляра данного Электронного документа невозможно;
- нет способа установить подлинность Электронной подписи.

6.2. Порядок проверки электронной подписи и подлинности электронного документа.

Все электронные документы, отправляемые и получаемые Сторонами, обязательно

проверяются на целостность (доставку в неискаженном виде, по отношению к первоначальному) и неизменность электронной подписи.

Полученный электронный документ проверяется на соответствие установленному для него формату.

Электронный документ подлежит дальнейшей обработке и исполнению только в случае положительного результата проверки целостности электронного документа, его соответствия установленному формату и подлинности ЭП.

В случае невозможности расшифровки электронного документа, а также при отрицательном результате проверки целостности электронного документа и/или соответствия установленному формату и/или подлинности ЭП документ считается не полученным и не подлежит дальнейшей обработке и исполнению. В этих случаях Получателем отправляется уведомление Отправителю с указанием причины неполучения документа.

В случае возникновения конфликтных ситуаций между Сторонами о порядке признания подлинности электронного документа, подписанного усиленной электронной подписью, криптографические ключи которой выдает Удостоверяющий центр, любая Сторона имеет право обратиться в Удостоверяющий центр для проверки электронной подписи Отправителя и установления подлинности электронного документа.

В случае необходимости получения доказательств фактов осуществления каких-либо действий в Информационной системе, включая, действия с электронными документами, а также установления лиц из числа сотрудников Организатора СЭД или Пользователей, осуществивших такие действия, необходимым и достаточным доказательством будет являться заверенная руководителем Организатора СЭД выписка из Системного журнала Информационной системы Организатора СЭД. Данным способом подтверждаются такие действия как: создание, модификация, уничтожение и подписание электронной подписью электронных документов в Информационных системах организатора СЭД.

6.3. Копия электронного документа на бумажном носителе (порядок изготовления).

Для преобразования электронного документа, подписанного усиленной электронной подписью, в копию электронного документа на бумажном носителе используются возможности сервиса ЛКЭ, СЭД «ЭмитентИнформСервис» и СВР «Вереком-2». Печатный экземпляр электронного документа, полученного Эмитентом от Регистратора, может также содержать графические изображения подписи уполномоченного лица и печати Регистратора.

Официальная копия электронного документа на бумажном носителе заверяется собственноручной подписью уполномоченного лица Регистратора или Эмитента, скрепляется соответствующей печатью и должна содержать обязательную отметку, свидетельствующую о том, что это копия.

В зависимости от целей использования, копия электронного документа может быть представлена, либо в виде распечатки машинных кодов, содержащихся в электронном документе, либо в форме, понятной третьим лицам (с учетом выполненных преобразований машинных кодов). Информация, содержащаяся в копии электронного документа на бумажном носителе должна соответствовать информации, содержащейся в подлиннике электронного документа, в том числе, с учетом преобразования машинных кодов в значения, понятные третьим лицам.

7. **Обязанности Организатора СЭД**

7.1. Обеспечивать бесперебойную работу электронных сервисов ЛКЭ и ЛКА и СЭД «ЭмитентИнформСервис».

7.2. Обеспечивать Пользователям сервисов ЛКЭ, ЛКА и СЭД «ЭмитентИнформСервис» возможность выполнения всей совокупности доступных действий в соответствии с условиями настоящего Регламента.

7.3. В отношении каждого Пользователя, предоставить Эмитенту неисключительные права на использование программного обеспечения, необходимого для доступа к СЭД «ЭмитентИнформСервис».

7.4. Организовывать работу с криптографическими ключами Пользователей (регистрацию, учет, аннулирование) в порядке и объеме, определяемыми настоящими Регламентом.

7.5. Соблюдать режим конфиденциальности, предпринимать необходимые и достаточные организационно-технические меры по защите информации, которая становится доступной Организатору СЭД в связи с выполнением им своих функций, и которая содержится в электронных сервисах ЛКЭ и ЛКА и в СЭД «ЭмитентИнформСервис», а также касается паролей, идентификаторов и Криптографических ключей.

7.6. Предпринимать организационные и технические меры в целях предотвращения конфликта интересов между деятельностью Организатора СЭД и Регистратора.

8. **Обязанности Регистратора**

8.1. Выполнять операции в системе ведения реестра в строгом соответствии с законодательством о рынке ценных бумаг.

8.2. Сохранять конфиденциальность информации, содержащейся в базах данных сервисов ЛКЭ и ЛКА, СЭД «ЭмитентИнформСервис», системе ведения реестра.

8.3. Предоставлять информацию из системы ведения реестра посредством электронного сервиса ЛКЭ и СЭД «ЭмитентИнформСервис», в строгом соответствии с параметрами запроса Пользователя.

8.4. Предоставлять информацию из системы ведения реестра посредством СЭД «ЭмитентИнформСервис» в автоматическом режиме (без участия оператора) в виде электронного документа в формате html или pdf.

8.5. Предоставлять информацию из системы ведения реестра посредством электронного сервиса ЛКЭ и СЭД «ЭмитентИнформСервис» с участием сотрудника Регистратора в течение сроков, установленных Правилами ведения реестра владельцев именных ценных бумаг АО «Реестр».

9. **Доступ к СЭД «ЭмитентИнформСервис»**

9.1. Доступ к сети Internet и электронной почте, а также поддержание их в работоспособном состоянии Стороны осуществляют самостоятельно на условиях, определенных договорными отношениями с провайдером соответствующих телекоммуникационных услуг сети Internet каждой из Сторон.

9.2. Для доступа к СЭД «ЭмитентИнформСервис» Эмитент должен заключить с Регистратором соответствующий договор/соглашение, определяющие условия и порядок предоставления услуг в СЭД «ЭмитентИнформСервис», иметь действующий сертификат ключа проверки усиленной ЭП, зарегистрированный в Удостоверяющем центре.

9.3. Порядок установки и работы с СЭД «ЭмитентИнформСервис» изложены в «Руководстве пользователя ЭДО «ЭмитентИнформСервис», размещенном в электронном сервисе ЛКЭ.

9.4. Срок действия одного сертификата, составляет 1 (один) календарный год с даты его регистрации в Удостоверяющем центре, по истечении указанного срока сертификат прекращает свое действие и доступ к СЭД «ЭмитентИнформСервис» становится невозможным.

9.5. За 1 (один) месяц до истечения срока действия сертификата, Организатор СЭД уведомляет об этом Пользователя при входе в СЭД «ЭмитентИнформСервис».

9.6. Организатор СЭД имеет право ограничить доступ и приостановить оказание услуг, посредством СЭД «ЭмитентИнформСервис», конкретному Пользователю, в случае нарушения им настоящего Регламента. Уведомление о приостановлении направляется на электронный почтовый ящик Пользователя в течение одного рабочего дня.

9.7. Организатор СЭД имеет право ограничить доступ и приостановить оказание услуг Эмитенту, посредством СЭД «ЭмитентИнформСервис», в случае нарушения им условий оплаты услуг Регистратора по договору на ведение и хранение реестра.

10. **Регистрация Пользователя в Удостоверяющем центре**

10.1. Сертификат ключа проверки усиленной электронной подписи, выдаваемый Удостоверяющим центром, необходимый для работы в СЭД «ЭмитентИнформСервис», регистрируется в реестре сертификатов удостоверяющего центра и может быть получен следующим образом:

- самостоятельное создание Пользователем ключевого носителя, секретных ключей электронной подписи и запроса на сертификат ключа проверки электронной подписи. Программное обеспечение и пошаговая инструкция размещены в специальном разделе сервиса ЛКЭ;
- создание ключевого носителя, секретных ключей и запроса на сертификат ключа проверки электронной подписи Организатором СЭД на основании Заявления (Приложение № 1) в электронном виде и подписанного усиленной ЭП Пользователя электронного сервиса ЛКЭ или в бумажном виде и подписанного личной подписью Пользователя. Пошаговая инструкция о порядке действий размещена в соответствующем разделе сервиса ЛКЭ.

10.2. Изготовление сертификата ключа проверки электронной подписи подлежит оплате Эмитентом в соответствии с Тарифами на пользование СЭД «ЭмитентИнформСервис». Для упрощения процедуры взаимодействия с удостоверяющим центром, все мероприятия по созданию ключевого носителя и обработке запроса на сертификат ключа проверки электронной подписи осуществляет Организатор СЭД в лице Администратора безопасности. После оплаты счета, запрос на сертификат направляется Администратором безопасности в удостоверяющий центр и вносится в реестр действующих сертификатов. После успешной регистрации сертификата в удостоверяющем центре, Администратор безопасности:

- высылает Пользователю Акт приема-передачи ПО (Приложение № 3) и сертификат ключа проверки электронной подписи (при самостоятельном варианте). Акт приема-передачи, подписанный Пользователем должен быть направлен Организатору СЭД не позднее 15 дней с даты передачи сертификата. В случае нарушения сроков отправки Акта приема-передачи, Организатор СЭД имеет право приостановить доступ пользователя к СЭД «ЭмитентИнформСервис».
- либо записывает сертификат на ключевой носитель (при варианте создания ключевого носителя Организатором СЭД) и передает его Пользователю по Акту приема-передачи (Приложение № 3).

10.3. По запросу Пользователя Организатор СЭД может выдать сертификат ключа проверки электронной подписи Пользователя на бумажном носителе, заверенный Администратором безопасности. Для получения сертификата на бумажном носителе, заверенного уполномоченным представителем Удостоверяющего центра, Пользователь должен обратиться непосредственно в публичный Удостоверяющий центр.

11. **Обязанности и ответственность Эмитента**

11.1. Для начала оказания услуг, с использованием электронного сервиса ЛКЭ и СЭД

«ЭмитентИнформСервис», Эмитент должен выполнить следующие условия:

- Получить у Организатора СЭД на основании Заявления о подключении простую электронную подпись для доступа и использования сервиса ЛКЭ;
- Для создания распоряжений на предоставление информации из реестра в сервисе ЛКЭ - сгенерировать и зарегистрировать усиленную ЭП;
- Для создания распоряжений на предоставление информации из реестра в СЭД «ЭмитентИнформСервис» - создать и подать Организатору СЭД, действующему в качестве уполномоченного представителя Удостоверяющего центра, заявление на регистрацию усиленной ЭП. Получить у Организатора СЭД под роспись сертификат ключа усиленной ЭП, Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи.

11.2. Эмитент должен обеспечить Пользователям организационно-технические возможности для безопасного хранения и использования ключевого носителя, содержащего закрытый ключ электронной подписи, предотвращения его порчи, потери, модификации или несанкционированного использования, в том числе:

- обеспечить защиту компьютера Пользователя от несанкционированного доступа лиц, не имеющих полномочий для доступа к электронным сервисам ЛКЭ и ЛКА, а также к СЭД «ЭмитентИнформСервис»;
- обеспечить антивирусную защиту компьютера Пользователя и регулярное обновление антивирусных баз.

11.3. Организовать, на срок не менее 5 лет, хранение ключевых носителей и/или ключей электронной подписи Пользователей, с истекшим сроком действия сертификата ключа проверки электронной подписи.

11.4. Организовать создание Пользователям электронных почтовых ящиков, необходимых им для обмена информацией в сервисах ЛКЭ и ЛКА, а также в СЭД «ЭмитентИнформСервис».

11.5. Обеспечить доступ Пользователей к электронным почтовым ящикам, необходимым для работы в сервисах ЛКЭ, ЛКА, а также в СЭД «ЭмитентИнформСервис» (в том числе, провести настройку спам-фильтров для пропуска почтовых сообщений, направляемых из доменной зоны aoreestr.ru).

11.6. В случае, если выбранный режим обслуживания Эмитента предполагает оплату услуг Регистратора за каждое распоряжение на предоставление информации из реестра, то Эмитент обязан оплатить заказанные услуги, даже если Пользователь - направил в адрес Регистратора множество идентичных распоряжений.

12. **Обязанности и ответственность Пользователя**

12.1. Пользователь не должен использовать ключевой носитель, содержащий секретный ключ электронной подписи, для целей отличных от целей доступа в сервисы ЛКЭ иили к СЭД «ЭмитентИнформСервис» (в том числе не использовать ключевой носитель для записи, хранения и переноса информации, кроме той, которая была записана в процессе формирования криптографических ключей электронной подписи).

12.2. Пользователь не должен совершать действий, могущих привести к утере, порче ключевого носителя, нарушению целостности криптографических ключей, и иным событиям, в результате которых доступ к ЛКЭ и/или СЭД «ЭмитентИнформСервис» окажется невозможен и/или такой доступ будет предоставлен неуполномоченным лицам.

12.3. Пользователь должен обеспечивать конфиденциальность информации, обеспечивающей доступ к ЛКЭ и/или ЛКА (включая простую электронную подпись) и/или СЭД «ЭмитентИнформСервис». Запрещается высылать указанную информацию кому бы то ни было по электронной почте, даже если такое указание получено от Администратора безопасности.

12.4. Пользователь несет ответственность за все риски несанкционированного распространения информации, полученной посредством доступа к ЛКЭ и/или ЛКА и/или СЭД «ЭмитентИнформСервис», в связи с передачей неуполномоченным лицам простой электронной подписи и/или ключевого носителя.

12.5. Пользователь должен незамедлительно известить Организатора СЭД по телефону и/или электронной почте о ставших ему известными действиях третьих лиц, способных привести к компрометации простой электронной подписи и/или нарушению целостности криптографических ключей и системы криптозащиты информации.

12.6. Пользователь должен не реже одного раза в год самостоятельно производить смену пароля для доступа к сервисам ЛКЭ и/или ЛКА и СЭД «ЭмитентИнформСервис» (подробнее о порядке действий см. Руководство пользователя).

12.7. Для предотвращения похищения и искажения информации, содержащейся на ключевом носителе, на компьютере, с которого производится доступ к ЛКА, ЛКЭ и/или СЭД «ЭмитентИнформСервис», необходимо регулярно проводить:

- обновление операционной системы, устанавливая свежие версии «заплаток безопасности»;
- антивирусную проверку со свежими антивирусными базами.

12.8. Для предотвращения похищения и искажения информации, содержащейся на ключевом носителе не рекомендуется пользоваться доступом к электронным сервисам ЛКЭ и/или ЛКА, и/или СЭД «ЭмитентИнформСервис» в небезопасных сетях и с компьютеров общего пользования.

12.9. Пользователь должен регулярно проверять электронный почтовый ящик, указанный Пользователем для работы в ЛКЭ и/или ЛКА и/или СЭД «ЭмитентИнформСервис». В случае получения сообщения от Администратора безопасности выполнить предписываемые действия.

12.10. Пользователь должен немедленно обратиться к Организатору СЭД с заявлением (подается через электронный сервис ЛКЭ, подписанное усиленной электронной подписью, или путем подачи данного заявления на бумажном носителе, заверенного собственноручной подписью) о прекращении действия сертификата ключа в случае компрометации ключа, то есть если стало известно, что носитель, содержащий простую электронную подпись и/или ключевой носитель, содержащий криптографические ключи, несанкционированно используется или использовался лицами, не имеющими на это право, а также в случае его потери или модификации. До момента получения такого заявления Организатором СЭД, Стороны предполагают, что простая электронная подпись и сертификат ключа ЭП являются действующими, документы, подписанные такой ЭП, являются юридически значимыми и действительными. Оспорить юридическую значимость таких документов только на том основании, что впоследствии сертификат ключа ЭП был скомпрометирован – невозможно.

Пользователь ЛКА в случае компрометации своего логина и/или пароля должен немедленно обратиться к организатору СЭД с заявлением о прекращении их действия и запросом на получение новых.

12.11. Пользователь не должен применять ключевой носитель с момента компрометации ключа электронной подписи.

12.12. При несоблюдении требований, изложенных в настоящем разделе Регламента, солидарная ответственность за убытки, причиненные вследствие использования скомпрометированного ключа электронной подписи, возлагается на Пользователя электронных сервисов и на Эмитента (для ЛКЭ), Пользователя и Акционера (для ЛКА).

12.13. Направляя распоряжение на предоставление информации из реестра, Пользователь полностью осознает свои действия, что согласно выбранному режиму обслуживания,

предоставление такой информации может быть платным.

12.14. Подписывая своей ЭП договоры/соглашения на оказание услуг Регистратора, Пользователь создает правовые последствия для Эмитента по приемке и оплате заказанных услуг Регистратора.

12.15. Авторизуясь в Информационной системе для ее использования в соответствии с функциональными возможностями, Пользователь соглашается с порядком предоставления услуг с использованием сервисов Информационной системы, обязуется соблюдать правила и инструкции по работе с данными сервисами, а также руководствоваться указаниями организатора СЭД.

13. **Система обеспечения информационной безопасности**

13.1. Соблюдение требований информационной безопасности при работе с сервисами ЛКЭ и ЛКА, и/или СЭД «ЭмитентИнформСервис» призвано обеспечить:

- защиту информации от несанкционированного доступа;
- целостность, достоверность и криптографическую защиту информации;
- однозначную аутентификацию Отправителя электронного документа.

13.2. Система обеспечения информационной безопасности реализуется посредством применения аппаратно-программных средств и организационных мер.

13.3. К аппаратно-программным средствам относятся:

- ключевой носитель, содержащий криптографические ключи усиленной электронной подписи, сформированные Пользователем и подтвержденные Удостоверяющим Центром (для усиленной ЭП);
- встроенные в электронные сервисы ЛКЭ, ЛКА и СЭД «ЭмитентИнформСервис» программные средства, обеспечивающие реализацию системы ЭДО между Регистратором и Эмитентом, Регистратором и Акционером.

13.4. К организационным мерам относятся:

- безопасное хранение Пользователем простой электронной подписи и ключевого носителя, предотвращающее компрометацию, в том числе - потерю или несанкционированное использование;
- размещение аппаратно-программных средств ЛКЭ, ЛКА и СЭД «ЭмитентИнформСервис» в защищенном помещении Организатора СЭД с контролируемым доступом;
- административное ограничение доступа специалистов и уполномоченных лиц Организатора СЭД к аппаратно-программным средствам ЛКЭ, ЛКА и СЭД «ЭмитентИнформСервис».

14. **Функции, осуществляемые Организатором СЭД от имени Удостоверяющего Центра**

14.1. На основании договора, заключенного между Организатором СЭД с Удостоверяющим центром, Организатор СЭД выполняет функции Регистрационного центра, в том числе:

- внесение в реестр сертификатов ключей, который ведет Удостоверяющий центр, регистрационной информации о зарегистрированных Пользователях;
- ведение субреестра изготовленных сертификатов ключей Пользователей СЭД «ЭмитентИнформСервис»;
- предоставление сертификатов ключей, находящихся в реестре изготовленных сертификатов, в электронной форме и на бумажном носителе;
- отзыв (аннулирование) сертификатов ключей;
- приостановление / возобновление действия сертификатов ключей;

- предоставление сведений об аннулированных и приостановленных сертификатах ключей.

15. **Порядок действий при компрометации ключей**

15.1. При компрометации регистрационных данных, предоставляющих доступ к сервисам ЛКЭ, ЛКА или СЭД «ЭмитентИнформСервис» - простой электронной подписи и/или ключей усиленных электронных подписей Пользователь обязан прекратить доступ к сервисам.

15.2. К событиям, на основании которых принимается решение о компрометации, относятся (включая, но не ограничиваясь):

- утрата (подозрение об утрате, обнаружение после утраты) носителя и/или компьютерного оборудования, содержащего простую электронную подпись и/или сертификаты усиленных электронных подписей;
- увольнение сотрудника, имевшего доступ к оборудованию и носителям, содержащим простую электронную подпись и/или сертификаты усиленных электронных подписей;
- возникновение подозрений на утечку и/или искажение информации, получаемой в рамках сервисов ЛКЭ, ЛКА или в СЭД «ЭмитентИнформСервис».

15.3. Пользователь скомпрометированного ключа обязан незамедлительно проинформировать Организатора СЭД о факте компрометации (включая, но не ограничиваясь оперативными средствами связи: телефон, факс, электронная почта). При этом организатор СЭД вправе запросить дополнительную информацию об обратившемся лице, с целью его идентификации как Пользователя (иного уполномоченного представителя Эмитента).

15.4. Уведомление о компрометации, сделанное с использованием оперативных каналов связи, должно быть подтверждено заявлением о компрометации (Приложение № 2). Оригинал заявления о компрометации должен быть предоставлен Организатору СЭД не позднее 10 календарных дней с даты оперативного уведомления.

15.5. Организатор СЭД, получив оперативную информацию о компрометации ключей, убеждается в ее достоверности и приостанавливает доступ Пользователя к сервисам ЛКЭ, ЛКА или СЭД «ЭмитентИнформСервис» без аннулирования простой электронной подписи и/или сертификата ключа. Аннулирование простой электронной подписи и/или сертификата ключа производится после получения оригинала заявления.

15.6. Датой и временем компрометации считается дата и время получения Организатором СЭД оригинала заявления о компрометации.

15.7. Организатор СЭД осуществляет учет заявлений.

16. **Аннулирование и замена простой электронной подписи и сертификатов ключей усиленных электронных подписей**

16.1. Аннулирование простой электронной подписи осуществляется в случае ее компрометации. При замене простой электронной подписи, старая подпись аннулируется, а новая выдается в порядке, описанном в разделе 3;

16.2. Аннулирование сертификата ключа усиленной электронной подписи осуществляется Организатором СЭД в случае:

- компрометации криптографических ключей (по заявлению Пользователя или Эмитента Приложение №2);
- истечения срока действия сертификата (по заявлению Пользователя Приложение №2);
- изменения регистрационных данных Пользователя, указанных в сертификате (по заявлению Пользователя Приложение №2);
- в случае если Организатору СЭД или Удостоверяющему центру стало достоверно

известно об изменении содержимого и/или о прекращении действия документа, на основании которого сертификат был оформлен;
- в иных случаях, установленных законодательством РФ в сфере электронного документооборота и электронных подписей.

16.3. Аннулирование простой электронной подписи или сертификата ключа усиленной электронной подписи осуществляется Организатором СЭД в течение 1 (одного) рабочего дня после получения информации или документов о наступлении событий, указанных в данном пункте.

16.4. Временем аннулирования сертификата ключа усиленной электронной подписи признается время внесения соответствующей записи в реестр отозванных сертификатов удостоверяющего центра, уведомление об аннулировании сертификата направляется Эмитенту.

16.5. В случаях «замены» (аннулирование «старого» и выдача «нового») сертификатов усиленной электронной подписи при истечении срока действия и/или изменения регистрационных данных, указанных в сертификате Пользователь через специальные разделы сервиса ЛКЭ:

- самостоятельно создает сертификат ключа усиленной ЭП, в соответствии с п. 4.2. настоящего Регламента;
- получает сертификат ключа усиленной ЭП, в соответствии с п.10.1. настоящего Регламента.

16.6. Изготовление нового сертификата ключа усиленной ЭП в случае компрометации осуществляется Организатором СЭД только на основании оригинала заявления, подписанного Пользователем.

17. **Порядок ведения электронного архива**

17.1. Доступ к архиву электронных документов Пользователь получает непосредственно при обращении к сервисам ЛКЭ, ЛКА или СЭД «ЭмитентИнформСервис».

17.2. Хранение электронных документов сопровождается хранением сертификатов ключей.

17.3. Срок хранения сертификата ключа в форме электронного документа в УЦ после аннулирования сертификата ключа подписи составляет 5 лет.

17.4. По истечении указанного срока хранения сертификат ключа подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения. Срок архивного хранения сертификата ключа электронной подписи составляет не менее чем 5 (пять) лет. Порядок выдачи копий сертификатов ключей электронных подписей в этот период устанавливается в соответствии с законодательством РФ.

17.5. Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством РФ об архивах и архивном деле.

17.6. Не реже одного раза в месяц Организатор СЭД осуществляет резервное копирование:

- информации в электронном виде, обеспечивающей доступ Пользователей к сервисам ЛКЭ, ЛКА, и СЭД «ЭмитентИнформСервис»;
- информации в электронном виде о сертификатах ключей;
- программного обеспечения, составляющего сервисы ЛКЭ, ЛКА, и СЭД «ЭмитентИнформСервис».

17.7. Организатор СЭД осуществляет ежедневное резервное копирование и архивное хранение электронных документов, их реквизитов, включая информацию о датах и времени получении и отправки, а также об адресатах.

18. **Обстоятельства непреодолимой силы**

18.1. Стороны не несут ответственности за убытки, причиненные одной Стороной противоположной Стороне по причине несвоевременного или ненадлежащего выполнения обязательств, если такое невыполнение было обусловлено обстоятельствами непреодолимой силы (в том числе, действия органов государственной власти и управления, военные действия, стихийные бедствия, эпидемии, сбои, неисправности и отказы систем связи, энергоснабжения и жизнеобеспечения), которые Стороны не могли предвидеть и предотвратить.

18.2. Сторона, надлежащее исполнение обязательств которой оказалось невозможным в силу влияния обстоятельств непреодолимой силы, в течение 2 (двух) рабочих дней после их наступления в письменной форме информирует другую Сторону о наступлении этих обстоятельств и об их последствиях одним из перечисленных способов: через ЛКЭ или ЛКА, курьерской связью, заказным письмом с уведомлением о получении сообщения, по электронной почте с уведомлением о прочтении сообщения и др., а также принимает все возможные меры с целью максимально ограничить отрицательные последствия, вызванные указанными обстоятельствами.

18.3. Не извещение или несвоевременное извещение об обстоятельствах непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства как обстоятельства, освобождающие от ответственности.

19. **Разрешение спорных ситуаций**

19.1. В случае возникновения споров или разногласий между Сторонами, вытекающих из настоящего Регламента или связанных с ним, Стороны принимают все меры к разрешению их путем переговоров.

19.2. В случае невозможности разрешения споров путем переговоров они подлежат рассмотрению в Арбитражном суде г. Москвы.

19.3. В качестве эксперта по СКЗИ и ЭП может быть привлечена третья сторона - Удостоверяющий центр.

20. **Техническая поддержка Пользователей**

20.1. Поддержка Пользователей по работе с электронными сервисами ЛКЭ и ЛКА, а также СЭД «ЭмитентИнформСервис» осуществляется:

- в разделе «Помощь» соответствующего электронного сервиса;
- специалистами службы технической поддержки по тел. (495) 617-01-01 доб. 7337 в рабочие дни (с понедельника по пятницу) с 9:30 до 18:00 по московскому времени;
- по электронной почте eis@aoreestr.ru.