Приложение к Решению
Единоличного исполнительного органа
ООО «Спутник ЦФА»
№ 20241004-1 от 04.10.2024 г.

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«СПУТНИК ЦФА»

ПРАВИЛА ИНФОРМАЦИОННОЙ СИСТЕМЫ ООО «СПУТНИК ЦФА»

Москва
2024 г.

Содержание

1. Термины и определения.....3
2. Общие положения.....4
3. Алгоритмы программ Системы и правила внесения изменений в них.....6
4. Правила взаимодействия оператора информационной системы с пользователями……6
5. Порядок присоединения к Правилам и регистрация Пользователей……...8
5.1. Регистрация Пользователей-индивидуальных предпринимателей……8
5.2. Регистрация Пользователей-юридических лиц или иностранных структур без образования юридического лица……..8
5.3. Заверения об обстоятельствах……8
5.4. Порядок ведения Реестра Пользователей……...9
5.5. Порядок обеспечения доступа к функционалу Платформы через Личный кабинет……....10
5.6. Порядок восстановления доступа к Личному кабинету в случае его утраты……11
5.7. Порядок приостановления и прекращения доступа Пользователей к Системе……11
6. Правила выпуска и погашения цифровых прав……...13
6.1. Правила выпуска Цифровых прав……13
6.2. Погашение записей о Цифровых правах……..14
7. Способы учета цифровых прав в системе, а также внесения (изменения) записей о цифровых правах в систему……15
7.1. Учет Цифровых прав……..15
7.2. Порядок привлечения Валидаторов……..15
7.3. Реализация волеизъявления Пользователя в случае сбоя в работе информационных технологий Системы……..16
8. Требования к защите информации, операционной надежности и к информационной безопасности оператора ЦФА……...……16
8.1. Требования к защите информации и операционной надежности……..16
8.2. Требования к информационной безопасности оператора ЦФА……....21
9. Правила привлечения операторов обмена……....22
9.1. Правила привлечения Операторов обмена……...22
10. Порядок заключения и исполнения сделок в системе……23
10.1. Порядок осуществления сделок с Цифровыми правами……..…23
10.2. Порядок исполнения Оператором требований Актов…….……24
10.3 Порядок подтверждения Транзакций……..24
11. Прочие положения……...25
11.1. Правила взаимодействия с Номинальными держателями……25
11.2. Определение тарифов Оператора и порядок оплаты услуг……..26
11.3. Ответственность……...26
11.4. Заверения об обстоятельствах…….……26
11.5. Порядок разрешения споров……27

1. Термины и определения.

Адрес – идентификатор Кошелька в распределенном реестре.

Акт – вступивший в законную силу судебный акт, исполнительный документ, в том числе постановление судебного пристава-исполнителя, акты других органов и должностных лиц при осуществлении ими своих функций, предусмотренных законодательством Российской Федерации, либо выданное в порядке, предусмотренном законом, свидетельство о праве на наследство, предусматривающее переход Цифровых прав в порядке универсального правопреемства, на основании которого Оператор обязан обеспечить внесение (изменение) записей о Цифровых правах.

Валидатор – Пользователь, обеспечивающий тождественность информации, содержащейся в Системе, с использованием процедур подтверждения действительности, вносимых в нее (изменяемых в ней) записей.

Закон о ЦФА – Федеральный закон от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

Закон № 115-ФЗ – Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Заявка –заявка на приобретение выпускаемых Цифровых прав.

Идентификатор пользователя – уникальный идентификатор, однозначно определяющий Пользователя, и представляющий собой символьную строку фиксированной длины.

Идентификатор профиля – уникальный идентификатор, однозначно определяющий Пользователя, а также его категорию в Системе (категории предусмотрены пунктом 4.5 Правил), и представляющий собой символьную строку фиксированной длины.

Информационная система – информационная система, организованная на основе распределенного реестра, в которой осуществляется выпуск и учет Цифровых прав. Внесение записей в отношении Цифровых прав (в том числе при их выпуске) осуществляется исключительно в Информационной системе.

Кошелек – совокупность записей в распределённом реестре, описывающая состояние остатков Цифровых прав, принадлежащих Пользователю или учитываемых Пользователем.

Код подтверждения – временный код, отправляемый на устройство или номер телефона Пользователя с помощью приложения, предназначенного для временных кодов, или СМС сообщения

Корпоративный Пользователь – Пользователь, являющийся юридическим лицом, индивидуальным предпринимателем.

Личный кабинет – веб-интерфейс, обеспечивающий взаимодействие Пользователя с Системой.

Одноранговый узел – Узел, который в рамках подтверждения Транзакций осуществляет функционал по записи сформированных Службой упорядочивания блоков Транзакций в Систему.

Оператор – ООО "Спутник ЦФА".

Отпечаток сертификата УКЭП Пользователя - хеш-функция сертификата УКЭП пользователя, вычисляемая по всем данным сертификата УКЭП и его подписи.

Платформа – программное обеспечение, которое включает Информационную систему и иные сопутствующие программные модули, обеспечивающие возможность взаимодействия Пользователя с Информационной системой. Платформа доступна на Сайте Оператора информационной системы.

ПОД/ФТ – противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Пользователь – юридическое лицо, получившее доступ к Системе в соответствии с настоящими Правилами.

Сайт – страница сайта Оператора в информационно-телекоммуникационной сети «Интернет»: sputnik-cfa.ru

Сеть – совокупность Узлов, находящихся под управлением Валидаторов.

Система – совокупность программного обеспечения, баз данных, в том числе на основе распределённого реестра, телекоммуникационных средств и другого оборудования, обеспечивающих возможность получения, хранения, обработки и раскрытия информации, необходимой для осуществления деятельности Оператора.

Служба упорядочивания – набор Узлов, которые в рамках подтверждения Транзакций осуществляет функционал по формированию блоков (упорядочиванию) Транзакций для их последующей записи в Систему.

Система ЭДО – организационно-техническая система, представляющая собой совокупность программного обеспечения, баз данных и вычислительных средств, обеспечивающая юридически значимый обмен электронными документами, подписанными электронной подписью. Оператором используется Система ЭДО - Контур Диадок.

Смарт-контракт – информационная технология, путем применения которой вносится запись в Систему без направления отдельно выраженного дополнительного волеизъявления сторон Транзакции.

Транзакция – операция с Цифровыми правами, осуществляемая в Системе.

Узел – программно-аппаратный комплекс, обеспечивающий выполнение функций Валидатора в соответствии с настоящими Правилами.

Узел Службы упорядочивания – Узел, участвующий в работе Службы упорядочивания.

УКЭП – ключ электронной подписи Пользователя Системы, с использованием которого Пользователь получает доступ к Системе и информации о Цифровых правах, которыми он обладает, а также к распоряжению этими Цифровыми правами посредством использования Системы. УКЭП выдается в порядке, предусмотренном Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Цифровые права – цифровые финансовые активы, а также цифровые права, включающие одновременно цифровые финансовые активы и иные цифровые права, определенные в соответствии с законодательством Российской Федерации, выпуск которых осуществляется или был осуществлен в Системе.

2. Общие положения.

2.1. ООО "Спутник ЦФА", юридическое лицо, зарегистрированное в соответствии с законодательством Российской Федерации, ОГРН 1247700609166, адрес места нахождения: 129344, г. Москва, вн. тер. г. муниципальный округ Бабушкинский, ул. Искры, д. 31, к. 1, помещ. 2Ч, осуществляет деятельность оператора Информационной системы, в которой осуществляется выпуск цифровых финансовых активов, в том числе деятельность по внесению, обработке, хранению информации, содержащейся в базах данных Информационной системы, а также осуществляет функции оператора обмена цифровых финансовых активов путем обеспечения заключения сделок с цифровыми финансовыми активами, выпущенными в Информационной системе ООО "Спутник ЦФА". Оператор начинает осуществлять свою деятельность с момента включения Оператора в Реестр Операторов Информационных систем.

2.2 Настоящие Правила разработаны в соответствии с требованиями Закона о ЦФА и принятых в соответствии с ним нормативных актов».

2.3. Настоящие Правила определяют порядок технологического функционирования Платформы и защиты информации, правила выпуска Цифровых прав в Информационной системе и способы их учета, порядок открытия Кошельков, внесения (изменения) записей в Информационную систему, правила совершения Сделок с Цифровыми правами, правила использования Номинального счета для осуществления расчетов по сделкам, совершенным с использованием Информационной системы, Требования к Пользователям, а также порядок обеспечения доступа Пользователей к Кошелькам.

2.4. Оператор вправе в одностороннем порядке вносить изменения в настоящие Правила. Изменения в настоящие Правила вступают в силу после их согласования со стороны Банка России.

2.5. Дата вступления изменений в настоящие Правила определяется Оператором в соответствующем решении Оператора. Оператор раскрывает информацию о внесении изменений в

Правила путем размещения на Сайте Правил в новой редакции, согласованных Банком России, и даты их вступления в силу.

2.6. Взаимодействие с Оператором осуществляется с использованием Системы ЭДО или в бумажном виде по адресу местонахождения адресата.

Сообщения, передаваемые Оператору, с использованием способов, предусмотренных настоящим пунктом, принимаются и обрабатываются Оператором в течение времени совершения операций, устанавливаемого Оператором в соответствии с пунктом 2.16 настоящих Правил.

2.7. Раскрытие информации в Системе и на Сайте в сети Интернет считаются надлежащими способами информирования Пользователей.

2.8. Настоящие правила являются условиями договора о предоставлении доступа к Системе, в соответствии с которым Оператор оказывает Пользователям услуги по обеспечению доступа и использованию Системы, а также получению информации из Системы.

Оператор обязуется в соответствии с настоящими Правилами оказывать услуги регулярно (систематически) по обеспечению доступа, а Пользователь обязуется соблюдать требования настоящих Правил и оплачивать указанные услуги.

Договор о предоставлении доступа к Системе заключается между Оператором и Пользователем путем присоединения Пользователя к указному договору в порядке, предусмотренном положениями статьи 428 Гражданского кодекса Российской Федерации.

2.9. Оператор оставляет за собой право отказаться от заключения договора о предоставлении доступа к Системе.

2.10. Пользователь использует функционал Системы на свой собственный риск. Оператор не принимает на себя никакой ответственности за соответствие Системы ожиданиям Пользователя.

2.11. Стороны осознают и соглашаются, что никакое программное обеспечение не свободно от ошибок. Право доступа Пользователя к Системе предоставляется на условиях "как есть". Оператор не предоставляет какую-либо явную или подразумеваемую гарантию безусловной и безошибочной работоспособности Системы или пригодности ее для определенной цели. Оператор подтверждает, что Система позволит Пользователю использовать ее для целей реализации действий Пользователя в соответствии с Правилами, согласно ее функциональным возможностям и требованиям Законодательства РФ.

2.12. Оператор не несет ответственности за отсутствие доступа Пользователя к Системе ввиду недоступности и (или) ограниченной доступности информационно-телекоммуникационной сети Интернет по тем или иным причинам, перебоев с электричеством и каналов связи, а также иными обстоятельствами, находящимися вне разумного контроля Оператора и обстоятельствами непреодолимой силы.

2.13. Время доступности Системы для использования ее функциональных возможностей Пользователями указывается на Сайте Оператора.

2.14. Оператор не несет ответственности за отсутствие доступа Пользователя к Системе в периоды осуществления технического обслуживания, решения технических инцидентов и (или) исправления ошибок, установки обновлений.

2.15. В случае, если положения настоящих Правил противоречат требованиям законодательства Российской Федерации, то применению подлежат соответствующие положения законодательства Российской Федерации.

2.16. Оператор устанавливает время начала и время окончания совершения операций или порядок определения указанного времени. При этом указанное время может различаться для одного или нескольких Цифровых прав.

Под временем совершения операций понимаются временные периоды, в течение которых Пользователи могут подавать Заявки, совершать сделки с Цифровыми правами.

Информация о времени совершения операций, об изменении времени совершения операций раскрывается на Сайте и (или) в Системе не менее чем за 1 (один) календарный день до установленного времени, если иное не предусмотрено решением Оператора.

3. Алгоритмы программ Системы и правила внесения изменений в них.

3.1. Корректность алгоритмов в Системе достигается за счет:

3.1.1. Отсутствия возможности внесения изменений в установленные Оператором алгоритмы иными лицами;

3.1.2. Применения на каждом Узле Системы криптографии, шифрования и защиты каналов для передачи данных, предотвращения несанкционированного доступа, соответствующих настроек Узла Системы.

3.2. В Системе используются следующие шаблоны Смарт-контрактов:

3.2.1. Смарт-контракт, содержащий уникальный идентификационный номер Пользователя, хеш-функцию сертификата УКЭП Пользователя, вычисляемую по всем данным сертификата УКЭП и его подписи, информацию о том, в каком качестве Пользователь Аутентифицирован в Системе, и предназначенный для обеспечения следующих процедур и процессов:

- первичная регистрация Пользователя;
- восстановление доступа Пользователя к Системе (доступа к записям Системы) путем замены Отпечатка сертификата УКЭП Пользователя;
- приостановление и прекращение доступа Пользователя к Системе в случаях, предусмотренных пунктом 5.7.1. и пунктами 5.7.7 – 5.7.8 настоящих Правил соответственно.

3.2.2. Смарт-контракт, содержащий уникальный идентификационный номер Пользователя, Отпечаток сертификата УКЭП Пользователя, информацию, необходимую для заключения Сделок с Цифровыми правами, в том числе необходимую для организации выпуска Цифровых прав, и предназначенный для выпуска, учета, оборота и погашения Цифровых прав, в том числе при исполнении Оператором требований актов.

3.3. Решение о внесении изменений в алгоритм (алгоритмы) программ Системы принимает Оператор.

3.4. Решением Оператора может быть сформирован коллегиальный консультативный орган, к компетенции которого будет относиться согласование сроков, формирование рекомендаций или принятие решений в части внесения изменений в алгоритм (алгоритмы) программ Системы.

3.5. Принятие Оператором решения о внесении изменений в алгоритмы осуществляется в целях: всестороннего развития функционала Системы, в том числе на основании предложений Пользователей, улучшения ее безопасности, операционной надежности и работоспособности.

3.6. Любые изменения в алгоритмы Системы должны соответствовать требованиям к защите информации и операционной надежности, предусмотренным разделом 8 настоящих Правил и могут быть внесены исключительно при условии успешного прохождения процесса их тестирования.

3.7. Не позднее, чем за 5 дней до внесения изменений в алгоритм (алгоритмы) программ Системы Оператор информирует об этом Пользователей, если такие изменения затрагивают интересы Пользователей и использование Системы. В иных случаях Пользователь не информируется о внесении изменений в алгоритмы Системы. Указанное в настоящем пункте уведомление должно содержать информацию о соответствующих изменениях в алгоритме (алгоритмах) программ Системы, а также о времени недоступности или ограниченной доступности Системы.

4. Правила взаимодействия оператора информационной системы с пользователями.

4.1. Пользователем может быть физическое лицо зарегистрированное в соответствии с Законодательством в качестве индивидуального предпринимателя, юридическое лицо, которые соответствуют всем требованиям, указанным в п. 4.2., а также в п. 4.3. (применительно к Корпоративным Пользователям) (по тексту также –«Требования к Пользователям»).

4.2. Ко всем Пользователям предъявляются следующие требования:

4.2.1. Пользователь должен обладать правоспособностью в соответствии с Законодательством в объеме, необходимом для обладания и распоряжения Цифровыми правами;

4.2.2. Пользователь должен иметь УКЭП;

4.3. К Корпоративным Пользователям предъявляются следующие требования:

4.3.1. С целью взаимодействия с Оператором информационной системы и для совершения юридически значимых действий на Платформе Корпоративный Пользователь (за исключением Пользователя индивидуального предпринимателя) обязан назначить одного или нескольких

Представителей Корпоративного Пользователя. Индивидуальный предприниматель вправе, но не обязан назначать Представителя Корпоративного Пользователя;

4.3.2. Представители Корпоративного Пользователя должны удовлетворять Требованиям к Пользователям, указанным в п. 4.2.;

4.3.3. Каждый Представитель Корпоративного Пользователя должен предоставить Оператору информационной системы согласие на обработку своих персональных данных с использованием функционала Платформы;

4.3.4. Представитель Корпоративного Пользователя должен обладать право- и дееспособностью в объеме, необходимом для Регистрации, открытия Кошелька Корпоративного Пользователя, совершения и исполнения сделок с Цифровыми правами

4.3.5. Соблюдение Требований к Пользователям обязательно для Пользователя на протяжении всего периода, в течение которого он пользуется услугами Оператора информационной системы в соответствии с Договором на пользование Платформой.

4.3.6. В случае если Пользователь перестает соответствовать какому-либо из Требований к Пользователю в рамках периода, в течение которого Пользователь использует Платформу, он обязуется уведомить Оператора информационной системы о таком несоответствии в течение 3 (трех) рабочих дней с даты, в которую данное обстоятельство стало ему известным.

4.4. Пользователь обязуется:

- не передавать Аутентификационные данные и Коды подтверждения третьим лицам, за исключением случаев передачи Аутентификационных данных и Кодов подтверждения Представителю(-ям) Корпоративного Пользователя;

- принимать меры по защите Аутентификационных данных и Кодов подтверждения от разглашения третьим лицам, в том числе воздерживаться от использования для доступа к Личному кабинету мобильных устройств со снятыми программными ограничениями производителя на установку неразрешенного программного обеспечения;

- информировать Оператора информационной системы путем направления уведомления через Личный кабинет о прекращении полномочий Представителя(-ей) Корпоративного Пользователя;

- предоставить Оператору информационной системы свой номер мобильного телефона;

- не использовать Платформу в целях совершения сделок, направленных на легализацию (отмывание) доходов, полученных преступным путем, финансирование терроризма и финансирование распространения оружия массового уничтожения;

- не использовать Цифровые права в качестве средства платежа при совершении Сделок на Платформе.

4.5. Пользователи получают и осуществляют доступ к Системе, действуя в качестве лиц, относящихся к одной или нескольким категориям из указанных ниже:

4.5.1. «Эмитент» – Пользователь, имеющий право на осуществление выпуска Цифровых прав в Системе в соответствии с настоящими Правилами.

4.5.2. «Инвестор» – Пользователь, имеющий право на приобретение и распоряжение Цифровыми правами, выпущенными в Системе.

4.5.3. «Номинальный держатель» – Пользователь, имеющий право на ведение учета прав на Цифровые права, принадлежащие иным лицам в соответствии с положениями законодательства Российской Федерации.

4.5.4. «Оператор Обмена» – Пользователь, имеющий право обеспечивать заключение сделок купли-продажи, а также иных сделок, связанных с Цифровыми правами, в соответствии с положениями законодательства Российской Федерации.

4.6. Категория Пользователя указывается в заявлении, предоставляемом в составе документов в соответствии с пунктом 5.1.1.3. настоящих Правил. Допускается указание нескольких категорий.

4.7. В случае необходимости получения доступа к Системе, в рамках категории, отличной от полученной при получении доступа к Системе, Пользователь повторно проходит процедуру получения доступа к Системе в соответствии с положениями раздела 5.1 настоящих Правил.

5. Порядок присоединения к Правилам и регистрация Пользователей.

5.1. Регистрация Пользователей-индивидуальных предпринимателей.

5.1.1. Для приобретения статуса Пользователя индивидуальному предпринимателю необходимо пройти следующие стадии процесса Регистрации:

5.1.1.1. Создание профиля Пользователя, которое включает ввод Пользователем с использованием функционала Платформы логина, пароля и номера мобильного телефона, которые могут использоваться для входа на Платформу;

5.1.1.2. Прохождение Идентификации индивидуального предпринимателя, его выгодоприобретателя и бенефициарного владельца через Оператора информационной системы или с использованием Сервиса делегированной идентификации. В случае, если у индивидуального предпринимателя имеются представитель(-и), выгодоприобретатель(-и) и (или) бенефициарный(-е) владелец(-цы), данным лицам также необходимо пройти Идентификацию;

5.1.1.3. Ознакомление и предоставление согласия с условиями следующих документов:

- Правила;
- Договор на пользование Платформой;
- Соглашение об электронном взаимодействии, предусматривающее использование простой электронной подписи и неквалифицированной электронной подписи в отношениях между Оператором информационной системы и Пользователем;
- Согласие на обработку персональных данных;
- Уведомление о рисках.

5.1.1.4. Очередность совершения действий, указанных в п. 5.1.1, может быть изменена Оператором информационной системы по собственному усмотрению.

5.1.2. Индивидуальному предприниматель становится Пользователем после совершения всех действий, указанных в п. 5.1.1, и получения подтверждения об успешном прохождении Регистрации.

5.2. Регистрация Пользователей-юридических лиц.

5.2.1. Для приобретения статуса Пользователя юридическим лицом уполномоченному представителю такого лица необходимо пройти следующие стадии процесса Регистрации:

5.2.1.1. Направление запроса на создание профиля Корпоративного Пользователя Представителем Корпоративного Пользователя-юридического лица;

5.2.1.2. Идентификация Представителя Корпоративного Пользователя юридического лица в порядке, предусмотренном п. 5.1.1.2., и Идентификация юридического лица;

5.2.1.3. Ознакомление и предоставление согласия с условиями следующих документов:

- Правила;
- Договор на пользование Платформой;
- Соглашение об электронном взаимодействии, предусматривающее использование простой электронной подписи и неквалифицированной электронной подписи в отношениях между Оператором информационной системы и Пользователем;
- Уведомление о рисках.

5.2.2. Юридическое лицо становится Пользователем после совершения всех действий, указанных в п. 5.2.1, и получения подтверждения об успешном прохождении Регистрации.

5.3. Заверения об обстоятельствах.

5.3.1. Совершая действия, необходимые для Регистрации, Пользователь заверяет (в понимании ст. 431.2 ГК РФ) Оператора информационной системы в следующем:

- Он ознакомился с Правилами, понимает их содержание и согласен с их условиями.
- Он соответствует всем применимым Требованиям к Пользователям на момент присоединения.

5.3.2. В случаях, когда Корпоративный Пользователь действует через Представителя Корпоративного Пользователя, о наличии у такого Представителя Корпоративного Пользователя всех необходимых полномочий для выполнения действий на Платформе и о соответствии

Представителя Корпоративного Пользователя Требованиям к Пользователям, указанным в п. 4.2. Пользователь обязан прекратить Регистрацию в случае, если какое-либо из заверений, указанных в п. 5.3., не соответствует действительности.

5.3.3. Во избежание сомнений, порядок Регистрации Пользователя, предусмотренный разделом 5, не применяется к Оператору информационной системы применительно к случаям, когда Оператор информационной системы выступает в качестве Эмитента. Оператор информационной системы считается зарегистрированным в качестве Пользователя – Эмитента с момента включения Оператора информационной системы в реестр операторов информационных систем, в которых осуществляется выпуск Цифровых прав, который ведет Банк России. На Оператора информационной системы, когда Оператор информационной системы выступает в качестве Эмитента, распространяются требования, предусмотренные в п. 4.2. и п. 6.1 Правил.

5.3.4. При Регистрации лица, обладающего лицензией на осуществление депозитарной деятельности, для целей обособления в Информационной системе Цифровых прав, принадлежащих его депонентам, от Цифровых прав, принадлежащих такому лицу, открывается два Личных кабинета, с отдельными Кошельками – один, предназначенный для учета собственных Цифровых прав, и второй, для учета Цифровых прав, принадлежащих депонентам такого лица.

5.4. Порядок ведения Реестра Пользователей.

5.4.1. Оператор информационной системы ведет Реестр Пользователей, в который вносятся сведения в отношении каждого Пользователя, прошедшего Регистрацию.

5.4.2. В Реестре Пользователей должна содержаться следующая информация:

5.4.2.1. идентификационные данные Пользователя, предоставляемые им при прохождении Идентификации. Идентификационные данные включают:

- в отношении физических лиц зарегистрированных в соответствии с Законодательством в качестве индивидуального предпринимателя – граждан Российской Федерации фамилию, имя, а также отчество (если иное не вытекает из национального обычая), идентификационный номер налогоплательщика;

- в отношении юридических лиц, зарегистрированных в соответствии с законодательством Российской Федерации – наименование, организационно-правовую форму, идентификационный номер налогоплательщика, сведения об имеющихся лицензиях на право осуществления деятельности, подлежащей лицензированию, доменное имя, указатель страницы сайта в сети «Интернет», с использованием которых юридическим лицом оказываются услуги (при наличии), основной государственный регистрационный номер и адрес юридического лица;

Состав идентификационных данных может быть изменен Оператором информационной системы в зависимости от требований применимого Законодательства.

5.4.2.2. Аутентификационные данные Пользователя, за исключением пароля, Приватного(-ых) ключа(-ей).

5.4.2.3. Сведения о том, в каком качестве Пользователь аутентифицирован в Информационной системе (в качестве лица, выпускающего Цифровые права (Эмитента), Обладателя Цифровых прав или Оператора обмена ЦФА, Пользователя-номинального держателя). При этом, сведения, содержащиеся в Реестре Пользователей, необходимые для аутентификации Пользователя-номинального держателя в Информационной системе, должны содержать информацию о том, что он является номинальным держателем.

5.4.3. В Реестре Пользователей могут содержаться следующие виды дополнительных сведений:

5.4.3.1. В отношении всех Пользователей – идентификационный номер Пользователя, присвоенный ему Оператором информационной системы, иные идентификационные сведения, присваиваемые Пользователям Оператором информационной системы для формирования категорий Пользователей.

5.4.3.2. В отношении Эмитентов – сведения обо всех выпусках Цифровых прав Эмитента, которые были осуществлены на Платформе, к которым относятся следующие данные в отношении каждого выпуска:

- дата начала размещения выпускаемых Цифровых прав;

- вид и объем прав, удостоверяемых Цифровыми правами;

- количество Цифровых прав в выпуске;

- идентификационный номер, присвоенный выпуску Цифровых прав Оператором информационной системы.

5.4.4. Оператор информационной системы вносит в Реестр Пользователей сведения о Пользователе не позднее, чем в течение 2 (двух) рабочих дней с даты прохождения соответствующим Пользователем Регистрации.

5.4.5. Оператор информационной системы хранит сведения, содержащиеся в Реестре Пользователей, а также документы, на основании которых такие сведения были внесены в реестр, в течение всего срока нахождения Пользователя в Реестре Пользователей, а также в течение 5 (пяти) лет после его исключения из такого реестра. Оператор информационной системы вправе уничтожить указанные сведения по окончании пятилетнего срока.

5.4.6. Хранение сведений, содержащихся в Реестре Пользователей, а также документов, на основании которых такие сведения были внесены в реестр, осуществляется в облачных ресурсах российских провайдеров облачных услуг. Указанные облачные провайдеры должны соблюдать меры по защите персональных данных в соответствии с требованиями, предъявляемыми к 4 (четвертому) уровню защищенности (УЗ-4) в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства РФ от 01.11.2012 № 1119.

5.4.7. При исключении Пользователя из Реестра Пользователей, Оператор информационной системы удаляет сведения из Реестра Пользователей, указанные в п. 5.4.2 и 5.4.3. Исключение Пользователя из Реестра Пользователей осуществляется Оператором информационной системы в течение 3 (трех) рабочих дней с даты удовлетворения заявки об исключении Пользователя из Реестра Пользователей.

5.4.8. В случае если при Регистрации Пользователя Аутентификационные данные или их часть предоставляется лицом, который предоставляет Пользователю доступ к Платформе и ее функционалу через свой сайт, то обязательным условием регистрации такого Пользователя на Платформе является передача лицом, обеспечивающим доступ к Платформе и ее функционалу, Аутентификационных данных Пользователя (за исключением Приватного ключа) Оператору информационной системы.

5.4.9. Пользователь обязан обеспечивать актуальность, достоверность и полноту предоставляемых им документов и информации, а также предоставление изменений в них в течение пяти рабочих дней с даты, когда Пользователь узнал / должен был узнать о таких изменениях.

5.5. Порядок обеспечения доступа к функционалу Платформы через Личный кабинет.

5.5.1. Доступ к Личному кабинету Пользователя осуществляется с использованием Сайта Оператора информационной системы. Доступ к Личному кабинету осуществляется при условии прохождения Пользователем Аутентификации.

5.5.2. Доступ к Платформе и ее функционалу с использованием Сайта Оператора информационной системы осуществляется с использованием веб-браузера, при этом установка какого-либо дополнительного программного обеспечения для получения доступа к Платформе не требуется.

5.5.3. Во избежание сомнений, при взаимодействии Платформы с лицом, указанным на сайте Оператора информационной системы, с использованием сайта которого осуществляется доступ к Платформе и ее функционалу, такое взаимодействие не предусматривает возможности доступа указанного лица и иных третьих лиц к Приватному(ым) ключу(ам) Пользователя. Все действия, для совершения которых в соответствии с Правилами и иными документами, предусмотренными п. 5.1.1.3. Правил, требуется использование Приватного ключа, совершаются Пользователем, получающим доступ к Платформе и ее функционалу через сайт и лиц, указанных на сайте Оператором информационной системы, самостоятельно.

5.5.4. Оператор информационной системы обеспечивает Пользователям доступ к следующему функционалу Платформы посредством Личного кабинета:

- возможность совершения Сделок по приобретению Цифровых прав при их выпуске;

- в отношении Эмитентов – возможность выпуска Цифровых прав; и

- иному функционалу, предусмотренному Правилами.

5.5.5. посредством функционала Личного кабинета Оператор информационной системы обеспечивает Пользователю постоянный доступ к следующей информации:

- о Кошельке(-ах) Пользователя, открытых на Платформе;

- об актуальном Балансе Пользователя;

- в отношении Пользователя-Эмитента – информацию о количестве выпущенных, непогашенных и предъявленных к погашению Цифровых прав, выпущенных таким Эмитентом и находящихся в обращении;

- иной информации, возможность доступа к которой со стороны Пользователя предусмотрена Правилами.

5.6. Порядок восстановления доступа к Личному кабинету в случае его утраты.

5.6.1. В случае утраты доступа к Личному кабинету Пользователь вправе направить Оператору информационной системы запрос на восстановление доступа, с указанием причины утраты, с использованием функционала Платформы.

5.6.2. При получении запроса на восстановление доступа к Личному кабинету Оператор информационной системы может временно заблокировать доступ к Личному кабинету Пользователя.

5.6.3. Для восстановления доступа к Личному кабинету Пользователь обязан пройти процедуру аутентификации.

5.6.4. После успешного прохождения аутентификации Пользователь получает ограниченный доступ к функционалу Платформы для генерации новой пары Публичного и Приватного ключа.

5.6.5. Оператор информационной системы обязан обновить Аутентификационные данные Пользователя и обеспечить возможность доступа Пользователя к полному функционалу его Личного кабинета с использованием сгенерированной в соответствии с п. 5.6.4 пары Публичного и Приватного ключей в течение 1 (одного) рабочего дня с даты их генерации.

5.7. Порядок приостановления и прекращения доступа Пользователей к Системе

5.7.1. Под приостановкой доступа к Системе понимается временное (на срок приостановки) прекращение возможности совершать Транзакции, не влекущее прекращения или приостановления действия договора о предоставлении доступа к Системе.

5.7.2. Оператор приостанавливает доступ Пользователя к Системе при получении от Пользователя информации о компрометации УКЭП. Оператор приостанавливает доступ Пользователя в отношении всех Личных кабинетов, для авторизации в которых используется скомпрометированная УКЭП.

5.7.3. Если иное не предусмотрено законодательством Российской Федерации, Оператор вправе приостановить доступ Пользователя к Системе при наличии хотя бы одного из следующих обстоятельств:

- непредставление запрашиваемых Оператором информации и документов;

- предоставление недостоверной или вводящей в заблуждение информации;

- неоплата Пользователем услуг Оператора;

- нарушение Пользователем требований законодательства Российской Федерации в сфере цифровых прав, ПОД/ФТ и (или) настоящих Правил;

- возникновение у Оператора подозрений в том, что сделки, совершаемые Пользователем с использованием Системы, совершаются в целях легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма или распространения оружия массового уничтожения;

- наличие оснований для применения или применение к Пользователю процедур, применяемых в деле о банкротстве в соответствии с законодательством Российской Федерации;

- наличие фактов ухудшения финансового состояния Пользователя и (или) информации, дающей основания считать возможными ухудшение финансового состояния Пользователя и (или) неспособность Пользователя своевременно и в полном объеме исполнять обязательства по Цифровым правам и (или) сделкам с Цифровыми правами;

- действие мер ограничительного характера, которые введены иностранным государством, объединением иностранных государств или международной организацией в отношении Пользователя;

- наличие информации, свидетельствующей о потере (риске потери) Пользователем деловой репутации;

- наличие оснований, предусмотренных требованиями законодательства о ПОД/ФТ и (или) иными требованиями, устанавливающими налоговый контроль в соответствии с законодательством Российской Федерации, законодательством иностранных государств и (или) международными договорами;

7-оказание Оператором услуг Пользователю в соответствии с настоящими Правилами повлечет и (или) может повлечь нарушение Оператором требований законодательства Российской Федерации;

- Пользователь перестал соответствовать требованиям, предусмотренным пунктом 4.2 настоящих Правил;

- Оператору стало известно о нарушении заверений, предусмотренных разделом 11.4 настоящих Правил.

5.7.4. Доступ Пользователя к Системе возобновляется по решению Оператора после прекращения действия обстоятельств, являвшихся основанием для приостановки доступа Пользователя к Системе. Пользователь вправе обратиться к Оператору с заявлением о возобновлении доступа к Системе. Оператор обязан рассмотреть указанное в настоящем пункте заявление в течение 10 рабочих дней с даты его поступления.

5.7.5. В течение 3 (трех) рабочих дней со дня приостановки / возобновления доступа Пользователя к Системе, Оператор направляет уведомления о приостановке / возобновлении доступа к Системе такому Пользователю, в отношении которого принято соответствующее решение, с указанием даты приостановки / возобновления доступа.

5.7.6. Под прекращением доступа к Системе понимается блокировка доступа Пользователя к Системе, влекущая прекращение договора о предоставлении доступа к Системе.

Оператор не вправе прекратить доступ Пользователя к Системе при наличии Цифровых прав на Кошельке Пользователя.

5.7.7. Оператор прекращает доступ Пользователя к Системе при прекращении деятельности Пользователя в результате прекращения юридического лица;

5.7.8. Оператор вправе прекратить доступ Пользователя к Системе при наличии хотя бы одного из следующих обстоятельств:

- получение Оператором заявления Пользователя о прекращении доступа к Системе;

- приостановка доступа к Системе в течение более чем 6 (шести) месяцев;

- не устранение выявленных ранее нарушений, повлекших за собой приостановление доступа к Системе, в установленный Оператором срок;

- наличие у Оператора подозрений в том, что сделки, совершаемые Пользователем с использованием Системы, совершаются в целях легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и финансирования распространения оружия массового уничтожения;

- Пользователь перестал соответствовать требованиям, предусмотренным пунктом 4.2 настоящих Правил;

- Оператору стало известно о нарушении заверений, предусмотренных разделом 11.4 настоящих Правил.

5.7.9. В случае направления Пользователем заявления о прекращении доступа к Системе, Оператор принимает решение о прекращении доступа такого Пользователя в течение 10 рабочих дней с момента получения Оператором такого заявления, при условии соблюдения следующих условий:

- у пользователя отсутствуют неисполненные обязательства перед Оператором и (или) иными Пользователями;

- на Кошельке Пользователя отсутствуют Цифровые права.

В случае невыполнения указанных выше условий Оператор отказывает в удовлетворении заявления и направляет Пользователю соответствующее уведомление.

5.7.10. В течение 3 (трех) рабочих дней со дня прекращения доступа Пользователя к Системе, Оператор направляет уведомление о прекращении доступа к Системе Пользователю, в отношении которого принято соответствующее решение, с указанием даты прекращения доступа.

5.7.11. Оператор вправе использовать информацию, ставшую общеизвестной, для принятия решения о приостановке, возобновлении или прекращении доступа Пользователя к Системе.

5.7.12. Решение о простановке, возобновлении или прекращении доступа Пользователя к Системе может быть принято в отношении одной или нескольких категорий Пользователя.

6. Правила выпуска и погашения цифровых прав.

6.1. Правила выпуска Цифровых прав.

6.1.1. С использованием Системы могут быть выпущены указанные ниже Цифровые права:

- цифровые финансовые активы, удостоверяющие денежные требования;
- цифровые права, включающие одновременно цифровые финансовые активы, удостоверяющие денежные требования, и иные цифровые права.

6.1.2. Эмитент вправе осуществить выпуск Цифровых прав после принятия Оператором решения о допуске таких Цифровых прав к выпуску в Системе.

6.1.3. Решение о выпуске Цифровых прав формируется Эмитентом с использованием функционала Личного кабинета. Сформированное решение о выпуске подписывается УКЭП Эмитента.

6.1.4. Выпуск Цифровых прав в Информационной системе может проводиться ежедневно, кроме установленных в соответствии с Законодательством выходных и нерабочих праздничных дней.

6.1.5. Решение о выпуске должно содержать сведения, предусмотренные Законом о ЦФА и принятыми в соответствии с ним нормативными актами.

6.1.6. После подписания Эмитентом решения о выпуске Оператор в течение 10 рабочих дней принимает одно из следующих решений:

- о допуске Цифровых прав к выпуску в Системе;
- об отказе в допуске Цифровых прав к выпуску в Системе.

Оператор вправе направить Эмитенту запрос на предоставление дополнительных документов в срок, предусмотренный таким запросом. В таком случае срок, предусмотренный настоящим пунктом, исчисляется с даты предоставления Эмитентом документов в соответствии с запросом Оператора.

6.1.7. Оператор вправе принять решение об отказе в допуске Цифровых прав к выпуску в Системе в том числе, но не ограничиваясь, в случаях:

- решение о выпуске не соответствует требования законодательства Российской Федерации;
- Эмитентом не предоставлены дополнительные документы, запрошенные Оператором в соответствии с пунктом 6.1.6 настоящих Правил, в срок, указанный в таком запросе;
- наличие основания для приостановления доступа Эмитента к Системе или приостановление доступа Эмитента к Системе;
- выпуск Цифровых прав может нарушать требования законодательства Российской Федерации;
- при наличии иных оснований, предусмотренных законодательством Российской Федерации.

6.1.8. В случае принятия решения об отказе в допуске Цифровых прав к выпуску в Системе Оператор уведомляет об этом Эмитента с использованием функционала Личного кабинета.

6.1.9. В случае принятия Оператором решения о допуске Цифровых прав к выпуску в Системе Оператор присваивает номер решению о выпуске. После присвоения Оператором номера решению о выпуске Эмитент размещает решение о выпуске на своем сайте в информационно-телекоммуникационной сети «Интернет», Оператор размещает решение о выпуске на Сайте.

Решение о выпуске должно находиться в открытом доступе на сайте Эмитента в информационно-телекоммуникационной сети «Интернет» и на Сайте Оператора до полного исполнения обязательств Эмитента перед всеми обладателями Цифровых прав, выпущенных на основании соответствующего решения о выпуске.

6.1.10. После размещения решения о выпуске на Сайте, оно становится доступным для Пользователей системы в их Личном кабинете.

Решение о выпуске является офертой, адресованной обозначенному в таком решении о выпуске кругу лиц, или, если решение о выпуске адресовано неопределенному кругу лиц, публичной офертой.

6.1.11. Приобретение выпускаемых Цифровых прав осуществляется в следующем порядке:

6.1.11.1. Пользователь, имеющий право на приобретение указанных Цифровых прав, с использованием функционала Личного кабинета формирует Заявку и подтверждает ее путем подписания своей УКЭП.

Формируемые в соответствии с настоящим пунктом Заявки являются Заявками, адресованными Эмитенту.

Заявка подтверждает принятие Пользователем условий решения о выпуске и является акцептом оферты Эмитента.

Заявка должна содержать информацию о выпускаемых Цифровых правах, на приобретение которых она подается, а также количество желаемых к приобретению Цифровых прав или, если это предусмотрено решением о выпуске Цифровых прав, сумму / количество встречного предоставления за приобретаемые Цифровые права.

Сделка по приобретению размещаемых Цифровых прав считается заключенной между Эмитентом и Пользователем в момент получения Эмитентом соответствующей Заявки и при условии, указанных в решении о выпуске для признания выпуска Цифровых прав состоявшимся.

6.1.11.2. В момент получения Эмитентом Заявки Пользователя, Заявке присваивается статус «Ожидает оплаты», а Пользователь самостоятельно производит оплату Цифровых прав в порядке и способом, предусмотренными решением о выпуске.

6.1.11.3. Эмитент самостоятельно осуществляет проверку оплаты выпускаемых Цифровых прав. Эмитент принимает на себя все риски, связанные с соответствующей проверкой.

В таком случае в момент подтверждения Эмитентом факта оплаты выпускаемых Цифровых прав с использованием функционала Системы, Заявке присваивается статус «Оплачена».

6.1.12. Выпуск Цифровых прав признается состоявшимся при наступлении условий для признания выпуска Цифровых прав состоявшимся, указанных в решении о выпуске.

6.1.13. В случае признания выпуска состоявшимся осуществляются следующие действия:

6.1.13.1. В Системе фиксируется факт признания выпуска состоявшимся;

6.1.13.2. Цифровые права перечисляются на Кошельки Пользователей путем применения Смарт-контракта, инициированного Эмитентом и связанного с соответствующим решением о выпуске, и не требуют дополнительного волеизъявления со стороны Эмитента и Пользователя, направившего соответствующую Заявку, а статус исполненных Заявок меняется на «Исполнено».

6.1.14. Расчеты денежными средствами при оплате выпускаемых Цифровых прав осуществляется вне Системы без участия Оператора. Эмитент и Пользователи, участвующие в выпуске Цифровых прав, принимают на себя все связанные с этим риски.

6.2. Погашение записей о Цифровых правах.

6.2.1. Записи о Цифровых правах погашаются в случае прекращения обязательств, удостоверенных Цифровыми правами, в силу их исполнения либо по иным основаниям, предусмотренным законодательством Российской Федерации или решением о выпуске Цифровых прав.

6.2.2. Запись о погашении Цифровых прав вносится в Систему на основании Смарт-контракта, исполнение которого осуществляется при возникновении оснований для погашения, предусмотренных решением о выпуске Цифровых прав, или в иных случаях, предусмотренных законодательством Российской Федерации, а также при условии исполнения обязательств, удостоверенных Цифровыми правами.

6.2.3. Обладатели соответствующих Цифровых прав самостоятельно проверяют факт прекращения Эмитентом обязательств, удостоверенных Цифровыми правами, и принимают на себя связанные с такой проверкой риски.

7. Способы учета цифровых прав в системе, а также внесения (изменения) записей о цифровых правах в систему.

7.1. Учет Цифровых прав.

7.1.1. В соответствии с ч. 1 ст. 4 ФЗ о ЦФА, Цифровые права, выпускаемые в Информационной системе, учитываются в Информационной системе в виде записей.

7.1.2. Цифровые права, выпускаемые в Информационной системе, не могут учитываться какими-либо иными способами, кроме предусмотренного п. 7.1.1.

7.1.3. Записи о Цифровых правах вносятся по указанию Эмитентов, Инвесторов, иных лиц в соответствии с требованиями законодательства Российской Федерации и положениями настоящих Правил.

7.1.4. Записи о Цифровых правах вносятся в Систему путем применения Смарт-контрактов. Инициация Смарт-контрактов, при исполнении которых вносятся записи о Цифровых правах, осуществляется в порядке и на условиях, установленных настоящими Правилами.

7.1.5. Записи о цифровых правах вносятся в реестр Транзакций. Реестр Транзакций ведется в распределенном реестре и содержит информацию о выпущенных в Системе Цифровых правах.

В записях реестра Транзакций также содержатся значения хеш-функций, примененных на содержимое электронных документов, подписанных УКЭП Пользователя, и открепленных подписей к ним.

7.1.6. Ограничение или обременение права распоряжаться Цифровыми правами возникает с момента внесения соответствующей записи в Систему.

7.1.6.1. Ограничения или обременения прав распоряжаться Цифровыми правами на основании сделки вносятся в систему в порядке, предусмотренном разделом 10.1 Правил, с учетом положений пунктов 7.1.4. и 7.1.6. Правил;

7.1.6.2. Ограничения или обременения прав распоряжаться Цифровыми правами на основании Акта вносятся в систему в порядке, предусмотренном разделом 10.3, с учетом положений пунктов 7.1.4. и 7.1.6. Правил.

7.1.7. Доступ к Системе и все действия, инициирующие запуск Смарт-контрактов, осуществляются с использованием принадлежащего Пользователю УКЭП.

7.1.8. Система осуществляет проверку наличия у Пользователя УКЭП и аутентификацию Пользователя, путем проверки электронной подписи, созданной Пользователем с использованием УКЭП.

7.1.9. При обмене информацией между Узлами в целях проверки и внесения (изменений) записей в Систему используются методы шифрования для исключения возможности чтения и изменения данных третьими лицами путем их сокрытия при передаче информации. Узлами также осуществляется подписание исходящих сообщений и проверка подписей входящих к ним сообщений для подтверждения неизменности (целостности) данных, а также идентификации отправителя.

7.2. Порядок привлечения Валидаторов.

7.2.1. Привлечение Валидаторов осуществляется Оператором на основании договора, заключаемого между Оператором и привлекаемым Валидатором.

7.2.2. Под управлением Валидатора может находиться один или несколько Узлов.

7.2.3. Валидаторы должны соблюдать следующие требования:

7.2.3.1. требования по информационной безопасности, определенные Оператором, и которые размещаются на сайте в сети «Интернет» Оператора;

7.2.3.2. требования по обеспечению регулярного и своевременного обновления программного обеспечения Узлов;

7.2.3.3. требования по обеспечению и поддержанию бесперебойной работоспособности Узлов Валидатора;

7.2.3.4. требования по наличию выделенной виртуальной машины или физического сервера с характеристиками необходимыми для выполнения функций Валидатора.

7.2.4. Оператор вправе запрашивать у Валидатора документы, необходимые для проверки соответствия последнего требованиям, установленным Оператором, а также осуществлять соответствующие мероприятия по проверке.

7.3. Реализация волеизъявления Пользователя в случае сбоя в работе информационных технологий Системы.

7.3.1. В случае если реализации волеизъявления Пользователя в Системе помешал сбой в работе информационных технологий и технических средств Системы, Оператор обеспечивает Пользователю возможность обратиться в техническую поддержку Оператора с заявлением о возникшем сбое и о действиях в Системе, которым такой сбой помешал.

7.3.2. При получении соответствующего заявления Оператор обязан совершить действия, реализующие волеизъявление Пользователя, реализации которого помешал такой сбой.

8. Требования к защите информации, операционной надежности и информационной безопасности оператора ЦФА.

8.1. Требования к защите информации и операционной надежности.

8.1.1. Защита информации обеспечивается путем реализации правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий в отношении информации;
- уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации;
- обеспечение конфиденциальности информации;
- реализацию права на доступ к информации в соответствии с законодательством Российской Федерации.

8.1.2. Оператором внедрена система управления информационной безопасностью, включающая в себя политику и процедуры, которые позволяют обеспечивать информационную безопасность и минимизировать информационные риски.

8.1.3. Выбор и применение Оператором мер защиты информации включает в себя:

- выбор мер защиты информации в соответствии с предъявляемыми законодательством требованиями;
- адаптацию (уточнение), дополнение при необходимости выбранного состава и содержания мер защиты информации с учетом модели угроз и нарушителей безопасности информации и структурно-функциональных характеристик объектов информатизации Оператора;
- выделение необходимых и достаточных ресурсов, используемых при применении организационных и технических мер, входящих в систему защиты информации;
- применение для конкретной области адаптированного (уточненного) и дополненного состава мер защиты информации в соответствии с требованиями законодательства.

8.1.4. Система управления информационной безопасностью определяет следующие процессы по защите информации:

- обеспечение защиты информации при управлении доступом, в том числе доступом к объектам информатизации контура инфраструктуры Системы и объектам информатизации контрагентов, привлекаемых Оператором на договорной основе с целью предоставления технических услуг;
- обеспечение защиты информации при назначении и распределении ролей;
- обеспечение защиты вычислительных сетей;
- контроль целостности и защищенности информационной инфраструктуры Оператора;
- обеспечение защиты информации на этапах жизненного цикла автоматизированных систем;
- обеспечение защиты информации средствами антивирусной защиты;

- обеспечение защиты информации при использовании ресурсов информационно-телекоммуникационной сети «Интернет»;

- управление рисками нарушения защиты информации;

- регламентация и документирование деятельности по обеспечению защиты информации, включая порядок регистрации и хранения информации;

- повышение осведомленности работников в области обеспечения защиты информации;

- обнаружение инцидентов информационной безопасности, реагирование на них;

- предотвращение утечек информации;

- мониторинг и анализ обеспечения защиты информации;

- своевременное совершенствование обеспечения защиты информации.

8.1.5. За соблюдение Оператором процессов, установленных системой управления информационной безопасностью, отвечает подразделение информационной безопасности Оператора.

8.1.6. Для проведения работ по защите информации Оператором могут привлекаться на договорной основе организации, имеющие лицензию на проведение работ и услуг, предусмотренных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

8.1.7. Обязательными требованиями для привлечения Оператором контрагентов, оказывающих инфраструктурные услуги для реализации технической составляющей функционала Системы, являются обеспечение такими контрагентами требований, установленных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», подзаконными актами, нормативными документами Банка России.

8.1.8. Правилами системы управления информационной безопасности Оператора определена политика контроля доступа, гарантирующая предоставления доступа к серверным, сетевым ресурсам и иным объектам информатизации, содержащим информацию о внутренней деятельности Оператора, только авторизованным работниками Оператора.

8.1.8.1. Работники Оператора имеют доступ только к тем ресурсам, доступ к которым необходим таким работникам исходя из их должностных обязанностей. Предоставление прав доступа к ресурсам определяется в соответствии с принципом наименьших привилегий.

8.1.8.2. Предоставление прав доступа ко всем помещениям, серверным и сетевым объектам доступа Оператора требует согласования со стороны руководителя подразделения, ответственного за физическую безопасность Оператора (лица, его замещающего).

8.1.8.3. Предоставление также прав доступа к исходному коду разрабатываемого Оператором программного обеспечения и проектной документации требует согласования со стороны руководителя подразделения информационной безопасности Оператора (лица, его замещающего).

8.1.8.4. Интерфейсы управления аппаратными и сетевыми ресурсами находятся в выделенной сети, доступ к которой строго ограничен.

8.1.8.5. Исходный код и доступ к базам данных Оператора предоставляется только авторизованному персоналу Оператора.

8.1.9. Физическая безопасность инфраструктуры (включая непосредственно прямой доступ к серверам, сетевым адаптерам, шинам обмена данными) обеспечивается как работниками Оператора, так и организациями, действующими в рамках полномочий по заключенным с Оператором договорам, привлекаемыми с целью предоставления технических услуг.

8.1.10. Организация Оператором процесса безопасной разработки программного обеспечения включает в себя:

8.1.10.1. планирование и определение требований к системе или отдельным модулям;

8.1.10.2. архитектурное планирование и выявление возможных уязвимостей с дальнейшим их устранением;

8.1.10.3. создание плана тестирования запланированного функционала;

8.1.10.4. реализацию функционала, написание кода Системы и отдельных ее компонентов;

8.1.10.5. тестирование в соответствии с планом тестирования, определенном на предшествующем этапе;

8.1.10.6. сборку релизов, их установку и поддержку сервисов на промышленной среде.

8.1.11. Оператором принята политика по защите окружения разработки, включающая в себя разделение среды разработки, тестирования и промышленной эксплуатации, а также внедрение системы контроля, препятствующей репликации данных из промышленного контура в другие окружения.

8.1.12. Оператором обеспечивается целостность и неизменность обрабатываемой информации, контроль целостности и защищенности информационной инфраструктуры.

8.1.13. Для защиты информации от воздействия вредоносного кода Оператором используются средства антивирусной защиты с функцией централизованного управления, мониторинга и автоматического реагирования в случаях выявления вредоносного кода.

8.1.14. Реагирование на инциденты информационной безопасности.

8.1.14.1. Процесс по управлению инцидентами организован подразделением информационной безопасности Оператора и осуществляется на основании внутренних регламентов Оператора.

8.1.14.2. Для надлежащего реагирования на инциденты информационной безопасности Оператором утверждены планы реагирования на типовые возможные инциденты, которые поддерживаются в актуальном состоянии и используются для качественного реагирования на инциденты.

8.1.14.3. Для оперативного реагирования на события и инциденты информационной безопасности Оператором создана группа реагирования на инциденты защиты информации, возглавляемая руководителем подразделения информационной безопасности. Для проведения расследований инцидентов информационной безопасности, при наличии обоснованной необходимости, руководитель подразделения информационной безопасности может привлекать для работы в составе группы реагирования работников других самостоятельных структурных подразделений Оператора на основе совмещения работы в группе со своими основными должностными обязанностями.

8.1.14.4. Ведется подробное описание процесса реагирования на события и инциденты информационной безопасности в учетных формах.

8.1.14.5. Пользователи, в случаях, когда инцидент информационной безопасности способен нанести / нанес ущерб Пользователям, уведомляются об инцидентах путем раскрытия информации об инцидентах на сайте Оператора в сети Интернет или посредством направления уведомления с использованием электронной почты или Системы ЭДО в течение 24 часов с момента обнаружения соответствующего инцидента.

8.1.15. Комплекс информационной безопасности Системы состоит в том числе из следующих компонентов:

8.1.15.1. Журналирование (логирование, протоколирование) событий Системы и анализ собранной информации: журналирование включает непрерывную запись необходимых событий в Системе, включая события начала, окончания обработки порций данных, указание объектов и субъектов данных доступа или обмена. Оператор осуществляет сохранение журналов с собранными событиями, как в неизменном виде событий, так и в машинно-обработанном виде. События используются для анализа, в том числе в режиме реального времени, а также при расследовании инцидентов и сбоев, произошедших в Системе. Оператор ведет и поддерживает систему точного времени, которая необходима для точной фиксации информационных событий в журналах регистрации событий в Системе.

8.1.15.2. Шифрование передачи данных: исключение возможности чтения и изменения данных третьими лицами путем их сокрытия при передаче информации. Персональные данные, идентификационные данные и аутентификационные данные передаются исключительно с использованием шифрования в соответствии с требованиями законодательства.

8.1.15.3. Управление ключами шифрования данных: доступ к ключам шифрования осуществляется способом, позволяющим контролировать и ограничивать доступ к ним кругом лиц,

имеющих на это право. Факты доступа к ключам шифрования и их использования фиксируются в системе для оценки и расследования событий информационной безопасности.

8.1.15.4. Ограничение доступа: Пользователи и работники Оператора получают персонализированный доступ в Систему с использованием аутентификационных данных. При работе в Системе каждое лицо имеет отдельные аутентификационные данные для выполнения различных функций в зависимости от роли, в соответствии с которой он действует в конкретный момент.

8.1.16 Защита данных и конфиденциальной информации.

8.1.16.1. Оператор обеспечивает меры по защите информации, предусмотренные Положением Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

8.1.16.2. Оператор обеспечивает хранение и защиту всей информации, связанной с организацией деятельности, в том числе путем создания резервной копии такой информации и определения процедур, направленных на предотвращение технических сбоев и ошибок, обеспечения целостности и неизменности хранимой информации.

8.1.16.3. Для хранения данных в базах данных, в том числе в реестрах Системы, Оператор использует шифровальные (криптографические) средства защиты информации в соответствии с законодательством Российской Федерации.

8.1.16.4. Оператор осуществляет меры по защите персональных данных, предусмотренные Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы безопасности России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

8.1.16.5. Оператор не раскрывает персональные данные, полученные от Пользователей, третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации.

8.1.16.6. Персональные данные, полученные от пользователей, а также данные, связанные с финансовыми операциями Пользователей, подлежат хранению в течение срока, предусмотренного Федеральным законом № 115-ФЗ.

8.1.16.7. Оператор обеспечивает защиту от проникновения, а именно: предотвращение вмешательства в работу Системы из общедоступных сетей передачи данных, в том числе из сети Интернет. Оператор проводит анализ и ограничение (при необходимости) входящего и исходящего потока данных на соответствие требованиям правил безопасности.

8.1.16.8. Взаимодействие с Системой должно осуществляться с использованием защищенных каналов связи.

8.1.17. Анализ и управление уязвимостями.

8.1.17.1. Оператор на регулярной основе проводит мероприятия по поддержанию уровня безопасности собственных систем, анализ технологического процесса с целью выявления уязвимости объектов информатизации.

8.1.17.2. Контроль уровня безопасности Системы осуществляется специализированными сервисами (сканерами) уязвимостей, которые при помощи специальных методов определяют версии программного обеспечения и наличие или отсутствие в них известных уязвимостей.

8.1.17.3. Процесс устранения выявленных уязвимостей проводится в соответствии с утвержденной Оператором политикой.

8.1.18. Обеспечение непрерывности функционирования и операционной надежности.

8.1.18.1. Оператор предпринимает необходимые меры, направленные на обеспечение заданного уровня непрерывности функционирования Системы, в том числе утверждает план обеспечения непрерывности и восстановления деятельности, который включает в себя требуемые показатели обеспечения операционной надежности Системы (допустимые точки восстановления, допустимое время восстановления, пороговый уровень времени простоя и (или) восстановления).

8.1.18.2. Оператор пересматривает пороговые уровни показателей бесперебойности с использованием результатов оценки рисков в Системе не реже одного раза в год. Значения показателей бесперебойности должны соответствовать требованиям нормативных актов Банка России.

8.1.18.3. Оператор осуществляет регулярные мероприятия по тестированию как общего плана непрерывности и восстановления деятельности в целом, так и отдельных частных направлений указанного плана. Результаты тестирования служат для улучшения процессов обеспечения операционной надежности Системы, повышения уровня ее устойчивости к внешним и внутренним факторам, привозящим к сбоям и отказам.

8.1.18.4. Требования к операционной надежности определяются в соответствии с применимыми нормативными актами, также указанные требования могут содержаться в соглашениях, заключаемых Оператором.

8.1.18.5. Требования к операционной надежности контрагентов, оказывающих услуги в сфере информационных технологий, связанные с выполнением технологических процессов Системы (поставщиков услуг), устанавливаются соглашениями, заключаемыми Оператором с поставщиками услуг. Обязательным является обеспечения безопасности канала связи и обеспечение безопасности ключа электронной подписи.

8.1.18.6. Оператор устанавливает внутренними регламентами следующие требования к операционной надежности:

- технологических процессов, реализуемых в Системе;
- технологических процессов, реализуемых внешними контрагентами, оказывающими услуги в сфере информационных технологий, связанные с выполнением технологических процессов Системы;
- технологических участков (этапов) технологических процессов;
- программно-аппаратных средств поставщиков услуг, задействованных при выполнении технологических процессов;
- пороговые уровни допустимого времени простоя и (или) деградации технологических процессов.

8.1.19. Механизмы осуществления целостности и конфиденциальности данных, записываемых в распределенный реестр.

8.1.19.1. Система построена и функционирует в соответствии с открытым международным стандартом NISTIR 8202 Blockchain Technology Overview.

8.1.19.2. Для обеспечения корректности реализации алгоритмов создания, хранения и обновления информации в распределенном реестре используются криптографические механизмы обеспечения безопасности, которые не позволяют вносить несанкционированные изменения в алгоритмы и данные Системы.

8.1.19.3. За счет привлечения Валидаторов, каждый из которых имеет свои ключи электронной подписи, обеспечивается подтверждение и проверка действий, таких как создание, хранение и обновление информации с использованием ключей и сертификатов неквалифицированных электронных подписей.

8.1.19.4. Использование технологий распределенного реестра позволяет минимизировать риски создания или изменения информации в случае несанкционированного доступа к одному из валидаторов или ресурсов Системы.

8.1.20 В рамках реализации процессов взаимодействия Пользователей с Системой Оператор выполняет следующие меры, направленные на обеспечение операционной надежности:

8.1.20.1. Обеспечение порогового уровня допустимого времени простоя и (или) деградации технологических процессов в соответствии со сроками, предусмотренными Положением Банка России от 15.11.2021 № 779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)»;

8.1.20.2. Обеспечение мер защиты информации в соответствии с Положением Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций», а также резервирование средств взаимодействия, включая каналы связи, аппаратное и программное обеспечение.

8.1.20.3. Проведение регулярного тестирования средств, обеспечивающих резервирование, не реже одного раза в год;

8.1.20.4. Меры, направленные на обеспечение операционной надежности, установленные внутренними регламентами Оператора.

8.1.21. При взаимодействии Пользователей с Системой Оператор выполняет обеспечивает выполнение следующих мер информационной безопасности:

8.1.21.1. Выделение отдельного контакта службы (подразделения), ответственного за выявление и устранение инцидентов информационной безопасности;

8.1.21.2. Регулярная, не реже одного раза в год, оценка безопасности средств взаимодействия между Оператором и Операторами обмена.

8.1.22. Целостность и достоверность информации обеспечивается Оператором путем использования программного обеспечения на основе технологии Распределенного реестра.

В случае необходимости проведения ремонтных и регламентных работ аппаратной части средств криптографической защиты информации должна быть обеспечена невозможность доступа нарушителя к ключевой информации, содержащейся в аппаратной части средств криптографической защиты информации.

8.2. Требования к информационной безопасности оператора ЦФА

8.2.1. Оператор обмена цифровых финансовых активов в значении, обеспечивает защиту информации, бесперебойность и непрерывность функционирования информационной Системы, в которой осуществляется выпуск цифровых финансовых активов.

8.2.2. Оператор обмена пересматривает пороговые уровни показателей бесперебойности с использованием результатов оценки рисков в информационной системе не реже одного раза в год.

8.2.3. Для проведения работ по защите информации Оператором обмена могут привлекаться на договорной основе организации, имеющие лицензию на проведение работ и услуг, предусмотренных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

8.2.4. Для защиты информации от воздействия вредоносного кода Оператором обмена используются средства антивирусной защиты с функцией централизованного управления, мониторинга и автоматического реагирования в случаях выявления вредоносного кода.

8.2.5. Оператор обмена должен обеспечить надлежащий уровень реагирования на инциденты информационной безопасности в соответствии с собственными внутренними регламентами.

8.2.6. Комплекс информационной безопасности должен содержать следующие основные компоненты:

8.2.6.1. Журналирование событий: непрерывная запись всех доступных событий системы для анализа, поддерживает системы точного времени, которая необходима для точной фиксации информационных событий;

8.2.6.2. Шифрование передачи данных: персональные, идентификационные и аутентификационные данные передаются исключительно с использованием шифрования в соответствии с требованиями законодательства;

8.2.6.3. Ограничение доступа: все пользователи информационной системы (в том числе работники Оператора обмена) получают персонализированный доступ, а информационную систему с использованием аутентификационных данных.

8.2.7. Взаимодействие с Оператором обмена должно выполняться с использованием защищенных каналов связи.

8.2.8. В рамках реализации процессов взаимодействия пользователей информационной системы Оператор обмена выполняет следующие меры, направленные на обеспечение информационной безопасности:

8.2.8.1. Выделение отдельного контакта службы (подразделения), ответственного за выявление и устранение инцидентов информационной безопасности;

8.2.8.2. Регулярная, не реже одного раза в год, оценка уровня безопасности программно-технического комплекса Оператора обмена.

8.2.9. В рамках реализации процессов взаимодействия пользователей информационной системы Оператор обмена выполняет следующие меры, направленные на обеспечение операционной надежности:

8.2.9.1. Резервирование средств взаимодействия, включая каналы связи, аппаратное и программное обеспечение;

8.2.9.2. Проведение регулярного тестирования средств, обеспечивающих резервирование, не реже одного раза в год.

8.2.10. Оператор обмена обеспечивает защиту от проникновения, а именно: предотвращение вмешательства в работу Системы из общедоступных сетей передачи данных, в том числе из сети Интернет. Оператор обмена проводит анализ и ограничение (при необходимости) входящего и исходящего потока данных на соответствие требованиям правил безопасности.

9. Правила привлечения операторов обмена.

9.1. Правила привлечения Операторов обмена.

9.1.1. В соответствии с действующим законодательством Российской Федерации и настоящими Правилами Оператор обеспечивает заключение сделок с Цифровыми правами в Системе.

9.1.2. Сделки с Цифровыми правами также могут заключаться (совершаться) через Оператора обмена.

9.1.3. Взаимодействие между Оператором и Операторами обмена, осуществляется на основании договора, определяющего условия взаимодействия. Положения настоящего пункта не применяются в случае, если Оператором обмена является Оператор.

9.1.4. Оператор обмена должен соответствовать следующим требованиям:

- включение в реестр Операторов обмена, предусмотренный законодательством Российской Федерации;

- наличие программно-технических средств, необходимых для заключения через него сделок с Цифровыми правами, исполнение которых осуществляется в Системе;

- соблюдение требований к защите информации, установленных Оператором, которые размещаются на сайте в сети «Интернет» Оператора.

9.1.5. Оператор обмена обязан передавать Оператору информацию о сделках с Цифровыми правами, которые были совершены через такого Оператора обмена, а также об участниках таких сделок, включая информацию об исполнении Эмитентом своих обязательств перед владельцем Цифровых прав.

9.1.6. Информационно-технологическое взаимодействие Оператора и Оператора обмена осуществляется с использованием соответствующих программно-технических средств.

10. Порядок заключения и исполнения сделок в системе.

10.1. Порядок осуществления сделок с Цифровыми правами.

10.1.1. Пользователи вправе заключать (совершать) любые предусмотренные действующим законодательством Российской Федерации сделки с Цифровыми правами.

Сделки с Цифровыми правами заключаются (совершаются) в Системе. Сделки с Цифровыми правами могут также заключаться (совершаться) через Оператора обмена. Расчеты денежными средствами по сделкам, заключаемым (совершаемым) с Цифровыми правами, осуществляется вне Системы без участия Оператора. Пользователи принимают на себя все связанные с этим риски.

10.1.2. Запрещается заключать (совершать) сделки, направленные на легализацию (отмывание) доходов, полученных преступным путем, финансирования терроризма или распространения оружия массового уничтожения, а также сделки, в которых Цифровые права используются в качестве средства платежа или иного встречного предоставления за передаваемые товары, выполняемые работы, оказываемые услуги, а также иного способа, позволяющего предполагать оплату Цифровыми правами товаров (работ, услуг), за исключением случаев, предусмотренных федеральными законами.

10.1.3. В целях совершения в Системе сделки с Цифровыми правами Пользователь-инициатор сделки, с помощью функционала Личного кабинета формирует заявку на заключение сделки, являющуюся безотзывной офертой на заключение соответствующей сделки, адресованной Пользователю, указанному в заявке на заключение сделки (Пользователю – контрагенту).

10.1.4. В заявке на заключение сделки указываются: вид сделки, реквизиты Пользователя-контрагента, информация о виде и количестве Цифровых прав, являющихся предметом сделки.

10.1.5. Направление заявки на заключение сделки осуществляется Пользователем-инициатором сделки посредством использования функционала Личного кабинета и УКЭП Пользователя. При подписании Заявки на заключение сделки УКЭП Пользователя – инициатора сделки инициируется вызов Смарт-контракта.

10.1.6. Информация о направленной заявке на заключение сделки отображается в Личном кабинете Пользователя – инициатора сделки и Личном кабинете Пользователя – контрагента.

10.1.7. Пользователь – контрагент вправе акцептовать заявку на заключение сделки, направленную Пользователем – инициатором сделки, или отклонить ее, выбрав соответствующий вариант в Личном кабинете и подтвердив его путем подписания своей УКЭП в течение 1 часа с момента направления заявки на заключение сделки, за исключением сделки по переводу Цифровых прав без перехода права собственности на них на Кошелек Номинального держателя (далее – «перевод Цифровых прав в Номинальное держание») или с Кошелька Номинального держателя (далее – «вывод Цифровых прав из Номинального держания»).

Заявка на перевод Цифровых прав в Номинальное держание или вывод Цифровых прав из Номинального держания может быть акцептована или отклонена Пользователем – контрагентом сделки путем выбора соответствующего варианта в Личном кабинете и подтверждения его путем подписания своей УКЭП в течение 30 дней с момента ее направления.

В случае, если по истечению срока, указанного выше, Пользователь – контрагент (в том числе Номинальный держатель) не предпримет никаких действий, заявка на совершение сделки считается не акцептованной.

Акцепт заявки со стороны Пользователя – контрагента является встречной заявкой по отношению к заявке на заключение сделки, направленной Пользователем – инициатором сделки.

10.1.8. В момент получения акцепта оферты в Системе Смарт-контрактом осуществляется фиксация и сопоставление разнонаправленных заявок Пользователя-инициатора сделки и Пользователя – контрагента, а сделка считается заключенной.

10.1.9. Условием для внесения Смарт-контрактом в Систему записи в отношении Цифровых прав, в том числе о переходе Цифровых прав от одного Пользователя к другому, является заключение сделки и не требует дополнительного волеизъявления сторон.

10.1.10. Для совершения сделки с Цифровыми правами, которая не предусмотрена функционалом Личного кабинета:

- Пользователь в порядке, предусмотренном пунктом 5.5 настоящих Правил, направляет Оператору запрос на совершение указанной сделки, содержащий описание планируемой к совершению сделки, сведения о сторонах указанной сделки, информацию о Цифровых правах, являющихся предметом сделки, их количестве, а также иную информацию, необходимую для совершения сделки;

- Оператор в течение 15 (пятнадцати) рабочих дней с даты получения запроса рассматривает указанный запрос и направляет Пользователю ответ с указанием порядка и способа заключения указанной сделки или отказ от обеспечения возможности ее заключения, в случае если содержание указанной сделки противоречит требованиям законодательства Российской Федерации.

10.2. Порядок исполнения Оператором требований Актов.

10.2.1. В случае получения Оператором Акта:

- не позднее рабочего дня, следующего за днем получения соответствующего Акта – Оператор путем применения Смарт-контракта обеспечивает внесение (изменение) записей о Цифровых правах на основании Акта;

- не позднее рабочего дня, следующего за днем внесения (изменения) записей, указанных в пункте 10.2.1 настоящих Правил – Оператор направляет уведомления Операторам обмена, привлеченных с целью организации оборота Цифровых прав, о внесении (изменении) записей, указанных в пункте 10.2.1. настоящих Правил.

10.3 Порядок подтверждения Транзакций.

10.3.1. Транзакция считается совершенной при условии ее подтверждения в порядке, предусмотренном настоящим разделом.

10.3.2. Процесс подтверждения Транзакций представляет собой совокупность этапов, перечисленных в пункте 10.3.5 настоящих Правил и представляющих собой упорядоченную последовательность совершающихся действий, осуществляемых Одноранговыми узлами и Узлами Службы упорядочивания в течение установленного временного интервала.

10.3.3. Временной интервал, в течение которого Транзакция должна быть подтверждена или отклонена составляет 10 минут с момента направления Транзакции на подтверждение. Транзакции, не подтвержденные в течение времени, указанного в настоящем пункте, считаются отклоненными.

10.3.4. В случаях отклонения Транзакции или отметки Транзакции в качестве невыполненной в соответствии с положениями настоящей статьи соответствующая информация отображается в Личных кабинетах Пользователей, участвующих в Транзакции. Отклоненная или невыполненная Транзакция может быть инициирована повторно.

10.3.5. Процесс подтверждения Транзакций состоит из следующих последовательных этапов:

- Этап определения Одноранговых узлов, участвующих в подтверждении Транзакции.
- Этап проверки Транзакции Одноранговыми узлами.
- Этап подтверждения транзакции Узлами Службы упорядочивания.
- Этап записи транзакции Одноранговыми узлами.
- Минимальное количество Узлов Службы упорядочивания, которые будут участвовать в подтверждении Транзакции, составляет 3 (Три) Узла.

В случае, если количество активных Узлов Службы упорядочивания составляет менее 50% от числа зарегистрированных в Сети Узлов Службы упорядочивания, направленные на подтверждение Транзакции отклоняются.

Оператор осуществляет постоянный мониторинг Сети на предмет минимального допустимого количества Узлов Службы упорядочивания. Если количество Узлов Службы упорядочивания в Сети составляет менее 50% от числа зарегистрированных в Сети Узлов Службы упорядочивания, Оператор и активные, т.е. подключенные к Сети в данный момент, Валидаторы запускают резервные Узлы Службы упорядочивания в количестве, необходимом для восстановления штатной работы Сети.

10.3.7. На этапе определения Одноранговых узлов, участвующих в подтверждении Транзакции, модуль Системы, отвечающий за взаимодействие с распределенным реестром

случайным образом, определяет Одноранговые узлы, которые будут участвовать в подтверждении Транзакции.

10.3.8. На этапе проверки Транзакции Одноранговыми узлами, Одноранговые узлы, определенные для подтверждения Транзакции, осуществляют проверку выполнения совокупности следующих условий:

- корректность электронной подписей Транзакции и отправителя Транзакции;
- соответствие Отпечатков сертификатов УКЭП Пользователей, - сторон сделки, содержащихся в Транзакции, данным об Отпечатках сертификатов их УКЭП, хранящимся в распределенном реестре Системы;
- корректность самих изменений данных в соответствии с бизнес-логикой Смарт-контрактов Системы.

В случае консистентности итогов проверки Транзакции инициируется следующий этап подтверждения Транзакции. В ином случае Транзакция отклоняется.

10.3.9. На этапе подтверждения Транзакции Узлами Службы упорядочивания из числа Узлов Службы упорядочивания случайным образом определяется лидер. Узел Службы упорядочивания, определенный в качестве лидера, агрегирует Транзакции в блоки распределенного реестра, и направляет сформированные блоки остальным Узлам Службы упорядочивания, участвующим в подтверждении Транзакции.

Узлы Службы упорядочивания проверяют корректность блоков, сформированных лидером. В случае достижения консенсуса о корректности сформированных блоков указанные блоки направляются на следующий этап подтверждения Транзакций.

В случае не достижения консенсуса происходит повторный выбор лидера с дальнейшим повторением действий, описанных в настоящем пункте.

10.3.10. На этапе записи транзакции Одноранговыми узлами Одноранговые узлы производят запись блоков в реестр Транзакций, содержащийся в Системе. Транзакция, записываемая в реестр Транзакций, может быть помечена как невыполненная в случае нарушения проверки корректности данных Транзакции, осуществляемой Одноранговыми узлами.

10.3.11. Подтверждение Транзакции считается завершенным с момента внесения в Систему соответствующей записи путем включения Одноранговыми узлами Транзакции в реестр Транзакций, содержащийся в Системе.

11. Прочие положения

11.1. Правила взаимодействия с Номинальными держателями

11.1.1. В Системе Цифровые права могут быть зачислены на Кошелек Пользователя – Номинального держателя в случаях, если депозитарным договором между ним и депонентом предусмотрена обязанность Номинального держателя, указанная в пункте 14 статьи 7 Федерального закона от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг».

11.1.2. Зачисление Цифровых прав Номинальному держателю осуществляется путем внесения записей о Цифровых правах в Системе. На Кошелек Номинального держателя не могут быть зачислены Цифровые права, принадлежащие такому Номинальному держателю.

11.1.3. Зарегистрироваться в Системе в качестве Номинального держателя вправе только профессиональный участник рынка ценных бумаг, имеющий лицензию на осуществление депозитарной деятельности.

11.1.4. Номинальный держатель и Оператор вправе заключить между собой договор с включением в него условий, устанавливающих порядок проведения регулярной сверки соответствия количества Цифровых прав, а также порядок взаимодействия Оператора информационной системы с Номинальным держателем при прекращении исполнения Номинальным держателем функций по учету Цифровых прав.

11.1.5. Если иное не предусмотрено федеральными законами, Номинальный держатель по указанию обладателя Цифровых прав - депонента осуществляет Цифровые права последнего, распоряжается ими, передает в залог или устанавливает их обременение другими способами в Системе без обращения к третьему лицу.

11.2. Определение тарифов Оператора и порядок оплаты услуг.

11.2.1. Пользователи обязуются оплачивать услуги Оператора в соответствии с тарифами, установленными Оператором (далее – «Тарифы»).

11.2.2. Тарифы подлежат опубликованию на сайте Оператора в сети «Интернет». Оператор вправе в одностороннем порядке изменять Тарифы. В случае внесения изменений новая редакция Тарифов раскрывается на сайте Оператора.

11.2.3. Неисполнение обязанностей по оплате услуг Оператора является основанием для применения следующих мер ответственности:

11.2.3.1. предупреждение;

11.2.3.2. приостановление доступа к Системе.

11.3. Ответственность.

11.3.1. Оператор несет ответственность в случаях и порядке, установленном Законом о ЦФА.

11.3.2. Оператор не несет ответственности:

- за содержание и достоверность информации, содержащейся в решениях о выпуске;
- за неисполнение Эмитентами обязательств, предусмотренных решением о выпуске;
- за неисполнение Пользователями обязательств по сделкам с Цифровыми правами, заключенным между Пользователями;
- за наличие правовых оснований по сделкам с Цифровыми правами, заключенным между Пользователями;
- за невозможность использования Системы по причинам, зависящим от Пользователей или третьих лиц;
- за убытки, возникшие у Пользователя вследствие доступа третьих лиц к его Личному кабинету по причине утраты или компрометации УКЭП;
- за убытки, которые могут возникнуть у Пользователя в случае неисполнения запроса, указанного в разделе 5.6 настоящих Правил, в случае если лицом, подавшим соответствующий запрос, не были корректно названы все требуемые реквизиты или если соответствующий запрос был передан в нерабочее время Оператора;
- за убытки, возникшие у Пользователя вследствие исполнения Оператором требований Актов.

11.3.3. Пользователи возмещают убытки Оператору в порядке и в объеме, предусмотренном действующим законодательством Российской Федерации, в случае:

- предоставления Оператору недостоверной, неполной или вводящей в заблуждение информации;
- совершения действий, нарушающих законодательство Российской Федерации, совершенных с использованием Системы;
- сбоя в работе информационных технологий и технических средств Системы по причинам, зависящим от Пользователей.

11.4. Заверения об обстоятельствах.

11.4.1. Присоединяясь к Договору о предоставлении доступа к Системе, а также заключая (совершая) сделки через Оператора в соответствии с настоящими Правилами, Заявители / Пользователи тем самым предоставляют Оператору следующие заверения об обстоятельствах в соответствии со статьей 431.2 Гражданского кодекса Российской Федерации:

11.4.1.1. Заявитель / Пользователь ознакомлен с настоящими Правилами, понимает их содержание и согласен с их положениями;

11.4.1.2. Заявитель / Пользователь отвечает всем требованиям, предусмотренным пунктом 4.2 настоящих Правил, а также подтверждает достоверность предоставленных им данных в соответствии со статьей 6 настоящих Правил;

11.4.1.3. Пользователем получены необходимые решения, требуемые в соответствии с положениями законодательства Российской Федерации, уставом, иными документами, регулирующими деятельность Пользователя, для заключения (совершения) сделок с Цифровыми правами, выпущенными (выпускаемыми) в Системе, в том числе приняты все корпоративные решения, в частности, в отношении порядка совершения крупных сделок и сделок, в совершении которых имеется заинтересованность;

11.4.1.4. Заявитель/Пользователь подтверждает наличие у него согласия физических лиц, являющихся субъектами персональных данных, включенных в регистрационные документы, а также документы, предоставляемые Оператору в соответствии с пунктами 5.1.1.3. и 5.4.9 настоящих Правил в целях заключения Договора о предоставлении доступа к Системе, предоставления доступа к Системе, обновления сведений о соответствующем Пользователе и оказания ему услуг Оператора.

11.4.2. Пользователь не вправе распространять каким-либо образом экземпляры Системы, осуществлять ее доведение до всеобщего сведения, осуществлять ее переработку (модификацию), декомпилирование или модификацию ее программных компонентов.

11.4.3. Пользователь обязуется не совершать каких-либо действий, которые могут нарушить работоспособность и функциональные возможности Системы.

11.4.4. Пользователь, осуществивший выпуск ЦП в Системе, обязуется по запросу Оператора представлять сведения о своем бенефициарном владельце/владельцах в срок, предусмотренный таким запросом.

11.5. Порядок разрешения споров

11.5.1. Все споры, разногласия и требования, возникающие в связи с оказанием Оператором услуг в соответствии с настоящими Правилами, подлежат разрешению в порядке арбитража (третейского разбирательства), администрируемого Арбитражным центром при Российском союзе промышленников и предпринимателей (далее – **«Арбитражный центр при РСПП»**) в соответствии с его правилами, действующими на дату подачи искового заявления.

11.5.2. Передача споров на разрешение в Арбитражный центр при РСПП возможна только после соблюдения предварительного претензионного порядка урегулирования споров. В случае полного или частичного отказа в удовлетворении претензии или неполучения ответа в течение 7 (семи) дней с момента получения претензии заявитель вправе предъявить иск в Арбитражный центр при РСПП.

11.5.3. Решения Арбитражного центра при РСПП являются окончательными и обязательными для сторон. Неисполненное добровольно решение Арбитражного центра при РСПП подлежит принудительному исполнению в соответствии с законодательством Российской Федерации.

11.5.4. Пользователи обязаны воздерживаться от действий, направленных на затягивание процесса рассмотрения спора в Арбитражном центре при РСПП, а в случае вынесения Арбитражным центром при РСПП решения – на затягивание сроков исполнения определений и решений, вынесенных Арбитражным центром при РСПП.