Приложение
к Приказу Генерального директора ООО «Атомайз»
от 23.12.2022 г. № АТМ/23.12.2022/1-п

Требования к валидаторам

1. Общие положения.

1.1. Настоящие Требования разработаны в целях принятия Оператором информационной системы решения о допуске Валидатора к подтверждению Транзакций или об отказе в таком допуске на Платформе ООО «Атомайз».

1.2. Настоящие Требования определяют требования к Валидаторам в зависимости от типа узлов валидации, требования к наличию у Валидаторов программного обеспечения и оборудования, необходимого для подтверждения Транзакций, а также требования к обеспечению защиты информации на узлах валидации.

1.3. Основные положения настоящих Требований раскрываются на сайте https://atomyze.ru.

1.4. Требования, содержащиеся в настоящем документе, могут быть изменены по соглашению сторон в рамках договора на оказание услуг валидации.

2. Термины и определения

Термин	Определение
Валидатор	Лицо, с которым Оператор информационной системы заключает договор на оказание Оператору информационной системы услуг по подтверждению Транзакций с Цифровыми правами, или непосредственно Оператор информационной системы. Под управлением Валидатора может находиться один или несколько Узлов валидации.
Оператор информационной системы (Оператор)	Общество с ограниченной ответственностью «Атомайз» (ОГРН 1207700427714), осуществляющее деятельность по эксплуатации Информационной системы в соответствии ФЗ о ЦФА и включенное Банком России в реестр операторов информационной системы, в которых осуществляется выпуск Цифровых прав.

Ордерер	Узел валидации, который в рамках подтверждения Транзакций с Цифровыми правами осуществляет функционал по формированию блоков (упорядочиванию) Транзакций для их последующей записи в Информационную систему.
Пир	Узел валидации, который в рамках подтверждения Транзакций с Цифровыми правами осуществляет функционал по записи сформированных Ордерером блоков Транзакций в Информационную систему. Функции Пира и Эндорсера могут быть совмещены в одном Узле валидации.
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 или посредством Мобильного приложения.
Транзакция	Операция по переходу Цифровых прав, осуществляемая в Информационной системе.
ФЗ о ЦФА	Федеральный закон № 259-ФЗ от 31.07.2020 "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации".
Цифровые активы	Цифровые финансовые активы по смыслу ч. 2 ст. 1 ФЗ о ЦФА, включающие денежные требования, и(или) цифровые права, включающие одновременно цифровые финансовые активы по смыслу ч. 2 ст. 1 ФЗ о ЦФА, включающие денежные требования, и иные цифровые права по смыслу части 6 ст. 1 ФЗ о ЦФА, которые выпускаются или выпущены в Информационной системе в соответствии с ФЗ о ЦФА, иными требованиями законодательства и настоящими Правилами. Каждому Цифровому праву соответствует определённый Смарт-контракт. Цифровые права не признаются и не являются средством платежа.
Эндорсер	Узел валидации, который в рамках подтверждения Транзакций с Цифровыми правами осуществляет функционал по одобрению Транзакций, который включает в себя проверку Приватных ключей и балансов Кошельков, передачу Транзакций Ордерерам для формирования блоков (упорядочивания) Транзакций. Функции Пира и Эндорсера могут быть совмещены в одном Узле валидации.

Иные термины и определения имеют значение, указанное в Правилах оператора информационной системы, размещенных на сайте Оператора информационной системы.

3. Требования к Валидаторам:

3.1. Валидатором Платформы может быть юридическое лицо, а также зарегистрированный в соответствии с законодательством Российской Федерации индивидуальный предприниматель.

4. Требования к программному обеспечению и оборудованию, необходимому для подтверждения Транзакций

4.1. Оборудование:

№	Тип узла валидации	Количество виртуальных ядер vCPU	Объем оперативной памяти, Gb	Объем жесткого диска, Gb	Тип жесткого диска
1.	Пир	4	16	1024	HDD
2.	Ордерер	4	16	1024	HDD
3.	Эндорсер	4	16	1024	HDD

4.2. Для поддержания работоспособности и отказоустойчивости аппаратные и программные средства валидации должны дублироваться и в случае сбоя основного комплекса переключаться на резервные узлы.

4.3. ЦОД Валидатора должен соответствовать Уровню II и выше по классификации отказоустойчивости:

- Уровень I — базовая инфраструктура без резервирования;
- Уровень II — инфраструктура с резервными мощностями;
- Уровень III — инфраструктура, поддерживающая параллельный ремонт;
- Уровень IV — отказоустойчивая инфраструктура.

4.4. Аппаратные и программные средства Валидатора должны быть защищены средствами противодействия DDoS-атакам.

4.5. Валидатору необходимо предусмотреть дублирование каналов связи, используемых для подключения аппаратно-программных средств к сети валидации.

4.6. Валидатору необходимо производить тестирование работоспособности всех компонентов аппаратно-программных средств перед подключением к сети Оператора информационной системы.

4.7. Аппаратно-программные средства валидации должны быть подключены к системе непрерывного мониторинга работы узлов для своевременного выявления сбоев и уведомления персонала Валидатора и персонала Оператора информационной

системы о неработоспособности узла Валидатора с целью скорейшего восстановления работы.

4.8. Инциденты и аварии, произошедшие в аппаратно-программной среде Валидатора, должны регистрироваться в системе учета событий операционной надежности Оператора информационной системы и по итогам устранения должны формироваться отчеты о причинах возникновения сбоев и аварий, методах их устранения и мероприятий по недопущению возникновения данных ситуаций в будущем.

5. Требования к обеспечению защиты информации

5.1. Валидатор обязан:

- Использовать на серверах валидации только лицензионное программное обеспечение.
- Производить на регулярной основе обновление системного ПО.
- Производить на регулярной основе обновление прикладного ПО.
- Использовать программные или программно-аппаратные средства для защиты от несанкционированного доступа к аппаратным, программно-аппаратным и программным средствам валидации.
- Использовать программные или программно-технические средства, реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков для защиты от реализации внутренних и внешних угроз безопасности к аппаратным и программным средствам валидации.
- Использовать системы обнаружения и предотвращения вторжений.
- На регулярной основе проводить мероприятия по анализу защищенности своих систем и сетей.
- Использовать средства защиты от вредоносного программного кода.
- Соответствовать актуальным требованиям законодательства к сети Оператора информационной системы в части операционной надежности и информационной безопасности.

5.2 Валидатору запрещается проводить анализ программного обеспечения, поставляемого Оператором информационной системы и осуществлять реверсинжениринг кода программного обеспечения.

6. Требования к операционной надежности

Валидатор обязан соблюдать следующие требования:

6.1. Поддерживать работоспособность узла валидации и его подключения к сети Оператора информационной системы на уровне доступности 99,65% общего времени работы;

6.2. Реагировать на сбой в работе узла валидации приведшего к недоступности узла или некорректной работы в течение 15 минут с момента получения оповещения о неработоспособности узла от систем мониторинга или от любого участника сети валидации Оператора информационной системы;

6.3. Восстанавливать работоспособность узла валидации не менее чем за 2 часа с момента обнаружения факта недоступности или некорректной работы узла;

6.4. В течение 3 (трех) рабочих дней с момента возникновения инцидента, связанного с неработоспособностью или некорректной работой узла валидации предоставлять Оператору информационной системы отчет о причинах возникновения инцидента и мерах по восстановлению и предотвращению подобных инцидентов.