Утверждено приказом Генерального директора ООО «ЛАЙТХАУС»

№ 28-01/03-2023 от «28» марта 2023 г.

ТРЕБОВАНИЯ К УЗЛАМ ВАЛИДАТОРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ООО «ЛАЙТХАУС»

2023 г.

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе используются следующие термины, определения и сокращения:

ВСИ – вычислительная и сетевая инфраструктуры.

Вычислительные ресурсы Валидатора – комплекс вычислительных ресурсов, включающий в себя серверное оборудование, сеть передачи данных, программные средства виртуализации, резервного копирования, управления и мониторинга. Оборудование Валидатора находится в его Центре обработки данных (далее – ЦОД).

ПО – программное обеспечение.

Распределенный реестр – совокупность баз данных, тождественность содержащейся информации в которых обеспечивается установленными алгоритмами.

Оператор – ООО «Лайтхаус», оператор информационной системы, в которой осуществляется выпуск, учет и обмен цифровых финансовых активов в соответствии с Законом о ЦФА.

СХД – система хранения данных.

Система – предусмотренная частью 9 статьи 1 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее - Закон о ЦФА) информационная система, в которой осуществляется выпуск, учет и обмен цифровых финансовых активов (ЦФА).

Узел Валидатора, Узел – виртуальная машина, выполняющая функции одобрения Транзакций, упорядочивания и (или) записи блоков Транзакций в Систему в рамках общего процесса подтверждения Транзакций.

ЦОД – центр обработки данных.

ТРЕБОВАНИЯ К ВАЛИДАТОРАМ

Вычислительные ресурсы Узлов Валидатора размещаются исключительно внутри действующего ЦОД Валидатора в отдельной от иной информационной инфраструктуры Валидатора изолированной зоне. ЦОД Валидатора обеспечен системой кондиционирования, бесперебойного питания, пожаротушения, телекоммуникационными

шкафами, высоконадежным серверным оборудованием и СХД, а также системами мониторинга и управления всем оборудованием внутри объекта.

ЦОД должен быть предназначен для обеспечения гарантированной безотказной работы вычислительных ресурсов Узла Валидатора с необходимым уровнем доступности, целостности, надежности, безопасности, а также управляемости с обеспечением сохранности максимально возможной функциональности Узла Валидатора при чрезвычайных обстоятельствах.

1. **Необходимый состав ВСИ ЦОД Узла Валидатора**

Система	**Функциональное назначение**
Серверное оборудование	– выполнение прикладных задач;
Хранения данных	– хранение данных; – осуществление доступа к архивным данным на уровне баз данных; – осуществление миграции данных; – обязательное резервное копирование и восстановление.
Передачи данных	– коммутация каналов передачи; – маршрутизация передачи данных; – обеспечение передачи данных со скоростью не менее 1 Гбит/с.
Обеспечения информационной безопасности	– межсетевое экранирование, для обеспечения обмена данными между подсистемой передачи данных и внешними сетями передачи данных; – обнаружение атак на информационную инфраструктуру и их предотвращение; – анализ и мониторинг действий администраторов информационных систем.

2. **Необходимый состав инженерных систем ЦОД Узла Валидатора**

Система	Функциональное назначение
Пожарной сигнализации и автоматического пожаротушения	- обеспечение автоматического пожаротушения ЦОД.
Бесперебойного электропитания	- обеспечение гарантированного электроснабжения дизель-генератором ЦОД.
Гарантированного электроснабжения	- обеспечение бесперебойного питания размещаемого оборудования в серверном помещении в течение 60 минут.
Климат-контроля	- охлаждение оборудования в серверном помещении до требуемых значений.
Охранной сигнализации	- предотвращение несанкционированного проникновения в помещение ЦОД.
Внутренней безопасности	- видеонаблюдение 24/7 за контуром здания ЦОД; - видеонаблюдение за серверным помещением; - видеонаблюдение за размещаемым оборудованием; - возможность мониторинга видеокамер с разных автоматизированных рабочих мест, при помощи авторизированного доступа; - хранение записанной информации не менее 30 дней.
Контроль управления доступом	- контроль доступа персонала в здание ЦОД; - организация доступа для персонала при помощи электронных пропусков.

3. Требования к оборудованию Узлов Валидатора

- 4GB RAM – объём оперативной памяти;
- 1 TB SSD – объём и тип жёсткого диска;

• x64 2.0 GHz 4 vCPUs – характеристики CPU.

4. Требования к обеспечению защиты информации

4.1. Валидатор обязан:

4.1.1. Размещать Узел Валидатора исключительно на вычислительных ресурсах Валидатора;

4.1.2. Обеспечить необходимый уровень информационной безопасности для информации, обрабатываемой и хранимой в вычислительных ресурсах Валидатора, полученной из Системы;

4.1.3. Использовать сетевой экран для защиты от несанкционированного доступа к аппаратным и программным средствам валидации;

4.1.4. Использовать на серверах валидации только лицензионное программное обеспечение.

4.1.5. Производить на регулярной основе обновление системного ПО.

4.1.6. Производить на регулярной основе обновление прикладного ПО.

4.1.7. Использовать программные или программно-аппаратные средства для защиты от несанкционированного доступа к аппаратным, программно-аппаратным и программным средствам валидации.

4.1.8. 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, в том числе:

4.1.8.1. применять журналирование событий: осуществлять непрерывную запись всех событий системе для анализа в режиме реального времени и при расследовании инцидентов и сбоев;

4.1.8.2. применять ограничение доступа: работники Валидатора получают персонализированный доступ с использованием аутентификационных данных. При работе используется ролевая модель, в которой каждый работник имеет отдельные аутентификационные данные для выполнения различных функций в зависимости от текущей роли. Роли, имеющие между собой конфликт интересов, не могут назначаться одному и тому же работнику.

4.1.9. Использовать системы обнаружения и предотвращения вторжений.

4.1.10. На регулярной основе проводить мероприятия по анализу защищенности своих систем и сетей.

4.1.11. Использовать средства защиты от вредоносного программного кода.

4.1.12. Использовать СКЗИ «КриптоПро CSP» актуальной версии.

4.2. Валидатору запрещено:

4.2.1. Самостоятельно производить подключение Узлов к сети распределённого реестра Системы без информирования Оператора, за исключением случаев:

4.2.1.1. технических работ по возобновлению работы Узлов для обеспечения операционной надёжности;

4.2.1.2. если указанная необходимость подключения Узлов вызвана наличием угрозы безопасности оборудования и конфиденциальной информации (включая информацию, составляющую коммерческую тайну) Валидатора, угрозы безопасности и обороноспособности государства, здоровью и безопасности людей;

4.2.1.3. в иных случаях, предусмотренных требованиями законодательства Российской Федерации.

4.2.2. Проводить анализ программного обеспечения, поставляемого Оператором и осуществлять реверсинжениринг кода программного обеспечения.

5. Требования к обеспечению операционной надежности

5.1. Валидатор обязан:

5.1.1. Обеспечить непрерывный информационный обмен с другими Узлами Системы и обеспечить дублирование каналов связи для операционной надежности;

5.1.2. Уведомлять Оператора о недоступности и сбоях в работе Узла Системы в течение 15 минут с момента обнаружения сбоя.

5.1.3. Поддерживать работоспособность Узла валидации и его подключения к Системе на уровне доступности 99,3% общего времени работы;

5.1.4. Реагировать на сбой в работе Узла валидации, приведшего к недоступности Узла или некорректной работе в течение 15 минут с момента получения оповещения о неработоспособности Узла от систем мониторинга или от любого участника Системы.

5.1.5. Восстанавливать работоспособность Узла валидации не менее чем за 2 часа с момента обнаружения факта недоступности или некорректной работы Узла.

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

5.1.7. Обеспечить резервирование средств взаимодействия, включая каналы связи, аппаратное и программное обеспечение. Обеспечить наличие как минимум одного резервного Узла ВСИ.

5.1.8. Обеспечить проведение регулярного тестирования средств, обеспечивающих резервирование, не реже одного раза в год.

5.1.9. Обеспечить доведение до сведения работников Валидатора порядка действий в нештатных ситуациях (реагирование и устранение).