Платформа цифровых активов

Общество с ограниченной ответственностью
«Токены – Цифровые Инвестиции» (ООО «Токены»)

УТВЕРЖДЕНО
Приказом от 11.09.2023 № 50/2023-П

ТРЕБОВАНИЯ

к узлам информационной системы

Общества с ограниченной ответственностью
«Токены – Цифровые Инвестиции»

(версия 1.1)

Москва, 2023

ИСТОРИЯ ИЗМЕНЕНИЙ ДОКУМЕНТА

Дата утверждения	Номер приказа	Номер версии	Изменения
07.04.2023	12/2023-П	1.0	-
11.09.2023	50/2023-П	1.1	Изменение требований к аппаратно-программному комплексу

Оглавление

1. ТРЕБОВАНИЯ К АППАРАТНО-ПРОГРАММНОМУ КОМПЛЕКСУ

1.1. Размещение в датацентре, удовлетворяющем требованиям Федерального закона «О персональных данных» от 27.07.2006 №152-ФЗ, с уровнем не ниже Tier-3.

1.2. Требования к аппаратному обеспечению:

- Процессор Intel/AMD: от 4 ядер / 2 ГГц;
- RAM: от 16 Гбайт;
- Дисковое пространство: от 900 Гбайт SSD;
- Ubuntu 22.04.

1.3. К аппаратному обеспечению должен быть привязан статический ipv4 адрес, который необходимо сообщить Оператору. Скорость интернета не ниже 100 Мбит/с. Необходимо открыть порты 9944 и 30333 для взаимодействия с другими узлами блокчейн-сети по статическим ipv4 адресам, которые сообщит Оператор при развертывании программного комплекса.

2. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Узел обеспечивает бесперебойность и непрерывность функционирования ИС в своей части.

2.2. Узел обязан установить и пересматривать не реже одного раза в год пороговые уровни показателей бесперебойности, с использованием результатов оценки рисков в ИС.

2.3. Узел использует комплекс мер и средств защиты информации, обеспечивающих необходимый уровень безопасности программных систем и продуктов, информационной инфраструктуры, а также позволяющих проводить мониторинг состояния информационной безопасности в реальном времени, отслеживать и своевременно реагировать на события, влияющие на информационную безопасность.

2.4. Для защиты информации Узлом должны использоваться только актуальные версии средств защиты информации. Все средства защиты информации проходят аудит не реже одного раза в два года. При появлении информации о новых, не учтенных видах угроз, средства защиты информации обновляются до полного соответствия возможностям противодействия вновь выявленным угрозам.

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

2.6. Комплекс информационной безопасности должен содержать следующие основные компоненты:

- **Журналирование событий**: непрерывная запись всех событий системы для анализа в режиме реального времени и при расследовании инцидентов и сбоев;
- **Ограничение доступа**: пользователи, являющиеся работниками Узла, получают персонализированный доступ с использованием аутентификационных данных. При работе используется ролевая модель в которой каждый пользователь 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 пользователю.

2.7. Узел выполняет следующие меры, направление на обеспечение информационной безопасности:

- выделение отдельного контакта службы (подразделения), ответственного за выявление и устранение инцидентов;
- регулярное, не реже одного раза в год, проведение оценки уровня обеспечения безопасности программно-технического комплекса Узла.

2.8. В рамках реализации процессов взаимодействия с другими узлами ИС Узел выполняет следующие меры, направление на обеспечение операционной надежности:

- резервирование средств взаимодействия, включая каналы связи, аппаратное и программное обеспечение;
- проведение регулярного тестирования средств, обеспечивающих резервирование, не реже одного раза в год;
- описание порядка действия работников Узла при реагировании и устранении нештатных ситуаций.

3. ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

3.1. Узел обеспечивает:

- бесперебойную работоспособность аппаратного обеспечения в части вычислительных мощностей и сетевых взаимодействий непрерывное предоставление удаленного взаимодействия с ИС Оператора.
- мониторинг работоспособности аппаратного обеспечения по следующим параметрам:

- доступность инфраструктуры (в частном случае, виртуальной машины);
- потребление вычислительных ресурсов;
- валидность сертификатов, предназначенных для функционирования программного комплекса.

3.2. Аппаратное обеспечение должно быть работоспособным и подключенным к сети Интернет не менее 99,3% всего времени в течение 1 (одного) месяца.

3.3. Узел незамедлительно сообщает Оператору обо всех событиях мониторинга в порядке, предусмотренном договором на осуществление функций Узла.

3.4. Узел не вправе вмешиваться в работу аппаратного обеспечения и настраивать режим его функционирования.