ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«СПУТНИК ЦФА»

ТРЕБОВАНИЯ

К УЗЛУ ИНФОРМАЦИОННОЙ СИСТЕМЫ «СПУТНИК ЦФА»

УТВЕРЖДЕНО
Единоличным исполнительным органом
Решение № 20250901-4 от 01.09.2025 г.

Версия 1.0

СПУТНИКЦФА

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аппаратное обеспечение - аппаратное обеспечение, на которое установлен Программный комплекс.

ИС - информационная система, в которой осуществляется выпуск цифровых финансовых активов, в значении, предусмотренном Правилам ИС и Федеральным законом «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 N 259-ФЗ, эксплуатируемая Оператором.

Правила ИС - правила информационной системы ООО «Спутник ЦФА», согласованные Банком России в порядке, предусмотренном законодательством Российской Федерации.

Программный комплекс - программа для ЭВМ или совокупность программ для ЭВМ, предназначенных для информационного взаимодействия между Оператором обмена и Оператором.

Оператор - ООО «Спутник ЦФА»

Узел - узел ИС в значении, предусмотренном Правилами ИС и Федеральным законом «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 No 259-ФЗ. обеспечивает бесперебойность и непрерывность функционирования информационной системы, в которой осуществляется выпуск цифровых финансовых активов, эксплуатируемой ООО «Спутник ЦФА» в своей части.

1. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЗЛА

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

1.2. 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.

1.3. 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.

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

1.5. Комплекс информационной безопасности должен содержать следующие основные компоненты:

1.5.1. Журналирование событий: непрерывная запись всех событий системы для анализа в режиме реального времени и при расследовании инцидентов и сбоев;

1.5.2. 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.

1.6. Узел выполняет следующие меры, направленные на обеспечение информационной безопасности:

1.6.1. выделение отдельного контакта службы (подразделения), ответственного за выявление и устранение инцидентов;

1.6.2. регулярное, не реже одного раза в год, проведение оценки уровня обеспечения безопасности программно-технического комплекса Узла.

2. ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ НАДЕЖНОСТИ УЗЛА

2.1. Узел обеспечивает:

2.1.1. бесперебойную работоспособность Аппаратного обеспечения в части вычислительных мощностей и сетевых взаимодействий;

2.1.2. мониторинг работоспособности Аппаратного обеспечения по следующим параметрам:

2.1.2.1. доступность инфраструктуры (в частном случае, виртуальной машины);

2.1.2.2. потребление вычислительных ресурсов;

2.1.2.3. валидность сертификатов, предназначенных для функционирования Программного комплекса.

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

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

2.4. Узел не вправе вмешиваться в работу Аппаратного обеспечения и настраивать режим его функционирования.

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

2.5.1. резервирование средств взаимодействия, включая каналы связи, аппаратное и программное обеспечение;

2.5.2. проведение регулярного тестирования средств, обеспечивающих резервирование, не реже одного раза в год;

2.5.3. описание порядка действия работников Узла при реагировании и устранении нештатных ситуаций.

3. ТРЕБОВАНИЯ К АППАРАТНО-ПРОГРАММНОМУ КОМПЛЕКСУ

3.1. Программно-технические требования

3.1.1. Размещение в датацентре, удовлетворяющем требованиям Федерального закона «О персональных данных» от 27.07.2006 №152-ФЗ.

3.2. Требования к аппаратному обеспечению:

- Процессор Intel/AMD: от 4 ядер / 2 ГГц;
- RAM: от 4 Гбайт;
- Дисковое пространство: от 50 Гбайт;
- Linux с ядром версии 3.0 и выше.

3.3. К аппаратному обеспечению должен быть привязан статический ipv4 адрес, который необходимо сообщить Оператору. Скорость интернета не ниже 100 Мбит/с.