Платформа цифровых активов

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

УТВЕРЖДЕНО
Приказом от 07.04.2023 № 12/2023-П

ТРЕБОВАНИЯ

к операторам обмена, привлекаемым для работы на платформе информационной системы, в которой осуществляется выпуск цифровых финансовых активов

Общества с ограниченной ответственностью
«Токены – Цифровые Инвестиции»

(версия 1.0.)

Москва, 2023

ИСТОРИЯ ИЗМЕНЕНИЙ ДОКУМЕНТА

Дата утверждения	Номер приказа	Номер версии	Изменения
07.04.2023	12/2023-П	1.0	-

Оглавление

1. ТРЕБОВАНИЯ К АППАРАТНО-ПРОГРАММНОМУ КОМПЛЕКСУ

Все серверы, ПО и иные вычислительные ресурсы информационной системы Оператора обмена (ИС) должны поддерживать работу в среде виртуализации и контейнеризации.

1.1. Требования к аппаратному обеспечению Платформы Оператора обмена

№	Наименование компонента	Кол-во	Центральный процессор (кол-во ядер / частота)	ОЗУ (ГБ)	Требуемые объемы данных (ГБ) SSD
1	Узел системы	1	4 ядра / 2 ГГц	20 Гб	500
2	Адаптер системы	1	8 ядер / 2 ГГц	16 Гб	500

1.2. Требования к системному программному обеспечению.

- ПЭВМ архитектуры x86, x64;
- Операционная система с ядром Linux версии 3.0 и выше, рекомендуемый дистрибутив: Ubuntu 20.04 или выше;
- СКЗИ «КриптоПро CSP», версия 5.0 R2 (КС1);
- Набор криптографических библиотек cprocsp-pki-cades версии не ниже 2.0.

Допускается развертывание компонентов ПО в следующих виртуальных средах (только в случае использования СКЗИ «КриптоПро CSP» версии 5.0 КС1, исполнение 1-Base):

- Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64);
- Microsoft Hyper-V 8/8.1/10 (x64);
- Citrix XenServer 7 (x64);
- VMWare WorkStation 11/12/14/15 (x86, x64);
- VMWare WorkStation Player 12/14/15 (x86, x64);
- VMWare vSphere ESXi/Hypervisor 5.5/6.0/6.5/6.7 (x64);
- RHEV 4 (x64);
- Платформа виртуализации серверов «Хост» (HOSTVM).

1.3. Требования к каналу связи:

- Скорость соединения не менее 20 МБит/сек.

2. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Оператор обмена обеспечивает бесперебойность и непрерывность функционирования информационной системы Оператора обмена.

2.2. Оператор обмена обязан установить и пересматривать не реже одного раза в год пороговые уровни показателей бесперебойности, с использованием результатов оценки рисков в информационной системе.

2.3. Оператор обмена обязан использовать 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 Оператором обмена 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. Оператор обмена 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.

2.6. Комплекс информационной безопасности Оператора обмена должен содержать следующие основные компоненты:

- журналирование событий: непрерывная запись всех событий системы для анализа в режиме реального времени и при расследовании инцидентов и сбоев;
- шифрование передачи данных: Персональные, идентификационные и аутентификационные данные передаются исключительно с использованием шифрования в соответствии с требованиями регулирующих органов;
- ограничение доступа: все пользователи (в том числе сотрудники каждой из Сторон) 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. Взаимодействие между Оператором обмена и информационной системой ООО «Токены» должно выполняться с использованием защищенных каналов связи.

2.8. Оператор обмена обеспечивает реализацию мероприятий по выявлению операций, направленных на совершение финансовых сделок без согласия Пользователей, в порядке, установленном Банком России.

2.9. Оператор обмена выполняет следующие меры, направление на обеспечение информационной безопасности:

- выделение отдельного контакта службы (подразделения), ответственного за выявление и устранение инцидентов, в том числе противодействие осуществлению незаконных операций без согласия пользователей;
- регулярное, не реже одного раза в год, проведение оценки уровня обеспечения безопасности программно-технического комплекса.

2.10. В рамках реализации процессов взаимодействия Пользователей с Оператором обмена и информационной системой ООО «Токены» Оператор обмена выполняет следующие меры, направленные 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 подразделений при реагировании и устранении нештатных ситуаций при взаимодействии с Пользователями.

3. ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

3.1. Оператор обмена при осуществлении своей деятельности 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».

3.2. Оператор обмена в соответствии с нормативными актами Банка России обеспечивает защиту информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в информационной системе, в том числе: информации о пользователях Платформы Оператора ИС, включая их персональные данные и (или) персональные данные их представителей; информации, на основании которой осуществляется выпуск и обращение ЦФА, в том числе информации, содержащейся в электронных сообщениях – указаниях о внесении или изменении записи о ЦФА в ИС.

3.3. Оператор обмена обязан установить и пересматривать не реже одного раза в год пороговые уровни показателей бесперебойности с использованием результатов оценки рисков в информационной системе оператора обмена. Значения показателей бесперебойности должны соответствовать требованиям нормативных актов Банка России.

3.4. Оператор обмена обеспечивает защиту от проникновения, а именно: предотвращение вмешательства в работу информационной 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.

3.5. Операционная надежность обеспечивается Оператором обмена в соответствии с утвержденными требованиями Банка России к операционной надежности Операторов обмена в целях обеспечения непрерывности оказания финансовых услуг.

3.6. Взаимодействие между Оператором обмена и информационной системой ООО «Токены» должно выполняться с использованием защищенных каналов связи.

3.7. Оператор обмена обеспечивает реализацию мероприятий по выявлению операций, направленных на совершение финансовых сделок с использованием информационной системы Оператора обмена без согласия Пользователей, а также, в порядке, установленном Банком России, направляет в Банк России информацию обо всех таких случаях.

3.8. В рамках реализации процессов взаимодействия Пользователей с ИС Оператор обмена выполняет следующие меры, направленные на обеспечение операционной надежности:

- 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)»;

- 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;

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

- описание порядка действия подразделений Оператора обмена при реагировании и устранении нештатных ситуаций при взаимодействии с Пользователями;

- выделение отдельного контакта службы поддержки для возможности прямого контакта Оператора обмена и Пользователей.