Требования к информационной безопасности оператора обмена цифровых финансовых активов

1. Оператор обмена цифровых финансовых активов в значении, предусмотренном правилами информационной системы ООО «Системы распределенного реестра» 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 (далее – **«Оператор обмена»**) обеспечивает бесперебойность и непрерывность функционирования информационной системы, в которой осуществляется выпуск цифровых финансовых активов, эксплуатируемой ООО «Системы распределенного реестра» (далее – **«информационная система»**) в своей части.

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.

3. Оператор обмена 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.

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.

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.

6. Комплекс информационной безопасности должен содержать следующие основные компоненты:

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

   6.2. **Шифрование передачи данных:** персональные, идентификационные и аутентификационные данные передаются исключительно с использованием шифрования в соответствии с требованиями регулирующих органов;

6.3. **Ограничение доступа:** все пользователи информационной системы (в том числе, работники Оператора обмена) 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;

7. Взаимодействие с Оператором обмена должно выполняться с использованием защищенных каналов связи.

8. Оператор обмена обеспечивает реализацию мероприятий по выявлению операций, направленных на совершение финансовых сделок без согласия пользователей информационной системы, в порядке, установленном Банком России.

9. В рамках реализации процессов взаимодействия пользователей информационной системы Оператор обмена выполняет следующие меры, направление на обеспечение информационной безопасности:

9.1. выделение отдельного контакта службы (подразделения), ответственного за выявление и устранение инцидентов, в том числе противодействие осуществлению незаконных операций без согласия пользователей информационной системы;

9.2. регулярное, не реже одного раза в год, проведение оценки уровня обеспечения безопасности программно-технического комплекса Оператора обмена.

10. В рамках реализации процессов взаимодействия пользователей информационной системы с Оператор обмена выполняет следующие меры, направление на обеспечение операционной надежности:

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

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

10.3. описание порядка действия подразделений Оператора обмена при реагировании и устранении нештатных ситуаций при взаимодействии с пользователями информационной системы.