Требования к информационной безопасности узла информационной системы

1. Узел информационной системы 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 – **«Узел»**), обеспечивает бесперебойность и непрерывность функционирования информационной системы, в которой осуществляется выпуск цифровых финансовых активов, эксплуатируемой ООО «Системы распределенного реестра» (далее – **«ИС»**), в своей части.
2. Узел обязан установить и пересматривать не реже одного раза в год пороговые уровни показателей бесперебойности, с использованием результатов оценки рисков в ИС.
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.
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.
5. 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.
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. **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.
7. Узел выполняет следующие меры, направление на обеспечение информационной безопасности:

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

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

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

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

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

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