Приложение № 1
к приказу НКО АО НРД
от «25» августа 2023 г. № 312-23

ТРЕБОВАНИЯ К ВАЛИДАТОРАМ ИНФОРМАЦИОННОЙ СИСТЕМЫ «ИС ЦФА» НКО АО НРД

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

НРД, Оператор информационной системы – Небанковская кредитная организация акционерное общество «Национальный расчетный депозитарий».

Информационная система – программное обеспечение, включая Распределенный реестр, совокупность баз данных, тождественность содержащейся информации в которых обеспечивается на основе установленных алгоритмов (алгоритма), с помощью которого осуществляется выпуск и обращение ЦФА.

Валидатор – Пользователь, заключивший с НРД договор на оказание услуг по обеспечению тождественности информации, содержащейся в Информационной системе или непосредственно НРД. Валидатор может иметь под управлением одну или несколько Нод. Привлечение новых и/или удаление действующих Валидаторов осуществляется по решению НРД.

Лернер – Нода, принимающая новые подтверждённые блоки и операции с ЦФА, осуществляемые в Информационной системе (транзакции), от любой из Нод.

Нода – программно-аппаратный комплекс, выполняющий функции по подтверждению и/или приему блоков и Транзакций в порядке, предусмотренном Правилами.

1. ТРЕБОВАНИЯ К АППАРАТНО-ПРОГРАММНОМУ КОМПЛЕКСУ ВАЛИДАТОРА

1.1. Требования к аппаратно-программному обеспечению Ноды, за исключением Ноды, выполняющей функции Лернера:

- Процессор: от 4 ядер / 2 ГГц;
- Объем оперативной памяти: от 20 Гбайт;
- Объем жесткого диска: от 500 Гбайт;
- Операционная система - CentOS 7.4, CentOS 8(x86, x64); Red Hat Enterprise Linux 7.4, Red Hat Enterprise Linux 8 (x86, x64); Astra Linux Special Edition 1.7 (x86, x64), AltLinux Server 10 (x86, x64);
- Средства криптографической защиты - СКЗИ КриптоПро CSP 5.0 (сборка 12000 - 6); СКЗИ КриптоПро CSP 5.0 (сборка 12000-6).

1.2. Требования к аппаратно-программному обеспечению Ноды, выполняющей функции Лернера:

- Процессор: от 4 ядер / 2 ГГц;

- Объем оперативной памяти: от 8 Гбайт;
- Объем жесткого диска: от 150 Гбайт;
- Операционная система - CentOS 7.4, CentOS 8(x86, x64); Red Hat Enterprise Linux 7.4, Red Hat Enterprise Linux 8 (x86, x64); Astra Linux Special Edition 1.7 (x86, x64), AltLinux Server 10 (x86, x64);
- Средства криптографической защиты - СКЗИ КриптоПро CSP 5.0 (сборка 12000 - 6); СКЗИ КриптоПро CSP 5.0 (сборка 12000-6).

1.3. Требования к сетевому взаимодействию:

- К Ноде должен быть привязан статический ipv4 адрес, который необходимо сообщить НРД;
- Необходимо открыть порты 30000 и 21000 для взаимодействия с другими узлами блокчейн-сети по статическим ipv4 адресам, которые сообщит НРД при развертывании Ноды;
- Необходимо открыть порты 80 и 433 до удостоверяющих центров КриптоПро по адреса, которые сообщит НРД при развертывании Ноды.

2. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Валидатор обязан:

2.1.1. Обеспечивать бесперебойность и непрерывность функционирования информационной системы в своей части.

2.1.2. Использовать комплекс мер и средств защиты информации, обеспечивающих необходимый уровень безопасности программных систем и продуктов, информационной инфраструктуры.

2.1.3. Осуществлять мониторинг состояния информационной безопасности, отслеживать и своевременно реагировать на события, влияющие на информационную безопасность.

2.1.4. Использовать только актуальные версии средств защиты информации, способные противодействовать в том числе новым видам угроз.

2.1.5. Обеспечивать защиту от проникновения: предотвращение вмешательства из общедоступных сетей передачи данных, в том числе из сети Интернет.

2.1.6. Проводить анализ и ограничение (при необходимости) входящего и исходящего потока данных на соответствие требованиям правил безопасности.

2.1.7. Использовать на Нодах только лицензионное программное обеспечение.

2.1.8. Использовать средства защиты от вредоносного программного кода.

2.1.9. Применять журналирование событий: осуществлять непрерывную запись всех событий системе для анализа в режиме реального времени и при расследовании инцидентов и сбоев.

2.1.10. Применять ограничение доступа: пользователи, являющиеся работниками Валидатора, получают персонализированный доступ с использованием аутентификационных данных. При работе используется ролевая модель, в которой каждый пользователь имеет отдельный набор прав и ограничений для выполнения различных функций в зависимости от текущей роли.

2.1.11. Выделить отдельный контакт службы (подразделения), ответственного за выявление и устранение инцидентов.

3. ТРЕБОВАНИЯ К ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

3.1. Валидатор обязан:

3.1.1. Обеспечить работоспособность аппаратного обеспечения в части вычислительных мощностей и сетевых взаимодействий и предоставление удаленного взаимодействия с информационной системой на уровне 99,3% общего времени работы аппаратного обеспечения.

3.1.2. Резервировать средства взаимодействия с другими узлами блокчейн-сети включая каналы связи, аппаратное и программное обеспечение.

3.1.3. Проводить регулярное тестирования средств, обеспечивающих резервирование, не реже одного раза в год.

3.1.4. Определить внутренним документом порядок действия работников Валидатора при реагировании и устранении нештатных ситуаций.

3.1.5. Обеспечить мониторинг работоспособности аппаратного обеспечения по следующим параметрам:

- доступность инфраструктуры (в частном случае, виртуальной машины);
- потребление вычислительных ресурсов.

3.1.6. Обеспечить валидность сертификатов, предназначенных для функционирования НОДы.

3.1.7. Уведомлять НРД о недоступности и сбоях в работе НОДы в течении 15 минут по контактам, указанным в договоре на осуществление функций Валидатора.

4. ВАЛИДАТОРУ ЗАПРЕЩЕНО

4.1. Вмешиваться в работу НОДы и настраивать режим её функционирования.

4.2. Проводить анализ программного обеспечения, поставляемого НРД и осуществлять реверсинжениринг кода программного обеспечения.