Система хранения данных SNR

Руководство администратора

SNR
Smart Networking Reliable

Оглавление

Обозначения и сокращения

В данном документе применяют следующие обозначения и сокращения:

BIOS	Basic Input/Output System
BMC	Baseboard Management Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ECC	Error-correcting code
FC HBA	Fibre channel host bus adapter
HDD	Hard Disk Drive
HTML	HyperText Markup Language
HTTPS	HyperText Transfer Protocol Secure
iSCSI	Internet Small Computer System Interface
LACP	Link Aggregation Control Protocol
NFS	Network File System

NTP	Network Time Protocol
NVMe	Non-Volatile Memory Express
PCIe	Peripheral Component Interconnect Express
SAN	Storage Area Network
SFF	Small Form Factor
SMB	Server Message Block
SSD	Solid-State Drive
SSL	Secure Sockets Layer
UEFI	Unified Extensible Firmware Interface
VLAN	Virtual Local Area Network
ZFS	Zettabyte File System
ГИС	геоинформационные системы
ИБП	источники бесперебойного питания
ИСПДн	информационная система персональных данных
ИТ	информационные технологии

ЛКМ	левая кнопка мыши
ОС	операционная система
ПО	программное обеспечение
СХД	система хранения данных
ТЗ	техническое задание
ЦОД	центр обработки данных

Термины и определения

В данном документе применяют следующие термины с соответствующими определениями:

Зеркалирование	дублирование дисков
Логи	записи событий и сообщений, создаваемые системой во время её работы
Пул	основная структура хранения данных, объединяющая физические устройства в единое виртуальное хранилище
Репликация	процесс копирования данных между файловыми системами, обычно расположенными на разных хранилищах. Позволяет создавать резервные копии, обеспечивать отказоустойчивость и синхронизацию данных

Настоящее руководство администратора содержит полное описание системы хранения данных (СХД) SpaceSAN, включая аппаратную часть, архитектуру, функции и процедуры администрирования, в том числе описание процедур настройки и управления СХД SpaceSAN версии 4.0.

Документ предназначен для системных администраторов и ИТ-специалистов, отвечающих за развертывание, настройку и эксплуатацию системы хранения данных SpaceSAN. Документ является обязательным для администраторов системы управления СХД SpaceSAN и содержит всю информацию, необходимую для эксплуатации серверного компонента решения.

Данный документ отражает основные функциональные возможности и порядок действий при выполнении операций, связанных с администрированием СХД.

Руководство администратора является основным документом по работе с СХД и должно использоваться вместе с другой технической документацией производителя.

1 Применение и структура

1.1 Область применения

Система хранения данных SpaceSAN является платформой для создания высокопроизводительных и отказоустойчивых систем хранения на базе файловой системы OpenZFS. Решение обеспечивает надёжное хранение данных за счёт использования пулов устройств, автоматического контроля целостности и гибких механизмов масштабирования.

В руководстве рассматриваются все аспекты работы с системой: от первоначальной настройки до повседневного администрирования, включая управление томами, мониторинг производительности и действия в аварийных ситуациях. Документ также содержит информацию об интеграции с внешними системами и особенностях работы с OpenZFS.

Система хранения данных SpaceSAN предназначена для использования в корпоративных ЦОД, виртуализированных средах и системах, требующих надежного хранения любых объемов данных.

1.2 Структура

Система хранения данных предназначена для организации системы хранения данных и предоставляет следующие возможности:

1) Установку 12 или 24 дисков формата SATA/SAS HS 3.5»/2.5». Высота базового блока не более 2 (Двух) юнитов;

2) поддержку процессоров поколения Intel Xeon Gen3 или более;

3) поддержку оперативной памяти формата DDR4,5 с функцией ECC;

4) поддержку встроенных сетевых карт от 10 Гбит/с;

5) поддержку дисковых контроллеров HBA LSI 9400, 9500, 9600;

6) поддержку адаптеров FC HBA QLogic 16/32 Гбит/с;

7)поддержку блоков питания с функцией отказоустойчивости мощностью не менее 1200 Вт для подключения к сети электроснабжения (220 В,
50 Гц);

8)установку дискового массива в монтажный шкаф;

9)графического интерфейса управления системой хранения данных по протоколу HTTPS;

10) интерфейс управления предоставляет возможность индикации расположения физического накопителя в корзине сервера;

11) интерфейс управления предоставляет информацию о контроллере дисков;

12) поддержку технологий создания логических групп из дисковых накопителей с возможностью отказа до 3 физических носителей без потери информации;

13) поддержку технологий создания распределенной логической группы из дисковых накопителей с возможностью отказа до 3 физических носителей без потери информации с добавлением логических устройств горячего резерва;

14) создание и управление параметрами единого логического хранилища с использованием комбинации логических групп;

15) расширение объема хранилища за счет добавления новых логических групп;

16) расширение логических групп за счет добавления новых физических носителей;

17) создание файловых ресурсов (далее datasets) в едином логическом хранилище для предоставления доступа по протоколу NFS 4.1;

18) создание блочных ресурсов (далее VVOL) в едином логическом хранилище для предоставления по протоколам iSCSI и Fiber Channel;

19) создание и управление моментальными снимками (далее snapshots) для datasets и vvol;

20) шифрование данных алгоритмами AES-256-gcm,
AES-128-gcm, AES-192-gcm, AES-128-ccm, AES-192-ccm, AES-256-ccm с гибкой

системой управления криптографическими ключами;

21) репликация данных на другие системы хранения с использованием шифрованного и нешифрованного канала.

1.3 Описание возможностей

Система хранения данных SpaceSAN представляет собой комплексное решение для организации надежного и производительного хранилища информации любого уровня. Основой продукта является современная файловая система OpenZFS, обеспечивающая широкий набор функциональных возможностей для эффективного управления данными.

Ключевой особенностью системы является гибкое управление структурой хранения. Администраторы могут создавать, модифицировать и удалять пулы хранения (storage pools), которые представляют собой объединенные группы физических носителей. В рамках пулов поддерживается работа с виртуальными томами (volumes) и наборами данных (datasets), позволяющими организовать логическое разделение хранимой информации с возможностью установки индивидуальных параметров для каждого элемента, включая квоты дискового пространства и резервирование ресурсов.

Система предлагает комплексные механизмы защиты и восстановления данных. Администраторы могут настраивать политики репликации как в ручном, так и в автоматическом режимах, обеспечивая надежное дублирование критически важной информации. Функционал снимков (snapshots) позволяет создавать мгновенные снимки состояния данных в определенный момент времени с возможностью последующего восстановления. Особое внимание уделено вопросам безопасности – система поддерживает создание зашифрованных данных с гибкой системой управления криптографическими ключами.

Для мониторинга состояния оборудования реализован специализированный инструментарий, предоставляющий детальную информацию о физических носителях, включая данные SMART,

показатели износа и статистику ошибок. Администраторы могут отслеживать состояние RAID-массивов и контроллеров, что позволяет оперативно выявлять потенциальные проблемы.

Система хранения данных SpaceSAN поддерживает все основные сетевые протоколы доступа к данным, обеспечивая совместимость с различными ИТ-инфраструктурами. Система предлагает:

iSCSI для организации блочного доступа по IP-сетям;

NFS для сетевого доступа к файловым ресурсам;

Fibre Channel (FC) для высокоскоростных SAN-решений.

Архитектура системы обеспечивает высокую масштабируемость и отказоустойчивость. Поддерживаются различные уровни RAID (включая ZFS RAIDZ, DRAID и зеркалирование), автоматические механизмы восстановления после сбоев и гибкое распределение ресурсов. Управление системой осуществляется через интуитивно понятный веб-интерфейс, что делает решение удобным для администраторов с разным уровнем подготовки.

Благодаря сочетанию перечисленных возможностей система хранения данных SpaceSAN представляет собой универсальную платформу для построения систем хранения данных различного масштаба – от небольших корпоративных хранилищ до крупных дата-центров, обеспечивая при этом высокий уровень надежности, производительности и удобства администрирования.

1.4 Уровень подготовки пользователей

Графический интерфейс пользователя Системы является интуитивно понятным.

Для эффективной работы с системой хранения данных SpaceSAN 4.0 пользователям требуется определенный уровень технической подготовки.

Базовые требования к администраторам:

знание принципов организации СХД;

понимание работы сетевых протоколов (iSCSI, NFS, Fibre Channel);

знакомство с концепциями RAID-массивов и отказоустойчивости.

Для выполнения специализированных задач потребуется:

при работе с шифрованием – понимание криптографических методов;

при настройке репликации – знание топологии сети и принципов синхронизации данных;

для диагностики проблем - навыки анализа журналов системы.

Для новых пользователей рекомендуется предварительное изучение сопроводительной документации.

Для выполнения критически важных операций (например, изменение структуры пулов хранения или настройка репликации) особенно важно наличие соответствующего опыта у администратора.

1.5 Перечень эксплуатационной документации

Администраторам Системы необходимо ознакомиться с настоящим Руководством.

2 Назначение программы

2.1 Сведения о назначении программы

Система хранения данных SpaceSAN предназначена для организации высоконадежного, производительного и масштабируемого хранилища информации в корпоративных средах, дата-центрах и виртуализированных инфраструктурах.

Система обеспечивает автоматизацию следующих функций и процессов:

обеспечение отказоустойчивого хранения данных за счет использования системы OpenZFS с поддержкой механизмов контроля целостности, самовосстановления и защиты от повреждения информации;

предоставление гибких инструментов управления ресурсами хранения, включая создание и настройку пулов устройств, виртуальных томов и наборов данных с индивидуальными параметрами (квоты, резервирование, шифрование);

автоматизация процессов резервного копирования и восстановления данных с помощью снимков (snapshots) и репликации, включая поддержку как локальных, так и распределенных конфигураций;

обеспечение совместимости с различными ИТ-инфраструктурами благодаря поддержке ключевых сетевых протоколов доступа: iSCSI, NFS и Fibre Channel (FC);

мониторинг состояния оборудования и диагностика потенциальных проблем через встроенные инструменты анализа SMART-данных, статистики ошибок и износа носителей;

повышение эффективности администрирования за счет интуитивного веб-интерфейса, сокращающего время на развертывание и обслуживание системы.

Система хранения данных SpaceSAN ориентирована на решение задач, требующих гарантированной сохранности данных, высокой доступности и простоты управления, что делает его оптимальным выбором для организаций любого масштаба – от небольших

предприятий до крупных
дата-центров.

2.2 Информация, достаточная для понимания функций программы и ее эксплуатации

Настоящее руководство содержит исчерпывающие сведения, необходимые для эффективного использования системы хранения данных SpaceSAN в различных сценариях развертывания и эксплуатации.

Ключевые аспекты, раскрываемые в документе:

архитектура системы – описание компонентов, их взаимодействия и принципов работы на базе OpenZFS;

функциональные возможности – управление пулами хранения, виртуальными томами, наборами данных, снимками, репликацией, шифрованием и сетевыми протоколами доступа (iSCSI, NFS, Fibre Channel);

процедуры администрирования – настройка, мониторинг, диагностика и устранение неисправностей;

безопасность и отказоустойчивость – механизмы защиты данных, контроль целостности, резервное копирование и восстановление;

интеграция с внешними системами – совместимость с виртуализацией, облачными платформами и корпоративными ИТ-инфраструктурами.

Для полного понимания работы системы рекомендуется:

ознакомиться с основными концепциями (ZFS, RAID-массивы, сетевые протоколы);

изучить интерфейс управления;

следовать рекомендациям по настройке в зависимости от задач;

использовать дополнительные материалы (официальную документацию, технические заметки, руководства по устранению неполадок).

Данного руководства достаточно для выполнения большинства

задач администрирования, однако в сложных сценариях может потребоваться консультация с технической поддержкой или углубленное изучение специализированной литературы.

3 Условия выполнения программы

3.1 Условия, необходимые для выполнения программы

Для корректной работы системы хранения SpaceSAN требуется выполнение следующих условий:

аппаратные требования:

серверное оборудование с поддержкой 64-разрядных процессоров (x86-64);

оперативная память (RAM): минимум: 64 Гбайт (для базовых конфигураций), рекомендуется: 128 Гбайт и более (для работы с большими пулами хранения);

дисковые накопители: поддержка формата HDD и SSD. Рекомендуется использование дисков с одинаковыми характеристиками (емкость, скорость) в рамках одного пула. Минимальный объем: зависит от задач, но не менее 2 дисков для зеркалирования или 3 и более дисков для RAID-Z;

сетевые интерфейсы:

от 1 Гбит/для iSCSI, NFS;

от 4 Гбит/с для Fibre Channel.

сетевые требования:

стабильное сетевое подключение (для работы с iSCSI, репликацией, кластерными конфигурациями);

б) настроенные DNS и NTP (для корректной работы аутентификации и синхронизации времени).

требования к безопасности:

доступ к системе только для авторизованных администраторов;

б) шифрование дисков (если требуется защита данных);

рекомендуемые условия для отказоустойчивости:

резервные источники питания (ИБП);

избыточные сетевые подключения (LACP, multipathing);

4 Описание функциональности

4.1 Установка SpaceOS

Условия, при которых возможно выполнение: наличие установочного образа операционной системы и доступ к серверу (виртуальной или физической машине), на который выполняется установка.

Процесс установки операционной системы начинается с отображения окна приветствия установщика, подтверждающего запуск процедуры установки (см. рисунок 1).

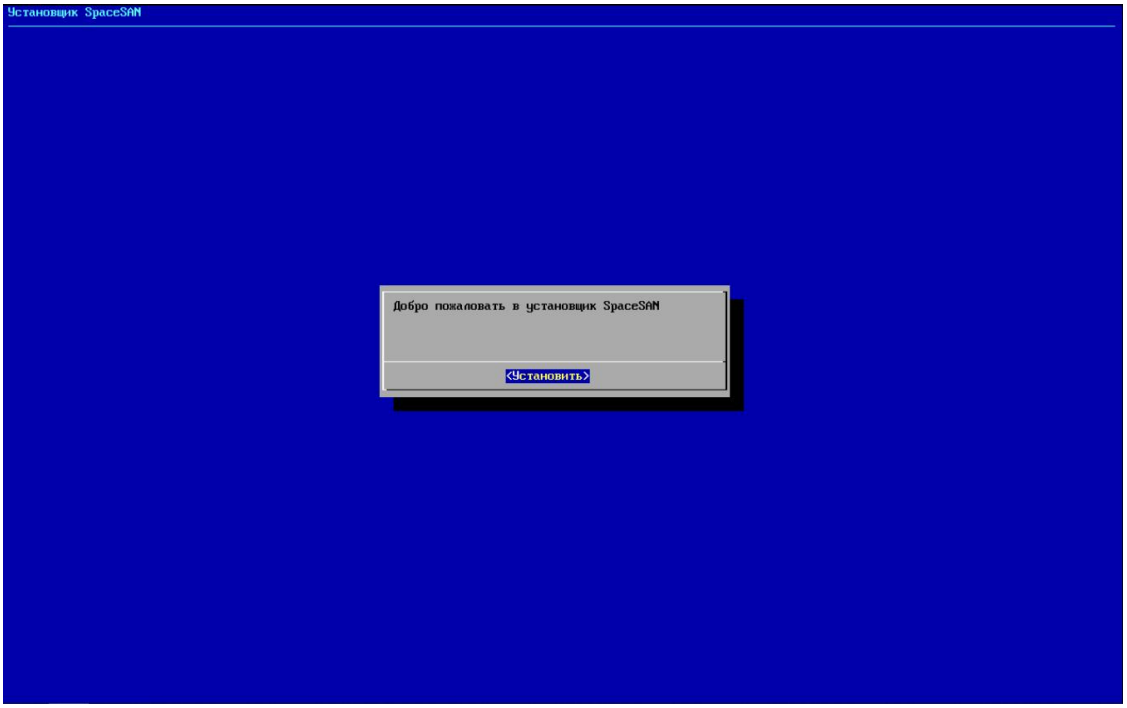

Рисунок 1 – Окно, подтверждающее запуск процедуры установки

Далее отображается окно с системной информацией, включающей сведения о процессоре, объёме оперативной памяти, наименовании сервера, модели материнской платы и версии BIOS, что позволяет администратору проверить корректность распознавания аппаратной платформы (см. рисунок 2).

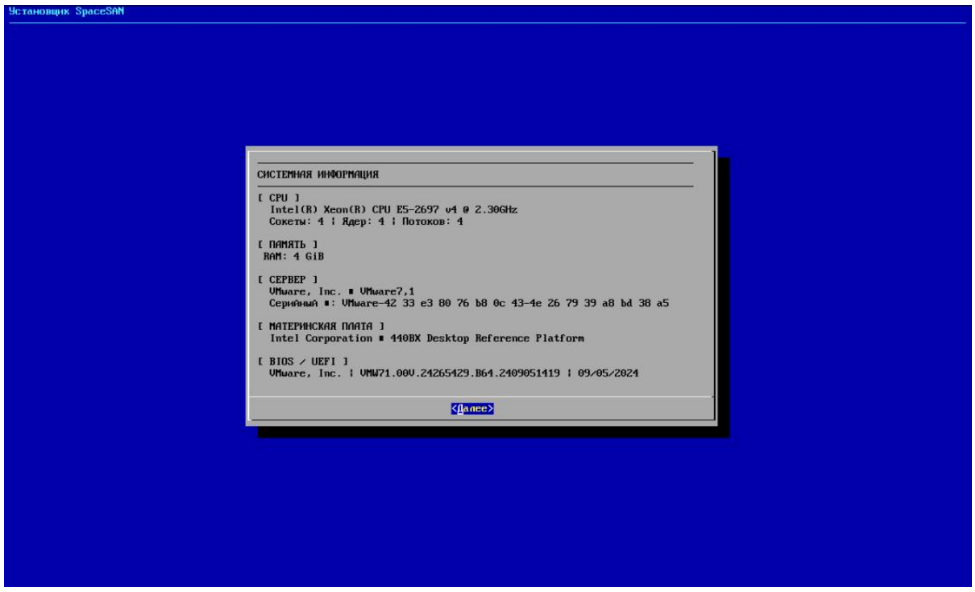

Рисунок 2 – Окно с информацией о системе

В следующем окне пользователю предоставляется возможность выбора варианта установки операционной системы: на одиночный физический диск либо на массив дисков, сформированный на базе RAID1 (см. рисунок 3).

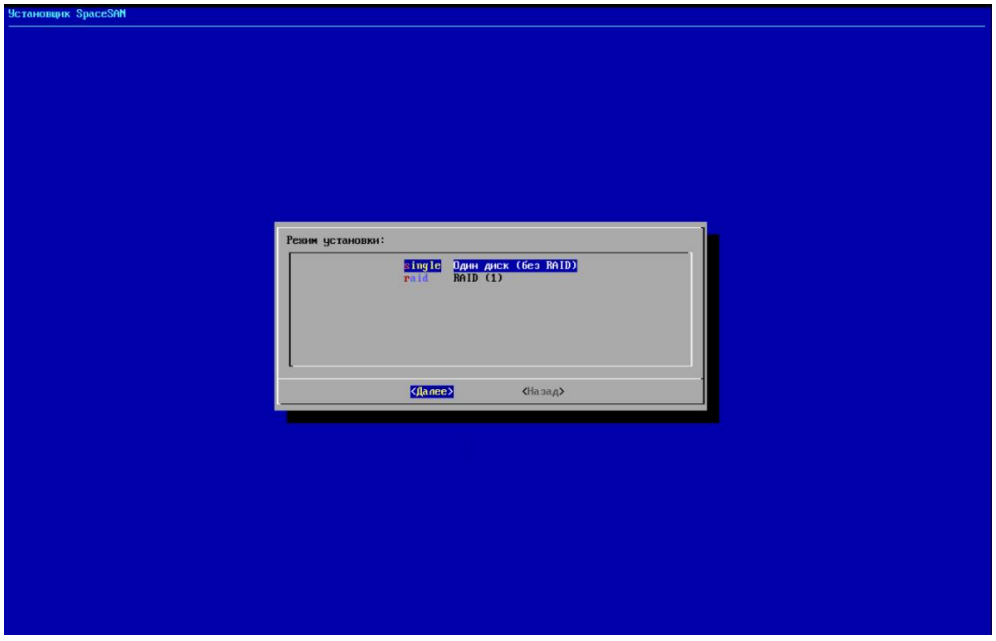

Рисунок 3 – Окно с выбором варианта установки

При выборе установки на одиночный физический диск отображается окно выбора способа разметки диска, в котором пользователю предлагается выполнить автоматическую разметку либо перейти к ручной настройке параметров разметки (см. рисунок 4). В случае выбора ручной разметки отображается окно выбора целевого физического диска для установки операционной системы.

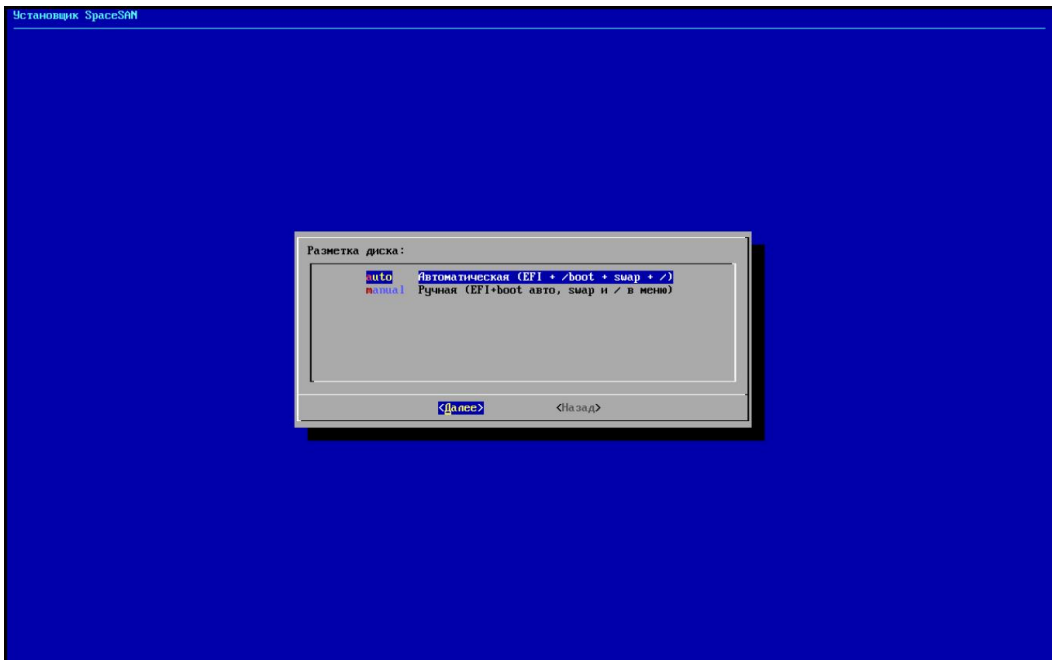

Рисунок 4 – Окно с выбором варианта установки

Далее отображается окно управления разделами диска, в котором предоставляется возможность создания, редактирования и удаления разделов, а также изменения их параметров, включая размер и тип файловой системы (см. рисунок 5).

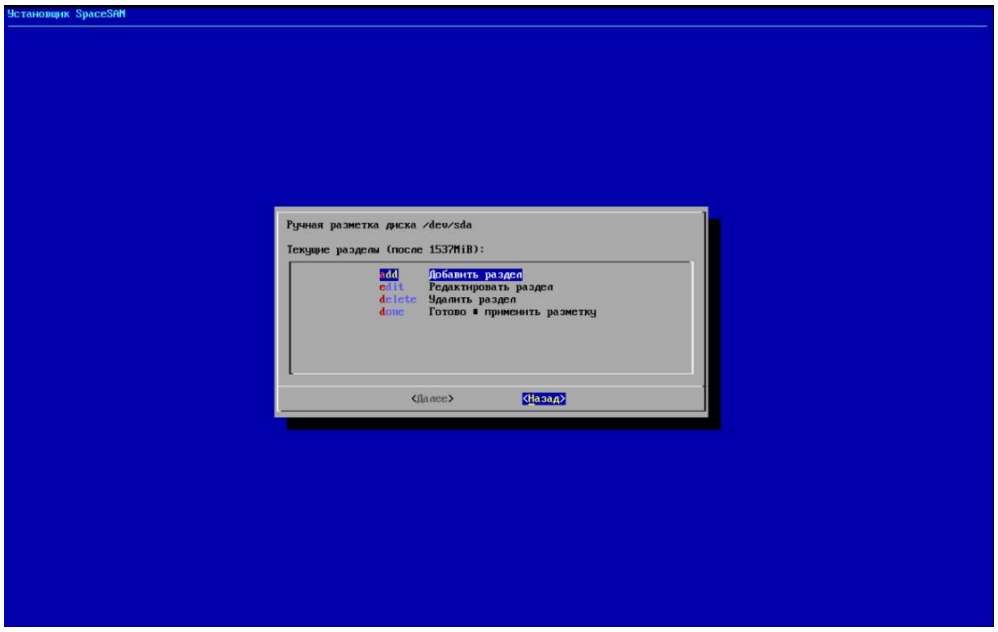

Рисунок 5 – Окно с выбором дисков

При выборе установки операционной системы на массив дисков, сформированный на базе RAID1, отображается окно выбора RAID-массива, предназначенного для размещения загрузочных дисков операционной системы (см. рисунок 6).

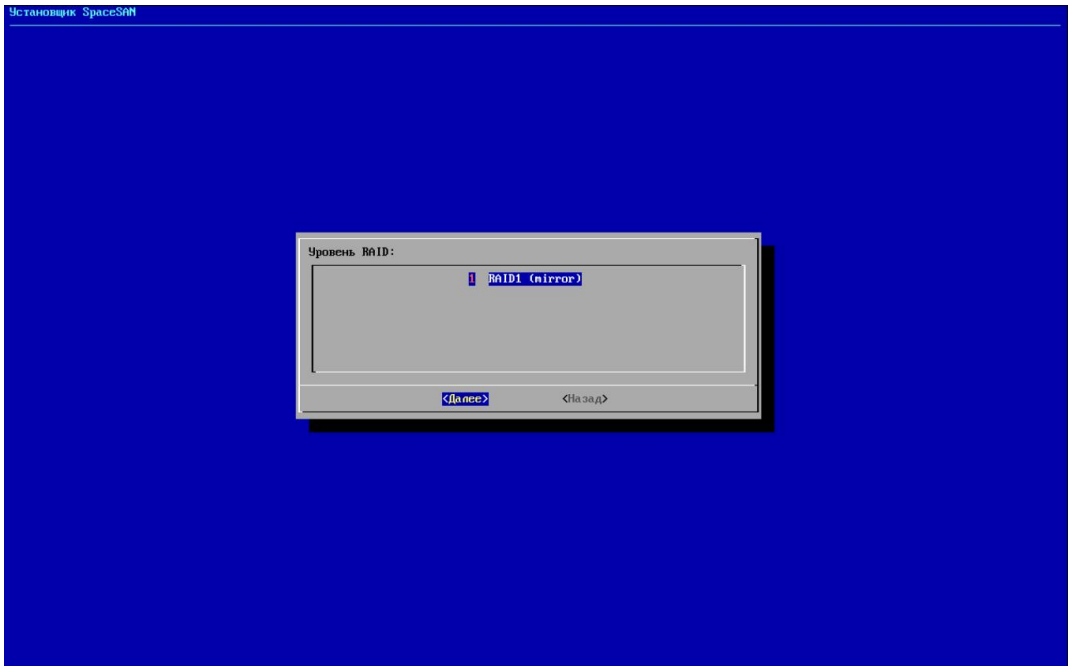

Рисунок 6 – Окно с выбором RAID-массива

После этого выполняется выбор физических дисков, входящих в RAID-массив. Для добавления диска в конфигурацию необходимо выбрать соответствующий диск и подтвердить выбор, после чего завершить формирование конфигурации (см. рисунок 7).

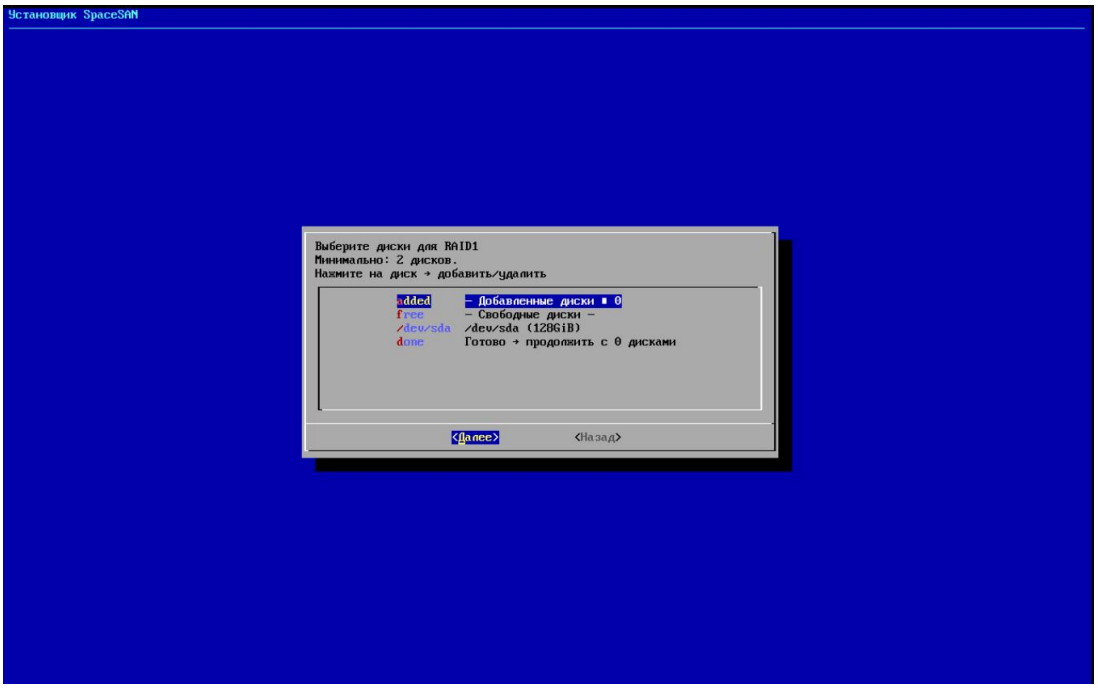

Рисунок 7 – Окно выбора физических дисков

Перед началом установки отображается предупреждение о том, что все данные на выбранных дисках будут удалены (см. рисунок 8).

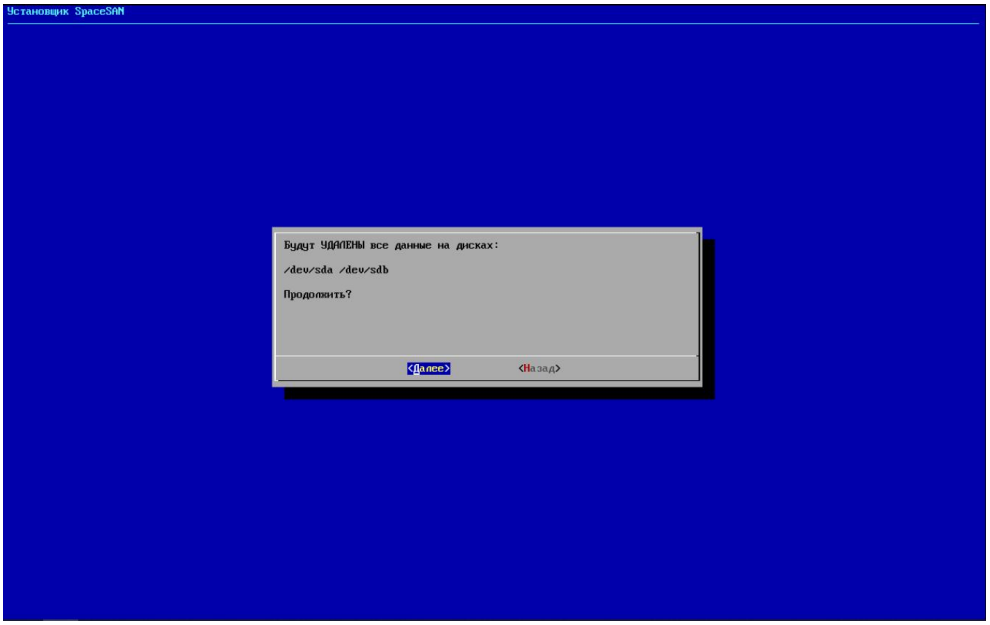

Рисунок 8 – Окно удаление данных с диска

Далее отображается окно конфигурации установки, в котором представлены выбранный режим дисковой подсистемы, используемые диски и описание выполняемых действий при запуске установки операционной системы (см. рисунок 9).

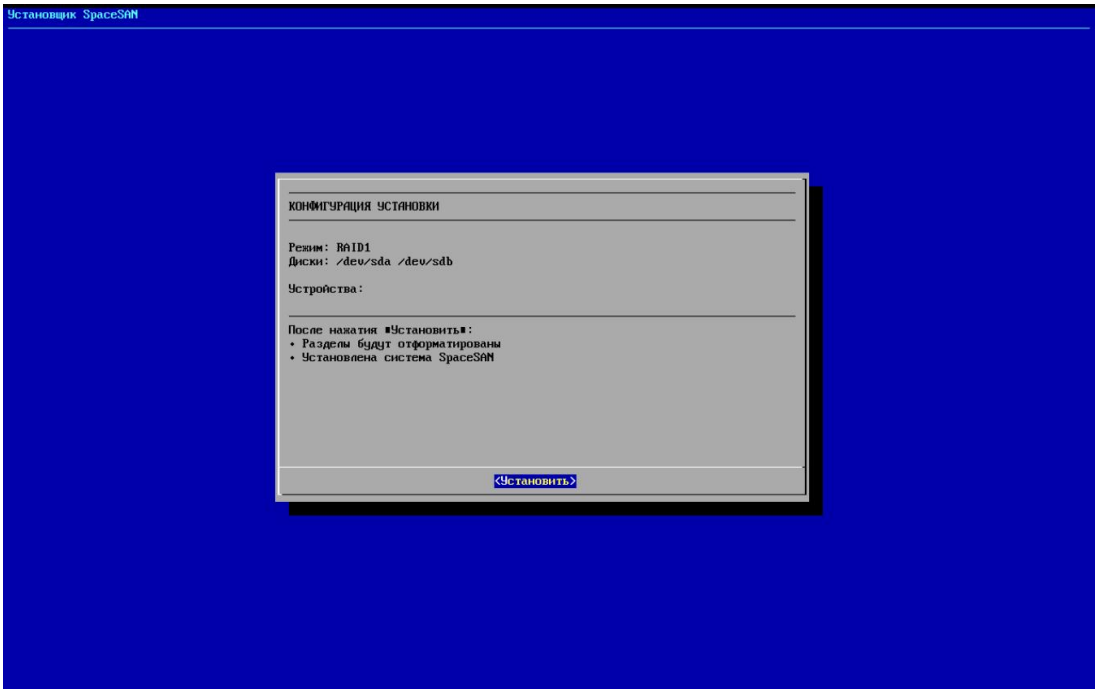

Рисунок 9 – Окно конфигурации установки

После подтверждения параметров выполняется установка операционной системы в автоматическом режиме (см. рисунок 10).

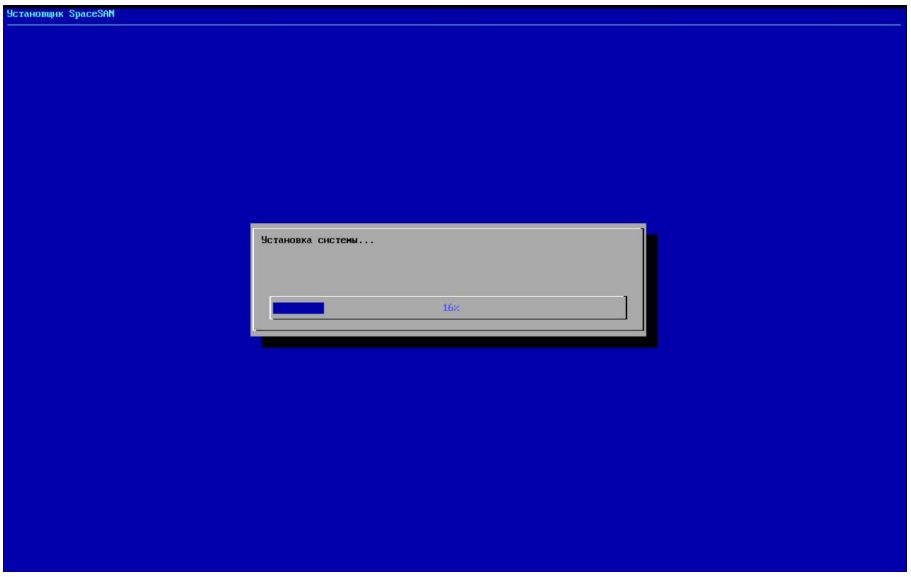

Рисунок 10 – Окно установки операционной системы

По завершении установки выполняется настройка сетевых интерфейсов. Пользователю предоставляется возможность пропустить ручную настройку, в результате чего параметры сети будут получены автоматически по протоколу DHCP, либо перейти к ручной настройке сетевого интерфейса (см. рисунок 11).

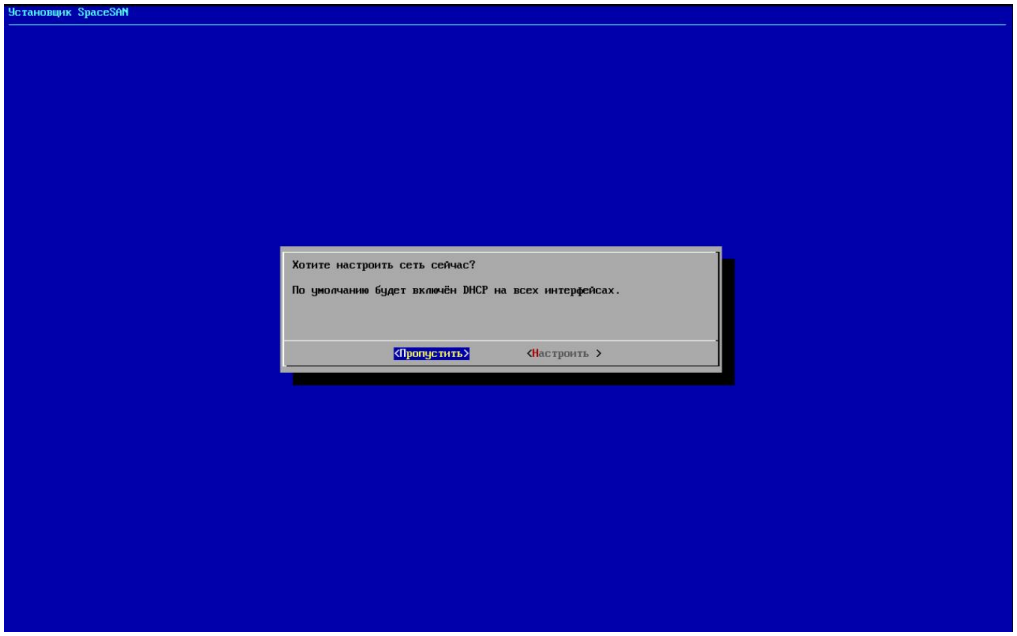

Рисунок 11 – Окно настройки сетевых интерфейсов

При выборе ручной настройки отображается список доступных сетевых интерфейсов, из которого необходимо выбрать интерфейс для дальнейшей конфигурации (см. рисунок 12).

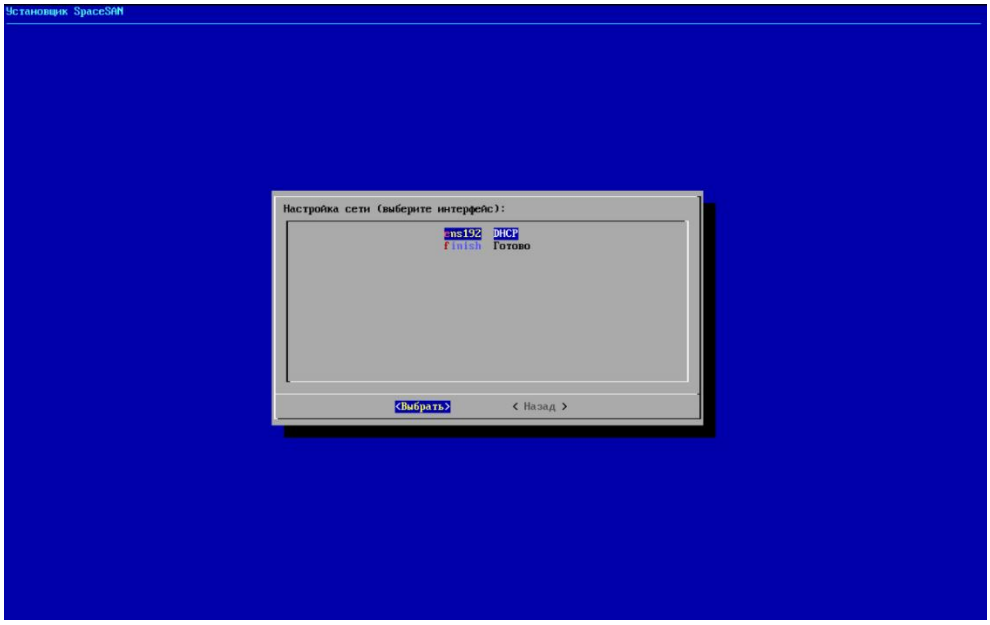

Рисунок 12 – Окно списка доступных сетевых интерфейсов

В окне настройки сетевого интерфейса осуществляется выбор режима конфигурации: автоматическое получение параметров по DHCP либо использование статических сетевых параметров (см. рисунок 13).

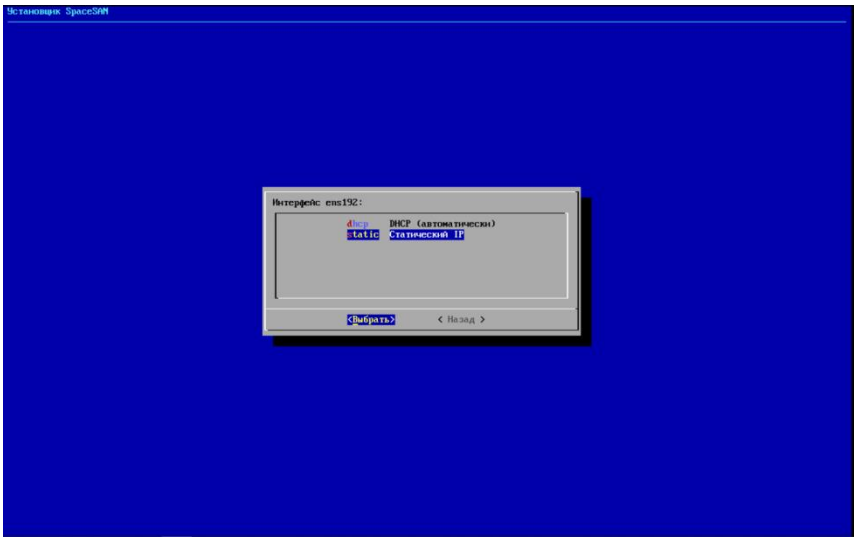

Рисунок 13 – Окно настройки сетевого интерфейса

При выборе статической конфигурации выполняется указание IP-адреса и маски сети, а также последующая настройка шлюза и DNS-серверов (см. рисунок 14).

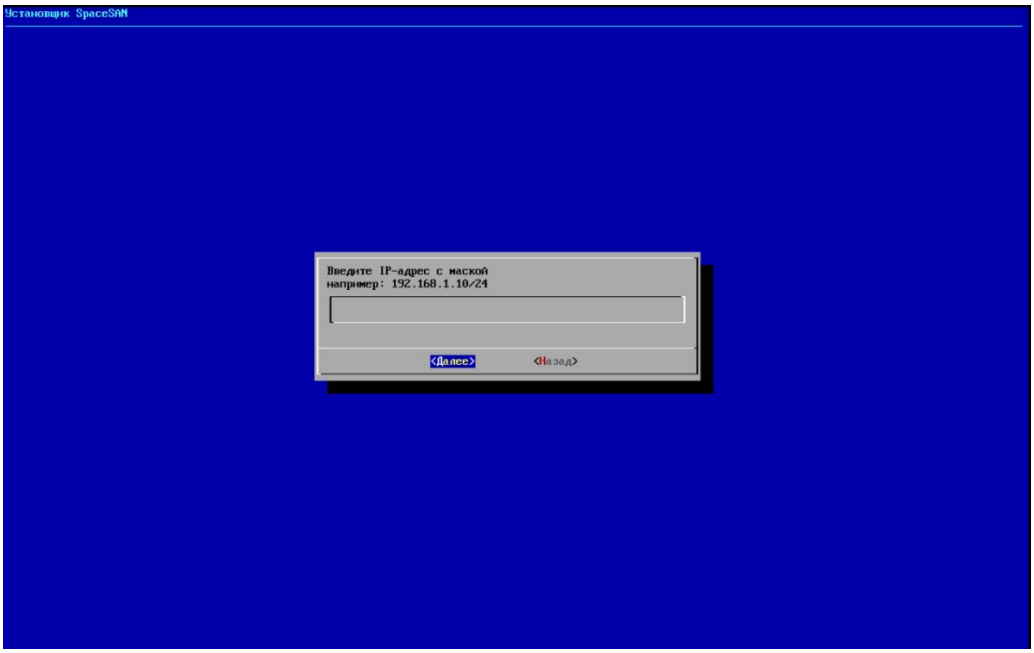

Рисунок 14 – Окно настройки статической конфигурации

После завершения настройки сетевых параметров выполняется настройка параметров локализации, включая выбор временной зоны и региона (см. рисунок 15 и 16).

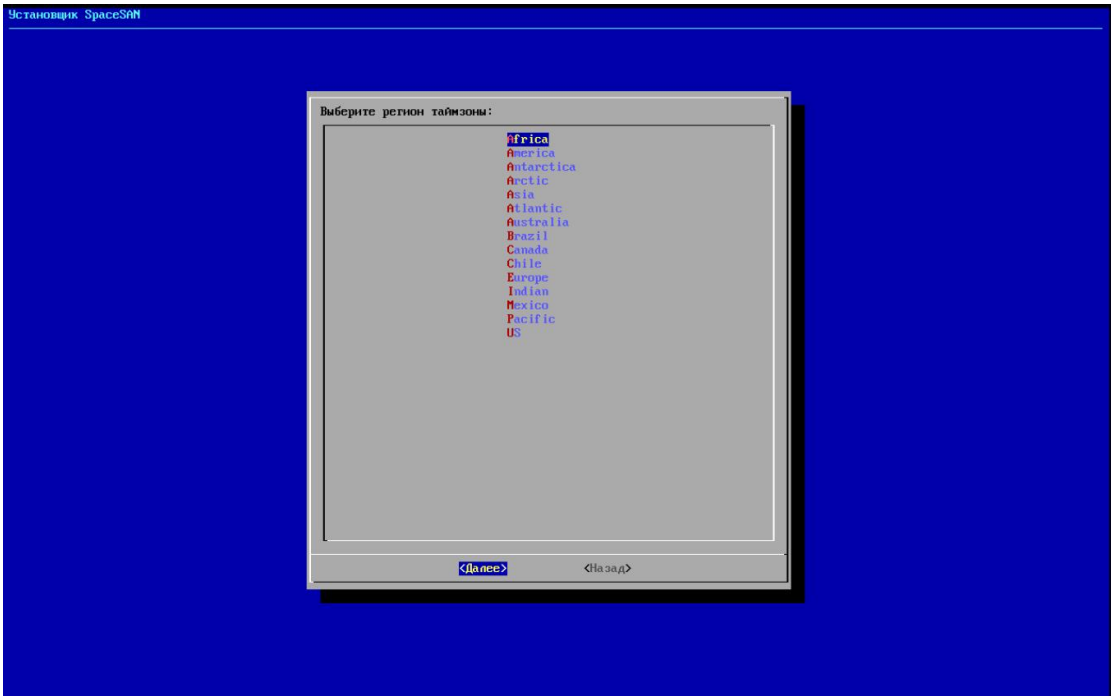

Рисунок 15 – Окно выбора временной зоны

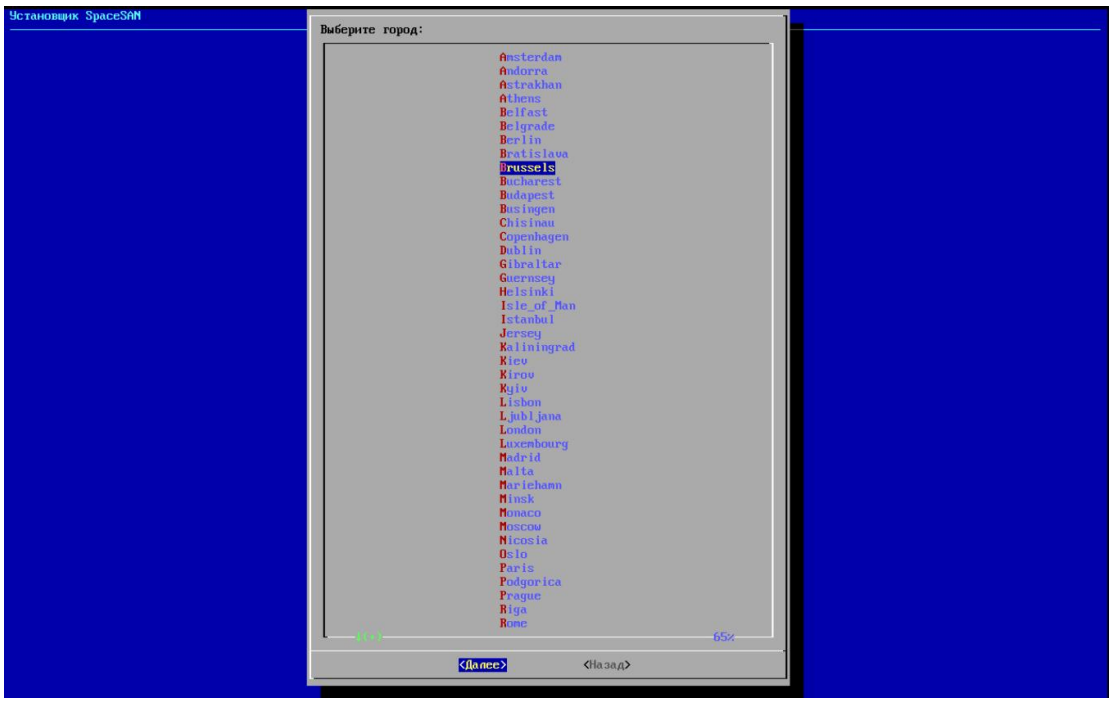

Рисунок 16 – Окно выбора региона

Далее задаётся имя хоста системы (см. рисунок 17).

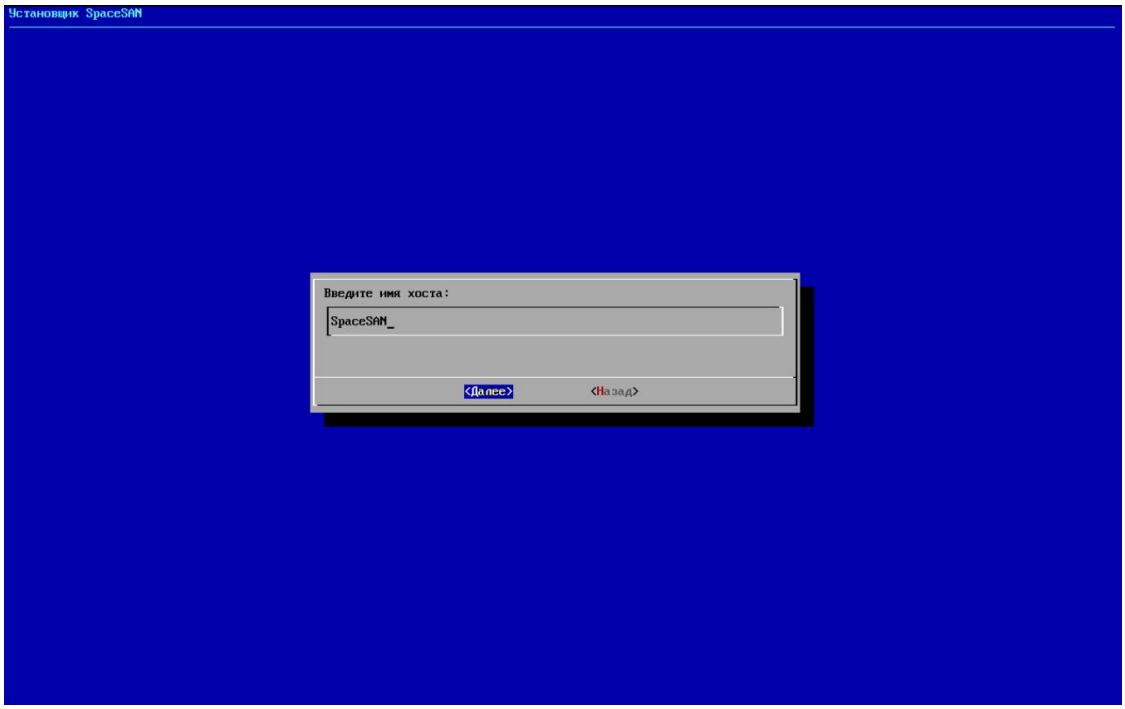

Рисунок 17 – Окно ввода имени хоста

На завершающем этапе установки выполняется установка пароля пользователя root с обязательным подтверждением введённого

значения (см. рисунок 18).

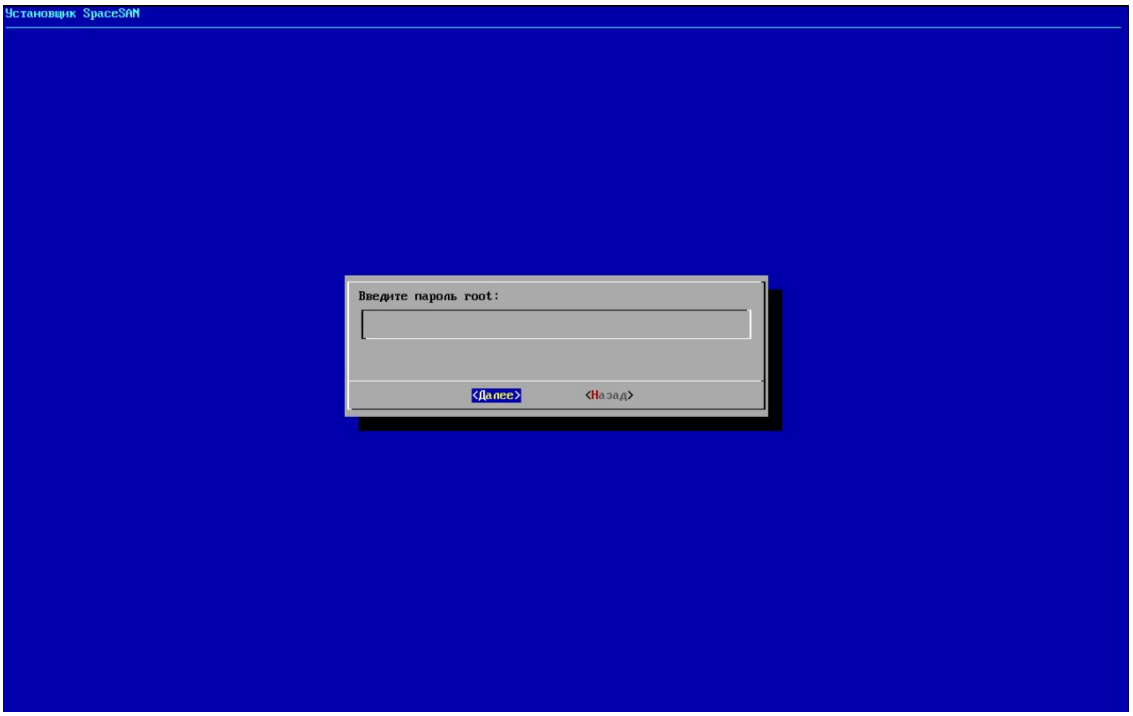

Рисунок 18 – Окно установки пароля пользователя root

После завершения всех настроек пользователю предоставляется возможность перезагрузить систему либо выполнить её выключение (см. рисунок 19).

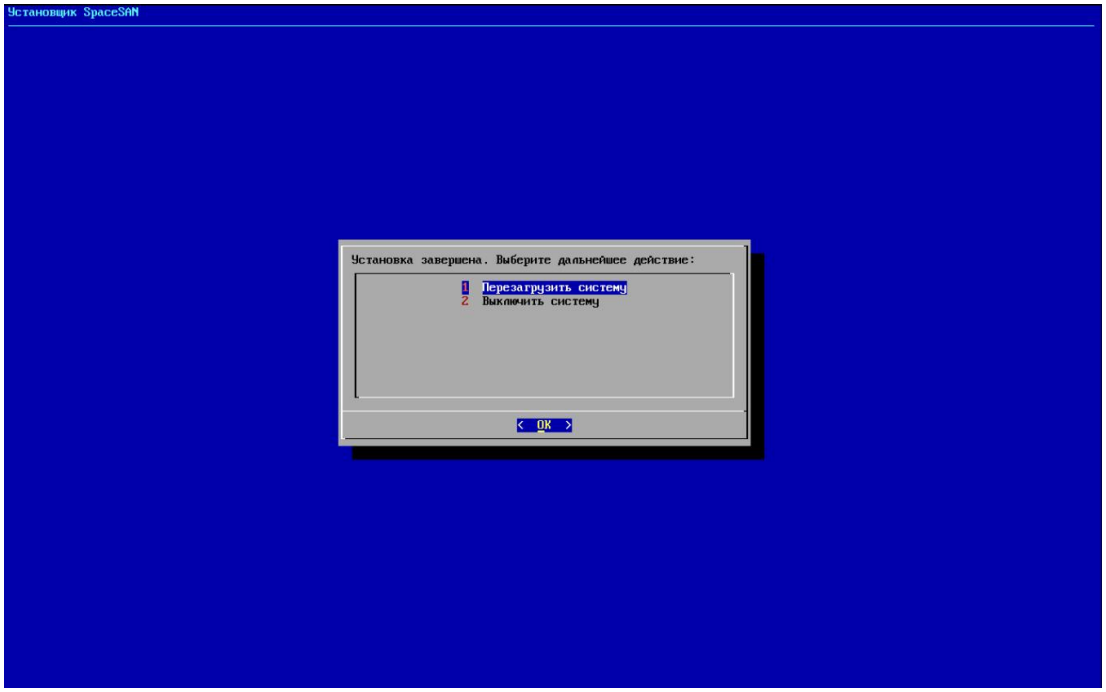

Рисунок 19 – Окно завершения установки

После перезагрузки системы отображается терминальный интерфейс, в котором выводится информация о установленной операционной системе, аппаратной платформе, сетевых интерфейсах, а также контактные сведения (см. рисунок 20).

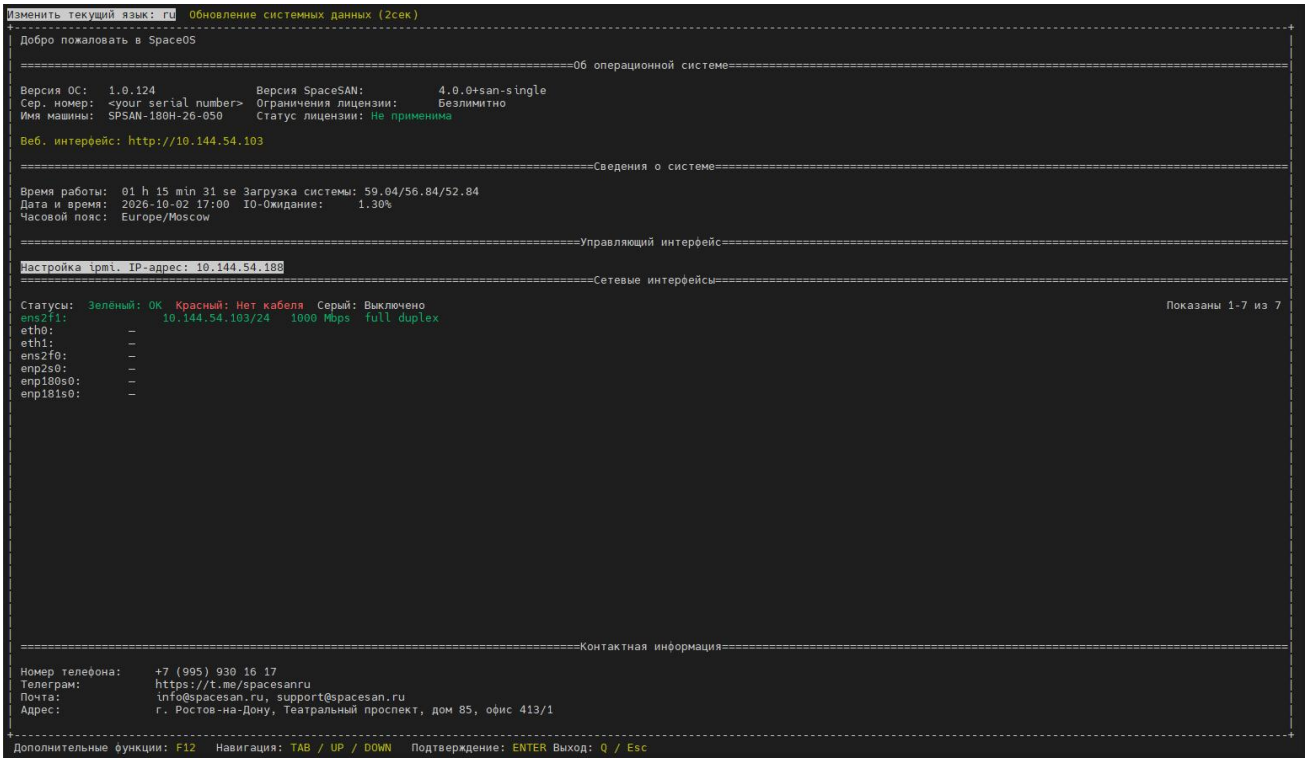

Рисунок 20 – Окно терминального интерфейса

4.2 Подключение и авторизация

Условия, при которых возможно выполнение: у СХД есть назначенный в системе IP-адрес и наличие любого браузера на устройстве, с которого будет осуществляться вход.

Вход в веб-интерфейс осуществляется через ввод IP-адреса СХД в адресную строку браузера, после чего открывается страница авторизации (см. рисунок 21).

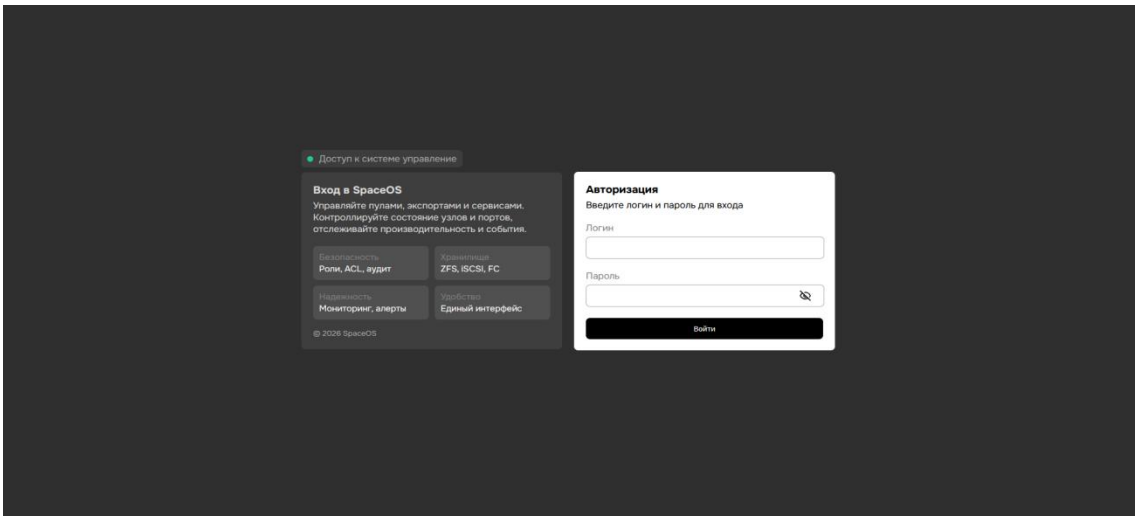

Рисунок 21 – Авторизация

Стандартные данные для подключения к веб-интерфейсу admin/demospace. При вводе корректных данных будет открыт веб-интерфейс управления СХД. При вводе некорректных учетных данных будет отображено соответствующее

уведомление об ошибке авторизации (см. рисунок 22).

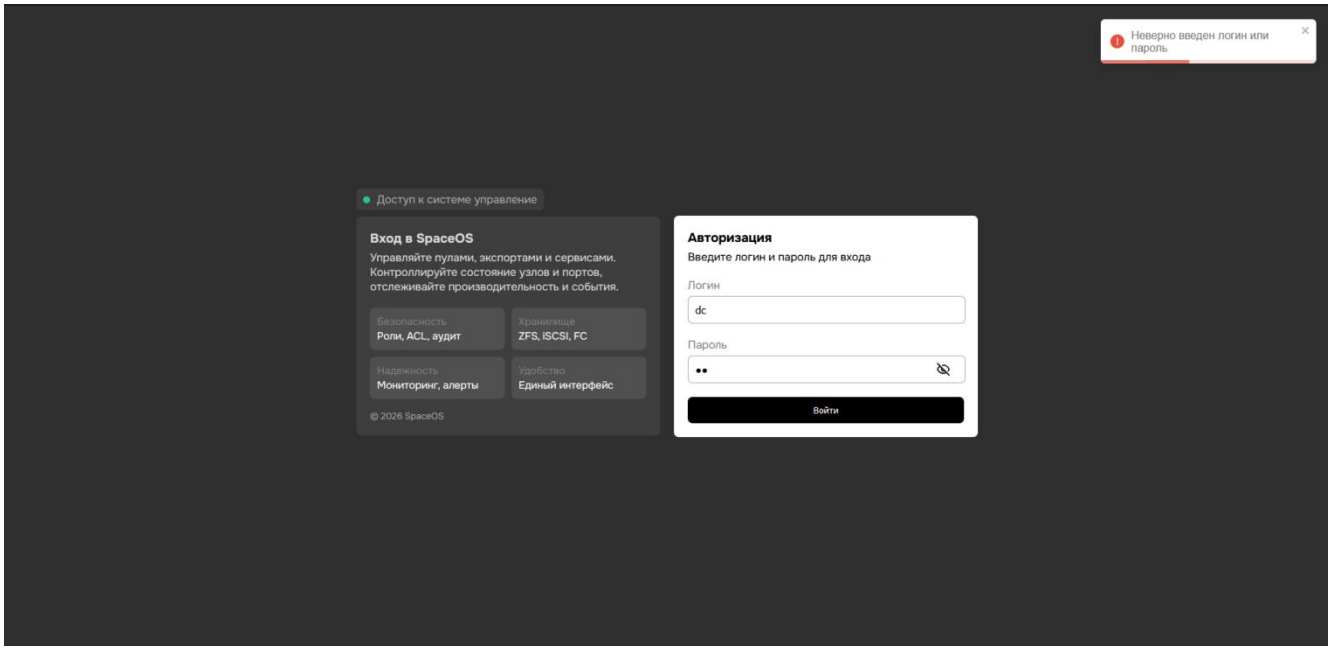

Рисунок 22 – Ввод некорректных данных в окне авторизации

4.3 Навигация по интерфейсу системы

Условия, при которых возможно выполнение: авторизация в Системе.

После авторизации появляется главный экран модуля управления

СХД – вкладка hardware (см. рисунок 23).

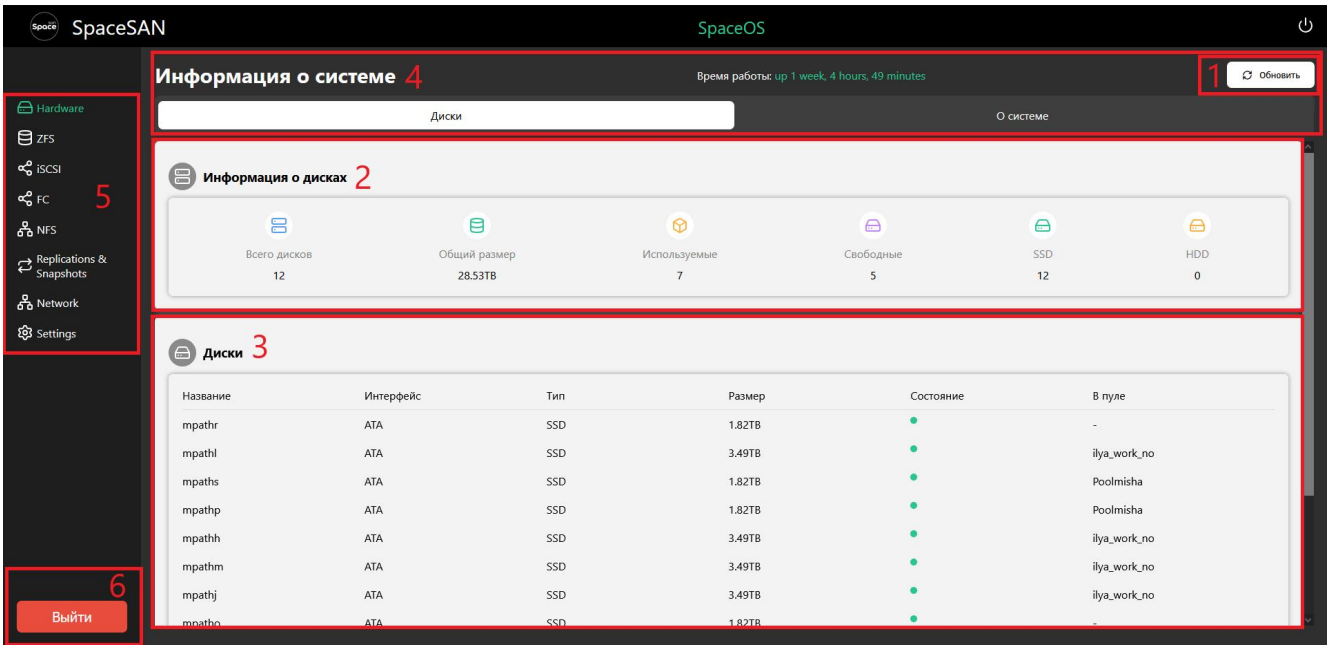

Рисунок 23 – Главный экран

В самом верху экрана находится управление питанием СХД (рисунок 23, область 1).

Под верхним блоком отображается сводная информация о дисках, установленных в корзине системы хранения данных, включая общее количество дисков, их суммарный объём, а также сведения о типе и состоянии накопителей (см. рисунок 23, область 2).

Ниже представлена таблица со списком установленных дисков (см. рисунок 23, область 3). При выборе отдельного диска отображается окно с подробной информацией о его состоянии, параметрах и принадлежности к пулу (см. рисунок 24). В данном разделе администратору доступны функции управления индикацией диска, предназначенной для визуальной идентификации накопителя на панели, сброса состояния индикации неисправности диска, а также очистки диска от устаревших метаданных.

Очистка метаданных используется для удаления метаданных файловой системы ZFS, содержащихся на диске, и применяется в случае, если диск ранее входил в состав пула ZFS и подготавливается к повторному использованию. В случае выхода диска из строя

активируется индикатор неисправности; после замены диска на новый требуется выполнить сброс состояния индикации в соответствующем слоте.

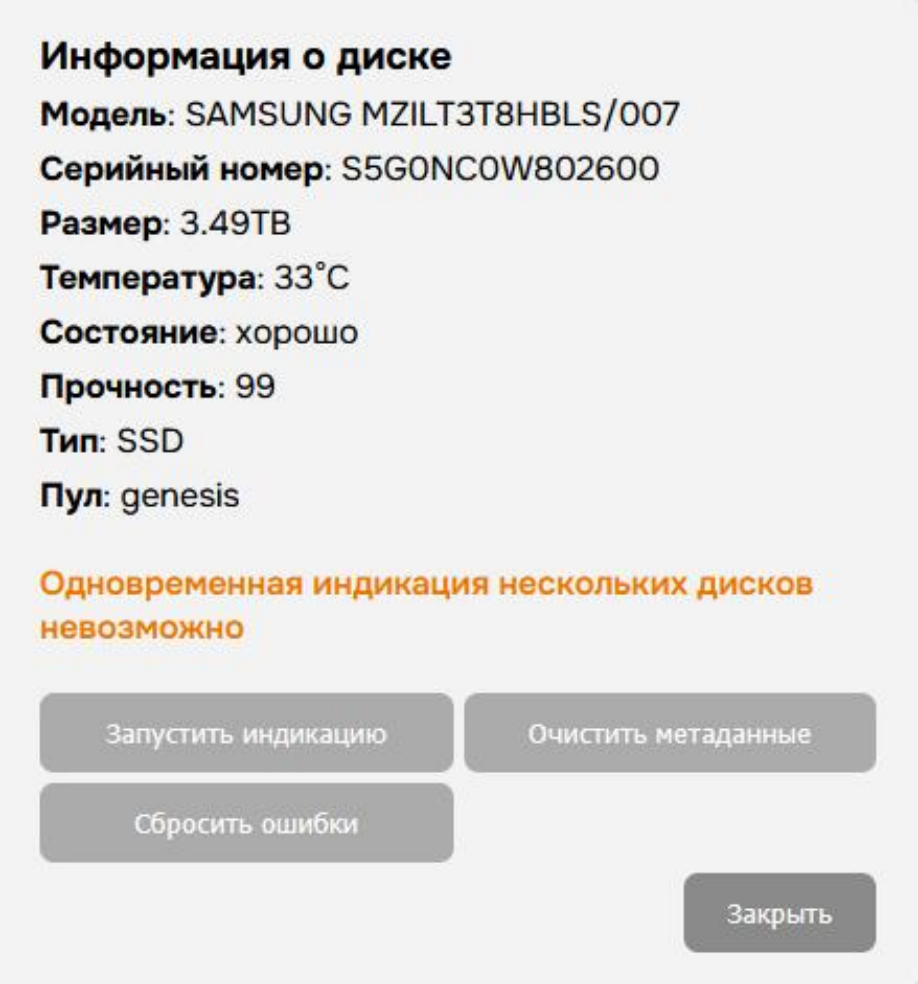

Рисунок 24 – Окно с подробной информацией о диске

Для получения подробной информации о системе предусмотрен переход на вкладку «О системе» (см. рисунок 23, область 4), также имеется информация о времени работы сервера. В данном разделе отображаются сведения о системе в целом, контроллерах, оперативной памяти,

процессоре, а также загрузочных дисках (см. рисунок 25).

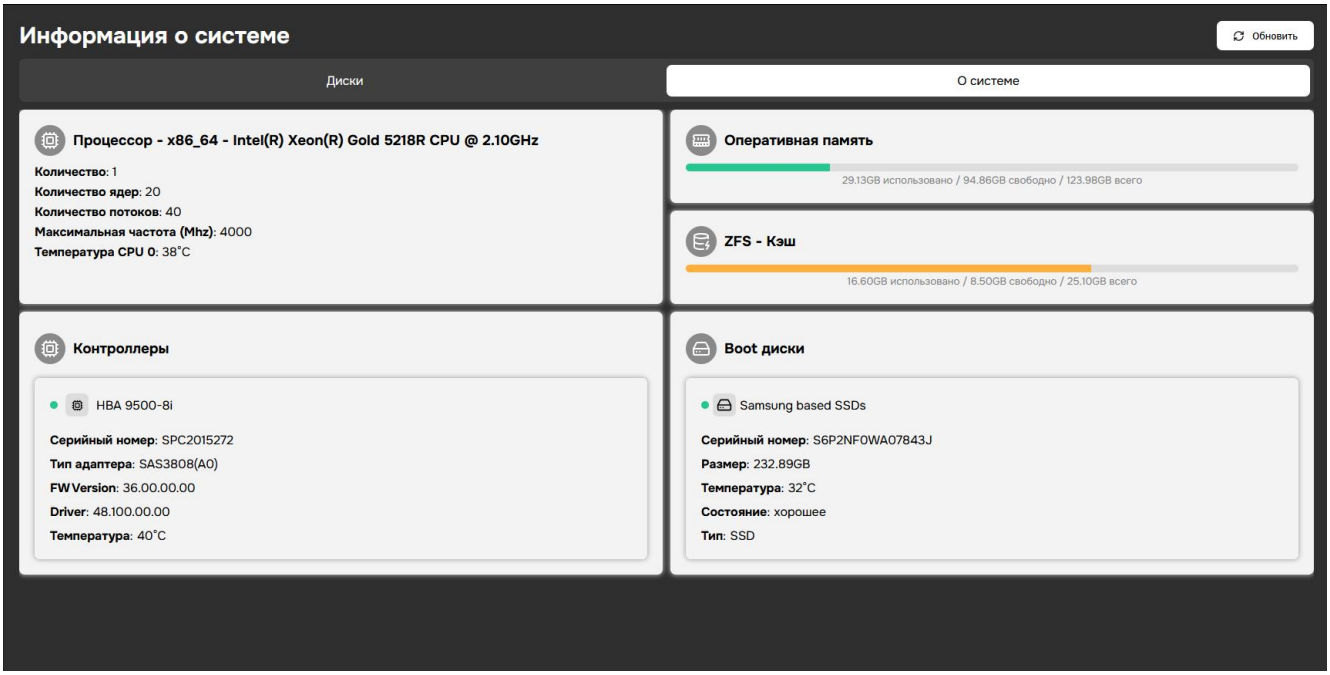

Рисунок 25 – Подробная информация о системе

В случае наличия более одного диска либо контроллера в системе отображается переключатель для выбора соответствующего устройства (см. рисунок 26). В рассматриваемой конфигурации установлен один контроллер. Для примера предоставлена конфигурация с двумя контроллерами.

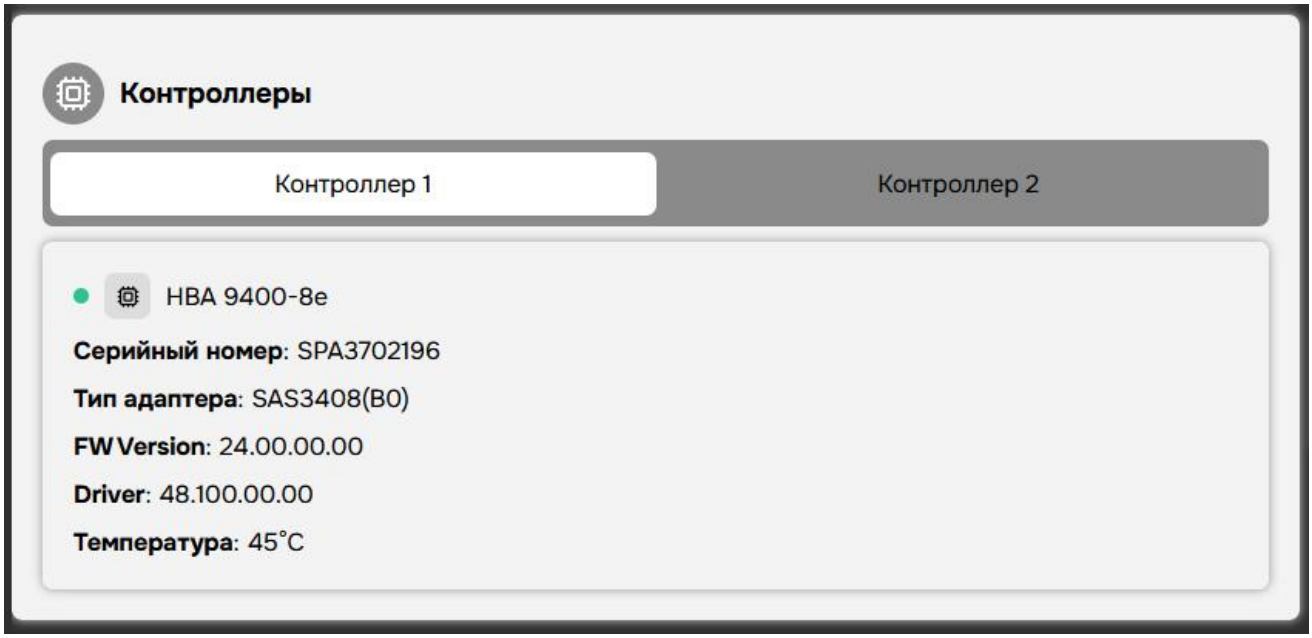

Рисунок 26 – Выбор контроллеров

Справа от заголовка «Информация о системе» располагается кнопка «Обновить», предназначенная для принудительного обновления отображаемых данных. Обновление информации выполняется в режиме реального времени; по умолчанию автоматическое обновление осуществляется с периодичностью 30 секунд.

В левой части страницы располагается блок для навигации по вкладкам администрирования (см. рисунок 23, область 5).

В левом нижнем углу находится кнопка выхода из сессии (см. рисунок 23, область 6).

4.4 Создание и работа с пулом

ZFS – это файловая система, кардинально меняющая принципы администрирования файловых систем с уникальными на сегодняшний день функциями и преимуществами. Система ZFS была разработана как надежный, масштабируемый и простой в администрировании инструмент.

Для управления физическим хранением в ZFS применяется принцип пулов устройств хранения данных. ZFS полностью исключает процесс управления томами. Вместо принудительного создания виртуализированных томов ZFS объединяет устройства в пул устройств хранения данных.

Пул устройств хранения данных описывает физические характеристики хранения (размещение устройств, избыточность данных и т. д.) и выступает в качестве хранилища данных для создания файловых систем. Файловые системы больше не ограничиваются отдельными устройствами, что позволяет им совместно использовать пространство в пуле.

4.4.1.1 Организация дисковых массивов RAID

RAID-массивы предназначены для объединения нескольких физических дисков в единый логический массив с целью повышения отказоустойчивости, производительности и эффективного использования дискового пространства. В системе поддерживаются

следующие типы RAID-массивов.

4.4.1.2 RAID 0 (Striping)

RAID 0 предназначен для повышения производительности за счёт распределения данных по нескольким дискам без избыточности. При отказе любого диска массив становится недоступен, так как часть данных теряется. Уровень RAID 0 применяется в случаях, когда приоритетом является скорость работы, а отказоустойчивость не требуется. Минимальное количество дисков — 2. Отказоустойчивость отсутствует.

4.4.1.3 RAID 1 (Mirroring)

RAID 1 обеспечивает отказоустойчивость за счёт зеркалирования данных на два (или более) диска. Запись выполняется на все диски зеркала, чтение может выполняться параллельно, что в отдельных сценариях повышает скорость чтения. При отказе одного диска массив продолжает работу, однако полезный объём составляет примерно 50% от суммарного объёма дисков (для пары). RAID 1 применяется для системных (boot) дисков и критически важных данных. Минимальное количество дисков — 2. Отказоустойчивость — отказ 1 диска в зеркальной паре.

4.4.1.4 RAIDZ1

RAIDZ1 обеспечивает избыточность с одной чётностью и допускает отказ одного диска без потери доступности пула. Данный уровень является функциональным аналогом RAID5, однако при выборе RAIDZ1 необходимо учитывать, что при восстановлении после отказа диска на больших объёмах возрастает время восстановления (resilver) и нагрузка на оставшиеся диски. Минимальное количество дисков: 3. Допустимое число отказов: 1 диск. Назначение: умеренная отказоустойчивость при максимальной ёмкости относительно RAIDZ2/3. Особенности

эксплуатации: при деградации повышается риск второй ошибки на период восстановления; предпочтителен для массивов с ограниченным числом дисков и дисками меньшей ёмкости либо для менее критичных данных.

4.4.1.5 RAIDZ2

RAIDZ2 обеспечивает избыточность с двумя независимыми чётностями и допускает отказ двух дисков. RAIDZ2 является распространённым вариантом для производственных систем, так как обеспечивает более высокий уровень надёжности при сохранении приемлемой эффективности использования дискового пространства. Минимальное количество дисков: 4. Допустимое число отказов: 2 диска. Назначение: повышенная устойчивость для критичных данных и массивов на больших дисках. Особенности эксплуатации: более безопасен при длительном восстановлении и при больших объёмах данных; операции записи обычно более ресурсоёмкие по сравнению с RAIDZ1.

4.4.1.6 RAIDZ3

RAIDZ3 обеспечивает избыточность с тремя чётностями и допускает отказ трёх дисков. Применяется в сценариях с повышенными требованиями к надежности (например, большие полки дисков, длительные окна восстановления, повышенные риски деградации или ошибки чтения при восстановлении). Минимальное количество дисков: 5. Допустимое число отказов: 3 диска. Назначение: максимальная устойчивость среди RAIDZ-схем. Особенности эксплуатации: обеспечивает высокий запас по надёжности, но снижает полезную ёмкость и увеличивает вычислительную нагрузку при записи по сравнению с RAIDZ1/2.

4.4.1.7 dRAID1

dRAID1 допускает отказ одного диска и является аналогом RAIDZ1 по уровню избыточности, но отличается распределённой организацией и ускоренным восстановлением на больших массивах. Минимальное количество дисков: зависит от выбранных параметров dRAID (число data/parity/children), но на практике применяется при большем числе дисков, чем для RAIDZ. Допустимое число отказов: 1 диск. Назначение: массивы с большим числом дисков, где важно минимизировать время восстановления. Особенности эксплуатации: быстрее восстановление относительно RAIDZ1 за счёт параллельной работы многих дисков.

4.4.1.8 dRAID2

dRAID2 допускает отказ двух дисков и является аналогом RAIDZ2 по уровню избыточности, при этом обеспечивает преимущества dRAID по скорости восстановления и поведению при деградации на больших конфигурациях. Допустимое число отказов: 2 диска. Назначение: типовой вариант для крупных дисковых групп, где требуется баланс надёжности и скорости восстановления. Особенности эксплуатации: повышенная устойчивость на период восстановления, особенно при больших объёмах данных.

4.4.1.9 dRAID3

dRAID3 допускает отказ трёх дисков и соответствует уровню защиты RAIDZ3, обеспечивая максимальный запас по отказоустойчивости в сочетании с ускоренным восстановлением на больших массивах. Допустимое число отказов: 3 диска. Назначение: высоконадежные конфигурации (большие дисковые полки, критичные данные, длинные окна восстановления). Особенности эксплуатации: максимальная устойчивость при наибольших накладных расходах по ёмкости и вычислениям.

4.4.1.10 Специальные опции

Ниже описаны опции, используемые совместно с основными группами данных. Эти опции настраиваются при создании пула либо при расширении конфигурации (в зависимости от возможностей реализации).

SLOG (Separate Intent Log) — ускорение синхронной записи (SLOG). Выделенное устройство для журнала операций синхронной записи. При наличии SLOG подтверждение синхронной записи клиенту происходит после фиксации данных в журнале, а затем данные переносятся в основной массив. Назначение: ускорение синхронных записей (например, при NFS с sync, iSCSI при определённых режимах, базах данных). Требования: предпочтительно использовать быстрые и надёжные накопители с защитой от потери питания (PLP), так как журнал участвует в сохранности подтверждённых операций. Замечание: SLOG не ускоряет асинхронные записи и не увеличивает скорость чтения.

L2ARC — L2ARC для ускорения чтения. Дополнительный уровень кэша чтения на SSD/NVMe, расширяющий возможности оперативного кэша (ARC) при дефиците RAM или при большом рабочем наборе данных. Назначение: повышение производительности чтения при повторяющихся обращениях к данным. Особенности: L2ARC не является частью отказоустойчивости пула; при отказе кэш-устройства данные не теряются, но временно снижается производительность до восстановления кэша.

Special vdev — выделенные диски для метаданных (special vdev). Применяется для размещения метаданных файловой системы (а при определённых настройках — и небольших блоков данных) на быстрых накопителях. Назначение: ускорение операций, завязанных на метаданные (работа с большим числом файлов, каталоги, списки, операции создания/удаления). Критичность: special vdev является частью пула; его отказ может привести к недоступности пула. Поэтому такие устройства должны быть надёжными и обычно организуются с избыточностью (например, mirror).

Dedup — таблица дедупликации. Включает дедупликацию данных,

при которой одинаковые блоки данных хранятся в одном экземпляре. Для работы дедупликации используется таблица дедупликации (DDT). Назначение: экономия пространства при высокой доле повторяющихся данных (например, типовые образы ВМ, резервные копии с большим количеством дублей). Ограничения: дедупликация требует значительных ресурсов (прежде всего оперативной памяти) и может снижать производительность. Рекомендуется применять только при обоснованной необходимости и после оценки нагрузки.

Hot-Spare — Резервные диски для быстрой замены. Резервный диск, который может быть автоматически (или по команде администратора) задействован при отказе диска в массиве. Назначение: сокращение времени нахождения пула в деградированном состоянии за счёт оперативной подмены отказавшего диска на резервный. Особенности: Hot-Spare не увеличивает полезную ёмкость пула, так как находится в резерве до момента использования.

4.4.1.11 Создание пула

Перейдя на вкладку ZFS, появится возможность создать пул. При нажатии на кнопку «Создание пула» (см. рисунок 27) откроется соответствующее окно.

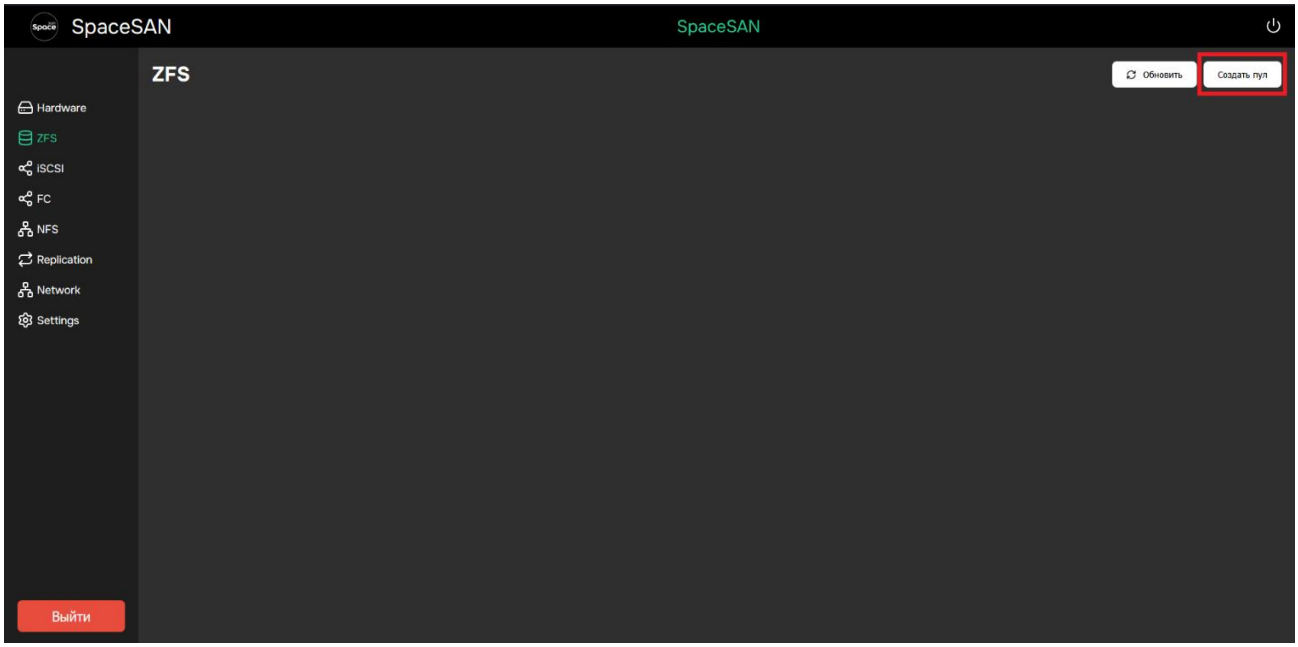

Рисунок 27 – Вкладка ZFS

Осуществляется переход на вкладку создания пула (см. рисунок 28).

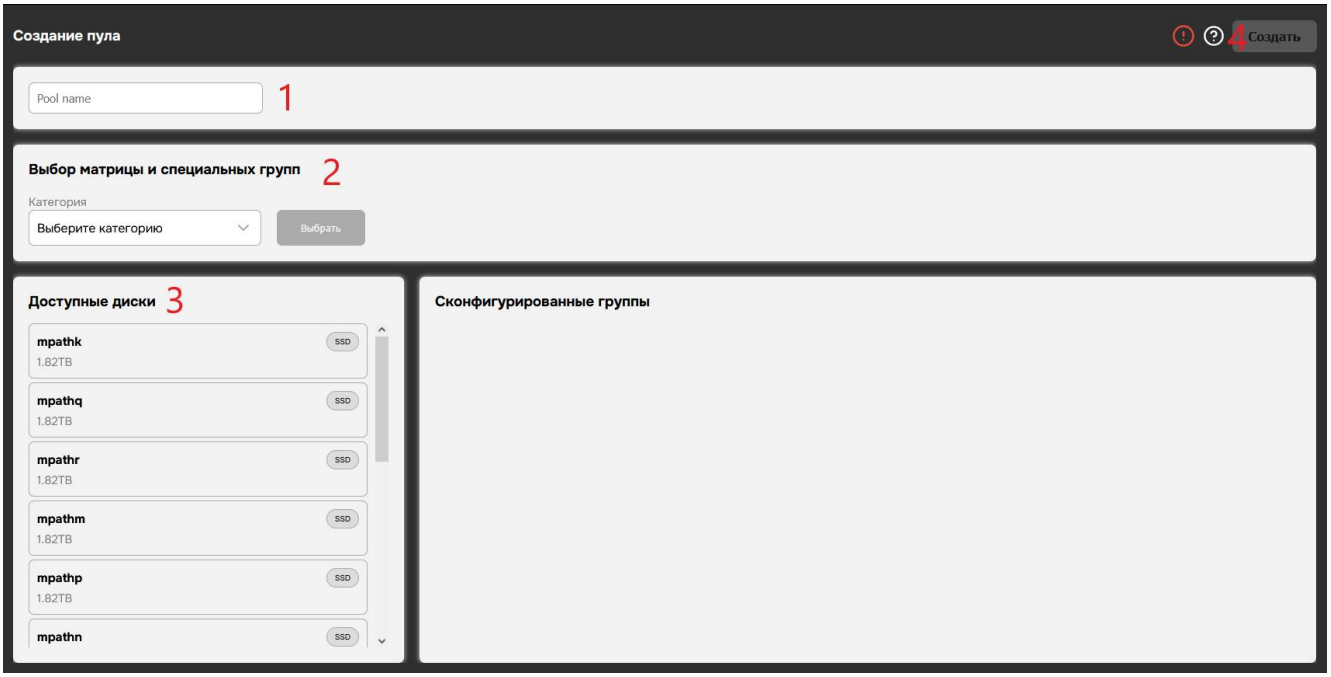

Рисунок 28 – Создание пула

Для начала необходимо дать название будущему пулу (см рисунок 28, область 1).

Далее администратор выбирает тип RAID в блоке выбора

конфигурации хранения (см. рисунок 28, область 2). После выбора отображается окно со списком доступных типов RAID, определяющих схему организации данных и избыточности (см. рисунок 29).

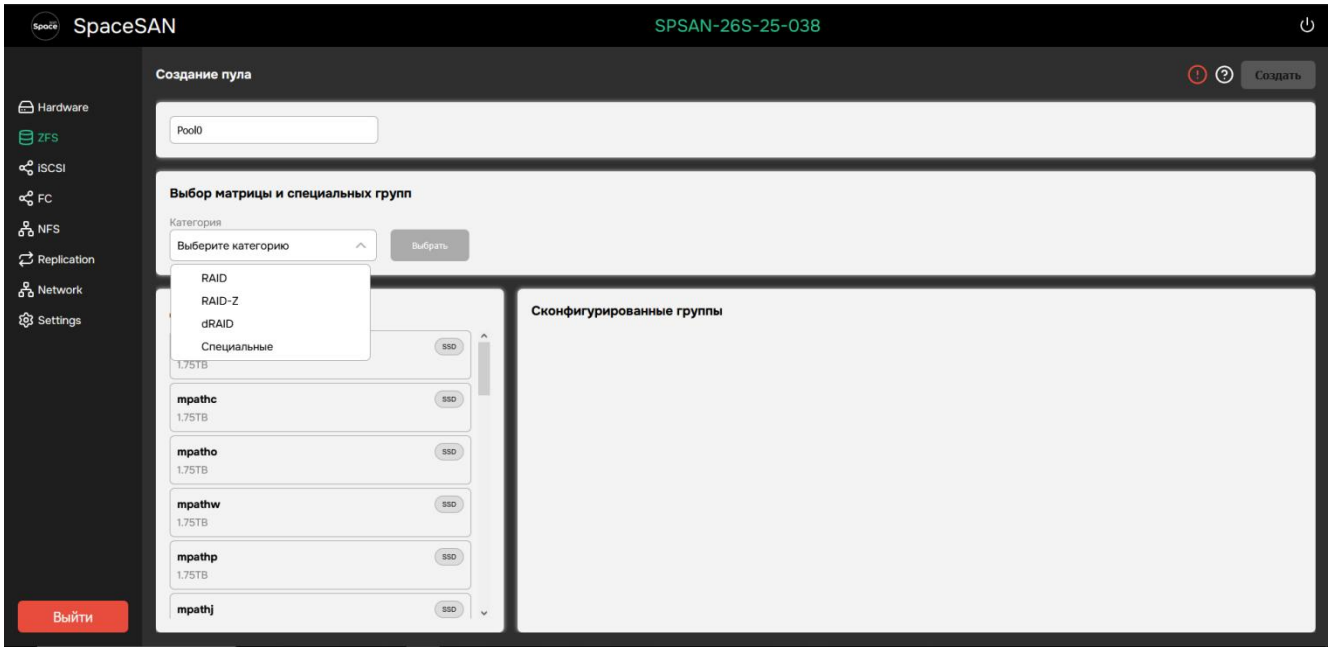

Рисунок 29 – Выбор категории

После выбора типа RAID отображается окно выбора уровня отказоустойчивости, в котором задаётся допустимое количество одновременных отказов дисков без потери данных (см. рисунок 30).

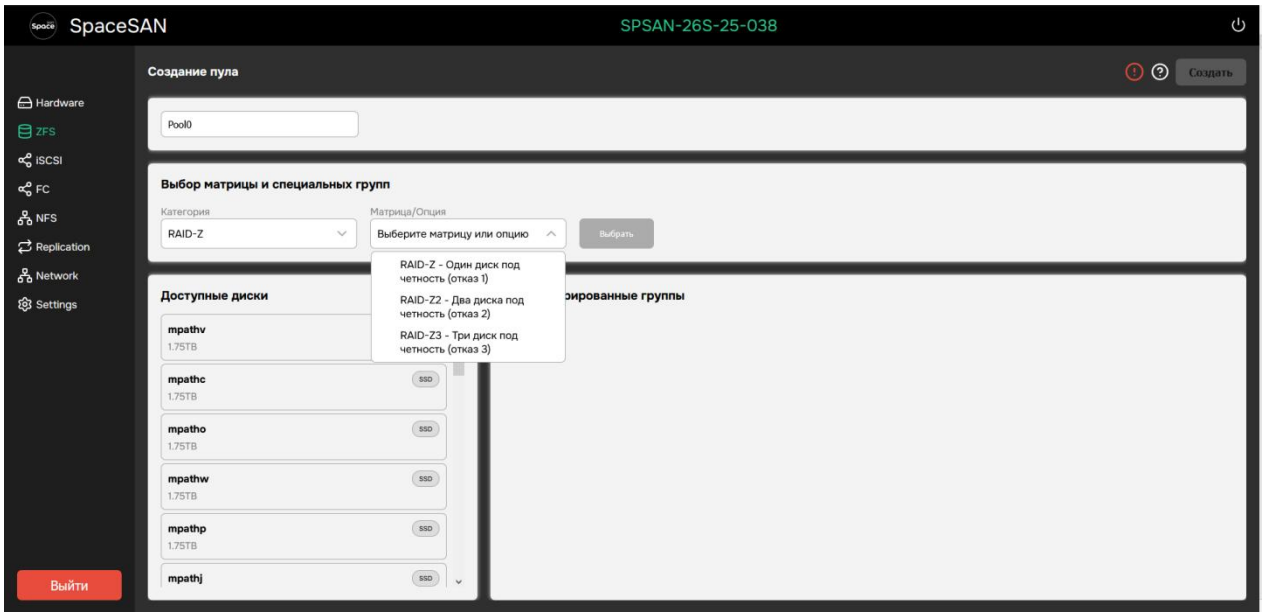

Рисунок 30 – Выбор матрицы/опции

После выбора необходимой избыточности, необходимо нажатием кнопки «Выбрать» добавить массив.

Далее при нажатии на соответствующую иконку (см. рисунок 31, область 1) появится возможность добавлять диски в массив.

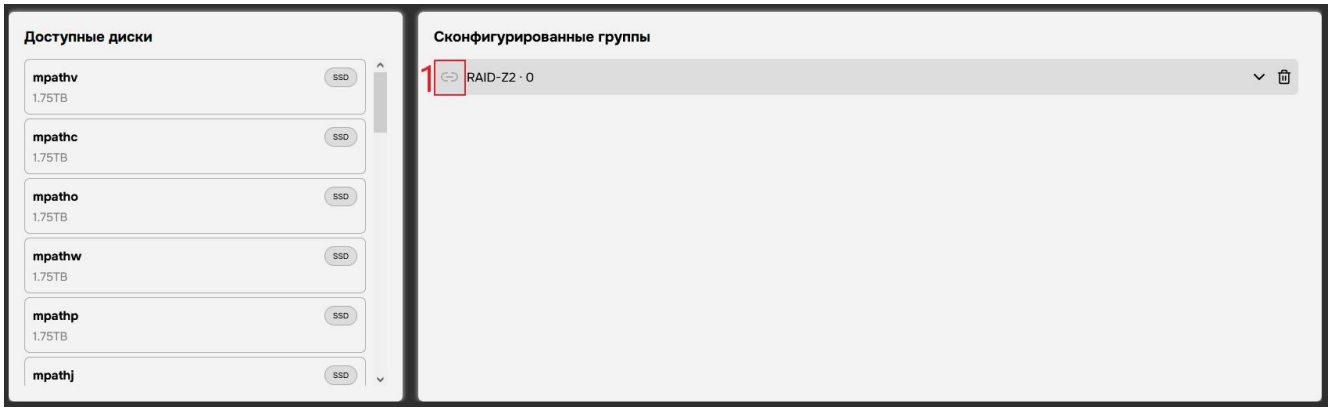

Рисунок 31 – Формирование пула

Индикация массива изменится на зеленый и появится возможность добавлять диски в формируемый пул (см. рисунок 32).

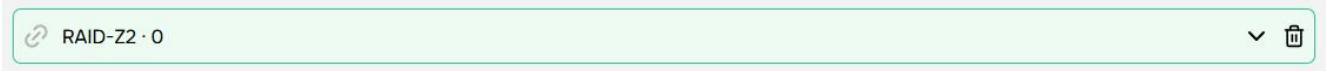

Рисунок 32 – Открытие пула

Далее необходимо добавить нужное количество дисков в пул нажатием ЛКМ (см. рисунок 33).

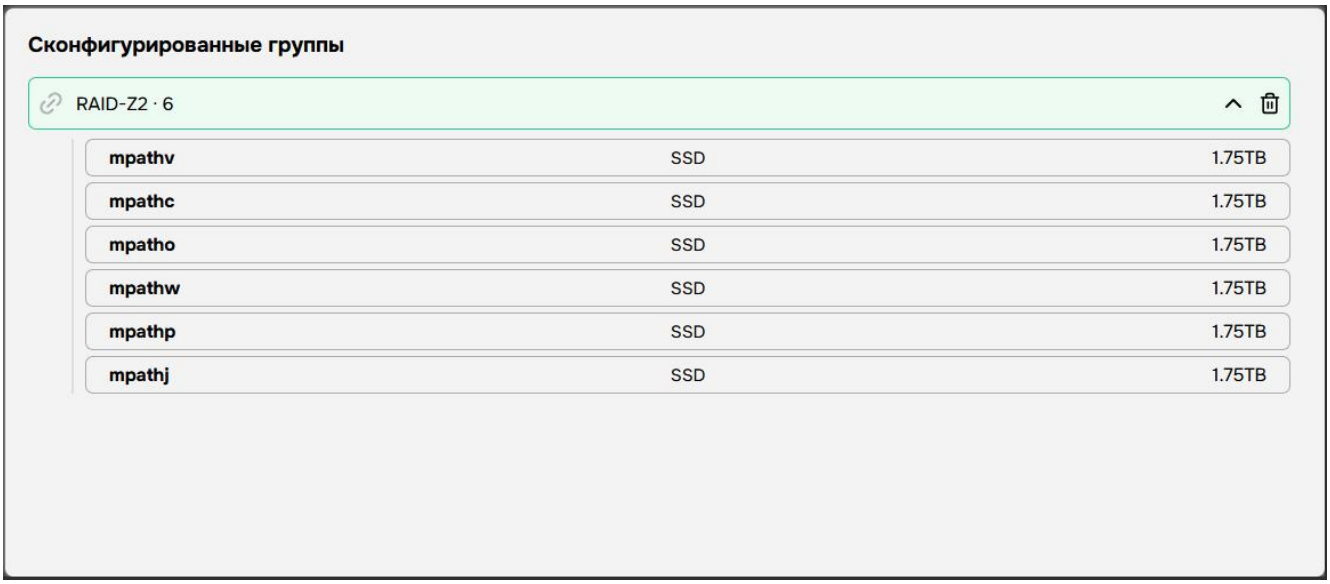

Рисунок 33 – Выбранные диски

Предусмотрена возможность добавить дополнительные опции к пулу (см. рисунок 29), если выбрать специальные матрицы. Расширенные опции (VDEV) – позволяют добиться повышения эффективности использования пула (см. рисунок 34).

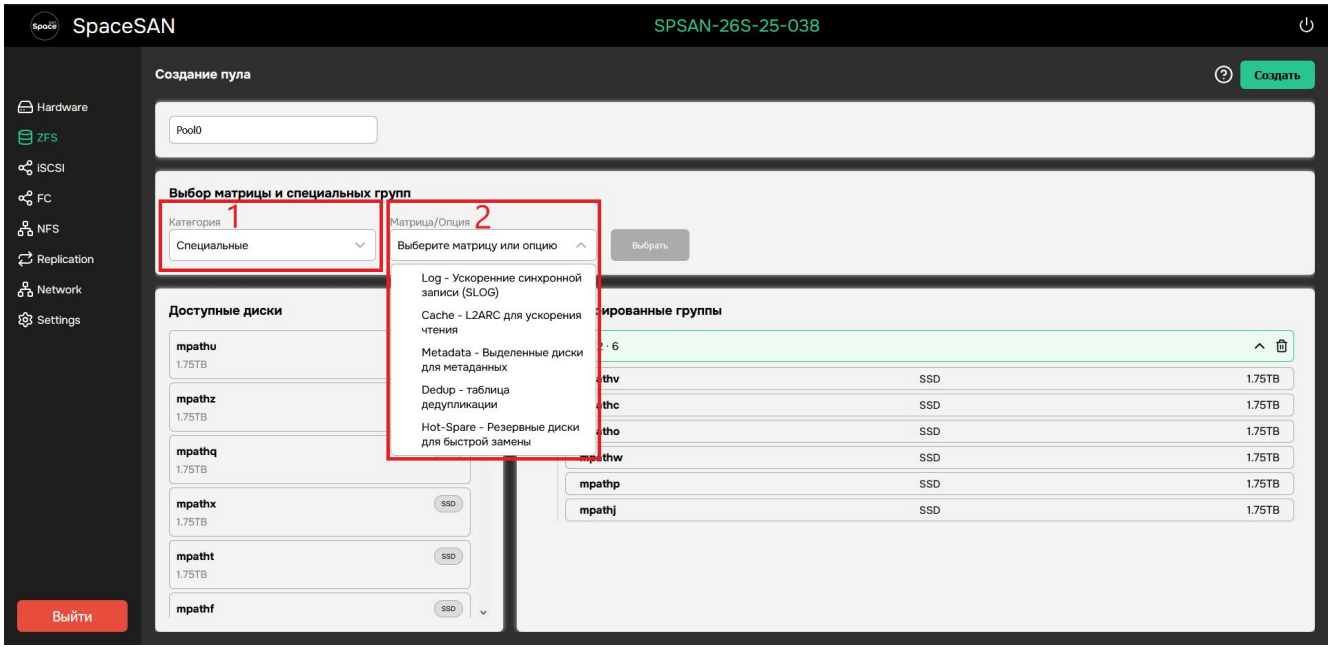

Рисунок 34 – Расширенные опции

При выборе нужных опций появится дополнительный раздел в окне создания пула. Необходимо выбрать нужное количество дисков (см. рисунок 35). Можно выбирать все требуемые опции.

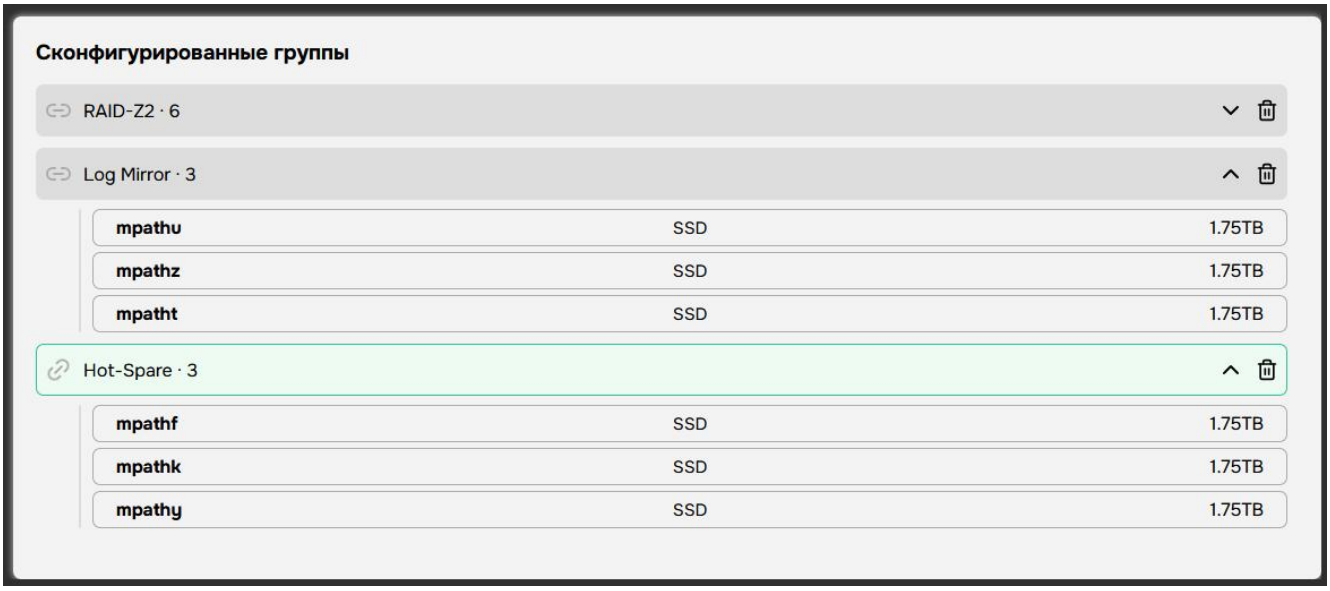

Рисунок 35 – Дополнительный раздел

Последним шагом будет непосредственное создание пула. Для этого необходимо нажать на соответствующую кнопку (см. рисунок 28, область 4).

После успешного завершения предыдущих этапов появится пул на главном экране вкладки ZFS, тут можно увидеть объем пула, также шкала наполненности в случае, если у пула есть ошибки появится сообщение, при нажатии на которое, будет переход на вкладку «Сервис» (см. рисунок 36).

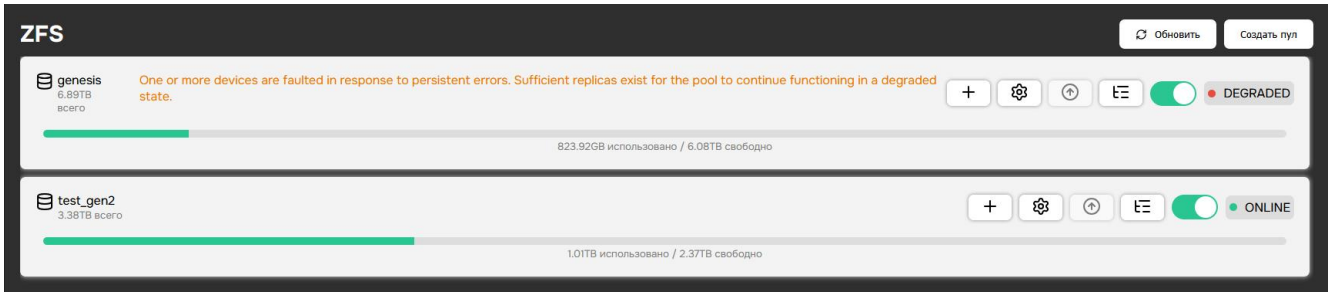

Рисунок 36 – Пулы ZFS

4.4.1.12 Настройки пула

Для работы с пулом следует перейти в его настройки, нажав на соответствующую кнопку (см. рисунок 37, область 1).

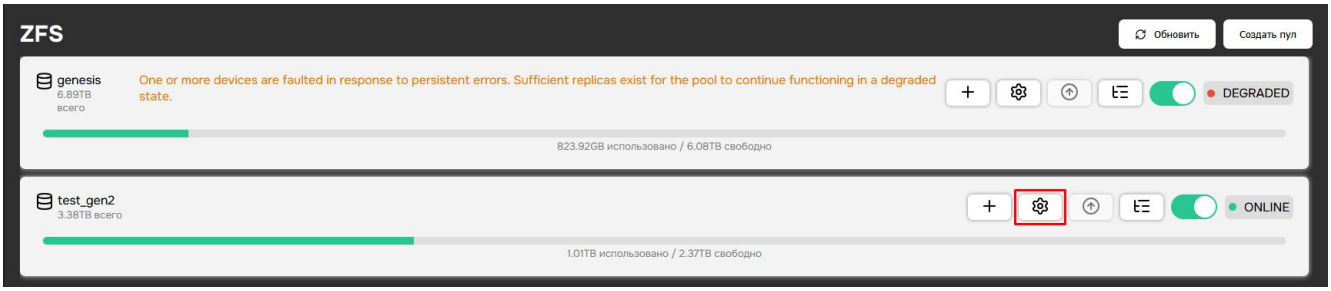

Рисунок 37 – Настройки пула

В данном разделе есть возможность просматривать или изменять параметры пула (см. рисунок 38). Подробнее о настройках пула описано в пункте 4.13.

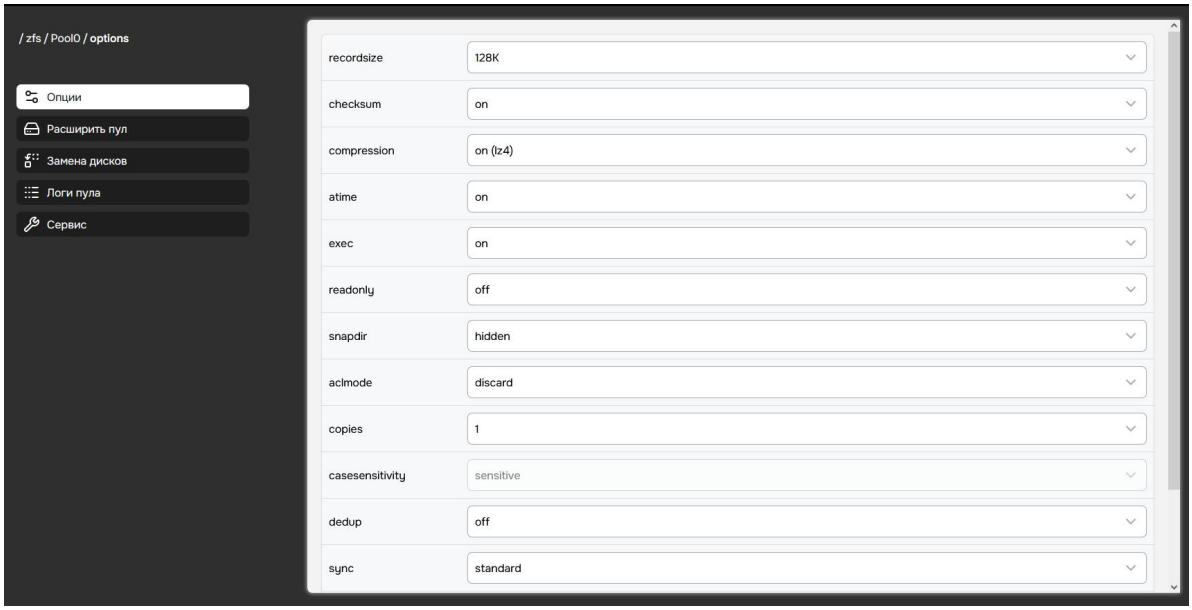

Рисунок 38 – Параметры пула

4.4.1.13 Расширение пула

На вкладке расширения пула можно увеличить количество дисков в пуле либо добавить массив к пулу. Переместить нужные диски в логическую группу (см. рисунок 39) или нажать на соответствующую кнопку (см. рисунок 31, область 1) простым нажатием ЛКМ.

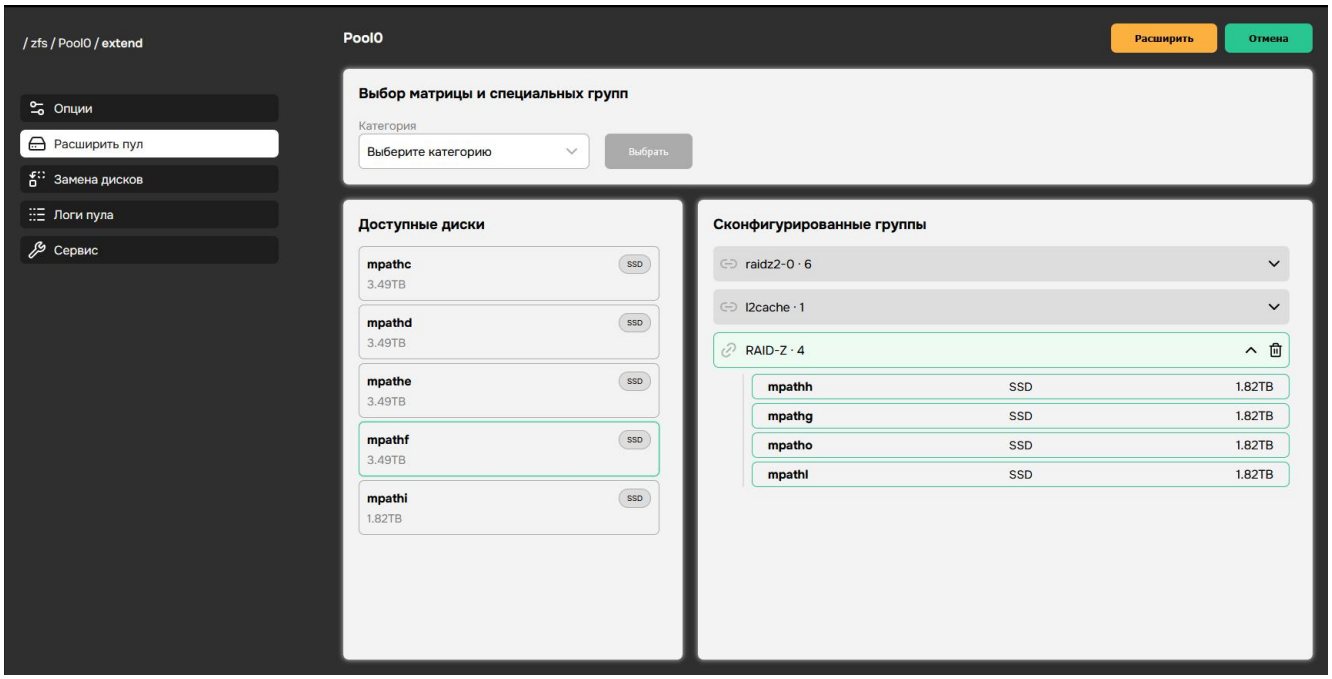

Рисунок 39 – Расширение пула

4.4.1.14 Замена диска в пуле

Предусмотрена возможность заменить диск в пуле на свободный (см. рисунок Error: Reference source not found).

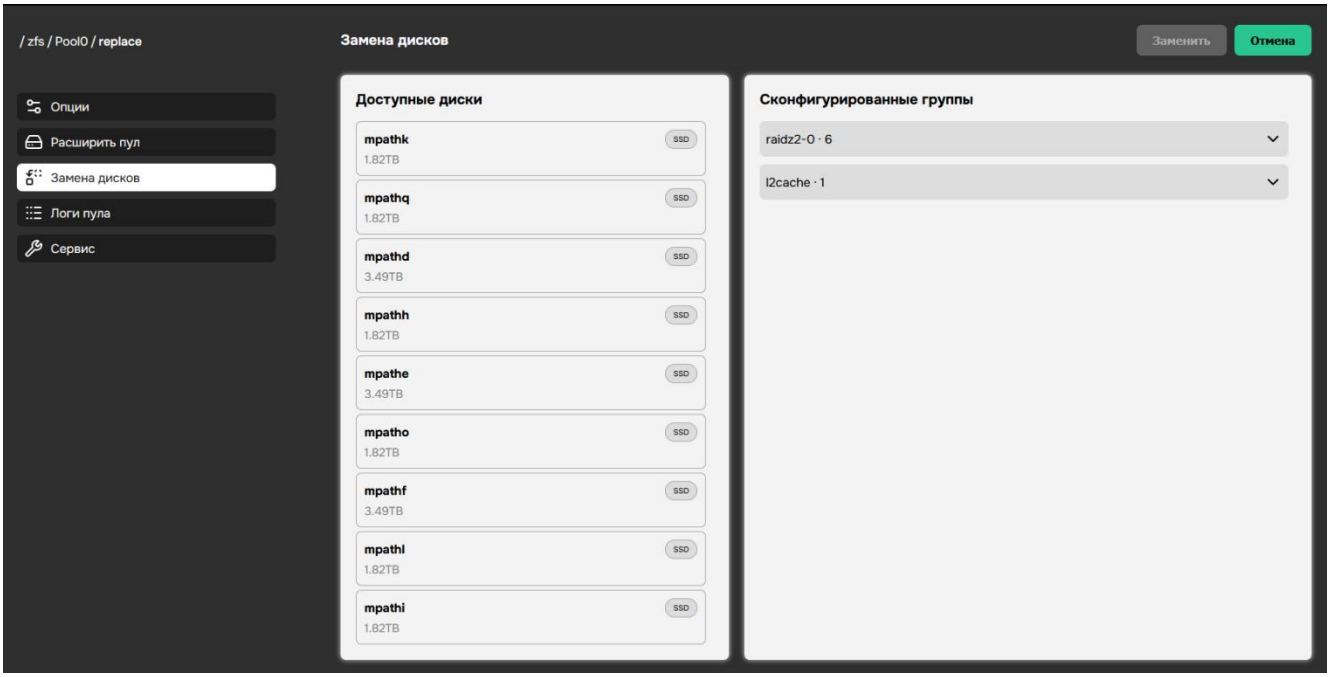

Рисунок 40 – Замена дисков

Для выполнения замены администратор выбирает неисправный диск в правом списке, после чего выбирает диск для замены в левом списке и подтверждает действие нажатием кнопки «Заменить». При выборе диска в левом списке он подсвечивается зелёным цветом. При выборе диска в правом списке отображается информация о том, какой диск подлежит замене и каким диском он будет заменён. (см. рисунок 41)

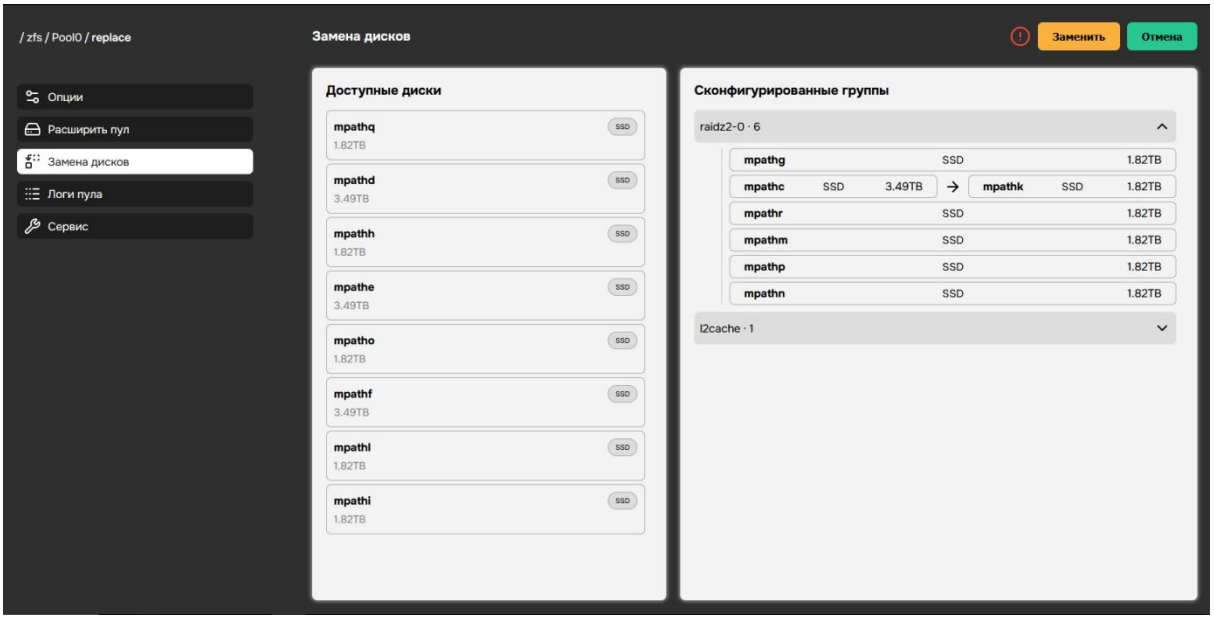

Рисунок 41 – Замена диска в пуле

4.4.1.15 Логи пула

В разделе «Логи пула» отображается журнал операций, связанных с выбранным пулом (см. рисунок 42). В журнале представлены команды и действия, выполняемые над пулом, а также время их выполнения.

Отображение журнала реализовано в виде списка записей, содержащих команды управления пулом и сопутствующие операции. Каждая запись включает текст команды и отметку времени её выполнения.

Для актуализации отображаемых данных предусмотрена кнопка «Обновить», позволяющая загрузить последние записи журнала. Также доступна кнопка «Скачать полный log файл», предназначенная для выгрузки полного журнала операций в файл для последующего анализа.

В правой части интерфейса доступен параметр «Количество последних логов», позволяющий задать число отображаемых записей журнала. Изменение данного параметра влияет на объём выводимых данных.

Журнал используется для мониторинга состояния пула, анализа

выполненных операций и диагностики возможных ошибок.

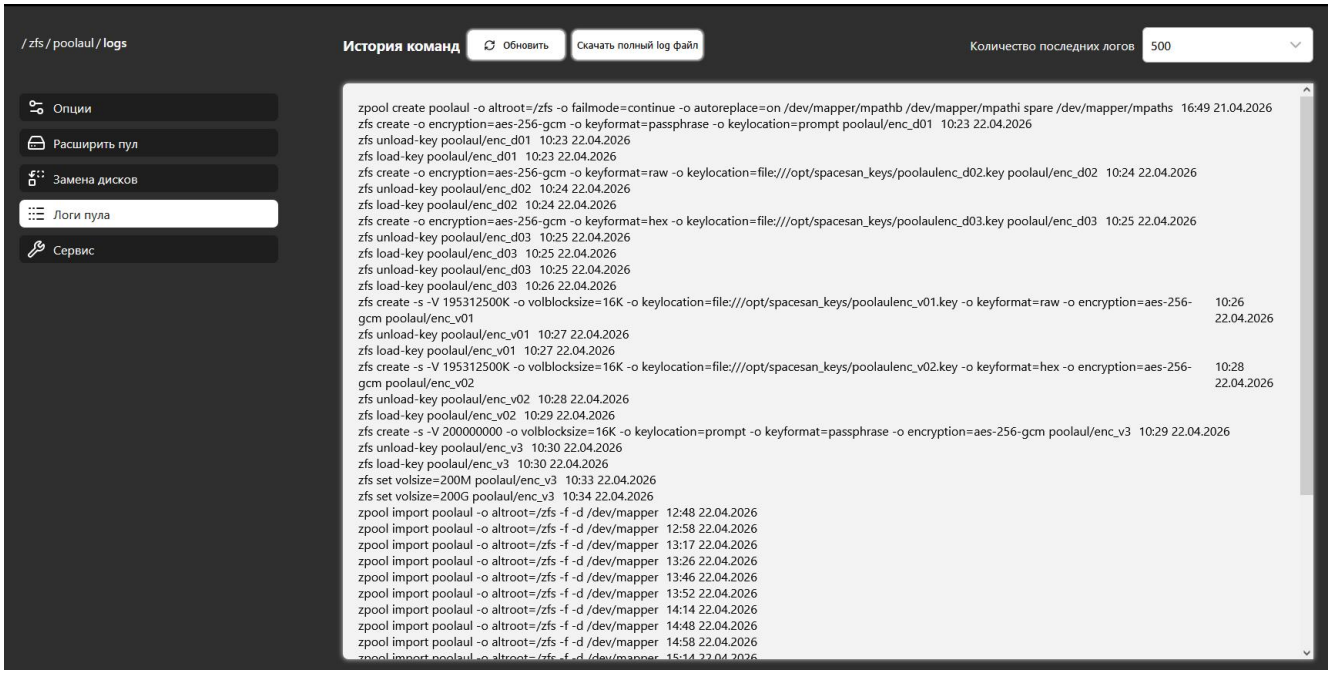

Рисунок 42 – Логи пула

4.4.1.16 Раздел сервис

Раздел «Сервис» предназначен для выполнения обслуживающих и административных операций над пулом хранения (см. рисунок 43). В данном разделе доступны следующие функции: очистка статуса пула, проверка целостности пула, удаление пула и статус сканирования.

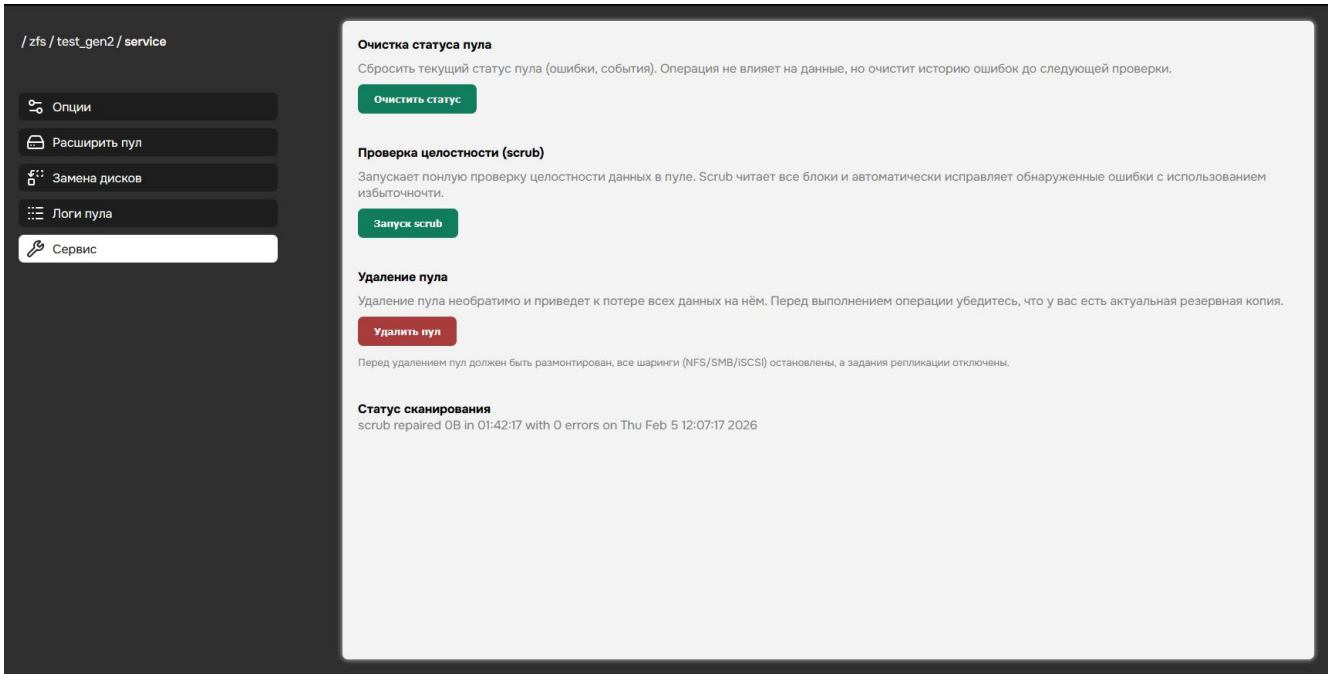

Рисунок 43 – Раздел «сервис»

Функция очистки статуса пула используется в случае, если на одном или нескольких дисках были зафиксированы ошибки чтения или записи (см. рисунок 44). Данная операция позволяет сбросить статус ошибок после их устранения. Перед выполнением очистки рекомендуется проверить состояние дисков на исправность. Если после очистки диск продолжает работать с ошибками, рекомендуется заменить его на исправный.

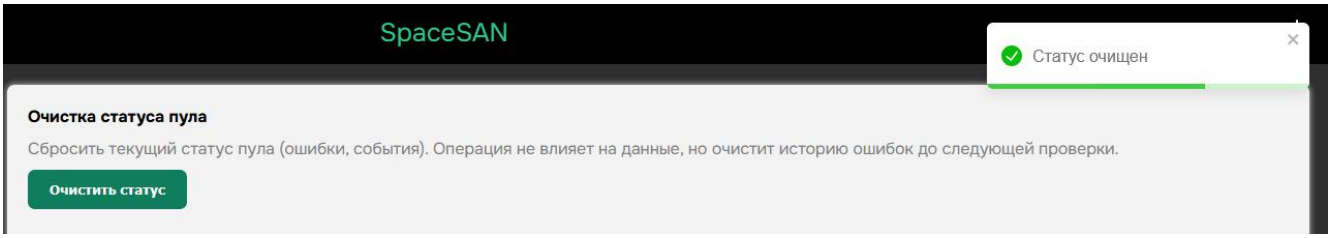

Рисунок 44 – Очистка статуса пула

В разделе «Сервис» доступна возможность запуска проверки целостности пула (scrub) (см. рисунок 45). В ходе данной операции система последовательно проходит по всем данным в пуле и проверяет возможность чтения всех блоков данных. Проверка выполняется с минимальным приоритетом ввода-вывода, чтобы не блокировать

обычную работу системы, однако в процессе выполнения операция может негативно влиять на производительность. При этом данные пула остаются доступными для использования на протяжении всей проверки.

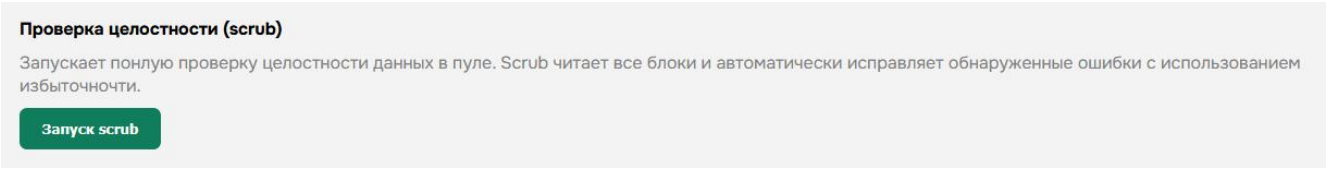

Рисунок 45 – Очистка статуса пула

Для удаления пула предусмотрена отдельная операция, требующая обязательного подтверждения (см. рисунок 46). В целях предотвращения случайного удаления необходимо ввести код подтверждения.

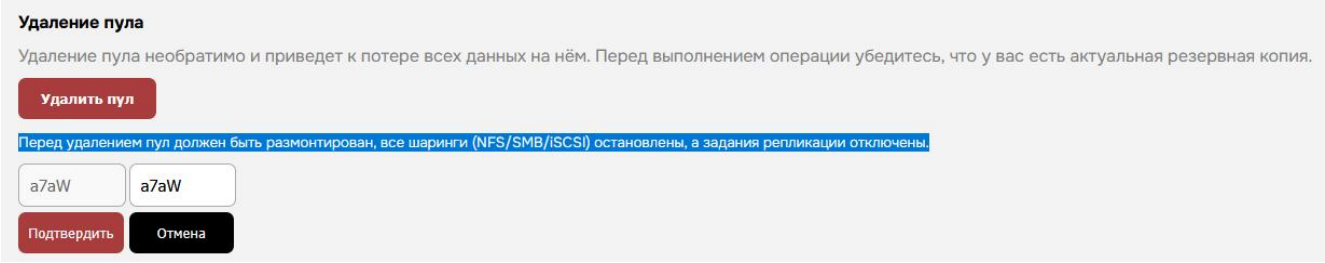

Рисунок 46 – Удаление пула

Перед выполнением операции удаления пул должен быть размонтирован. Все связанные с пулом сервисы и ресурсы, включая сетевые шаринги (NFS, SMB, iSCSI), должны быть остановлены, а задания репликации — отключены. После выполнения указанных условий и подтверждения операции пул будет полностью удалён вместе со всеми содержащимися в нём данными.

Пункт «Статус сканирования» отображает диагностические сообщения ZFS, включающие: дату последней проверки целостности, выявленные ошибки пула и текущий прогресс операции миграции данных при замене диска (см. рисунок 47).

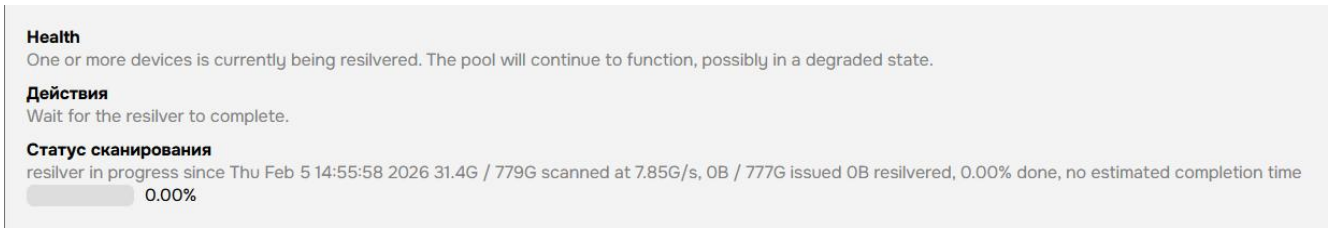

Рисунок 47 – Статус сканирования

4.4.1.17 Импорт и экспорт пула

При нажатии на соответствующий переключатель, выделенный рамкой (см. рисунок 48) есть возможность импортировать/экспортировать пул.

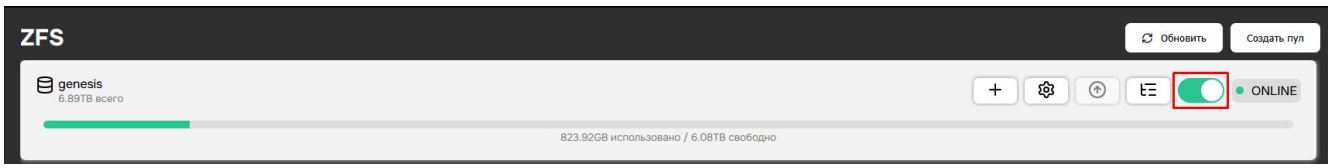

Рисунок 48 – Импорт/экспорт пула

4.4.1.18 Обновление версии пула

В случае обновления до новой версии ZFS есть возможность обновить версию пула нажатием на соответствующую кнопку. В случае если пул актуальной версии, то кнопка будет неактивной (см. рисунок 49).

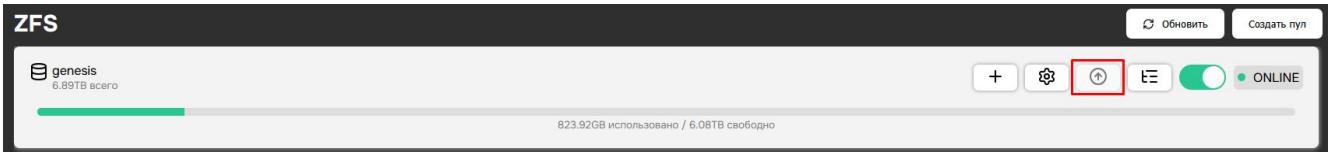

Рисунок 49 – Обновление версии пула

4.4.1.19 Список дисков пула

При нажатии на соответствующую кнопку открывается окно со списком дисков, используемых в пуле (см. рисунок 50).

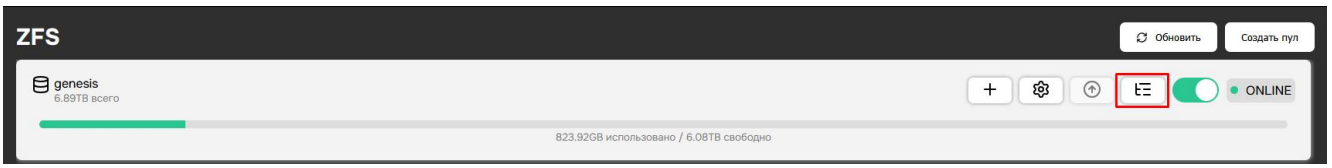

Рисунок 50 – Окно просмотра дисков, используемых в пуле

Открывается окно, в котором отображается информация о дисках, входящих в состав пула, что позволяет проанализировать их состав, состояние, роль в пуле и количество ошибок (см. рисунок 51).

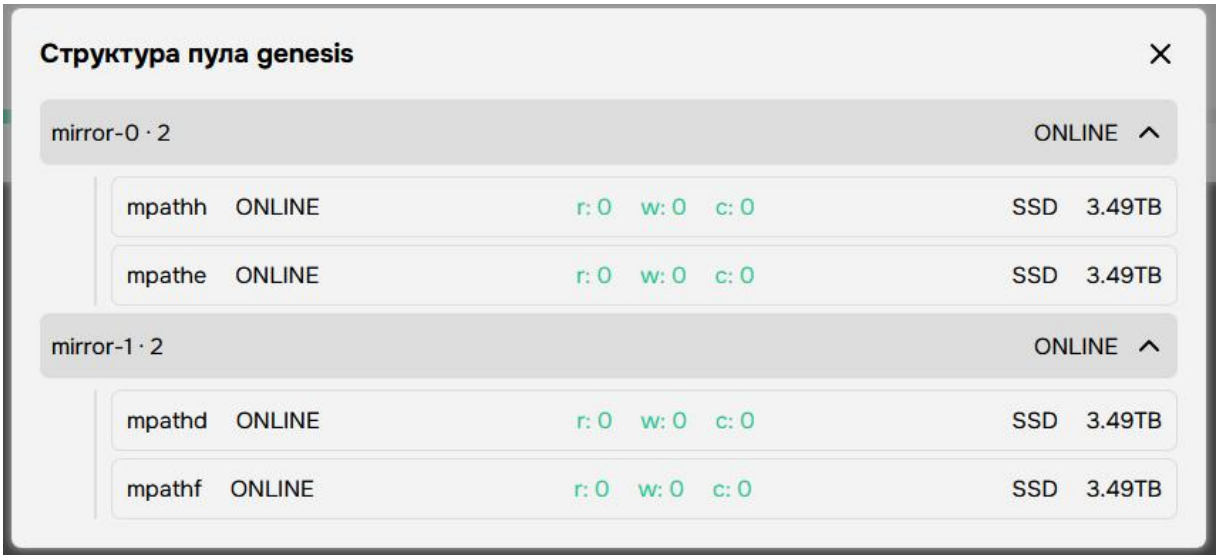

Рисунок 51 – Список дисков в составе пула

4.4.1.20 Создание Dataset/VVol

При нажатии на соответствующую кнопку (см. рисунок 52) откроется окно создания dataset и vvol.

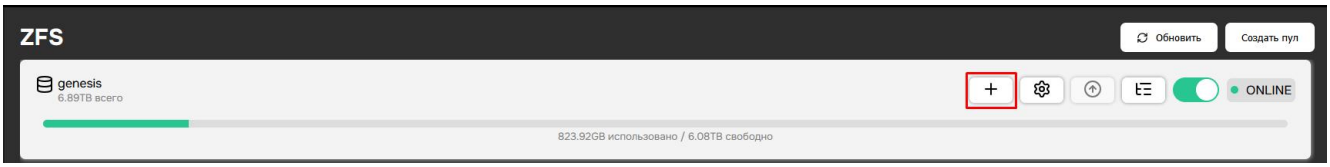

Рисунок 52 – Кнопка создания dataset/vvol

4.4.1.21 Datasets

ZFS datasets – это мощный и гибкий организационный инструмент, позволяющий легко и быстро структурировать данные, отслеживать размер с течением времени и делать резервные копии. Виртуальная файловая система внутри пула ZFS, позволяющая гибко управлять хранилищем, настройками и снимками (snapshots). ZFS datasets похожи на подразделы в файловой системе, но с уникальными свойствами и управлением. Наборы данных используются для предоставления

передачи данных по протоколам NFS.

Для создания набора данных необходимо нажать на соответствующую кнопку (см. рисунок 52) и в появившемся окне ввести его будущее название (см. рисунок 53).

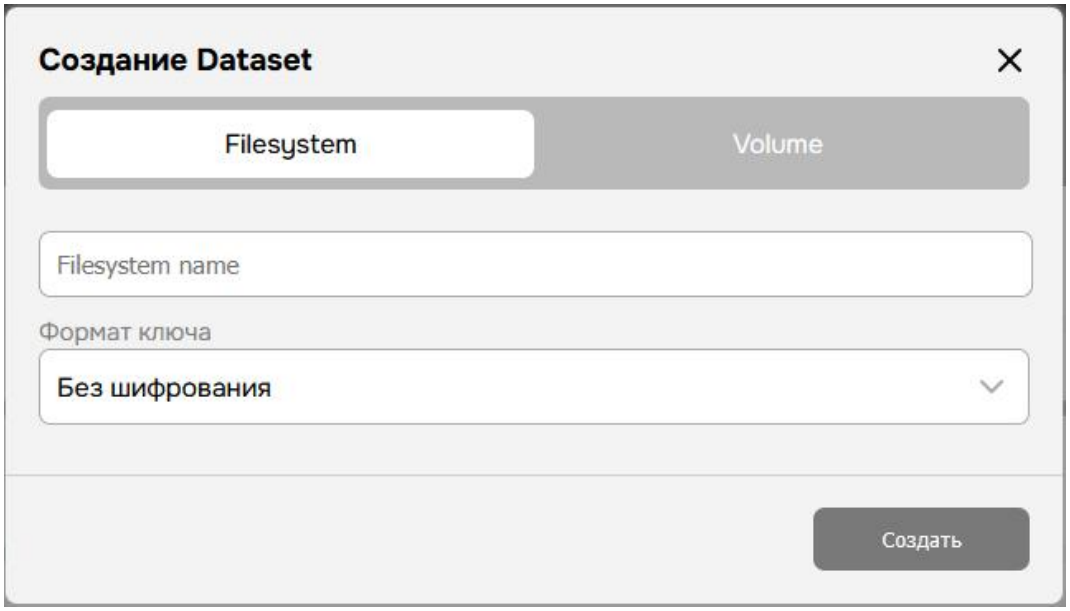

Рисунок 53 – Создание набора данных

После успешного создания набор данных будет отображаться в пуле (см. рисунок Error: Reference source not found).

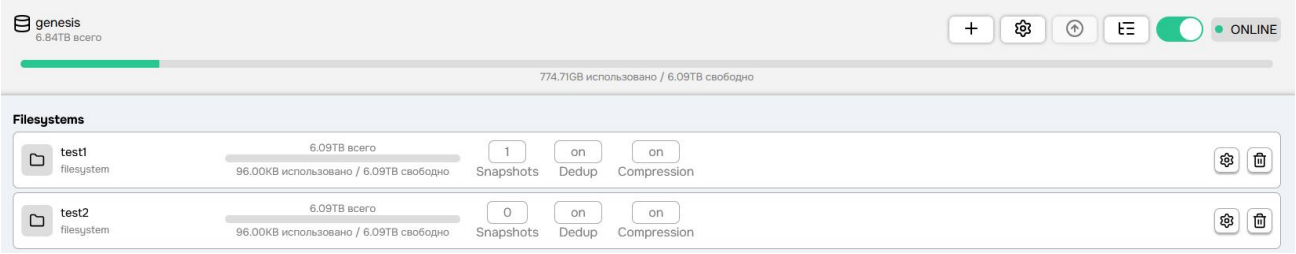

Рисунок 54 – Набор данных

У каждого набора данных предусмотрен набор индивидуальных свойств. Кнопка доступа к свойствам набора данных отображается в интерфейсе после загрузки информации о наборе данных, что может потребовать некоторого времени (см. рисунок 55).

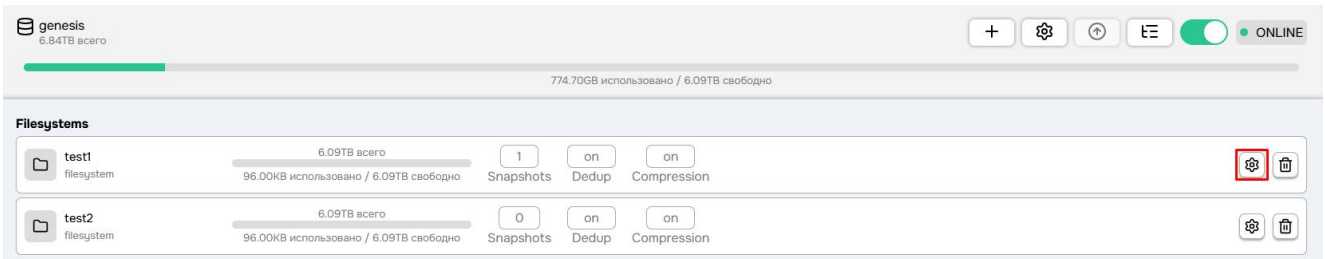

Рисунок 55 – Кнопка свойств набора данных

После нажатия на указанную кнопку открывается окно свойств набора данных, в котором отображаются его параметры и настройки (см. рисунок 56). Подробнее о настройках описано в пункте 4.13.

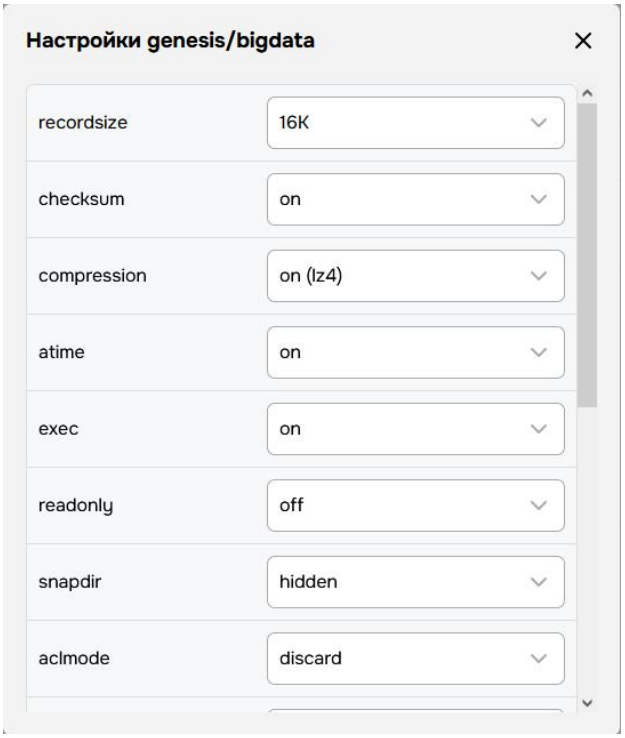

Рисунок 56 – Свойства набора данных

4.4.1.22 Виртуальные тома

ZFS также может создавать дисковые устройства называемые томами (VVol). Виртуальные тома могут быть полезны для запуска других форматов файловых систем поверх ZFS, таких как iSCSI и Fibre Channel. Для создания необходимо ввести название будущего тома, размер диска, блока и указать формат
диска – тонкий или толстый (см. рисунок 57).

Thin provisioning — механизм динамического выделения физического пространства на устройстве хранения, при котором объём ZVOL резервируется логически, а физические блоки выделяются по мере записи данных. Данная технология позволяет эффективно использовать ресурсы хранилища, исключая предварительное выделение объёма,

соответствующего заявленному размеру ZVOL.

Примечание — при использовании thin provisioning рекомендуется мониторить уровень заполнения физического пула, поскольку переполнение приводит к недоступности ZVOL.

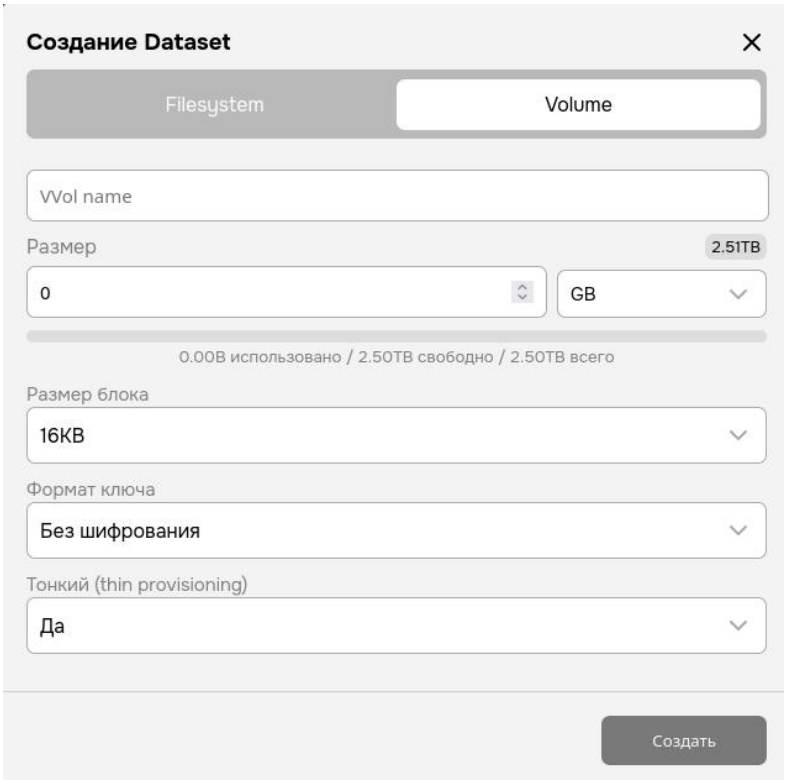

Рисунок 57 – Создание виртуального тома

При необходимости задействовать весь доступный свободный объем пула применяется специальная функция, активируемая нажатием кнопки «Использовать весь объем» (см. рисунок 58).

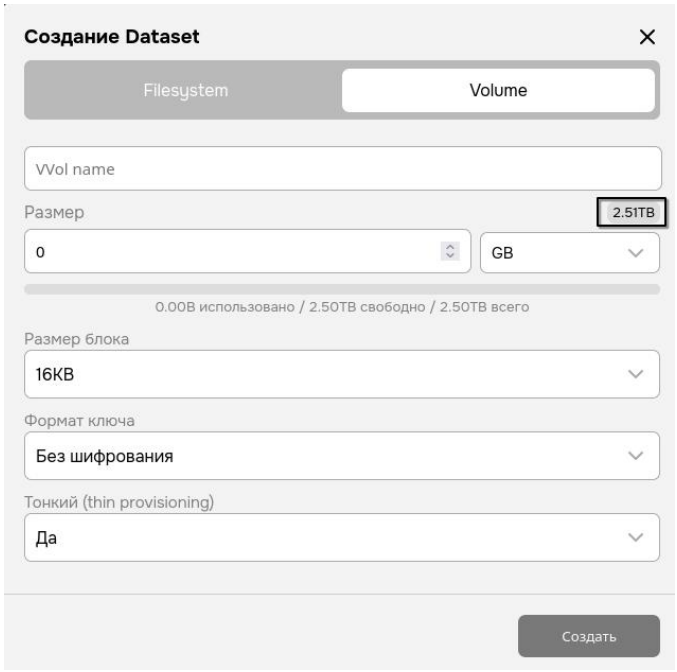

Рисунок 58 – Кнопка «Использовать весь объем»

После успешного создания тома, он появится в пуле (см. рисунок 59).

Рисунок 59 – Виртуальный том

У виртуальных томов так же, как и у наборов данных есть свои уникальные свойства (см. рисунок 60). Подробнее о настройках описано в пункте 4.13.

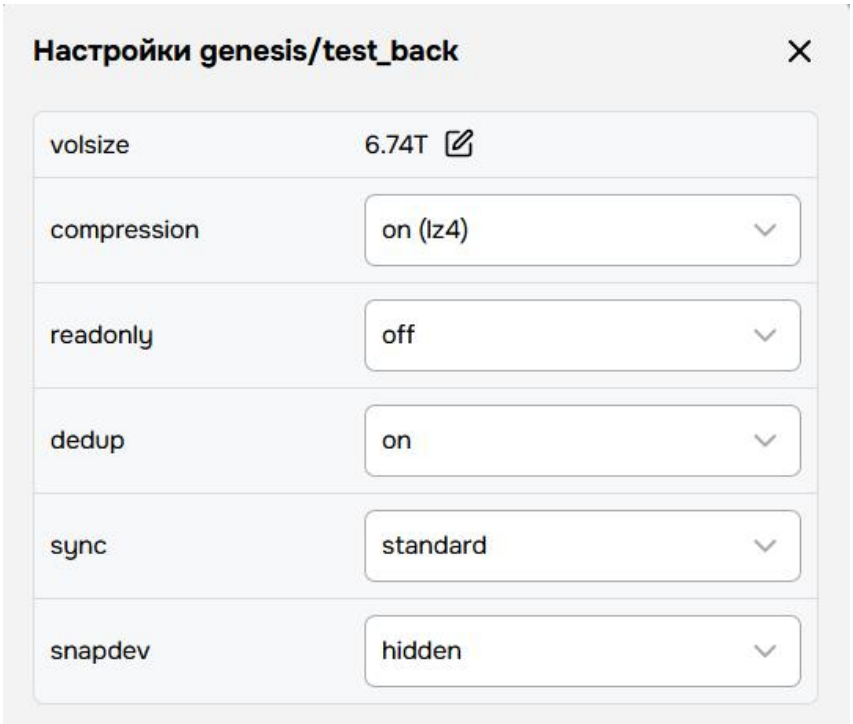

Рисунок 60 – Опции виртуального тома

Удаление виртуальных томов и наборов данных осуществляется нажатием на «корзину» (см. рисунок 61).

Рисунок 61 – Удаление vvol/dataset

4.5 Fibre Channel

Перейдя на вкладку Fibre Channel, появится возможность наблюдать за доступными портами (см. рисунок 62).

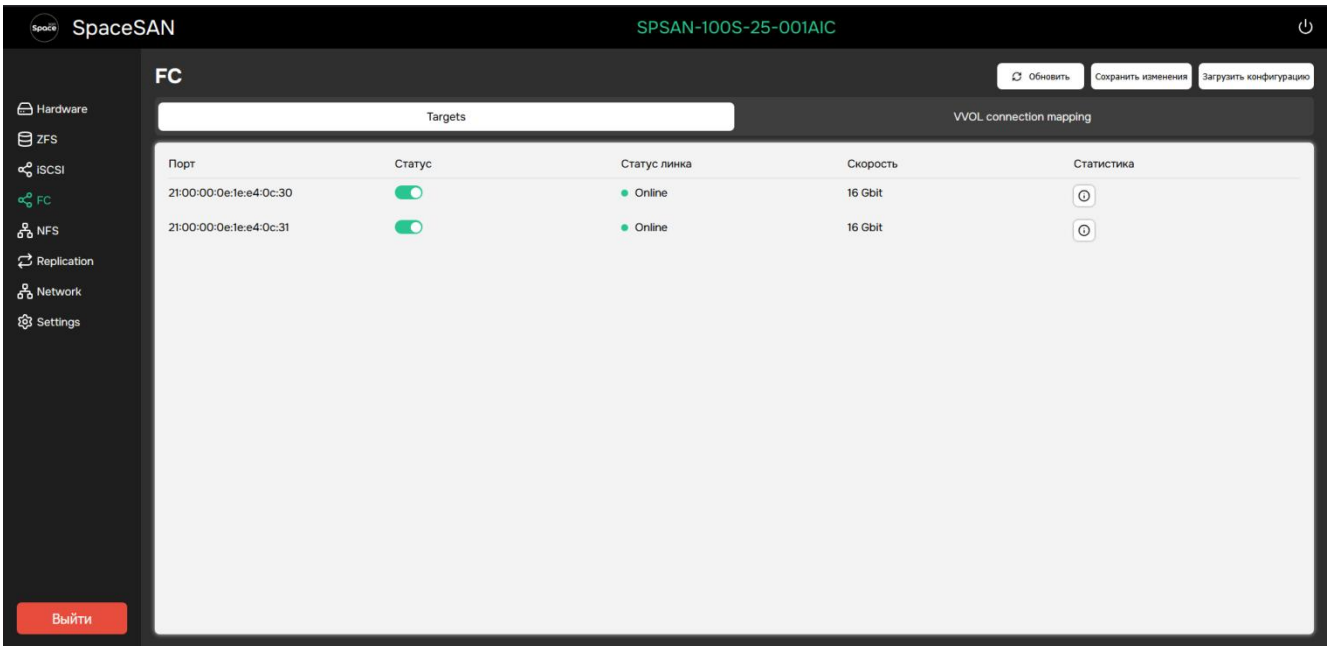

Рисунок 62 – Fibre Channel

В данном окне отображается статус физического соединения, его скорость и статистика передачи данных (см. рисунок 63).

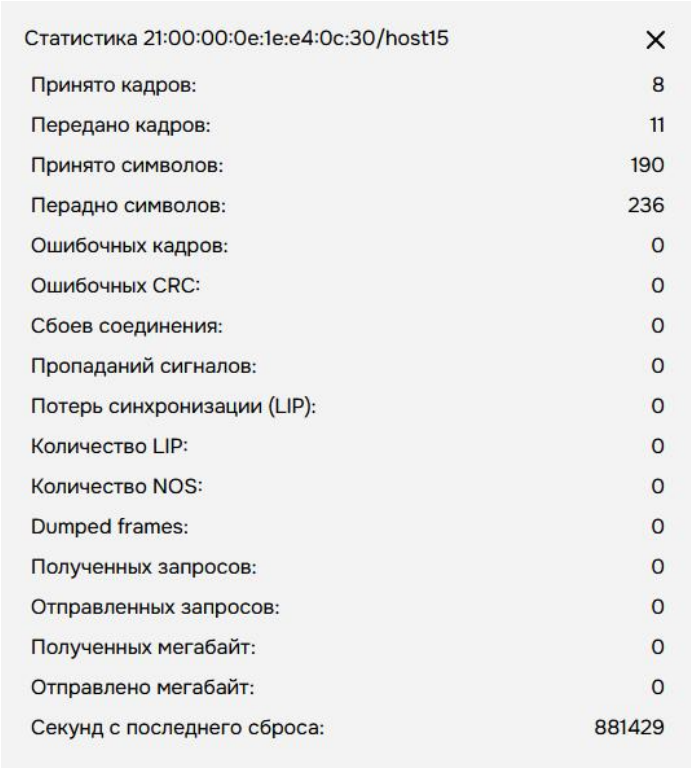

Рисунок 63 – Окно статистики порта

Для активации порта следует нажать на него ЛКМ и переключить ползунок на активное состояние (см. рисунок 64).

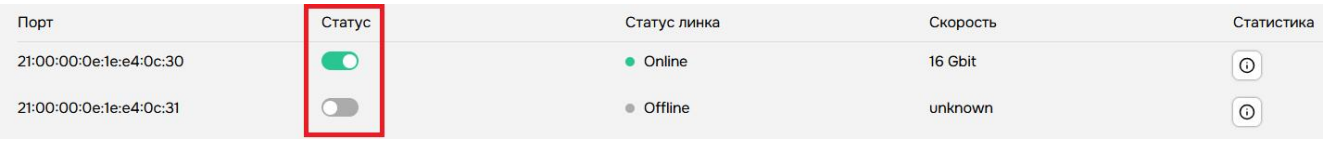

Рисунок 64 – Активация порта

Далее необходимо перейти на вкладку «VVOL connection mapping» (см. рисунок 65).

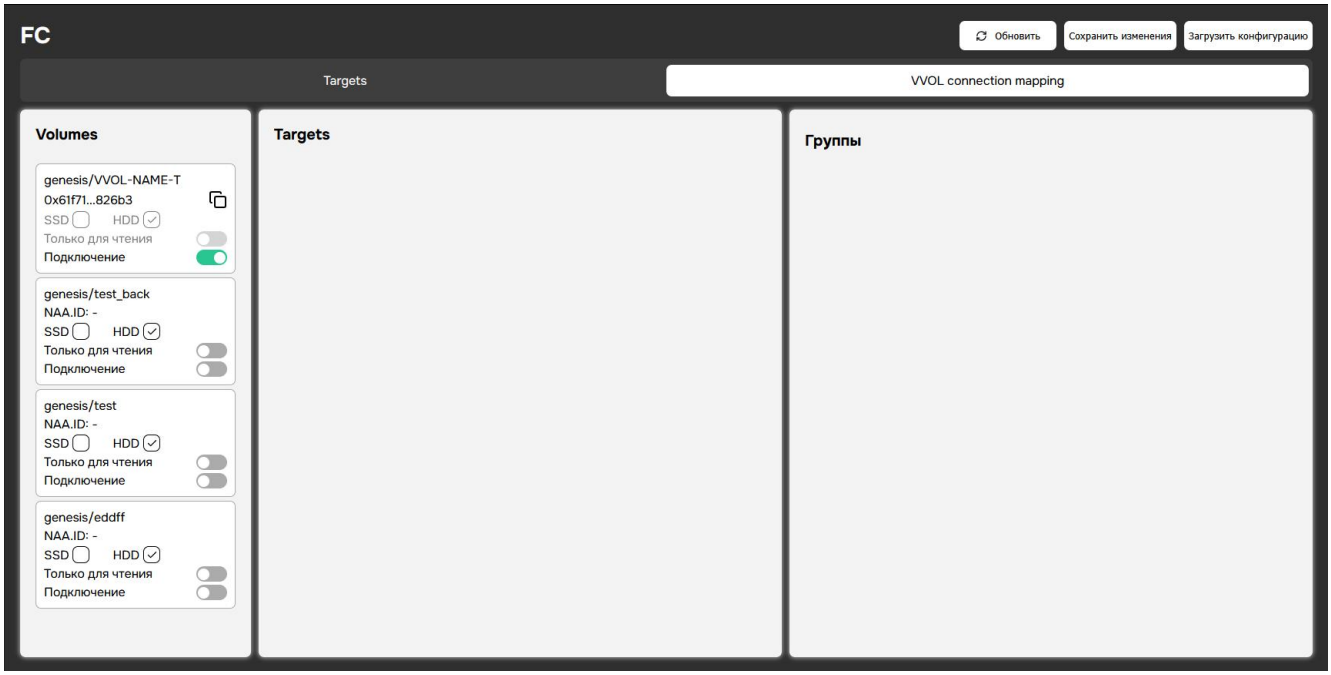

Рисунок 65 – Вкладка «VVOL connection mapping»

Данное окно разделено на три секции. В первой секции «Volumes» отображаются виртуальные тома (VVol). Для начала работы необходимо выбрать тип носителя (SSD или HDD), указать режим доступа «только чтение» при необходимости и выполнить подключение, нажав соответствующую кнопку (см. рисунок 66). Если все сделано правильно появится ID.

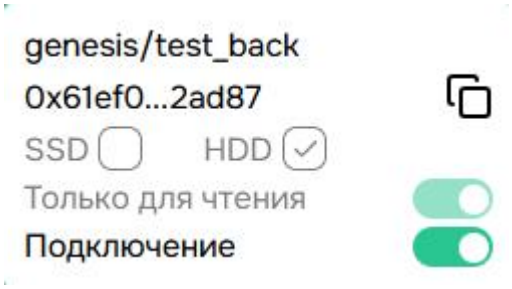

Рисунок 66 – Настройка и подключение VVol

Следующая секция «Targets» предназначена для выбора таргетов, через которые будет осуществляться предоставление виртуального тома (VVol). В данной секции отображается перечень доступных целевых объектов.

Предусмотрена возможность выполнения глобального подключения VVol ко всем таргетам с использованием соответствующей кнопки. Для настройки индивидуального подключения необходимо выбрать конкретный таргет в списке; выбранный таргет подсвечивается, что указывает на его активное состояние. После выбора таргета отображается последняя секция, предназначенная для настройки групп подключений. (см. рисунок 67).

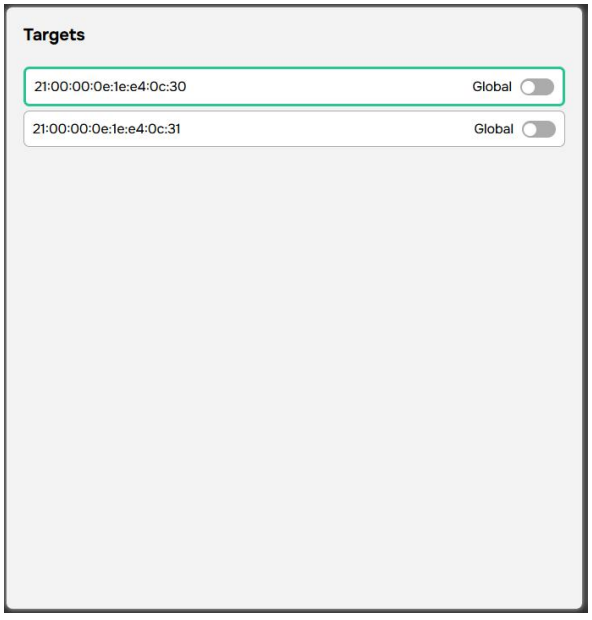

Рисунок 67 – Таргеты

Следующим шагом выполняется настройка групп. С помощью кнопки «Добавить» создаётся новая группа (см. рисунок 68, область 1). Далее, используя соответствующую кнопку, в группу добавляются инициаторы (см. рисунок 68, область 2). При необходимости группу можно скопировать на другой таргет с помощью кнопки «Копировать» (см. рисунок 68, область 3). На завершающем этапе выполняется подключение группы к выбранному таргету с использованием кнопки подключения (см. рисунок 68, область 4).

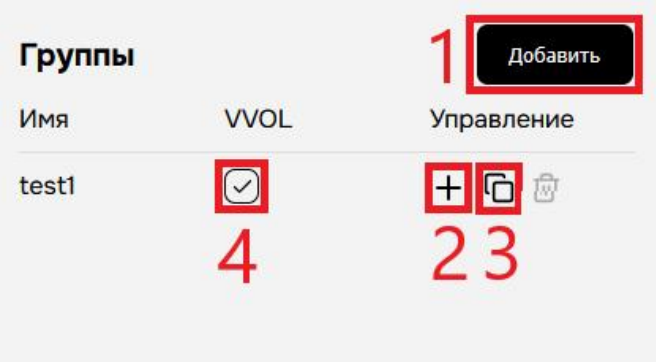

Рисунок 68 – Настройка групп

В завершение конфигурации предусмотрена возможность сохранить внесённые изменения, чтобы они были применены и сохранены после перезагрузки системы, а также выполнить их загрузку с помощью соответствующей кнопки (см. рисунок 69).

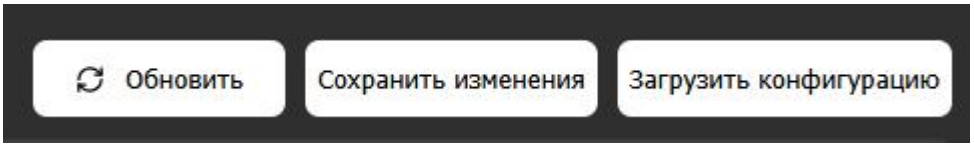

Рисунок 69 – Сохранение и загрузка конфигурации

Аналогичные действия необходимо выполнить со всеми портами Fibre Channel.

4.6 iSCSI

При работе с протоколом iSCSI интерфейс управления во многом аналогичен интерфейсу Fibre Channel. В настоящем разделе приведено

описание только тех элементов и функциональных возможностей, которые отличаются от Fibre Channel и являются специфичными для iSCSI.

При использовании протокола iSCSI во вкладке «Targets» отображается список iSCSI-таргетов с указанием их IQN и текущего состояния (см. рисунок 70). Для каждого таргета предусмотрено управление его состоянием, а также операции добавления и удаления таргетов.

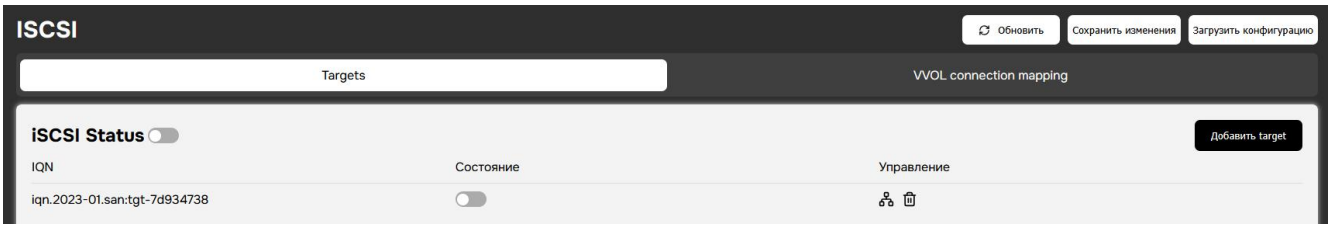

Рисунок 70 – Протокол iSCSI

Для создания нового таргета используется кнопка «Добавить target». После выбора таргета доступна настройка параметров подключения, включая порталы и инициаторы.

В окне настройки таргета администратор может выбрать IP-адреса порталов, через которые будет доступен таргет, а также задать список инициаторов, которым разрешено подключение (см. рисунок 71). Добавление инициаторов выполняется вручную с возможностью поэлементного управления списком.

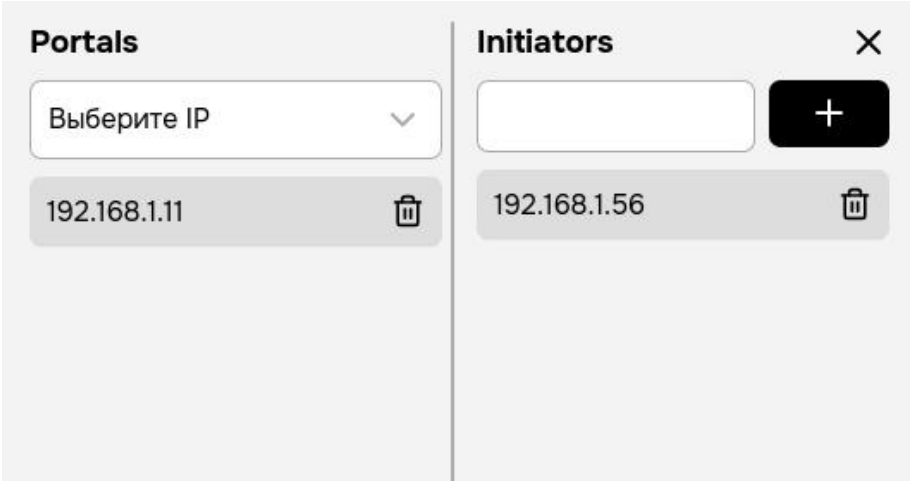

Рисунок 71 – Настройка портала и инициаторов

При добавлении инициаторов в группу необходимо указать их идентификаторы IQN, используемые для аутентификации и управления доступом инициаторов к соответствующему таргету (см. рисунок 72)

Рисунок 72 – Доступ инициаторов к таргету

4.7 NFS

Раздел «NFS-соединения» предназначен для управления экспортами файловых систем по протоколу NFS (см. рисунок 73). В верхней части интерфейса располагаются элементы обновления данных и кнопка создания нового NFS-соединения.

Рисунок 73 – Раздел NFS

Для создания нового NFS-соединения необходимо нажать кнопку «Создать соединение», после чего открывается окно добавления NFS-экспорта (см. рисунок 74).

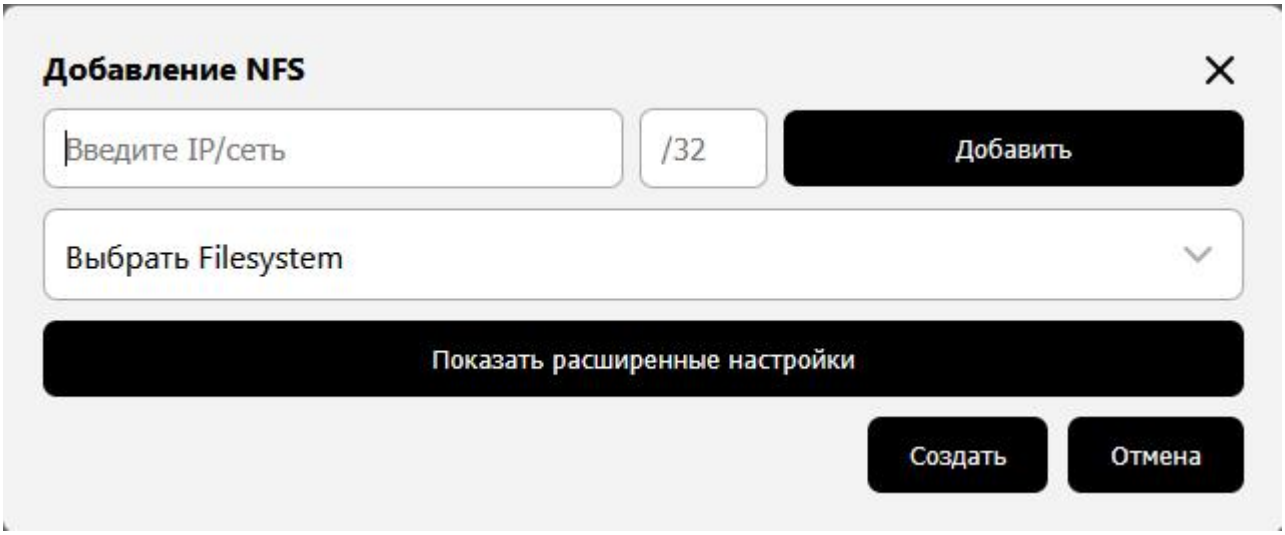

Рисунок 74 – Создание нового NFS-соединения

В окне добавления NFS указывается IP-адрес или подсеть клиента, также для глобальной раздачи можно использовать «*», которому предоставляется доступ, а также выбирается файловая система, предназначенная для экспорта. После выбора и заполнения основных параметров, администратор может перейти к расширенным настройкам, используя соответствующую кнопку (см. рисунок 75).

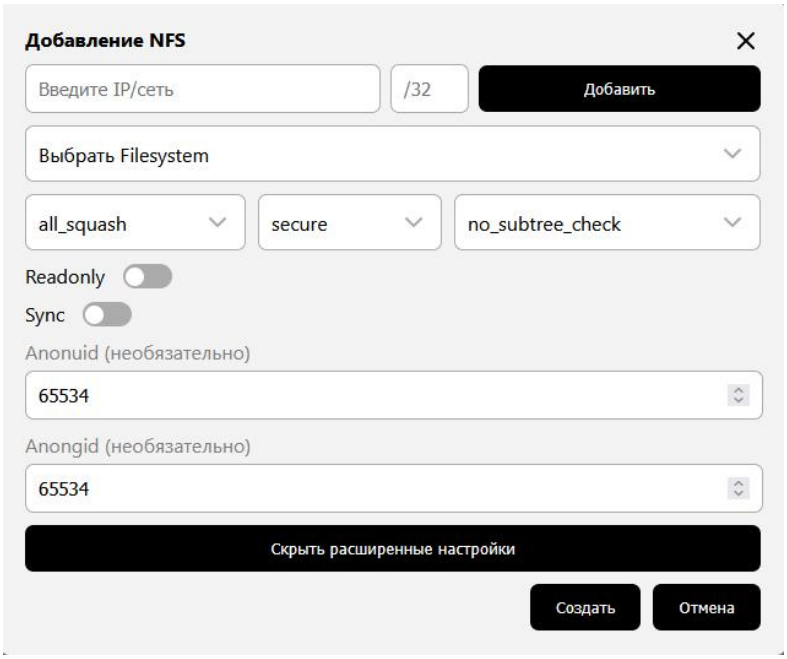

Рисунок 75 – Расширенные настройки

В разделе расширенных настроек доступны параметры управления доступом и поведением NFS-экспорта, включая режимы сопоставления пользователей, параметры безопасности, настройки проверки подкаталогов, а также параметры синхронной записи и режима «только чтение». При необходимости могут быть заданы значения анонимных идентификаторов пользователя и группы (Anonuid и Anongid).

Режимы сопоставления пользователей (user mapping)

Данные параметры определяют, каким образом идентификаторы пользователей и групп на клиентской системе сопоставляются с пользователями на сервере NFS.

root_squash — пользователь root на клиенте сопоставляется с анонимным пользователем на сервере. Используется по умолчанию и рекомендуется для повышения безопасности, так как предотвращает полный административный доступ клиента к данным на сервере.

no_root_squash — пользователь root на клиенте сохраняет права root на сервере. Применяется только в доверенных средах, так как значительно снижает уровень безопасности.

all_squash — все пользователи клиента сопоставляются с анонимным пользователем. Используется для общего доступа, когда не

требуется различать пользователей на сервере.

no_all_squash — пользователи клиента сопоставляются со своими реальными UID/GID. Применяется в средах с согласованными учетными записями между сервером и клиентами.

Параметры безопасности:

Определяют, с каких портов клиенты могут подключаться к NFS-серверу.

- secure — разрешает подключения только с привилегированных портов (обычно <1024). Рекомендуемый режим, так как считается более безопасным.
- insecure — разрешает подключения с любых портов. Может потребоваться для некоторых клиентов или контейнеризированных сред, но снижает уровень безопасности.

Настройки проверки подкаталогов (subtree check)

- subtree_check — сервер выполняет дополнительную проверку, что файл действительно находится в экспортируемом подкаталоге. Повышает корректность, но может снижать производительность и вызывать ошибки при перемещении файлов.
- no_subtree_check — проверка подкаталогов отключена. Рекомендуется для большинства сценариев, так как повышает производительность и стабильность работы.

Параметры синхронной записи (Sync)

- sync (включено) — данные записываются на физический носитель до подтверждения операции клиенту. Обеспечивает максимальную целостность данных, но снижает производительность.
- async (выключено) — сервер может подтверждать запись до фактической записи данных на диск. Повышает производительность, но увеличивает риск потери данных при сбое.

Режим «только чтение» (Readonly)

- Read-only — клиентам разрешено только чтение данных. Используется для справочных данных или в целях безопасности.
- Read-write — клиентам разрешены операции чтения и записи.

Анонимные идентификаторы пользователя и группы (Anonuid и

Anongid)

- Anonuid — UID, под которым будут выполняться операции анонимного пользователя на сервере.
- Anongid — GID, под которым будут выполняться операции анонимной группы.

После завершения настройки параметров NFS-соединения создание экспорта подтверждается нажатием кнопки «Создать». В случае отказа от операции используется кнопка «Отмена».

После создания NFS-соединения оно отображается в общем списке экспортов (см. рисунок 76). В списке указывается путь экспортируемой файловой системы, а также дополнительные элементы управления, расположенные в карточке соединения.

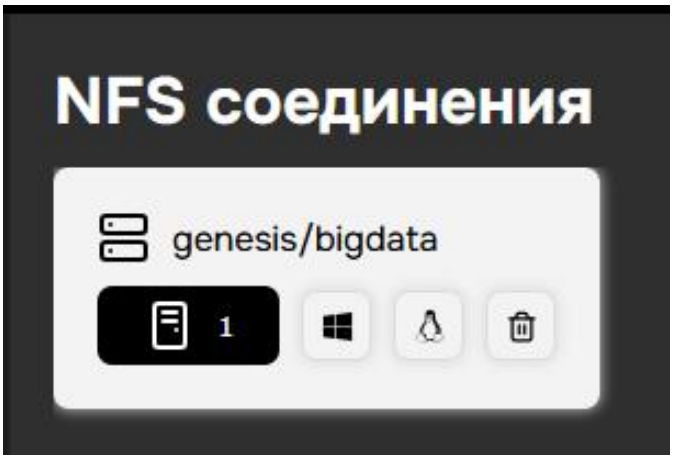

Рисунок 76 – Расширенные настройки

Для каждого NFS-соединения доступны следующие операции:

- Просмотр списка клиентов, которым разрешён доступ к данному экспорту;
- Получение команд подключения для клиентских операционных систем Windows и Linux;
- Удаление экспорта.

Функция просмотра разрешённых подключений позволяет определить, каким IP-адресам, подсетям или клиентам предоставлен доступ к данному NFS-экспорту в соответствии с его параметрами. Это позволяет администратору оперативно проверить, для каких узлов был опубликован ресурс.

Отдельная кнопка предназначена для отображения команд подключения NFS-экспорта с клиентских систем. Интерфейс предоставляет готовые варианты подключения для операционных систем Windows и Linux, что упрощает использование ресурса на различных платформах.

При подключении из Linux используется стандартная команда монтирования NFS с указанием адреса сервера, экспортируемого пути и локальной точки монтирования.

При подключении из Windows используется встроенный клиент NFS. В зависимости от конфигурации возможно как подключение с сопоставлением пользователей, так и подключение в анонимном режиме. Для анонимного подключения может использоваться параметр anon, при котором клиент подключается без передачи учетных данных, а сервер рассматривает доступ как анонимный.

В случае анонимного подключения, а также при отсутствии корректного сопоставления пользователей, сервер применяет параметры Anonuid и Anongid, определяющие пользователя и группу, от имени которых выполняются операции. Это означает, что фактический доступ к файлам и каталогам определяется правами файловой системы и ACL, назначенными для соответствующего UID и GID.

По умолчанию в большинстве реализаций NFS используются следующие значения:

- Anonuid = 65534
- Anongid = 65534

Данные значения соответствуют системному пользователю типа nobody и применяются в сценариях анонимного доступа или отсутствия сопоставления учетных записей.

При использовании клиентов Windows отсутствие корректной настройки сопоставления пользователей может приводить к ошибкам доступа, включая невозможность создания или изменения файлов. Одной из распространённых причин является отсутствие или некорректная настройка параметров AnonymousUid и AnonymousGid в реестре Windows.

Для устранения данной проблемы необходимо проверить

наличие следующих параметров:

”HKEY_LOCAL_MACHINE\Software\Microsoft\ClientForNFS\CurrentVersion\Default”

При отсутствии параметров необходимо добавить:

- AnonymousUid — идентификатор пользователя (например, 65534);
- AnonymousGid — идентификатор группы (например, 65534).

После внесения изменений требуется повторно выполнить монтирование NFS-ресурса, чтобы новые параметры вступили в силу.

Корректная настройка данных параметров обеспечивает согласованность прав доступа между клиентом и сервером. При этом необходимо учитывать, что при анонимном подключении все операции выполняются от имени пользователя, заданного через Anonuid и Anongid, поэтому соответствующему UID и GID должны быть предоставлены необходимые права доступа на уровне файловой системы и ACL.

Кнопка удаления используется для исключения NFS-экспорта из конфигурации системы. После удаления ресурс становится недоступным для клиентов.

Обновление информации о состоянии NFS-соединений выполняется автоматически, а также может быть инициировано вручную с использованием кнопки обновления, расположенной в верхней части интерфейса.

4.8 SMB

Раздел «SMB» предназначен для управления файловыми ресурсами, предоставляемыми по протоколу SMB. Данный раздел позволяет администратору создавать сетевые ресурсы, настраивать права доступа к каталогам файловой системы, управлять учетными записями пользователей и групп, а также задавать основные параметры работы сервиса SMB (см. рисунок 77).

В верхней части интерфейса располагаются элементы управления, включающие кнопку «Обновить», предназначенную для обновления информации о текущем состоянии ресурсов, и кнопку «Создать ресурс», предназначенную для создания нового сетевого ресурса SMB.

В центральной части страницы отображается таблица существующих SMB-ресурсов. Для каждого ресурса указывается его имя, путь к каталогу файловой системы, состояние гостевого режима, а также элементы управления. С помощью переключателя гостевого режима администратор может разрешить или запретить доступ к ресурсу без обязательной аутентификации пользователя. В колонке управления располагаются элементы для перехода к настройкам ACL доступа к ресурсу и удаления ресурса из системы.

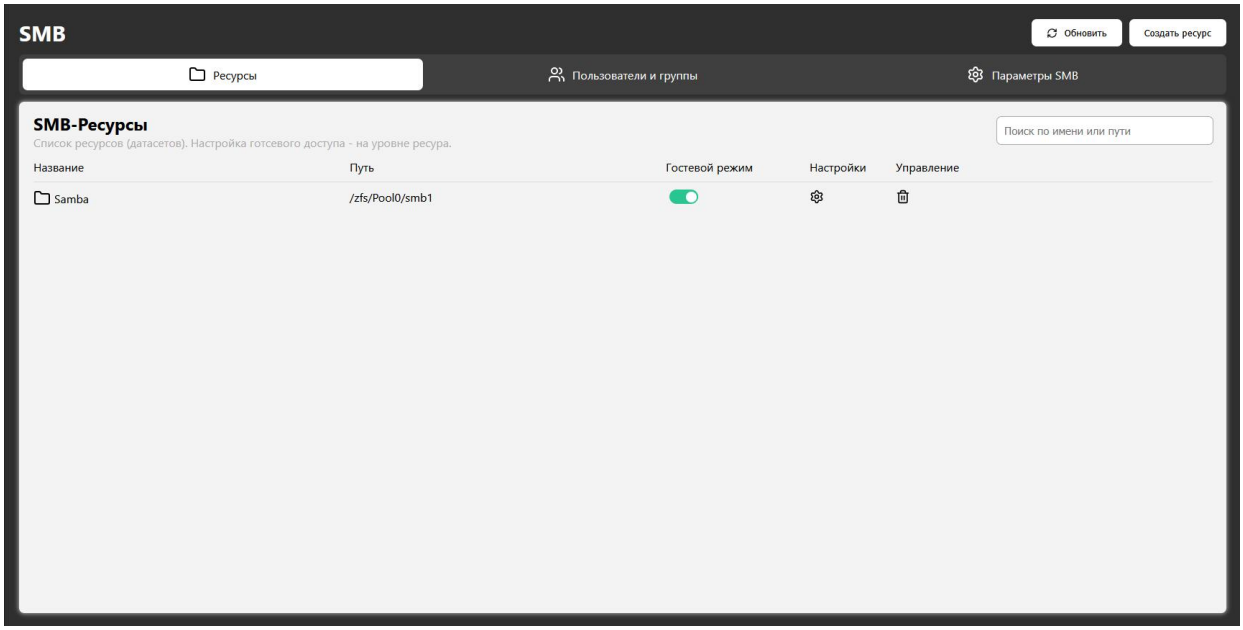

Рисунок 77 – Раздел SMB

Для создания нового сетевого ресурса необходимо нажать кнопку «Создать ресурс», после чего открывается окно создания ресурса (см. рисунок 78). В данном окне администратор указывает каталог файловой системы, который будет опубликован по протоколу SMB, а также имя сетевого ресурса. Каталог выбирается из доступных путей файловой системы, после чего вводится имя ресурса, под которым он будет отображаться в сети.

После заполнения необходимых параметров создание ресурса подтверждается нажатием кнопки «Создать». В случае отказа от выполнения операции используется кнопка «Отмена», закрывающая окно без сохранения изменений.

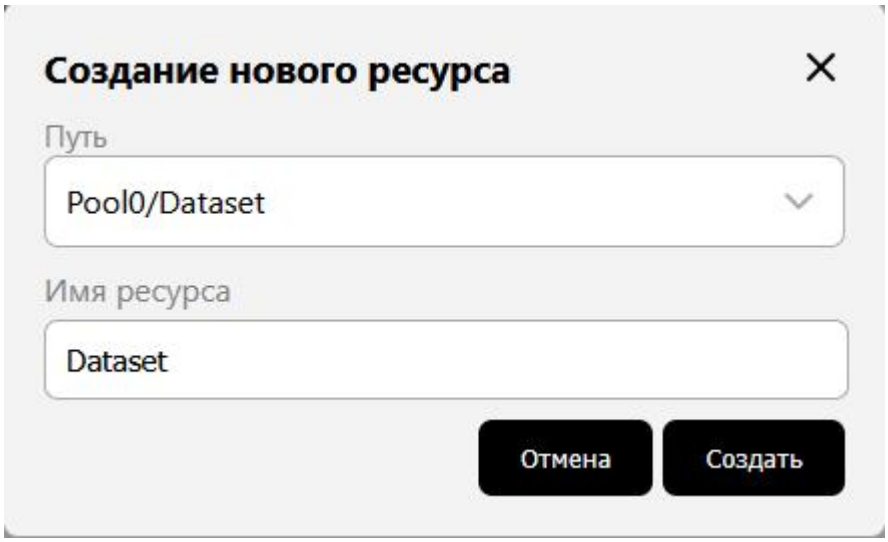

Рисунок 78 – Создание SMB-ресурса

После создания ресурс автоматически добавляется в общий список SMB-ресурсов и становится доступным для дальнейшего администрирования. Из списка ресурсов администратор может перейти к настройке параметров доступа, а также управлять правами пользователей и групп.

Для настройки прав доступа к каталогу ресурса используется окно управления списками контроля доступа через ACL (см.рисунок 79). Данный механизм позволяет назначать права на доступ к ресурсу отдельным пользователям или группам пользователей.

В верхней части окна администратор выбирает тип субъекта доступа. В качестве субъекта может выступать пользователь или группа пользователей. После выбора типа субъекта из списка выбирается конкретная учетная запись или группа, для которой необходимо задать права доступа.

Далее настраиваются разрешения доступа. Интерфейс позволяет назначить следующие типы прав:

Чтение — предоставляет возможность просматривать содержимое файлов и каталогов;

Запись — позволяет создавать новые файлы, а также изменять или удалять существующие;

Выполнение — разрешает выполнение файлов и переход по каталогам.

После выбора требуемых прав доступ сохраняется нажатием кнопки «Сохранить». Добавленные субъекты отображаются в таблице ниже, где указываются имя субъекта, его тип и назначенный уровень доступа. Для каждой записи ACL доступны операции редактирования параметров доступа или удаления записи.

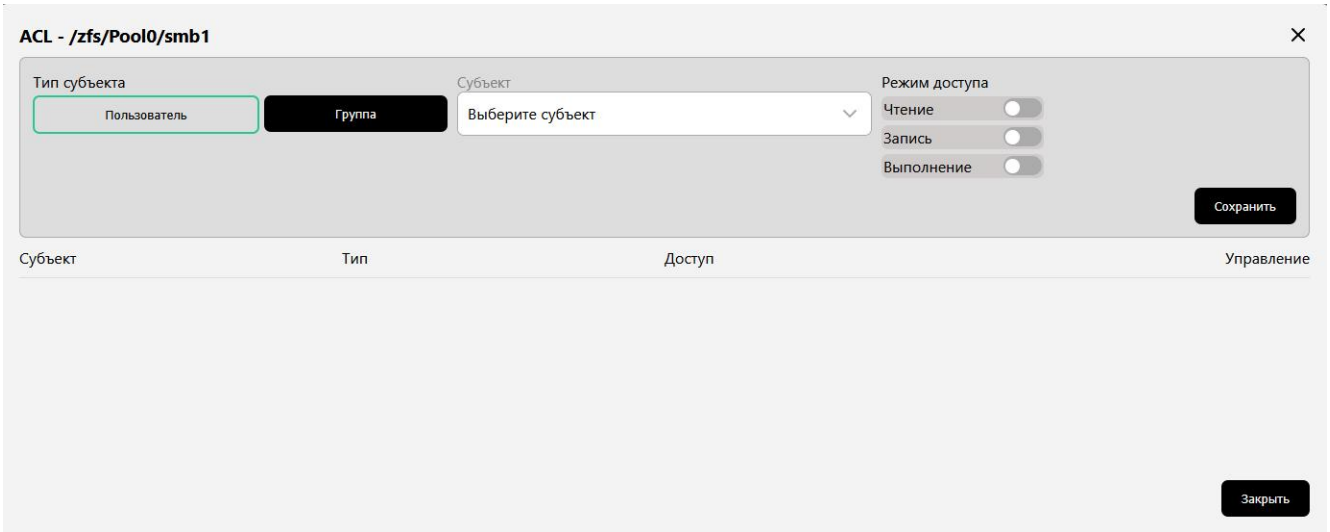

Рисунок 79 – Настройка ACL ресурса

Для управления учетными записями пользователей и групп используется вкладка «Пользователи и группы», интерфейс которой представлен на рисунке 80. Данный раздел предназначен для создания пользователей, формирования групп и последующего использования этих объектов при назначении прав доступа к SMB-ресурсам.

Интерфейс раздела разделён на две функциональные области. В левой части располагается таблица пользователей. Для каждого пользователя отображается его имя, количество групп, в которые он включён, а также элементы управления учетной записью. Администратор может управлять параметрами пользователя, изменять его настройки или удалять учетную запись.

В правой части интерфейса располагается таблица групп. Для каждой группы отображается её имя, количество пользователей, входящих в данную группу, и элементы управления. Использование групп позволяет упростить управление доступом, так как права могут назначаться сразу группе пользователей, а не каждой учетной записи

отдельно.

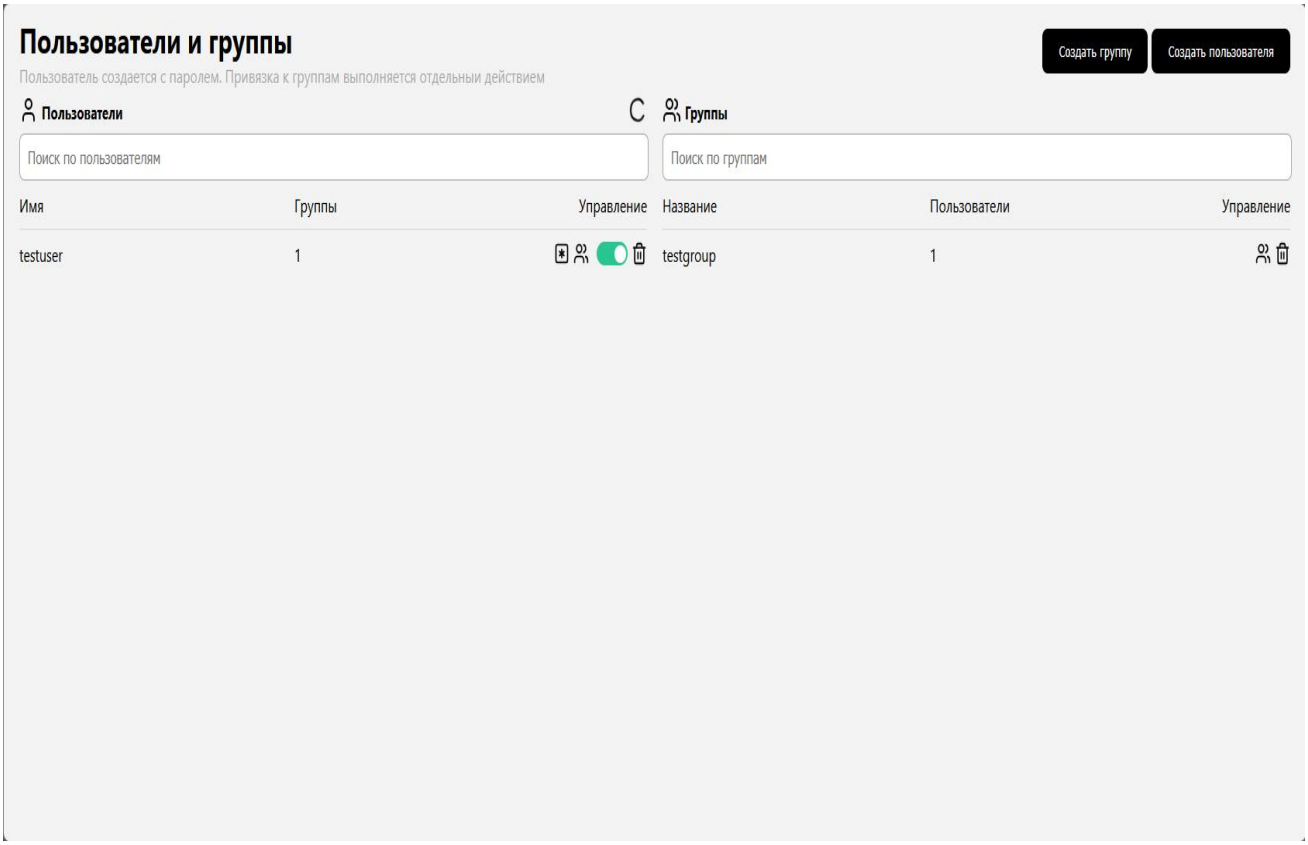

Рисунок 80 – Пользователи и группы

Для добавления нового пользователя используется кнопка «Создать пользователя», после нажатия которой открывается окно создания пользователя (см. рисунок 81). В данном окне необходимо указать имя пользователя, а также задать пароль и его подтверждение. Минимальная длина пароля составляет восемь символов.

После заполнения всех обязательных полей создание пользователя подтверждается нажатием кнопки «Создать». Если операция не требуется, окно можно закрыть с помощью кнопки «Отмена».

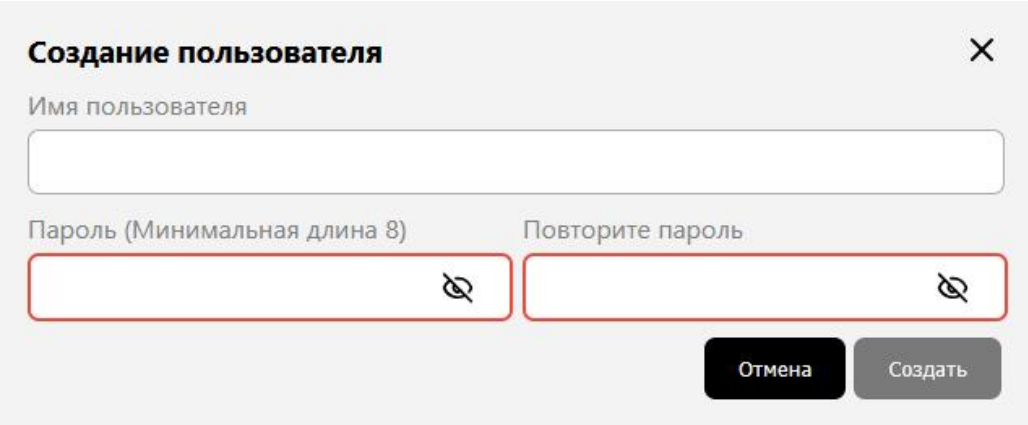

Рисунок 81 – Создание пользователя

Создание новой группы выполняется с использованием кнопки «Создать группу», расположенной в разделе управления группами. После нажатия данной кнопки открывается окно создания группы (см. рисунок 82). В форме необходимо указать название новой группы, после чего создание подтверждается нажатием кнопки «Создать».

Созданные группы могут использоваться для объединения пользователей и последующего назначения прав доступа к SMB-ресурсам.

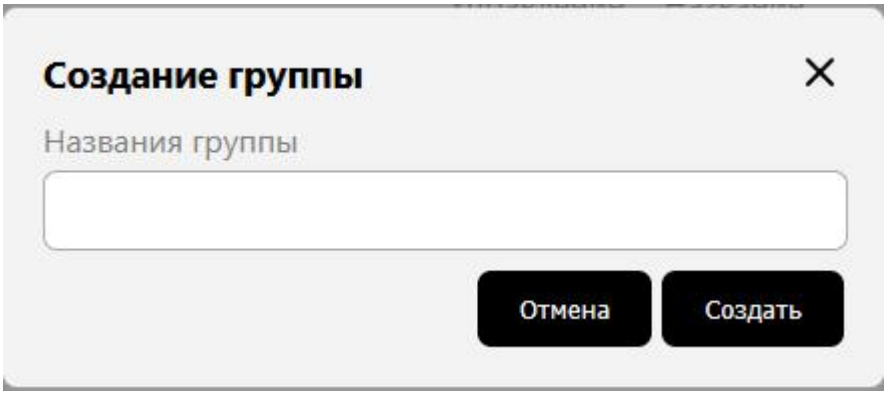

Рисунок 82 – Создание группы

В разделе управления пользователями предусмотрены дополнительные элементы администрирования учетных записей. Интерфейс данных элементов представлен на рисунке 83.

В таблице пользователей доступны следующие функции управления:

изменение пароля пользователя;

настройка принадлежности пользователя к группам;

включение или отключение учетной записи пользователя;

удаление пользователя из системы.

Эти функции позволяют администратору централизованно управлять параметрами учетных записей и контролировать доступ пользователей к SMB-ресурсам.

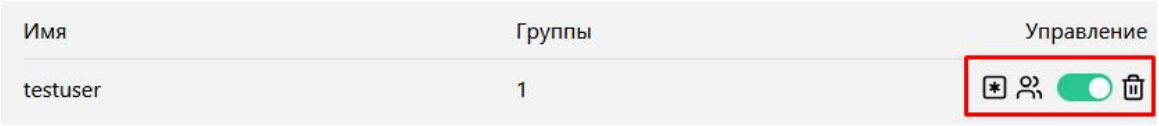

Рисунок 83 – Элементы управления пользователями

При выборе функции настройки принадлежности пользователя к группам открывается окно управления группами пользователя, представленное на рисунке 84.

В данном интерфейсе отображаются две области: список всех доступных групп и список групп, в которые включён пользователь. Администратор может добавить пользователя в одну или несколько групп либо удалить его из ранее назначенных групп. После выполнения необходимых изменений настройки сохраняются нажатием кнопки «Сохранить», либо отменяются нажатием кнопки «Отмена».

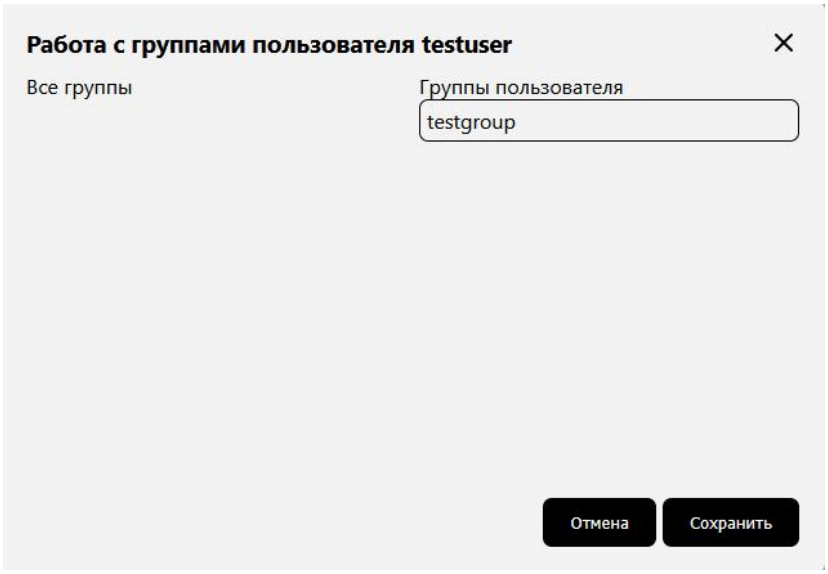

Рисунок 84 – Управление группами пользователя

Аналогичный механизм используется для управления составом группы. При выборе соответствующего элемента управления в таблице групп открывается окно редактирования состава группы, представленное на рисунке 85.

В данном окне отображается список всех пользователей системы и список пользователей, входящих в выбранную группу. Администратор может добавлять пользователей в группу или удалять их из неё. Такой подход упрощает централизованное управление правами доступа, поскольку доступ к ресурсам может назначаться группе пользователей.

После завершения изменения состава группы необходимо нажать кнопку «Сохранить» для применения настроек. Для отмены изменений используется кнопка «Отмена».

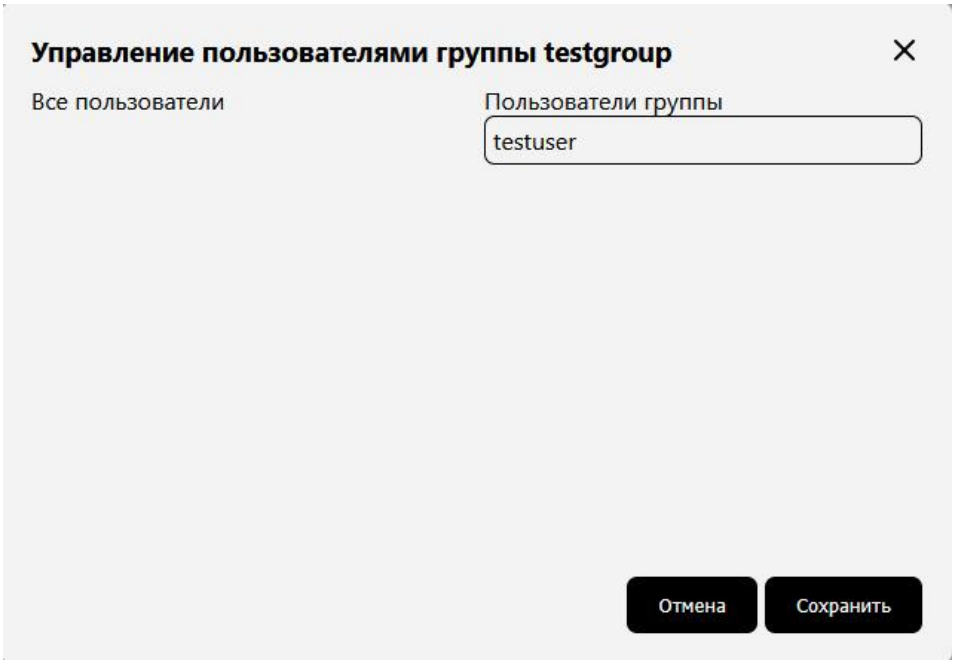

Рисунок 85 – Управление пользователями группы

Раздел настройки параметров SMB (см. рисунок 86) предоставляет администратору возможность задать базовые параметры функционирования сервиса, влияющие на совместимость с клиентскими системами, уровень безопасности и режим доступа.

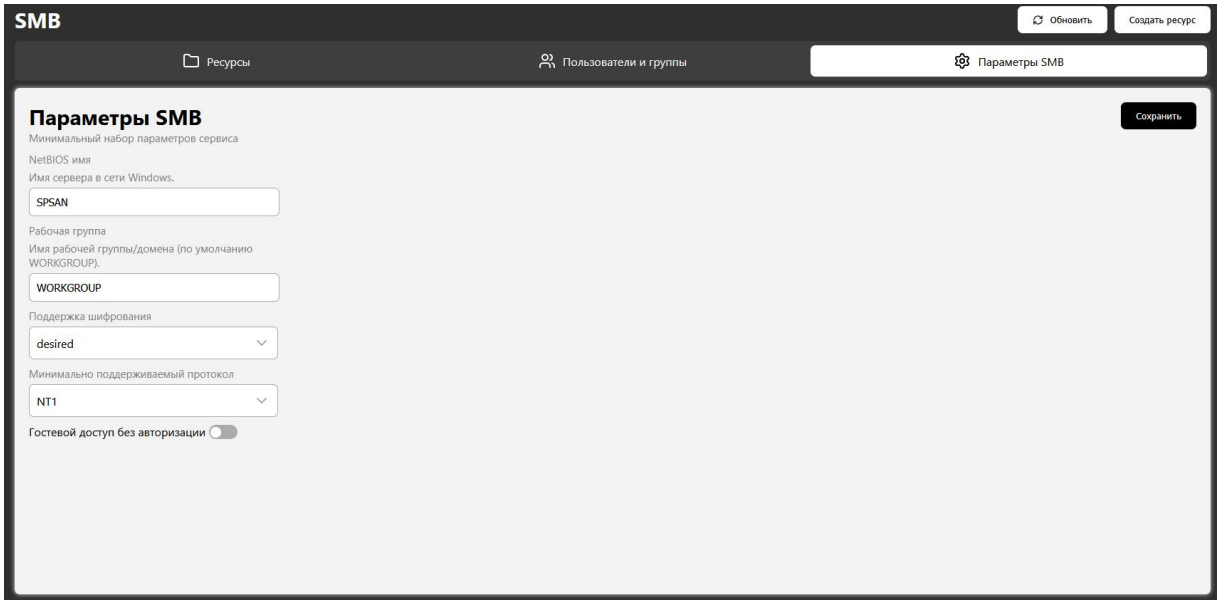

Рисунок 86 – Параметры SMB

В данном разделе доступны параметры, определяющие сетевое представление сервера и поведение протокола SMB.

Параметр NetBIOS имя задаёт имя сервера, под которым он будет отображаться в сетевом окружении Windows. Данное имя используется клиентскими устройствами при обнаружении сервера и подключении к нему.

Параметр Рабочая группа определяет логическую группу или домен, к которому относится сервер. По умолчанию используется значение WORKGROUP. Данный параметр необходим для корректной интеграции в локальные сети Windows без доменной инфраструктуры.

Параметр Поддержка шифрования определяет режим использования SMB-шифрования при взаимодействии клиента и сервера. Доступны следующие режимы:

off — шифрование отключено. Передача данных выполняется без дополнительной защиты средствами SMB-шифрования. Данный режим используется в доверенных или изолированных сетях, а также в случаях, когда требуется обеспечить совместимость со старыми клиентскими системами. Может применяться при работе с Windows 7 и более ранними версиями, а также в сценариях, где приоритетом является

совместимость или производительность;

desired — шифрование используется только в том случае, если клиентская система его поддерживает. Если клиент не поддерживает SMB-шифрование, соединение всё равно будет установлено без шифрования. Такой режим целесообразно использовать в смешанных инфраструктурах, где одновременно присутствуют современные и устаревшие клиентские системы. Может использоваться при наличии клиентов Windows 7, для которых требуется сохранить возможность подключения, а также более новых версий Windows;

required — использование шифрования является обязательным. Соединение устанавливается только с теми клиентами, которые поддерживают SMB-шифрование. Если клиент не поддерживает данный механизм, подключение будет отклонено. Такой режим рекомендуется применять в средах с повышенными требованиями к защите данных. Практически ориентирован на использование с клиентами Windows 10 и более новых версий.

Выбор режима шифрования зависит от требований к безопасности и состава клиентских операционных систем. Если в инфраструктуре используются устаревшие рабочие станции, в том числе Windows 7, рекомендуется применять режимы off или desired. Если подключение должны выполнять только современные клиентские системы, например Windows 10 и выше, рекомендуется использовать режим required.

Параметр «Минимально поддерживаемый протокол» определяет минимальную версию протокола SMB, с которой сервер принимает соединения от клиентов. Доступны следующие варианты:

NT1 (SMB1) — устаревшая версия протокола SMB. Обладает низким уровнем безопасности и не рекомендуется к использованию. Может применяться только для обеспечения совместимости со старыми операционными системами и оборудованием;

SMB2 — более современная версия протокола, обеспечивающая улучшенную производительность и безопасность по сравнению с SMB1. Используется в большинстве современных систем;

SMB3 — актуальная версия протокола, поддерживающая

расширенные возможности, включая шифрование, улучшенную обработку ошибок и более эффективную работу с сетью. Рекомендуется для использования в современных инфраструктурах.

Выбор минимальной версии протокола напрямую влияет на уровень безопасности системы. Рекомендуется использовать SMB2 или SMB3, отключая поддержку SMB1, если это не требуется для совместимости.

Дополнительно в разделе представлен параметр Гостевой доступ без авторизации, который позволяет разрешить подключение к SMB-ресурсам без аутентификации пользователя. При включении данного параметра клиенты могут получать доступ к ресурсам без ввода учетных данных. Рекомендуется использовать на Windows 7.

Использование гостевого доступа рекомендуется только в следующих сценариях:

предоставление общего доступа к не критичным данным;

тестовые или демонстрационные среды;

изолированные сети без требований к аутентификации.

В производственных средах с конфиденциальными данными рекомендуется отключать гостевой доступ и использовать механизм аутентификации пользователей с назначением прав через ACL.

После изменения параметров конфигурации необходимо нажать кнопку «Сохранить» для применения настроек. Изменения вступают в силу для новых подключений клиентов.

Репликации

Раздел «Репликации и снимки» предназначен для управления узлами репликации, заданиями репликации данных и снимками файловых систем (см. рисунок 87). В верхней части интерфейса доступны вкладки перехода между подразделами, а также кнопка обновления отображаемой информации.

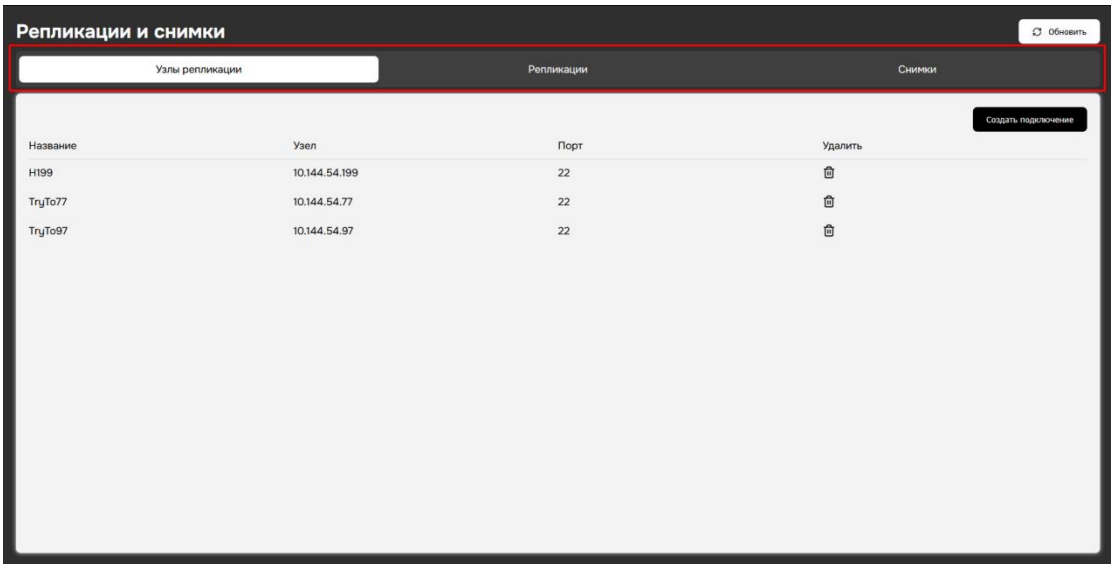

Рисунок 87 – Раздел «Репликации и снимки»

Во вкладке «Узлы репликации» отображается список удалённых узлов, используемых для выполнения репликации данных (см. рисунок 88). Для каждого узла указываются его наименование, адрес, используемый сетевой порт и доступные действия управления.

Рисунок 88 – Список узлов репликации

Для добавления нового узла репликации необходимо нажать кнопку «Создать подключение», после чего открывается окно создания хоста (см. рисунок 89). В данном окне указываются наименование узла,

адрес хоста, сетевой порт, а также учётные данные для подключения, указывает данные «root» пользователя. После заполнения параметров создание узла подтверждается нажатием кнопки «Создать».

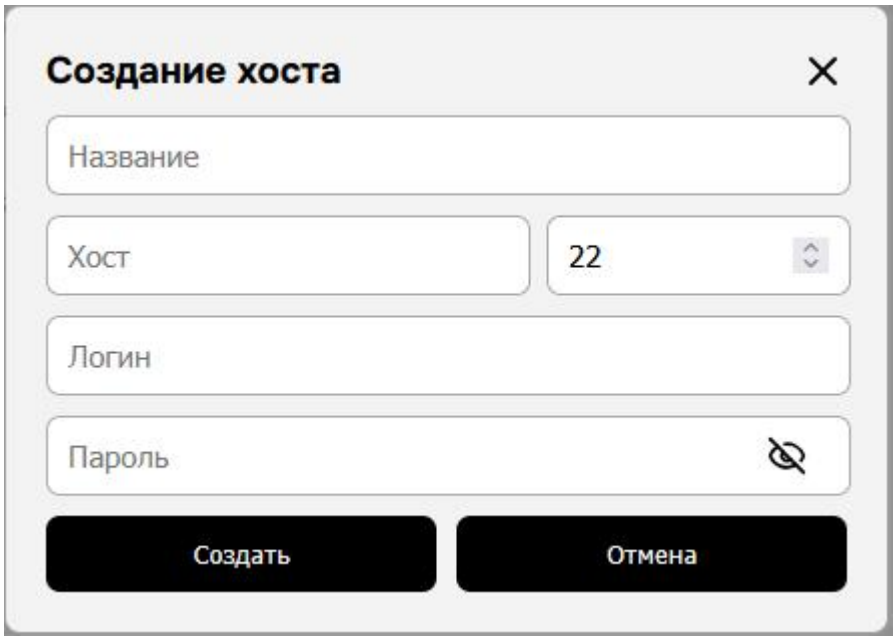

Рисунок 89 – Окно создания узла репликации

Удаление узла репликации выполняется с помощью соответствующей кнопки управления в списке узлов.

Во вкладке «Репликации» отображается список заданий репликации данных (см. рисунок 90). Для каждого задания указываются исходный объект, целевой объект, используемый узел репликации, интервал выполнения, время последнего запуска и состояние последней репликации.

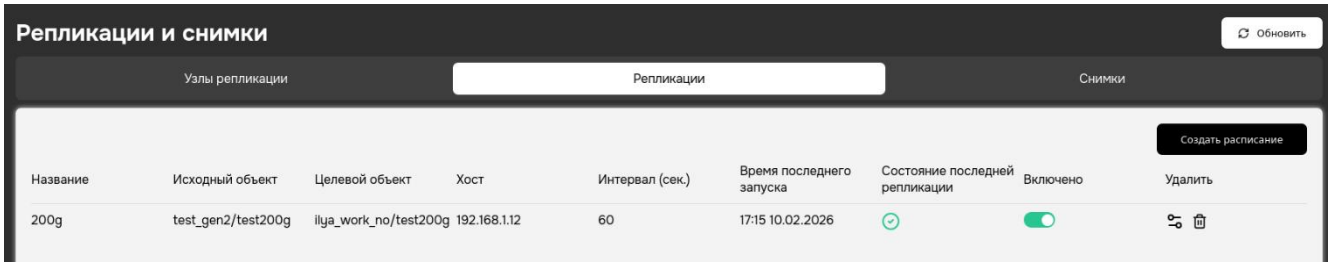

Рисунок 90 – Список заданий репликации

Для создания нового задания репликации необходимо нажать кнопку «Создать расписание», после чего открывается окно создания

репликации (см. рисунок 91). В данном окне указывается наименование задания, исходный dataset, узел репликации и целевой dataset. Также доступна настройка мгновенного запуска и задание интервала выполнения в секундах.

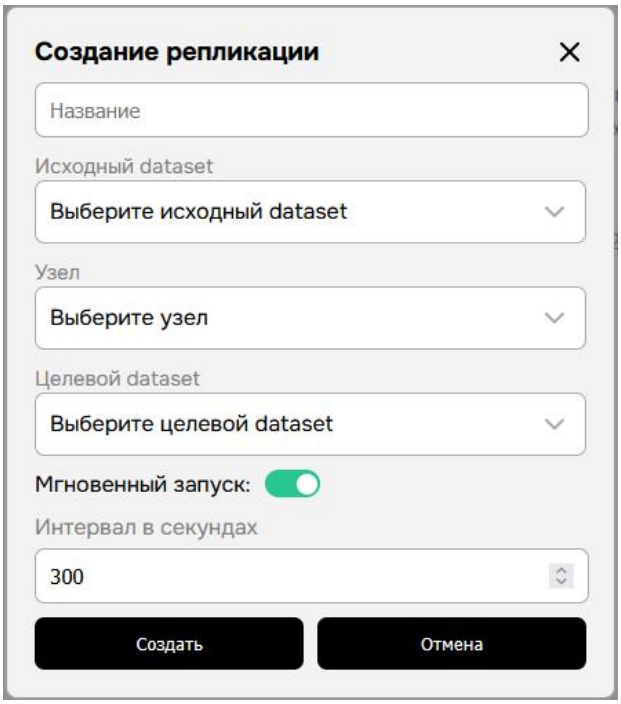

Рисунок 91 – Окно создания задания репликации

Управление заданиями репликации включает возможность включения и отключения расписания, редактирования параметров и удаления задания.

Во вкладке «Снимки» отображается список созданных снимков файловых систем (см. рисунок 92). Для каждого снимка указываются его имя, исходный объект, объём занимаемого пространства, метки и дата создания.

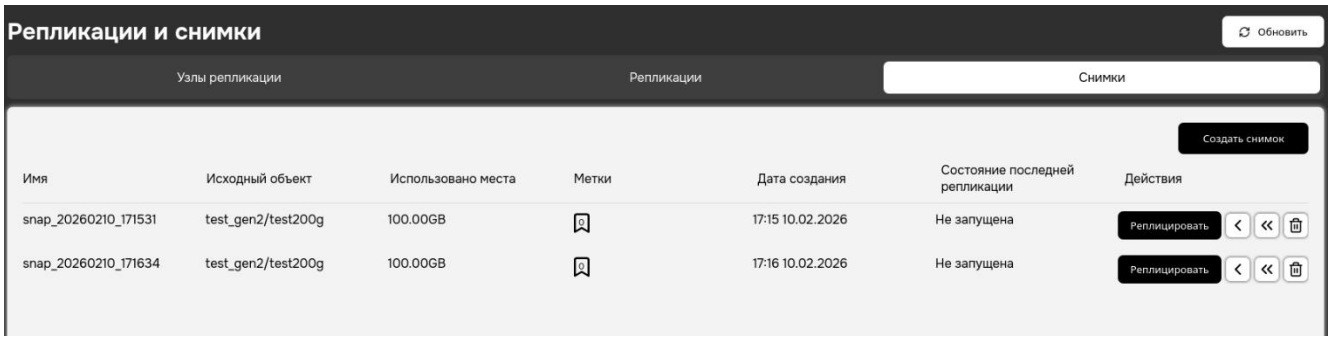

Рисунок 92 – Список снимков файловых систем

В данном разделе доступны операции управления снимками, включая создание нового снимка, запуск репликации на основе выбранного снимка, навигацию между связанными снимками и удаление снимка.

Для создания нового снимка необходимо нажать кнопку «Создать снимок», после чего открывается окно создания снимка (см. рисунок 93). В окне указывается имя снимка и выбирается dataset, для которого будет создан снимок. Создание подтверждается нажатием кнопки «Создать».

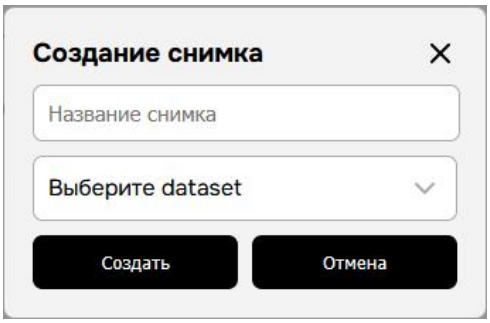

Рисунок 93 – Окно создания снимка

5 Настройки сети

Раздел «Сетевые настройки» предназначен для просмотра и конфигурирования сетевых интерфейсов системы (см. рисунок 94). В данном разделе отображается таблица сетевых устройств с указанием их параметров и текущего состояния.

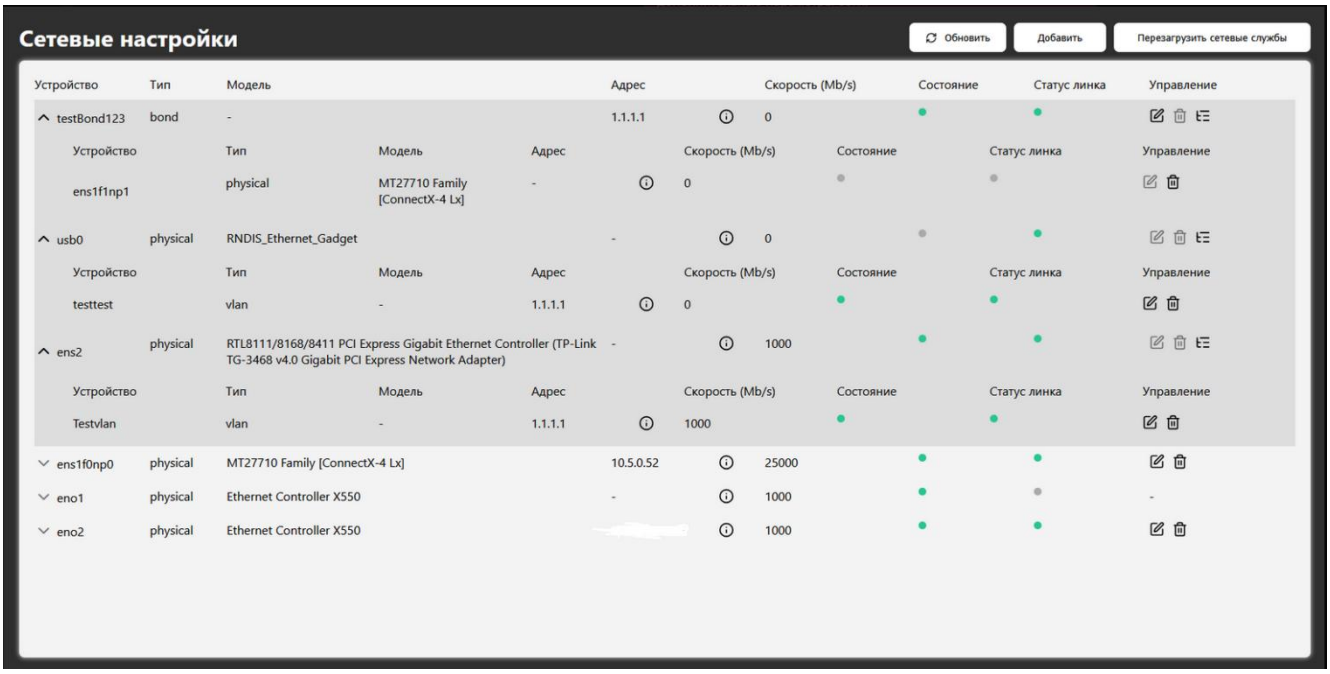

Рисунок 94 – Раздел «Сетевые настройки»

В таблице приведены сведения об имени интерфейса, его типе, модели устройства, назначенном IP-адресе, скорости соединения, значении MTU, общем состоянии интерфейса и статусе физического соединения.

В таблице приведены сведения об имени интерфейса, его типе, модели устройства, назначенном IP-адресе, скорости соединения, значении MTU, общем состоянии интерфейса и статусе физического соединения.

Интерфейс реализует представление сетевых устройств в виде иерархической структуры (дерева зависимостей). Вложенные элементы отображаются в виде раскрывающихся списков, что позволяет визуально отследить взаимосвязи между интерфейсами. Например:

физические интерфейсы могут входить в состав агрегированных интерфейсов (bond);

на физических интерфейсах или bond могут быть созданы виртуальные интерфейсы (VLAN);

интерфейсы могут быть включены в мосты (bridge).

Такое представление позволяет администратору контролировать структуру сети и понимать зависимости между объектами конфигурации.

Для каждого интерфейса доступны операции управления, включая редактирование параметров, удаление конфигурации, а также управление зависимыми элементами.

Для добавления новой сетевой конфигурации необходимо нажать кнопку «Добавить», после чего открывается окно добавления конфигурации (см. рисунок 95).

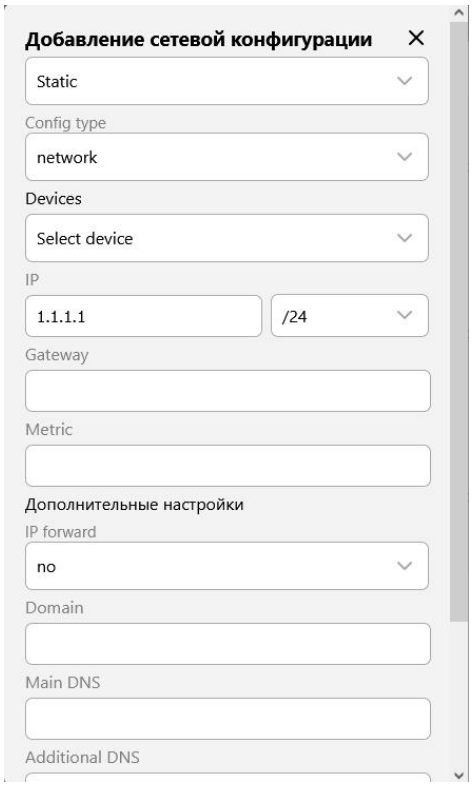

Рисунок 95 – Окно добавления сетевой конфигурации

В окне задаются следующие параметры:
тип конфигурации (DHCP или Static);
тип создаваемого объекта (network, vlan, bond, bridge);
сетевое устройство (или набор устройств);
IP-адрес и маска подсети;
шлюз по умолчанию;
значение metric.
В разделе дополнительных настроек задаются:
параметр IP forward;
доменное имя;
основной DNS-сервер;

дополнительный DNS-сервер;

значение MTU.

При выборе типа network создаётся конфигурация сетевого интерфейса с заданием параметров IP-адресации и сетевых параметров.

При выборе типа vlan создаётся виртуальный интерфейс VLAN. Указываются имя виртуального интерфейса, идентификатор VLAN (ID), протокол и родительский интерфейс.

Поддерживаются следующие протоколы VLAN:

802.1Q — стандартный протокол тегирования VLAN;

802.1ad (Q-in-Q) — расширенный протокол, позволяющий инкапсулировать один VLAN в другой.

Идентификатор VLAN задаётся в диапазоне от 1 до 4094. Значения 0 и 4095 зарезервированы и не используются. На одном родительском интерфейсе не допускается создание нескольких VLAN с одинаковым идентификатором.

VLAN обеспечивает логическое разделение сети и используется для изоляции трафика в пределах одного физического или агрегированного интерфейса.

При выборе типа bond создаётся агрегированный интерфейс, объединяющий несколько физических интерфейсов в один логический канал. Указываются имя интерфейса, список входящих в него устройств и параметры работы.

Параметр Mode определяет алгоритм агрегации каналов:

balance-rr — последовательная передача пакетов через все интерфейсы;

active-backup — использование одного активного интерфейса с резервированием;

802.3ad — динамическая агрегация каналов с использованием LACP;

balance-xor — распределение трафика на основе хэширования;

balance-tlb — балансировка исходящего трафика;

balance-alb — балансировка входящего и исходящего трафика.

Параметр MIIMonitorSec задаёт интервал проверки состояния

канала и используется для обнаружения отказа интерфейса.

Параметры UpDelaySec и DownDelaySec задают задержки изменения состояния интерфейса при восстановлении или потере соединения.

Параметр LACP применяется в режиме 802.3ad и определяет частоту обмена служебными пакетами.

Параметр Transmit Hash Policy (xmit_hash_policy) определяет алгоритм распределения трафика между интерфейсами.

Использование bond обеспечивает повышение отказоустойчивости и распределение сетевой нагрузки.

При выборе типа bridge создаётся сетевой мост, объединяющий интерфейсы в единый логический сегмент. Указываются имя моста, состав интерфейсов и параметры IP-адресации. Bridge функционирует на канальном уровне и обеспечивает прозрачное объединение интерфейсов в одну сеть.

Для изменения параметров существующего сетевого интерфейса используется функция редактирования, доступная в таблице сетевых устройств. При выборе данной операции открывается окно обновления сетевых настроек (см. рисунок 96), в котором администратор изменяет тип конфигурации, параметры IP-адресации и дополнительные параметры.

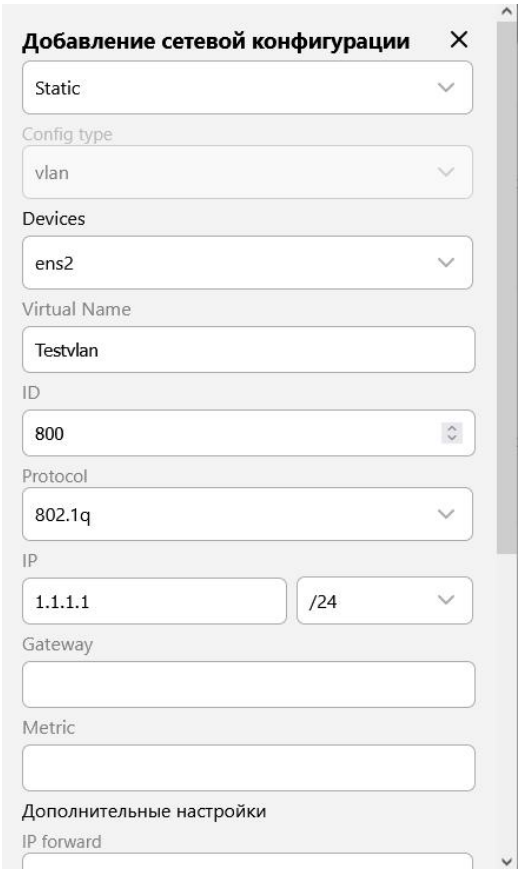

Рисунок 96 – Окно обновления сетевых настроек

Применение изменений выполняется нажатием кнопки «Сохранить», отмена — нажатием кнопки «Отмена».

После внесения изменений для применения конфигурации необходимо нажать кнопку «Перезагрузить сетевые службы». Операция выполняется без перезагрузки системы и обеспечивает вступление изменений в силу.

5.1 Настройки

Раздел «Настройки» предназначен для конфигурирования общесистемных параметров, а также параметров уведомлений и синхронизации времени (см. рисунок 97). В верхней части интерфейса расположены вкладки перехода между подразделами: «Система», «SMTP», «Telegram» и «О системе».

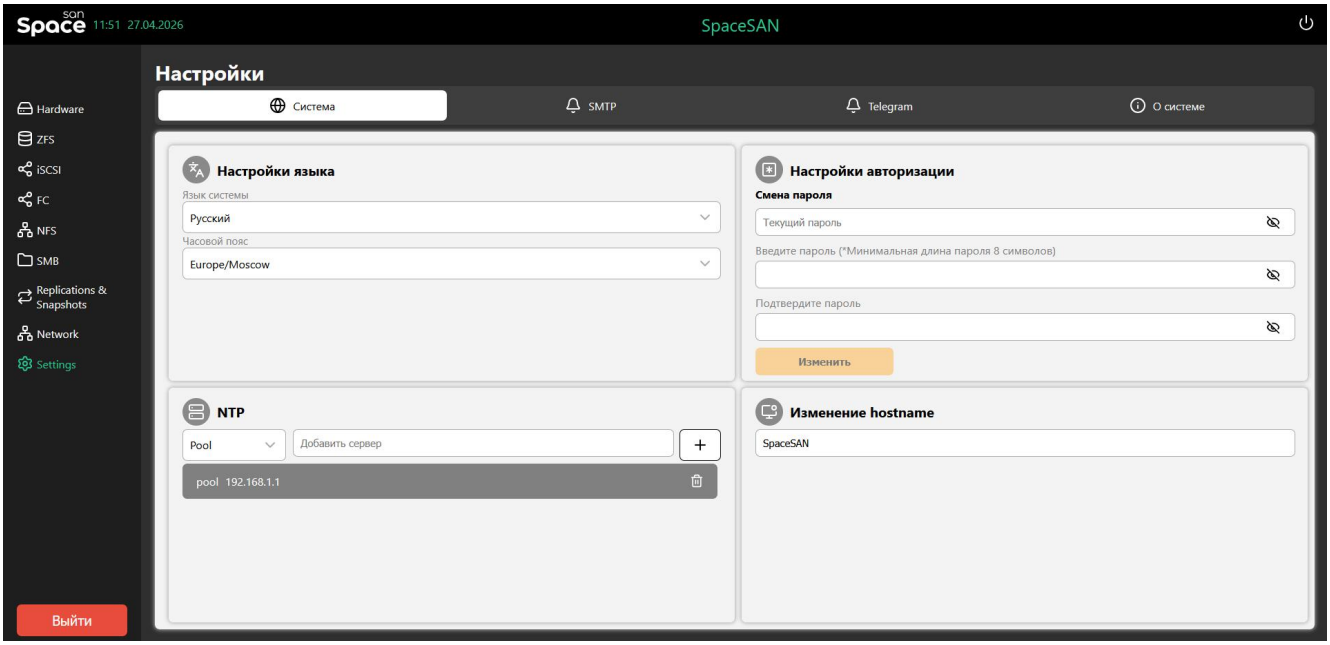

Рисунок 97 – Раздел «Настройки»

Во вкладке «Система» выполняется настройка основных параметров пользовательской среды (см. рисунок 98). В данном разделе администратор может выбрать язык интерфейса системы и настроить часовой пояс.

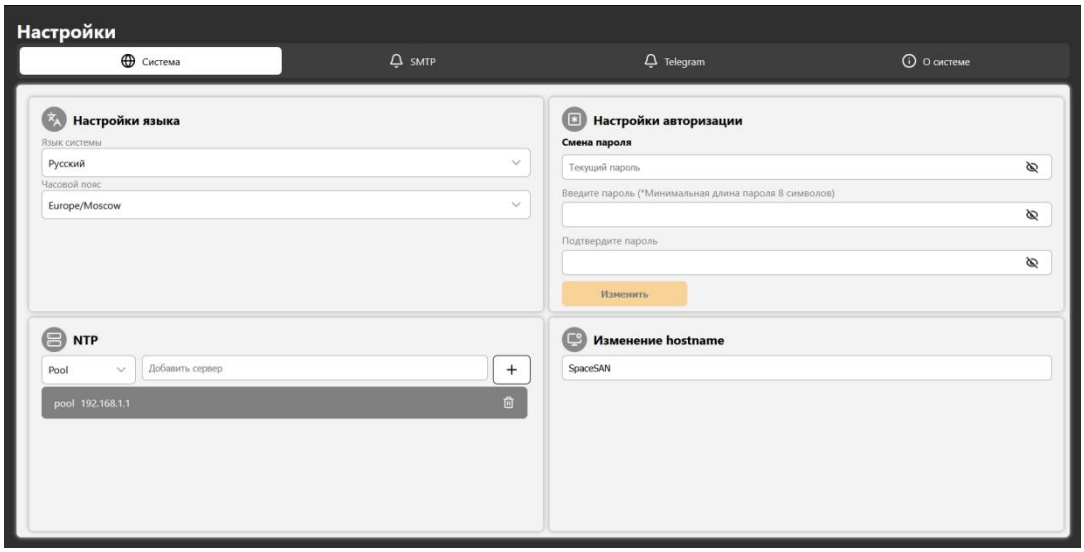

Рисунок 98 – Вкладка «Система»

В разделе «Настройки авторизации» доступна функция смены пароля пользователя. Для изменения пароля необходимо указать текущий пароль, задать новый пароль и подтвердить его повторным

вводом, после чего нажать кнопку «Изменить». Минимальная длина пароля составляет 8 символов.

В разделе «Изменение hostname» выполняется настройка имени хоста системы. Указанное имя используется для идентификации системы в сети.

В разделе «NTP» выполняется настройка серверов синхронизации времени (см. рисунок 99). Администратор может добавить NTP-сервер, указав его адрес, а также удалить ранее добавленные серверы. Настройка NTP обеспечивает синхронизацию системного времени с внешними источниками.

Рисунок 99 – Настройка «NTP»

Синхронизация времени используется для корректной работы журналов событий, репликаций и системных сервисов.

Во вкладке «SMTP» настраиваются параметры отправки почтовых уведомлений (см. рисунок 100). В данном разделе указываются адрес SMTP-сервера, сетевой порт, адрес отправителя и пароль для аутентификации.

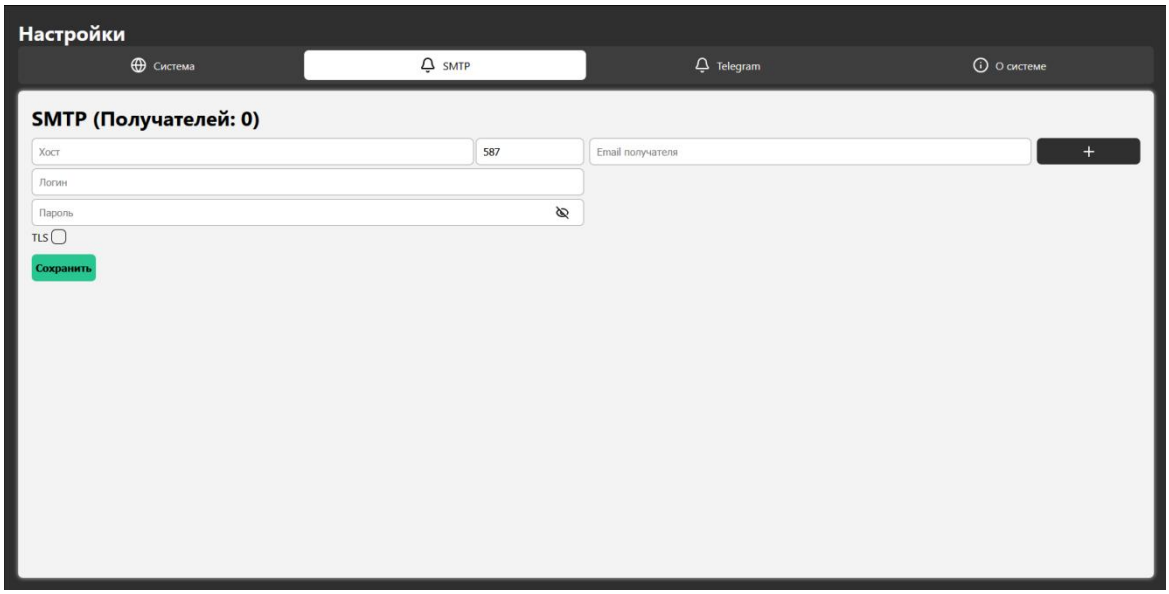

Рисунок 100 – Вкладка «SMTP»

Также предусмотрена возможность добавления одного или нескольких адресов электронной почты получателей уведомлений. После изменения параметров настройки сохраняются нажатием кнопки «Сохранить». Для удаления адреса электронной почты, необходимо нажать на иконку «Корзина».

Во вкладке «Telegram» выполняется настройка уведомлений через сервис Telegram (см. рисунок 101). Для настройки необходимо указать токен Telegram-бота и идентификатор канала или Chat ID получателя уведомлений.

Рисунок 101 – Вкладка «Telegram»

После добавления параметров конфигурация сохраняется с использованием соответствующей кнопки. Уведомления используются

для информирования о системных событиях и ошибках. Для удаления Chat ID, необходимо нажать на иконку «Корзина».

Во вкладке «О системе» отображается справочная информация о программно-аппаратной конфигурации системы (см. рисунок 102). В данном разделе выводятся сведения о версии программного обеспечения, версии ZFS, операционной системе, имени хоста, серийном номере устройства и версии ядра.

Дополнительно в разделе отображается информация о лицензировании системы, включая сведения об организации, адресе электронной почты, сроках действия лицензии и номере лицензии. Подробное описание параметров лицензии и управления лицензированием приведено в соответствующем разделе документа.

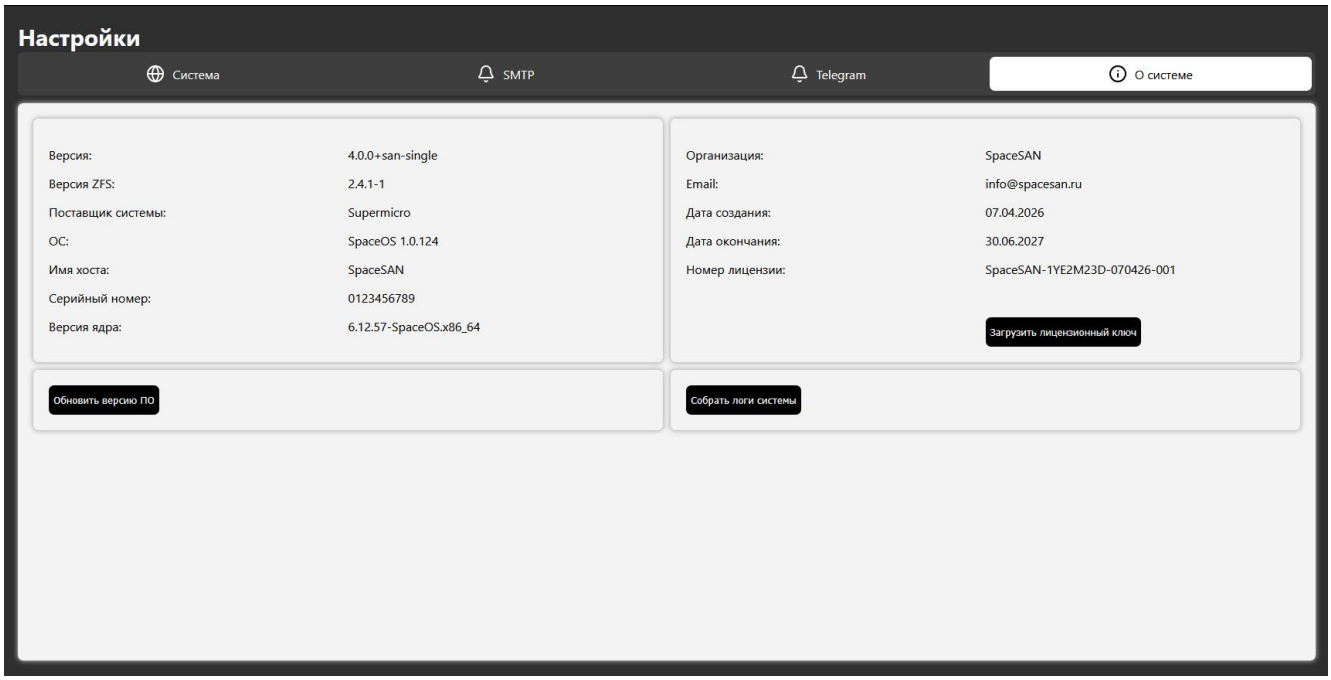

Рисунок 102 – Вкладка «О системе»

В данном разделе доступна функция обновления программного обеспечения системы. Для выполнения обновления необходимо нажать кнопку «Обновить версию ПО», после чего открыть окно загрузки архива обновления. В открывшемся окне требуется выбрать файл архива на локальном устройстве администратора и подтвердить его загрузку.

После завершения загрузки система автоматически выполняет проверку файла архива с отображением статуса проверки и

информации о текущей версии программного обеспечения. При успешном завершении проверки становится доступна кнопка «Обновить», предназначенная для запуска процесса установки обновления.

После нажатия кнопки «Обновить» начинается процесс обновления системы. Необходимо дождаться завершения данной операции для корректной установки новой версии программного обеспечения (см. рисунок 103).

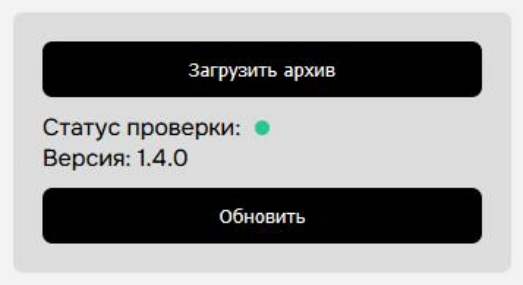

Рисунок 103 – Обновление версии ПО

В разделе также доступна функция формирования диагностической информации. Для получения журналов системы используется кнопка «Собрать логи системы», позволяющая сформировать и выгрузить архив с логами для последующего анализа (см. рисунок 104).

Рисунок 104 – Результат формирования архива логов системы

5.2 Шифрование

Функциональность шифрования предназначена для защиты данных, размещённых в наборах данных (dataset), от несанкционированного доступа. Шифрование настраивается при создании набора данных и применяется на уровне выбранного объекта хранения. Для зашифрованных наборов данных предусмотрены операции управления состоянием (блокирование/разблокирование) и

механизмы предоставления ключевого материала.

При создании Dataset или VVol администратор выбирает формат ключа шифрования (см. рисунок 105).

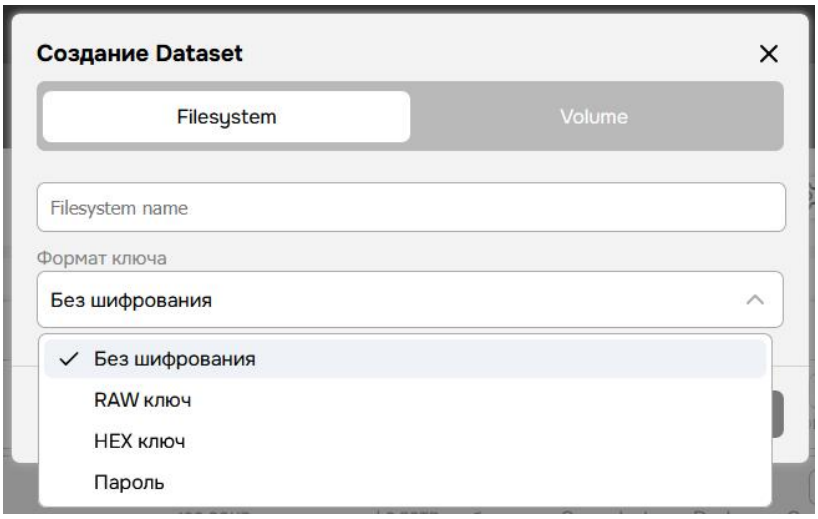

Рисунок 105 – Настройка шифрования Dataset и VVol

Поддерживаются следующие варианты:

- Без шифрования — объект создаётся без применения криптографической защиты.
- RAW-ключ — используется ключевой файл в формате RAW, формируемый системой автоматически.
- HEX-ключ — используется ключевой файл в формате HEX, формируемый системой автоматически.
- Пароль — ключевой материал формируется на основе пароля, задаваемого администратором.

При выборе форматов RAW-ключ или HEX-ключ дополнительно выбирается алгоритм шифрования из перечня поддерживаемых (например, aes-256-gcm). После подтверждения создания зашифрованного Dataset или VVol система автоматически генерирует ключ шифрования, формирует файл ключа и инициирует его загрузку на устройство администратора.

Файл ключа шифрования является обязательным элементом для последующего доступа к данным при использовании форматов RAW-ключ и HEX-ключ. Данный файл не сохраняется в системе и должен быть сохранён администратором в надёжном месте.

Потеря файла ключа шифрования приводит к невозможности восстановления доступа к данным, размещённым в соответствующем Dataset или VVol.

В случае использования парольного формата ключа доступ к данным обеспечивается путём ввода заданного пароля при выполнении операции разблокирования.

Зашифрованные Dataset и VVol отображаются в интерфейсе с признаком блокировки (см. рисунок 106). В заблокированном состоянии доступ к данным ограничен, и объект недоступен для эксплуатации до выполнения процедуры разблокирования.

Рисунок 106 – Зашифрованный Dataset/VVol в заблокированном состоянии

Для получения доступа к зашифрованному Dataset или VVol необходимо выполнить операцию разблокирования.

При использовании шифрования с форматами RAW или HEX разблокирование выполняется путём выбора и загрузки ранее сохранённого файла ключа шифрования, после чего операция подтверждается нажатием соответствующей кнопки (см. рисунок 107).

При использовании парольного шифрования разблокирование выполняется путём ввода заданного пароля и подтверждения операции (см. рисунок 108).

Рисунок 107 – Разблокирование Dataset/VVol с использованием RAW/HEX ключа

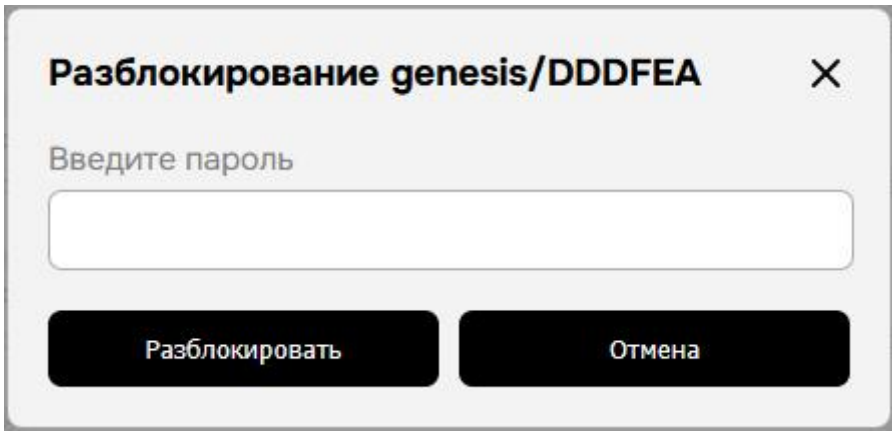

Рисунок 108 – Разблокирование Dataset/VVol с использованием пароля

После успешного разблокирования Dataset или VVol переводится в рабочее состояние и становится доступным для использования файловыми и блочными сервисами системы.

5.3 Замена диска при выходе из строя

При выходе диска из строя данное событие может быть обнаружено по индикатору состояния во вкладке «Hardware», при этом индикация неисправного диска отображается красным цветом (см. рисунок 109).

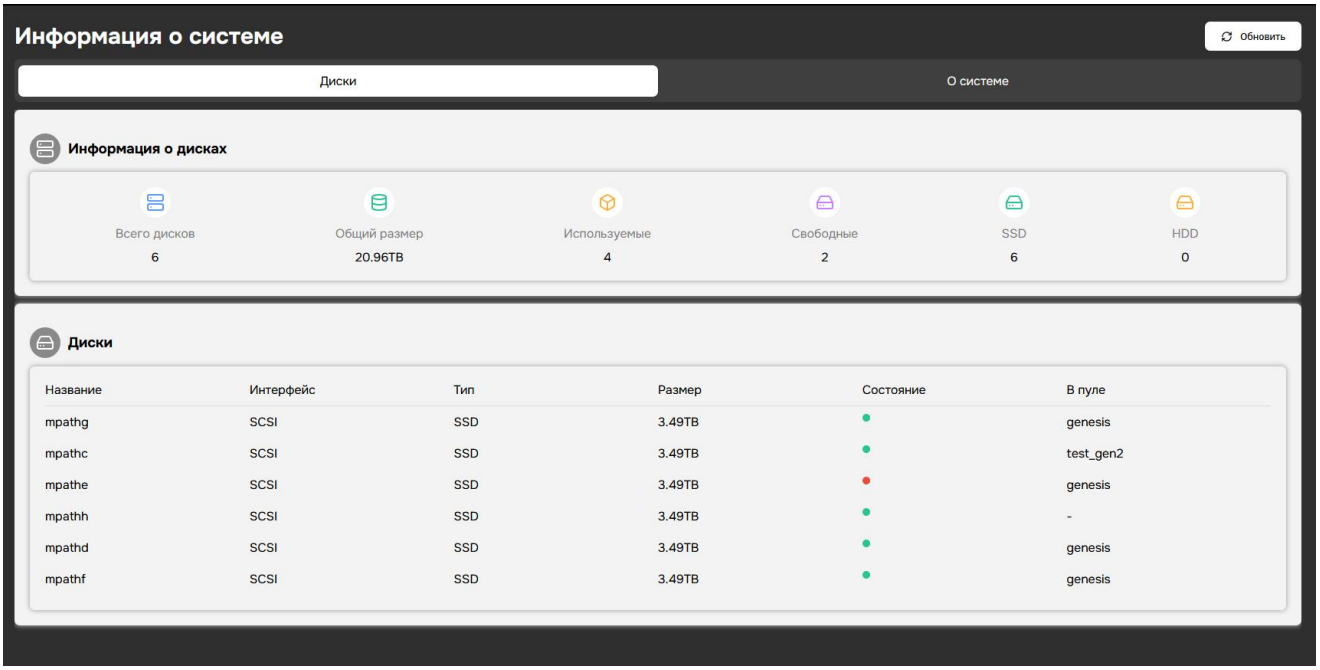

Рисунок 109 – Индикатор состояния диска

Далее необходимо перейти на вкладку «ZFS». В случае возникновения проблем с пулом над его показателями будет отображаться предупреждающее сообщение, а состояние пула может измениться на «DEGRADED» (см. рисунок 110).

Рисунок 110 – Пул в состоянии «DEGRADED»

Для устранения неисправности требуется заменить диск в настройках соответствующего пула. (см. рисунок 111).

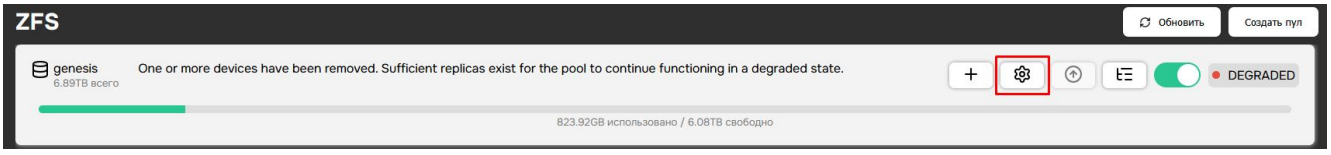

Рисунок 111 – Переход в настройки пула

Далее следует перейти на вкладку «Замена дисков». В разделе со сконфигурированными группами необходимо найти отказавший диск;

такой диск выделяется красным цветом, что указывает на наличие неисправности (см. рисунок 112).

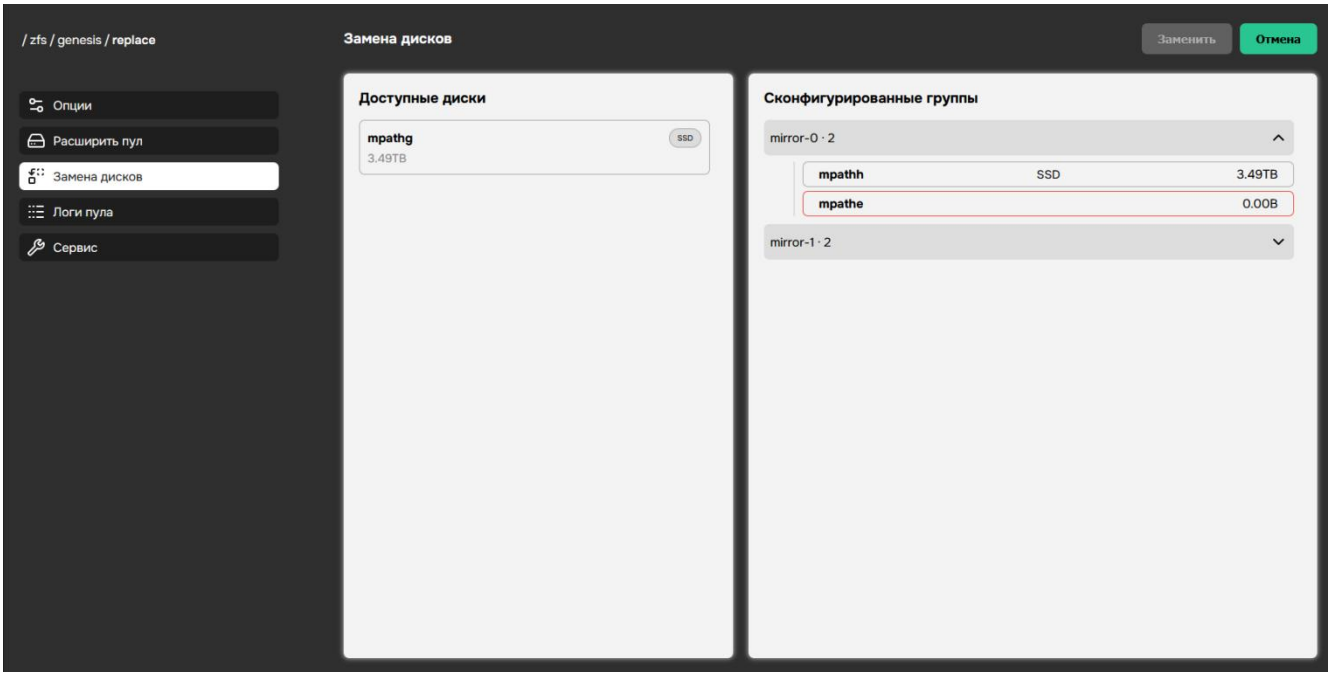

Рисунок 112 – Отказавший диск в пуле

При замене диска, данные будут копироваться с одного диска на другой, пул не поменяет состояния пока оно не закончится, прогресс можно будет увидеть в нижней части вкладки сервис (см. рисунок 113).

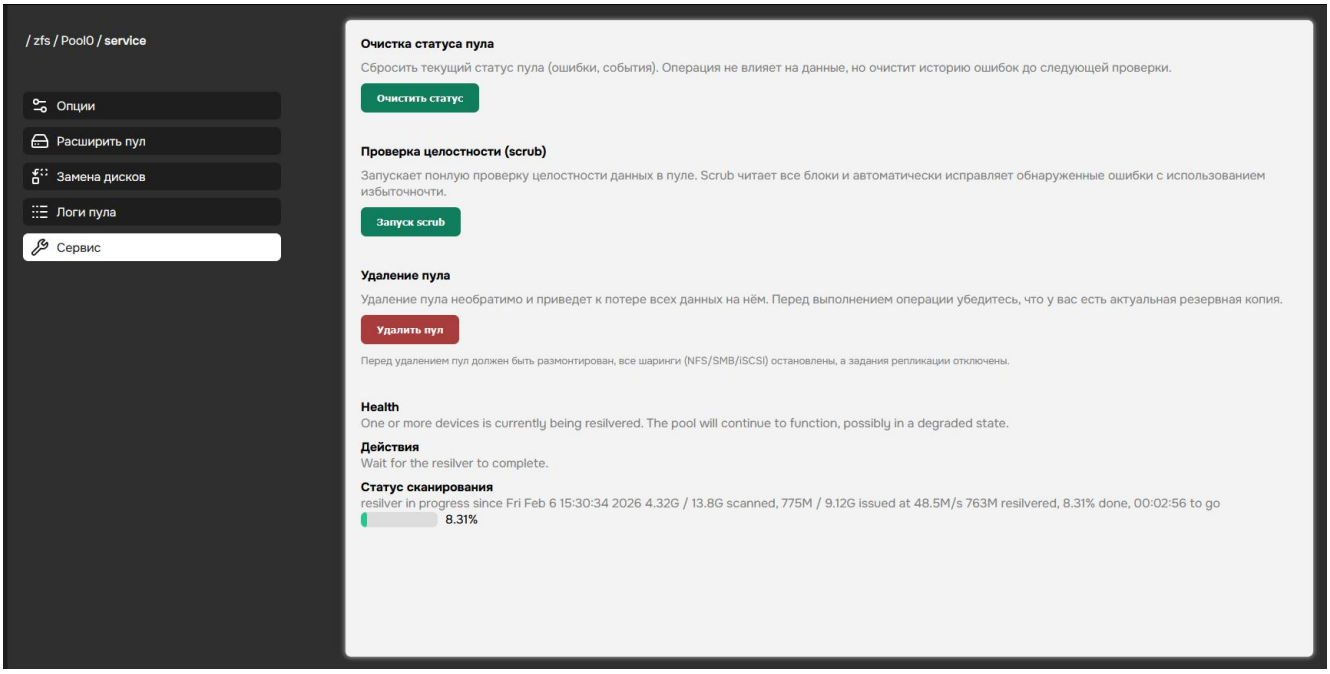

Рисунок 113 – Шкала прогресса копирования

Теперь необходимо во вкладке «Сервис» очистить статус пула (см. рисунок 114).

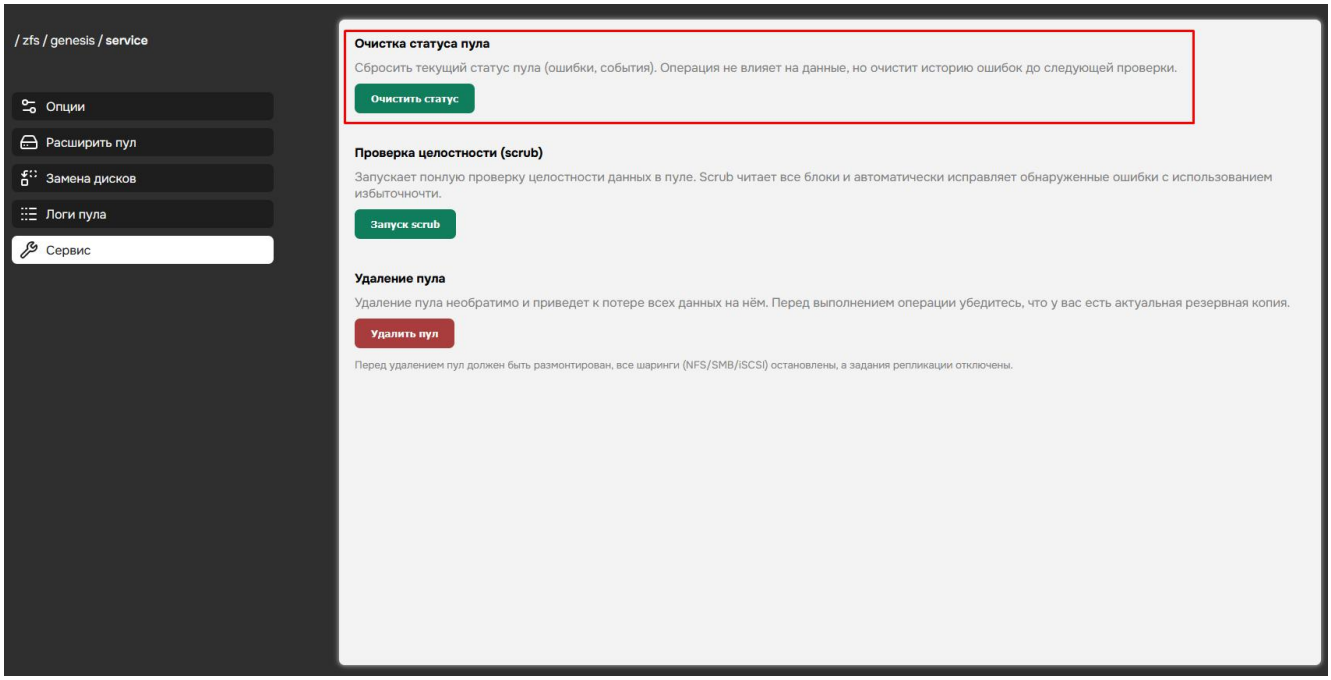

Рисунок 114 – Очистка статуса пула

После выполнения указанных действий состояние пула изменяется на ONLINE, и пул становится полностью готовым к дальнейшей эксплуатации. (см. рисунок 115).

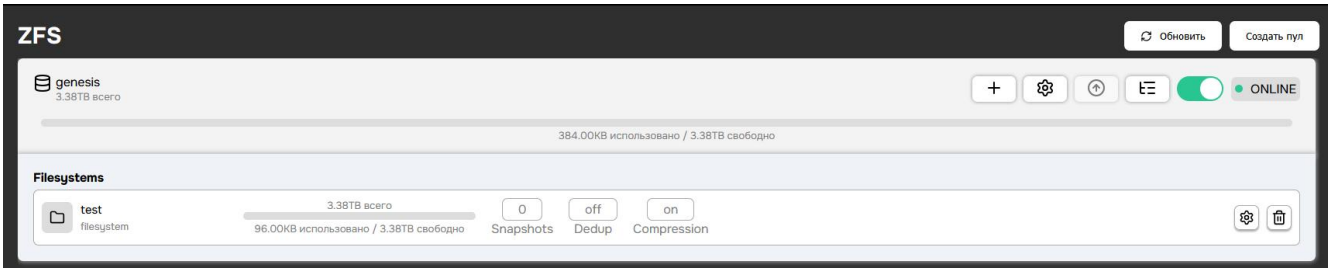

Рисунок 115 – Статус пула после замены диска

5.4 Описание настроек пула и dataset/vvol

Параметры конфигурации ZFS-пула определяют поведение файловых систем, создаваемых на его основе. Они влияют на производительность, надёжность, безопасность и управляемость хранилища. Настройки задаются при создании файловой системы и в

большинстве случаев не подлежат изменению после её создания. Ниже приведены рекомендуемые значения параметров для серверных систем общего назначения.

recordsize — размер записи, используемый ZFS для записи данных. Значение по умолчанию — 128 КБ. При работе с базами данных рекомендуется устанавливать 16 КБ. Для архивных хранилищ, содержащих крупные файлы, допустимо увеличение до 1 МБ. Для общего использования рекомендуется значение по умолчанию.

checksum — алгоритм контрольной суммы для обнаружения повреждений данных. Значение по умолчанию — on. Отключение контрольных сумм (off) недопустимо.

compression — метод сжатия данных на лету. Рекомендуется использовать lz4. Данный алгоритм обеспечивает высокую скорость сжатия и разжатия при среднем коэффициенте сжатия 1,5–2,0. Использование gzip допустимо только при наличии специфических требований к объёму хранения, при этом необходимо учитывать увеличение нагрузки на ЦП.

atime — управление записью времени последнего доступа к файлу. Значение по умолчанию – on. Рекомендуется устанавливать значение off, если необходимо увеличить производительность. Включение atime приводит к дополнительной записи метаданных при каждом чтении файла, что снижает производительность, особенно на системах с высокой частотой обращений.

exec — разрешение выполнения файлов как программ. Рекомендуется значение on. Значение off допустимо только для файловых систем, содержащих исключительно архивные или неисполняемые данные (например, /backup, /archive).

readonly — режим только для чтения. Рекомендуется значение off. Значение on применяется исключительно для архивных копий, системных образов или резервных данных, которые не подлежат изменению.

snapdir — видимость директории снапшотов. Рекомендуется значение hidden. При значении visible снапшоты доступны как скрытая директория zfs/snapshot внутри файловой системы, что увеличивает риск случайного удаления или модификации. Значение hidden

обеспечивает безопасный доступ через специальный путь.

aclmode — управление поведением ACL при изменении прав доступа.

discard — при изменении прав доступа все ACL сбрасываются.

passthrough — ACL сохраняется без изменений, даже если права изменяются.

copies — количество копий каждого блока данных. Значение по умолчанию — 1. Для файловых систем, содержащих критически важные данные (конфигурации, базы данных, системные файлы), рекомендуется устанавливать copies=2. Значение copies=3 применяется в исключительных случаях. Значение copies=1 допустимо только для некритичных данных.

casesensitivity — учёт регистра символов в именах файлов. По умолчанию всегда sensitive. В актуальной версии является не изменяемым.

dedup — включение дедупликации данных. Рекомендуется значение off. Дедупликация требует значительного объёма оперативной памяти (1–5 ГБ на 1 ТБ данных) и снижает производительность. Применение возможно только при наличии высокой степени дублирования данных (например, множество одинаковых виртуальных машин). Вместо дедупликации рекомендуется использовать compression=lz4.

sync — режим синхронной записи. Рекомендуется значение standard. Значение always применяется только для систем с высокими требованиями к целостности данных (например, финансовые или медицинские системы). Значение disabled недопустимо в продакшн-средах.

snapdev — доступ к снепшотам как к блочным устройствам. Рекомендуется значение hidden. Значение visible допустимо только при необходимости прямого доступа к снепшотам ZVOL (например, для восстановления виртуальных машин), но требует строгого контроля доступа.

acltype — тип системы управления доступом. Рекомендуется

значение posix для систем, работающих исключительно под Unix-подобными ОС. Значение nfsv4 при интеграции с Windows-клиентами или при необходимости сложной модели прав доступа. Значение none применяется только в простых сценариях без необходимости управления доступом на уровне ACL.

Параметры recordsize, checksum, compression, atime, exec, readonly, snapdir, copies, dedup, sync, snapdev, acltype, aclmode являются наследуемыми от пула. Они задаются единообразно для пула и файловых систем и не подлежат изменению после создания последних.

Исключением является параметр direct, который не наследуется от пула и может устанавливаться индивидуально для каждой файловой системы.

direct — управляет прямым вводом-выводом в обход кэша ARC.

disabled (по умолчанию) — флаг O_DIRECT игнорируется, используется кэш ARC.

standard — флаг O_DIRECT учитывается при соблюдении требований к выравниванию (для СУБД с собственным кэшированием).

always — принудительный прямой ввод-вывод (только для тестирования, существенно снижает производительность).

Для блочных томов (ZVOL) используется параметр volsize, определяющий видимый размер блочного устройства.

volsize — задаёт логический размер тома. Указывается в байтах с возможными суффиксами (K, M, G, T).

Значение устанавливается при создании тома и не подлежит изменению.

Должно соответствовать потребностям подключаемой системы (например, размеру диска виртуальной машины).

5.5 Лицензия и поддержка

Раздел лицензирования предназначен для просмотра информации о текущем состоянии лицензии и управления лицензионным ключом системы (см. рисунки 116–118).

В разделе отображаются сведения о лицензии, включая наименование организации, адрес электронной почты, дату создания

лицензии, дату окончания действия и номер лицензии. При наличии активной лицензии в интерфейсе отображаются фактические значения указанных параметров (см. рисунок 116). Срок действия лицензии определяет доступность функций системы, связанных с технической поддержкой и обновлениями программного обеспечения.

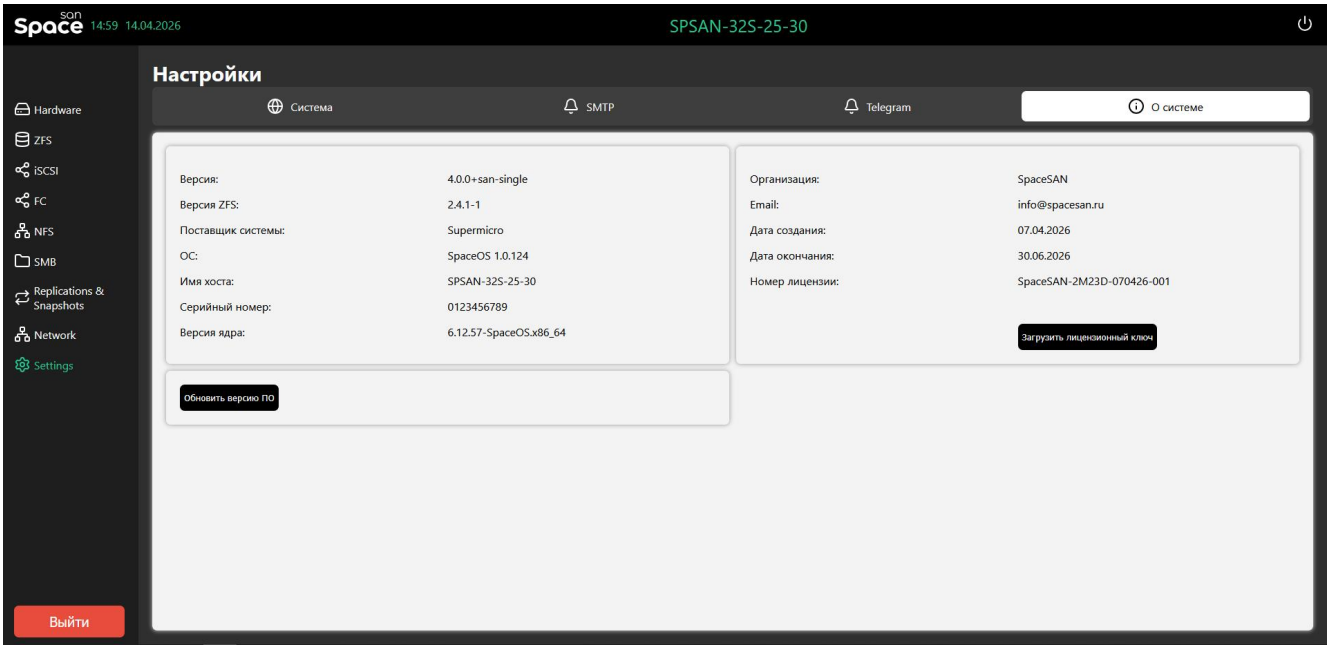

Рисунок 116 – Информация об активной лицензии

В случае отсутствия лицензии или при использовании пробного режима соответствующие поля принимают значение «TRIAL MODE» (см. рисунок 117), что указывает на отсутствие активированной лицензии.

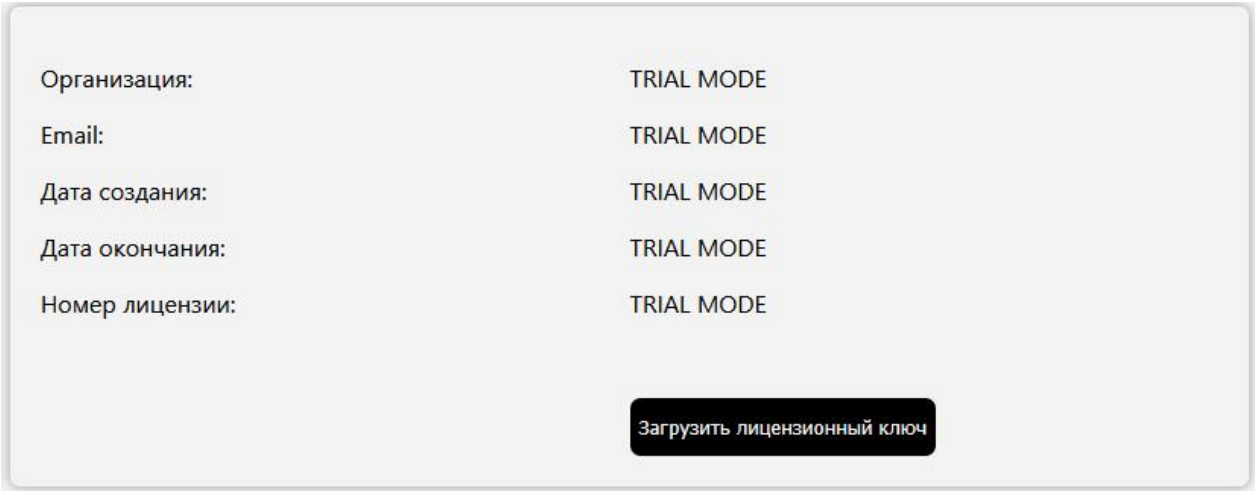

Рисунок 117 – Информация о лицензии в режиме TRIAL MODE

При истечении срока действия лицензии в интерфейсе системы отображается уведомление о завершении срока действия технической поддержки (см. рисунок 118). Уведомление выводится в верхней части интерфейса и информирует администратора о необходимости обновления лицензии.

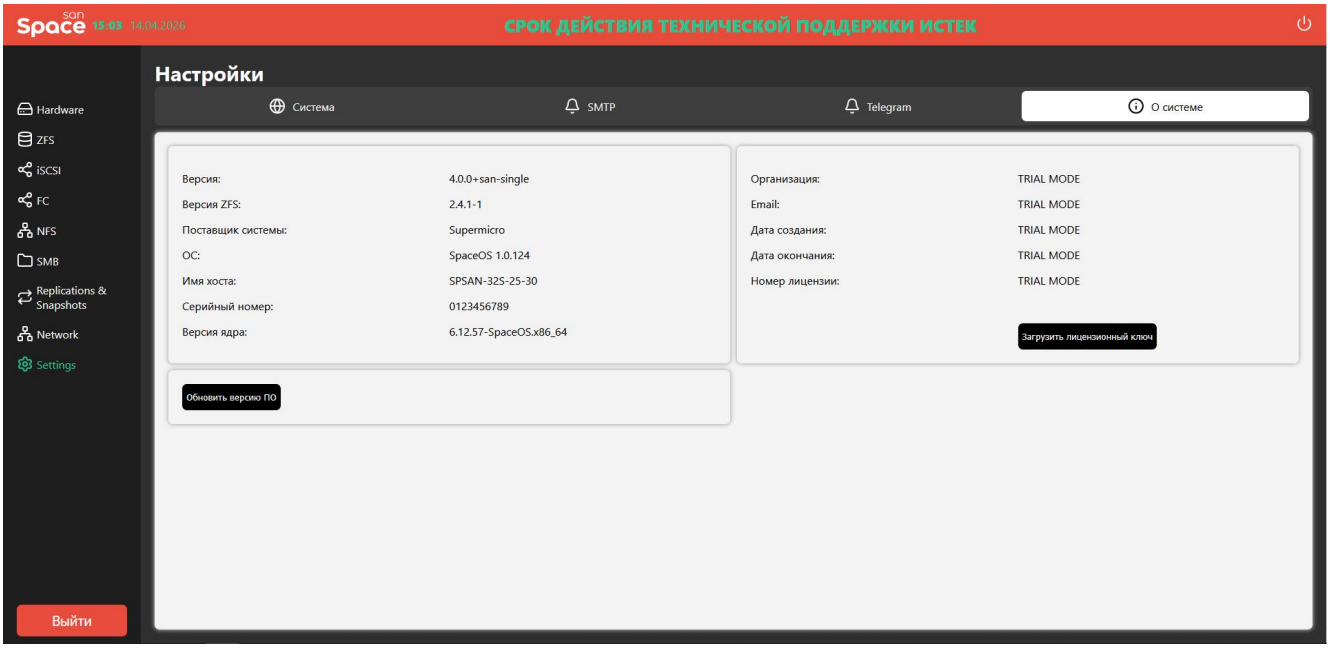

Рисунок 118 – Уведомление об истечении срока действия лицензии

Для загрузки или обновления лицензии используется кнопка «Загрузить лицензионный ключ». После нажатия открывается окно выбора файла, в котором необходимо указать файл лицензионного ключа и подтвердить загрузку.

При загрузке лицензионного ключа выполняется его проверка. В случае, если файл лицензии является некорректным, повреждённым или не соответствует системе, операция отклоняется и отображается сообщение об ошибке.

Если загружаемый лицензионный ключ имеет истёкший срок действия, система уведомляет пользователя о просроченной лицензии и не применяет данный ключ.

После успешной загрузки и применения корректного лицензионного ключа информация о лицензии обновляется, а уведомления о пробном режиме или истечении срока действия перестают отображаться