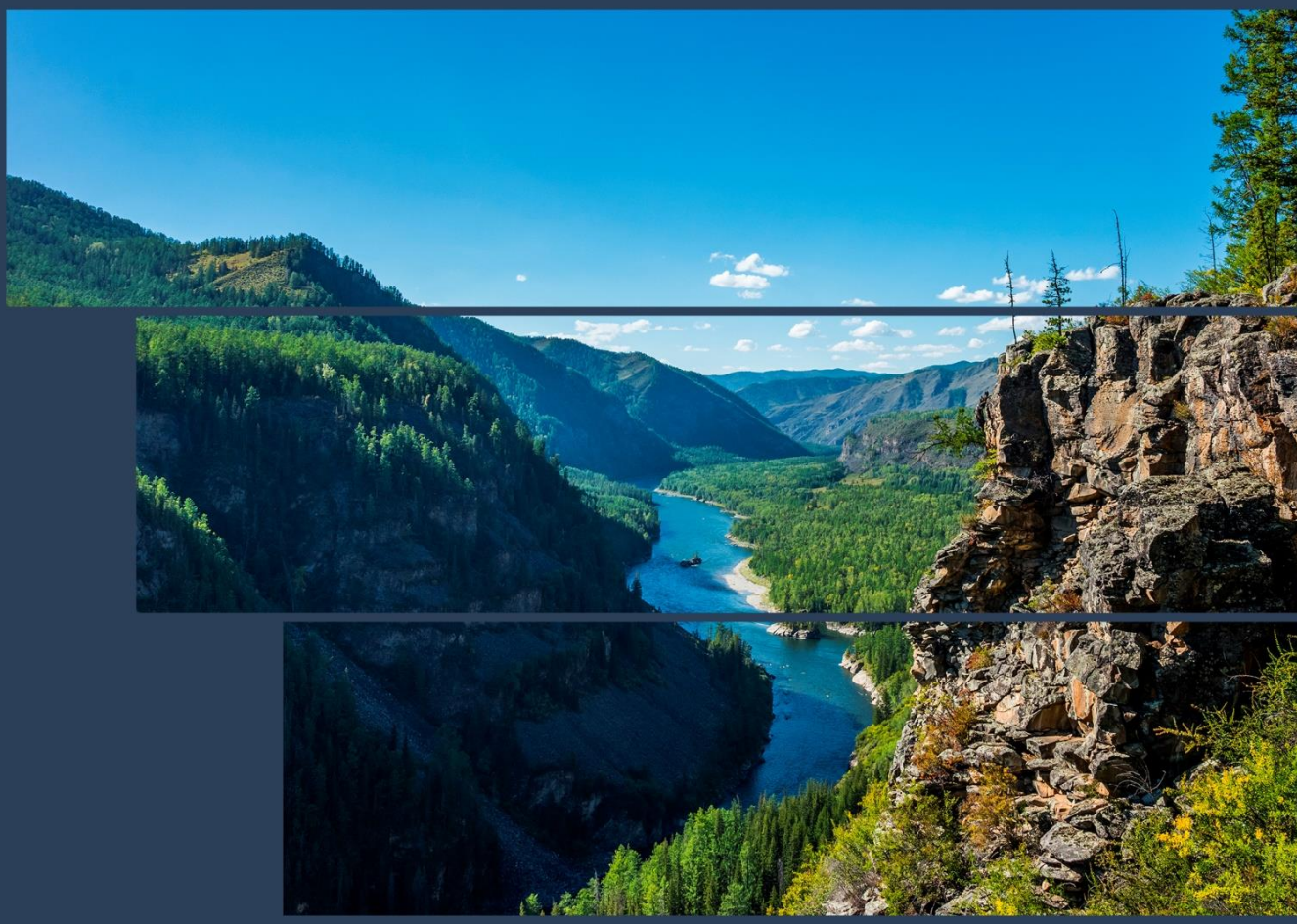

Система управления семейством серверов СИЛА

Сила КУБ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

СИЛА

Версия 4.12

06.06.2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 5
1 ОСНОВНОЙ ФУНКЦИОНАЛ СИЛА КУБ 6
2 ИНТЕРФЕЙСЫ И ПРОТОКОЛЫ ДОСТУПА К СИЛА КУБ 7
2.1 Доступ к системе через web-интерфейс 7
2.2 Доступ к системе для использования командного интерпретатора 7
2.3 Доступ к системе через IPMI 8
2.4 Доступ к системе через REST API 8
2.5 Доступ к системе через Redfish 8
2.6 Протоколы, используемые для оповещения администратора 8
2.6.1 SNMP 8
2.6.2 SMTP 8
2.6.3 SYSLOG 8
3 ИНФОРМАЦИЯ О ПОРТАХ 9
4 АВТОРИЗАЦИЯ 10
4.1 Способы авторизации в Сила КУБ 10
4.2 Сброс пароля 10
4.3 Изменение пароля 10
4.4 Политика надежности пароля 11
5 ОБНОВЛЕНИЕ ПРОШИВКИ 12
6 ПОДКЛЮЧЕНИЕ К СИЛА КУБ 15
6.1 Подключение с использованием SSH 15
6.1.1 Создание открытых ключей для Windows/Linux 15
6.1.2 Загрузка ключей SSH 16
6.1.3 Отображение SSH ключей 17
6.1.4 Удаление SSH-ключей 17
6.2 Взаимодействие с Сила КУБ с помощью IPMI 18
6.3 Взаимодействие с Сила КУБ через RESTful API 20
6.4 Взаимодействие с Сила КУБ через протокол Redfish 20
7 НАСТРОЙКА УЧЕТНЫХ ЗАПИСЕЙ И ПРИВИЛЕГИЙ ПОЛЬЗОВАТЕЛЕЙ 21
7.1 Текущие сессии пользователей 21
7.2 Роли и привилегии в Сила КУБ 21
7.3 Рекомендуемые символы в именах пользователей 22
7.4 Настройка локальных пользователей 22
7.4.1 Добавление пользователей через BIOS для моделей CP2-5422, CP4-5422 25
8 ОТПРАВКА ОПОВЕЩЕНИЙ И ПРЕДУПРЕЖДЕНИЙ 27
8.1 Настройка отправки оповещений и предупреждений по протоколу SNMP v2 27
8.2 Настройка отправки оповещений и предупреждений по протоколу SMTP 28
8.2.1 Управление состоянием протокола SMTP 28
8.2.2 Управление авторизацией SMTP 28
8.2.3 Редактирование адреса отправителя сообщений по SMTP 29
8.3 Настройка отправки оповещений и предупреждений по протоколу SYSLOG 29
8.4 Настройка отправки оповещений и предупреждений по IPMI 30
8.5 Иные способы отправки оповещений и предупреждений 30

9 УПРАВЛЕНИЕ ЛОГАМИ ... 32
9.1 Отображение журнала событий ... 32
9.2 Авторешение событий ... 33
9.3 Выгрузка логов ... 34
10 УПРАВЛЕНИЕ ЭЛЕКТРОПИТАНИЕМ ИЗ ИНТЕРФЕЙСА СИЛА КУБ ... 35
11 НАСТРОЙКА И МОНИТОРИНГ СЕТЕВЫХ ИНТЕРФЕЙСОВ BMC ... 37
12 УПРАВЛЕНИЕ УСТРОЙСТВАМИ ХРАНЕНИЯ ... 39
13 УПРАВЛЕНИЕ ВИРТУАЛЬНЫМИ УСТРОЙСТВАМИ ... 40
13.1 Режимы/предопределённые типы устройств ... 40
13.2 Особенности контроля устройств со стороны web-браузера ... 41
13.3 Загрузка с виртуального носителя ... 41
13.4 Формат образа с поддержкой EFI загрузки ... 42
14 УПРАВЛЕНИЕ RAID-КОНТРОЛЛЕРАМИ ... 44
14.1 Отображение информации о RAID ... 44
14.1.1 Информация о RAID-массивах ... 44
14.1.2 Информация о физических накопителях ... 44
14.1.3 Информация о дисковых массивах ... 46
14.1.4 Информация о логических накопителях ... 46
14.2 Переключение режима RAID-контроллера ... 46
14.3 Операции с физическими накопителями ... 48
14.3.1 Управление LED-индикацией накопителя ... 50
14.3.2 Обновление информации о состоянии ... 50
14.3.3 Операции в состоянии UNCONFIGURED GOOD ... 51
14.3.4 Операции в состоянии HOT SPARE ... 54
14.3.5 Операции в состоянии UNCONFIGURED BAD ... 54
14.3.6 Операции в состоянии ONLINE ... 54
14.3.7 Операции в состоянии OFFLINE ... 54
14.3.8 Операции в состоянии PREPARE FOR REMOVAL ... 54
14.3.9 Операции в состоянии REBUILD ... 54
14.3.10 Операции в состоянии COPYBACK ... 55
14.3.11 Операция замены отсутствующих накопителей ... 55
14.3.12 Управление FOREIGN-конфигурациями ... 56
14.4 Добавление дискового массива ... 56
14.4.1 Добавление дискового массива уровня RAIDx ... 56
14.4.2 Добавление дискового массива уровня RAIDxx ... 58
14.5 Добавление логического накопителя ... 59
14.5.1 Сегментация свободного пространства в RAID ... 60
14.6 Удаление логического накопителя ... 61
14.7 Операции с логическими накопителями ... 61
14.7.1 Управление LED-индикацией накопителя ... 63
14.7.2 Обновление информации о состоянии ... 63
14.7.3 Операции видимости накопителей ... 64
14.7.4 Операции проверки целостности данных накопителей ... 64
14.7.5 Операции инициализации накопителей ... 64
14.7.6 Операции модификации накопителей ... 65
14.7.7 Операции очистки накопителей ... 67

14.8 Сброс конфигурации ... 68
14.9 Логирование событий RAID ... 68

15 РАБОТА С ОСНОВНЫМИ ФУНКЦИЯМИ В РАЗДЕЛЕ «ИНФОРМАЦИЯ О СЕРВЕРЕ» ... 69

15.1 Статическая информация о конфигурации сервера ... 69
15.2 Информация об установленных процессорах и материнской плате, и их состоянии ... 71
15.3 Обновление микрокода BMC и BIOS ... 71
15.4 Отображение функции управления ОС и сервера, проверки выключения сервера ... 72

16 РАБОТА С ОТДЕЛЬНЫМИ РАЗДЕЛАМИ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА ... 75

16.1 Раздел «Система» ... 75
16.1.1 Отображение информации о сетевых адаптерах ... 75
16.1.2 Отображение настроек даты и времени, настроек параметров сети ... 76

16.2 Раздел «Статус оборудования» ... 76
16.2.1 Просмотр перечня датчиков ... 76

16.3 Раздел «Управление» ... 78
16.3.1 Проверка отображения перезагрузки BMC ... 78

16.4 Аналитическая панель «Модуль памяти» ... 79
16.4.1 Отображение динамической информации о состоянии модулей памяти ... 79

16.5 Аналитическая панель «Вентиляторы» ... 81
16.5.1 Перечень отображаемой динамической информации о текущем состоянии вентиляторов ... 81

16.6 Аналитическая панель «Материнская плата» ... 83
16.6.1 Отображение динамической информации о состоянии материнской платы ... 83

16.7 Аналитическая панель «Процессоры» ... 84
16.7.1 Отображение динамической информации о состоянии процессоров ... 84

16.8 Аналитическая панель «Источники питания» ... 85
16.8.1 Отображение динамической информации о состоянии источников питания ... 85

16.9 Отдельные элементы управления ... 86

17 ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ... 88

17.1 Сообщения об ошибках ... 88
17.2 Особенности систем ... 89
17.2.1 Доступ к IPMI ... 89

17.3 Рекомендации ... 89
17.3.1 Для сервера CP2-5422, CP4-5422 ... 89
17.3.2 Для серверов CP1-6326, CP2-6327, CP9-6426 ... 90

ВВЕДЕНИЕ

Система управления семейством серверов СИЛА «Сила КУБ» (далее Сила КУБ) представляет собой программное обеспечение, включающее в себя графический пользовательский web-интерфейс с адаптивной версткой, позволяющий работать с мобильных устройств, для контроллеров управления базовой платы BMC серверов СИЛА.

Данное руководство распространяется на Сила КУБ, работающую на серверах: CP2-5422, CP4-5422, CP1-6326, CP2-6327, CP9-6426.

BMC содержит интегрированное видеоядро, взаимодействует с компонентами системной платы сервера через различные интерфейсы и обеспечивает необходимый функционал в соответствии со стандартом IPMI. Работа Сила КУБ не зависит от операционной системы (далее ОС) сервера. В этом заключается основное отличие от программных средств удаленного управления и мониторинга, требующих наличия работоспособной ОС (например, удаленный доступ к ОС через RDP, Radmin и т. д.). Доступ к графической консоли можно использовать для удаленной прошивки BIOS системной платы или для установки ОС.

Сила КУБ позволяет удаленно управлять электропитанием сервера, скоростью вращения вентиляторов, предоставлять доступ к консоли главной операционной системы через Serial Over LAN (далее SOL), считывать показания системных датчиков (скорость вентиляторов, напряжение на блоках питания и VRM, температура компонентов), следить за исправностью компонентов, хранить журнал ошибок. Кроме того, Сила КУБ предоставляет возможности удаленного доступа к графическому терминалу (KVM), подключения виртуальных носителей (DVD, ISO, USB), поддерживает различные протоколы out-of-band подключения (IPMI, SSH, Redfish, RESTful).

Данное руководство содержит основные параметры настроек доступа к Сила КУБ, инструкцию по обновлению прошивки Сила КУБ, информацию по администрированию конфигурации системы и описание web-интерфейса системы.

1 ОСНОВНОЙ ФУНКЦИОНАЛ СИЛА КУБ

Основные функции Сила КУБ:

- Предоставление удаленного доступа к серверу с помощью REST, web-интерфейс, IPMI, SSH;
- Обновление прошивки Сила КУБ;
- Предоставление информации о конфигурации оборудования сервера и его мониторинг;
- Получение логов с оборудования;
- Аналитическая панель графического отображения параметров конфигурации и работы сервера.

2 ИНТЕРФЕЙСЫ И ПРОТОКОЛЫ ДОСТУПА К СИЛА КУБ

2.1 ДОСТУП К СИСТЕМЕ ЧЕРЕЗ WEB-ИНТЕРФЕЙС

При таком подключении браузер подключается к web-серверу, используя защищенный протокол HTTPS.

Для HTTPS по умолчанию используется TCP-порт 443.

Для подготовки web-сервера для обработки HTTPS-соединений по умолчанию используется самоподписанный сертификат. При этом администратор может получить и установить в систему сертификат открытого и закрытого ключа для этого web-сервера.

При подключении к web-интерфейсу пользователь попадает на главную страницу, где отображена основная информация о системе. Все страницы web-интерфейса имею заголовок, основное меню расположенное слева и непосредственно содержимое страницы.

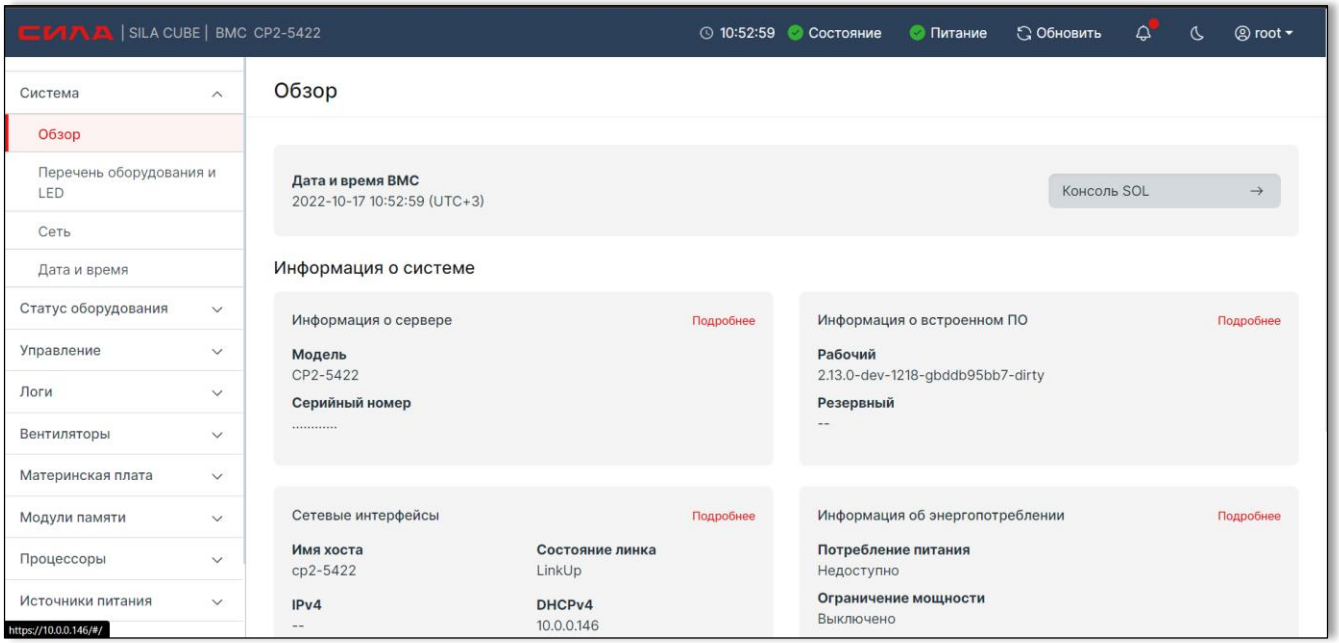

Рисунок 1. Главная страница web-интерфейса системы

2.2 ДОСТУП К СИСТЕМЕ ДЛЯ ИСПОЛЬЗОВАНИЯ КОМАНДНОГО ИНТЕРПРЕТАТОРА

Для подключения к BMC используется SSH для доступа к командному интерпретатору. Поддерживается SSH версии 1.x и 2.x.

2.3 ДОСТУП К СИСТЕМЕ ЧЕРЕЗ IPMI

Для подключения к BMC могут использоваться утилиты, поддерживающие протокол IPMI, для доступа к основным функциям управления удаленной системой с помощью встроенного ПО Сила КУБ. Используется спецификация IPMI v2.0

2.4 ДОСТУП К СИСТЕМЕ ЧЕРЕЗ REST API

Используйте REST API команды.

2.5 ДОСТУП К СИСТЕМЕ ЧЕРЕЗ REDFISH

Используйте URI запросы через API Redfish.

2.6 ПРОТОКОЛЫ, ИСПОЛЬЗУЕМЫЕ ДЛЯ ОПОВЕЩЕНИЯ АДМИНИСТРАТОРА

2.6.1 SNMP

Используйте SILA-MIB.txt с BMC и snmp утилиты для получения данных snmp протоколу.

Файл SILA-MIB.txt можно загрузить из каталога BMC /usr/share/snmp/mibs или через https – клиент (например браузер или curl) по адресу:

wget--no-check-certificate https://<IP-addres-of-BMC-host>/mibs/SILA-MIB.txt.

2.6.2 SMTP

Доступно оповещение администратора по протоколу передачи электронной почты SMTP

2.6.3 SYSLOG

Используйте Rsyslog для получения системных журналов из BMC.

3 ИНФОРМАЦИЯ О ПОРТАХ

Таблица 1. Порты, которые сканируются Сила КУБ для подключения

Номер порта	Тип (TCP или UDP)	Протокол	Порт конфигурируемый? (Да или Нет)	Максимальный уровень шифрования
22	TCP	SSH	Да	
443	TCP	HTTP		SSL
162	UDP	SNMP		
443	TCP	Доступ к web-интерфейсу через https		SSL

Таблица 2. Порты, которые Сила КУБ использует как клиент

Номер порта	Тип (TCP или UDP)	Протокол	Порт конфигурируемый? (Да или Нет)	Максимальный уровень шифрования
161	UDP	SNMP		
	TCP,UDP	DNS	Да	
	UDP	NTP	Да	
		CIFS	Отсутствуют в системе	

4 АВТОРИЗАЦИЯ

4.1 СПОСОБЫ АВТОРИЗАЦИИ В СИЛА КУБ

По умолчанию в Сила КУБ присутствует учётная запись с правами администратора с именем «root» и паролем «5uperS!L@». Для локальных пользователей.

ВНИМАНИЕ:

Для моделей CP1-6326, CP2-6327, CP9-6426 также доступна учетная запись с правами администратора с именем admin и паролем «admin».

В систему можно авторизоваться, используя локальный логин и пароль. Добавление локального пользователя подробно описано в разделе 7 НАСТРОЙКА УЧЕТНЫХ ЗАПИСЕЙ И ПРИВИЛЕГИЙ ПОЛЬЗОВАТЕЛЕЙ

Для авторизации в системе можно подключить удаленный LDAP сервер. Подробно описано в разделе 7 НАСТРОЙКА УЧЕТНЫХ ЗАПИСЕЙ И ПРИВИЛЕГИЙ ПОЛЬЗОВАТЕЛЕЙ

4.2 СБРОС ПАРОЛЯ

В целях безопасности в текущей реализации система не позволяет сбросить пароль пользователю.

4.3 ИЗМЕНЕНИЕ ПАРОЛЯ

Для изменения пароля необходимо зайти в настройки профиля пользователя справа в верхней панели интерфейса, на открывшейся странице профиля пользователя ввести новый пароль, подтвердить его и сохранить изменения.

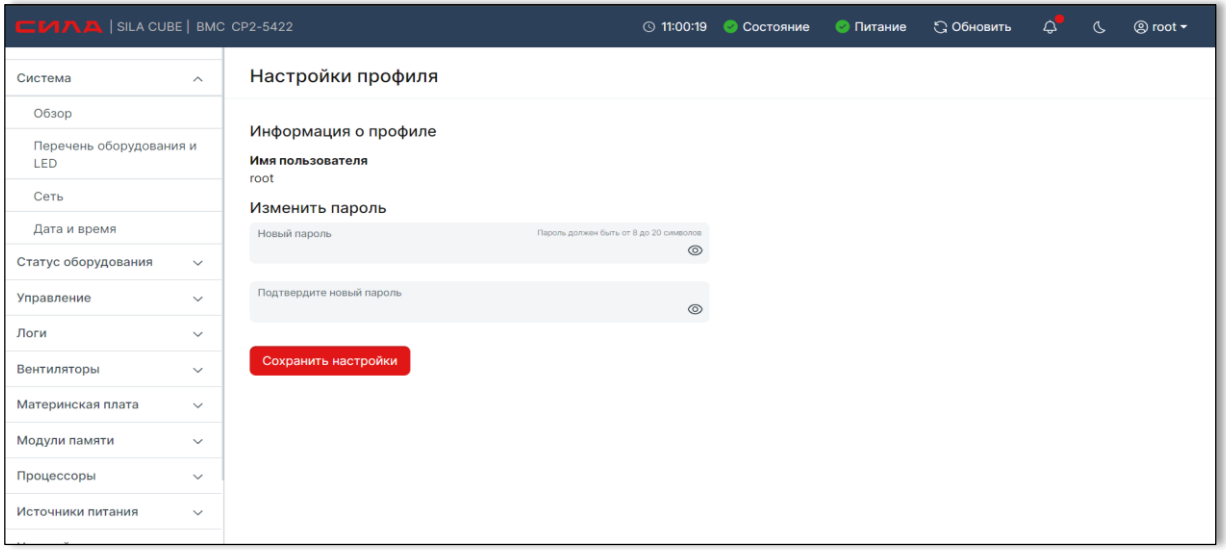

Рисунок 2. Страница «Настройки профиля»

4.4 ПОЛИТИКА НАДЕЖНОСТИ ПАРОЛЯ

В текущей реализации пароль должен содержать от 8 до 20 символов.

Пароль пользователя с доступом через ipmitool, не должен содержать управляющих спецсимволов интерпретатора shell/bash.

5 ОБНОВЛЕНИЕ ПРОШИВКИ

Пользователь может обновлять прошивки BMC и BIOS через интерфейс Сила КУБ.

Для обновления прошивки необходимо зайти в основном меню в раздел **Управление -> Встроенное ПО**.

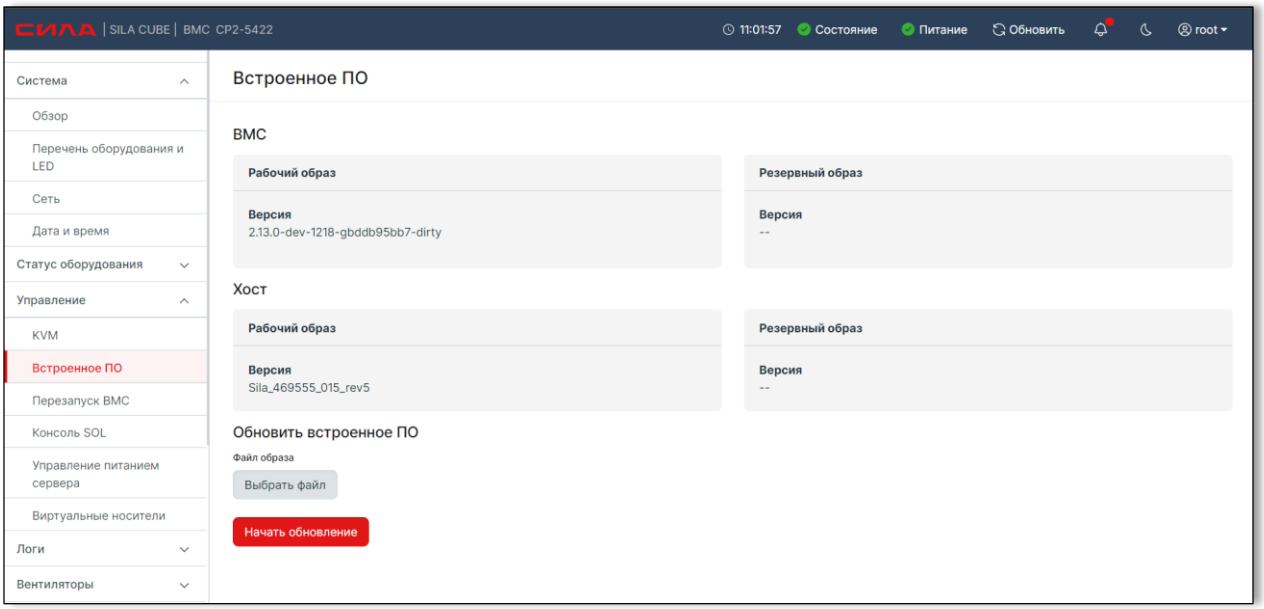

Рисунок 3. Страница «Встроенное ПО»

Нажать на кнопку «Выбрать файл» и загрузите файл, который относится к обновлению BMC или BIOS.

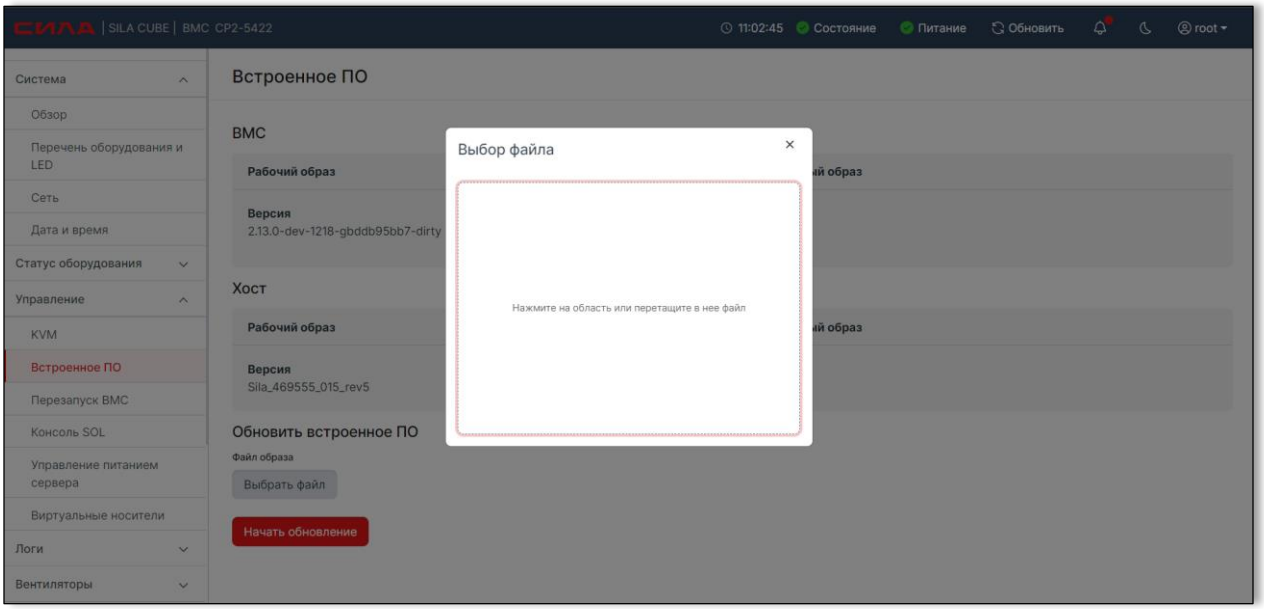

Рисунок 4. Окно «Выбор файла»

После загрузки файла на странице «Встроенное ПО» отобразится поле с наименованием выбранного файла.

Для удаления выбранного файла необходимо нажать на кнопку «Очистить поле» (элемент под цифрой 1 на Рисунок 5).

Для того, чтобы начать обновление необходимо нажать на кнопку «Начать обновление» (элемент под цифрой 2 на Рисунок 5).

ВНИМАНИЕ:

Сведения об устройствах не сохраняются при прошивке файлом *.all.tar. Для получения сведений необходимо перезапустить хост.

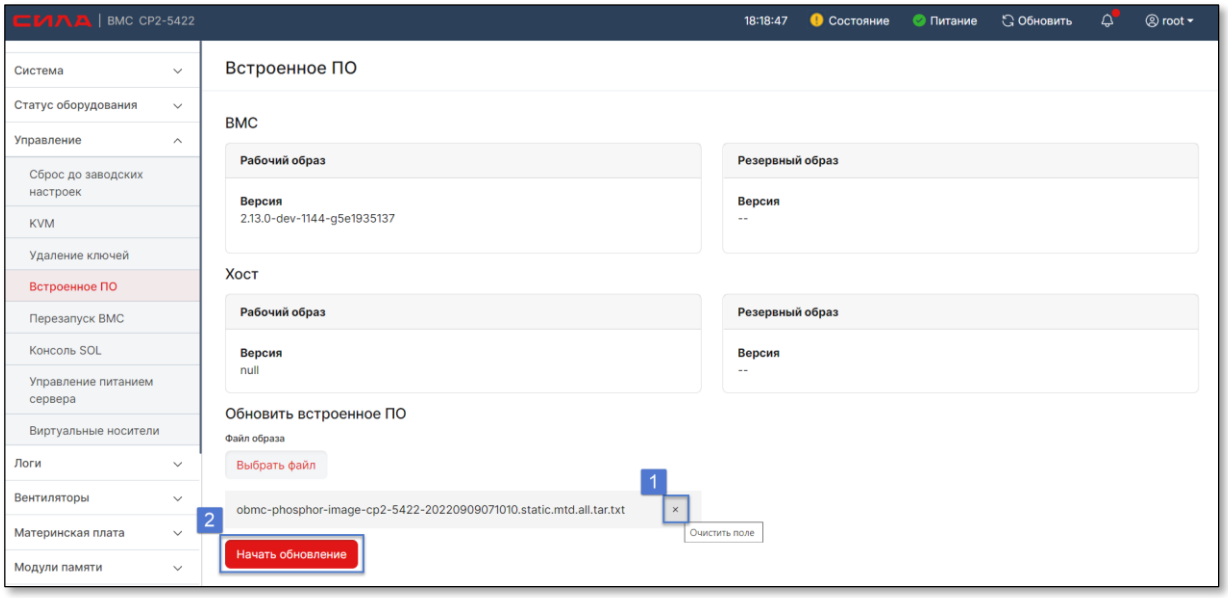

Рисунок 5. Страница «Встроенное ПО» после выбора файла

В появившемся диалоговом окне «Обновить встроенное ПО» необходимо подтвердить обновление нажав на кнопку «Начать обновление».

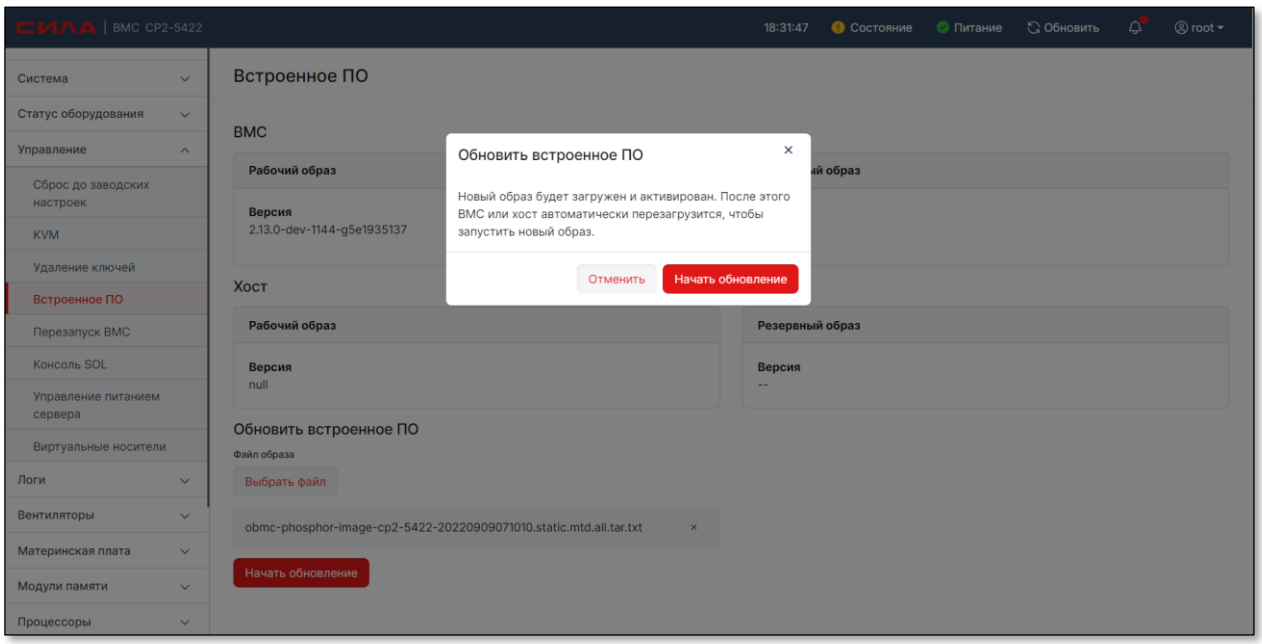

Рисунок 6. Окно «Обновить встроенное ПО»

После запуска обновления отобразится уведомление о начале выполнения обновления (элемент под цифрой 1 на Рисунок 7).

После окончания обновления ПО отображается уведомление о необходимости проверки обновления (элемент под цифрой 2 на Рисунок 5).

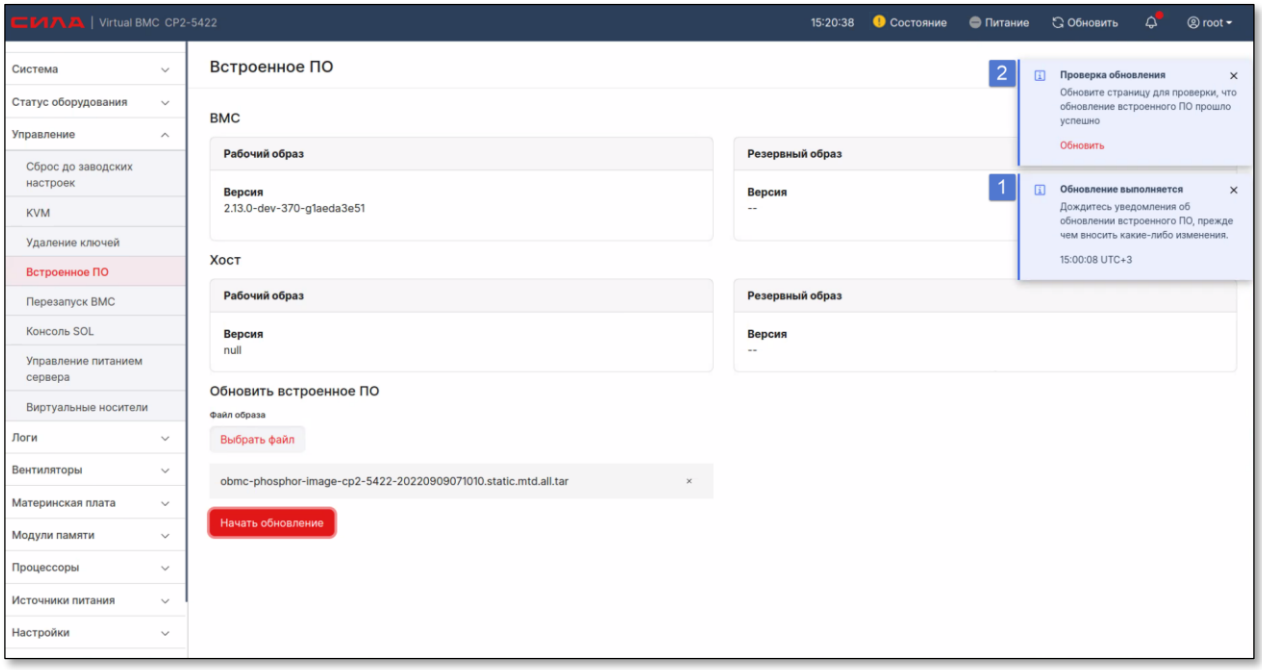

Рисунок 7. Уведомления об обновлении встроенного ПО

Для проверки обновления необходимо обновить страницу и заново авторизоваться в Системе (способы авторизации описаны в разделе 4 АВТОРИЗАЦИЯ).

6 ПОДКЛЮЧЕНИЕ К СИЛА КУБ

6.1 ПОДКЛЮЧЕНИЕ С ИСПОЛЬЗОВАНИЕМ SSH

- Поддерживаемые SSH криптографические схемы: RSA.
- Использование аутентификации с открытым ключом для SSH: пользователь может использовать публичный ключ при работе через любой командный интерпретатор от имени пользователя root.

6.1.1 СОЗДАНИЕ ОТКРЫТЫХ КЛЮЧЕЙ ДЛЯ WINDOWS/LINUX

Для создания открытых ключей необходимо зайти в основном меню в раздел **Безопасность и доступ -> Сертификаты.**

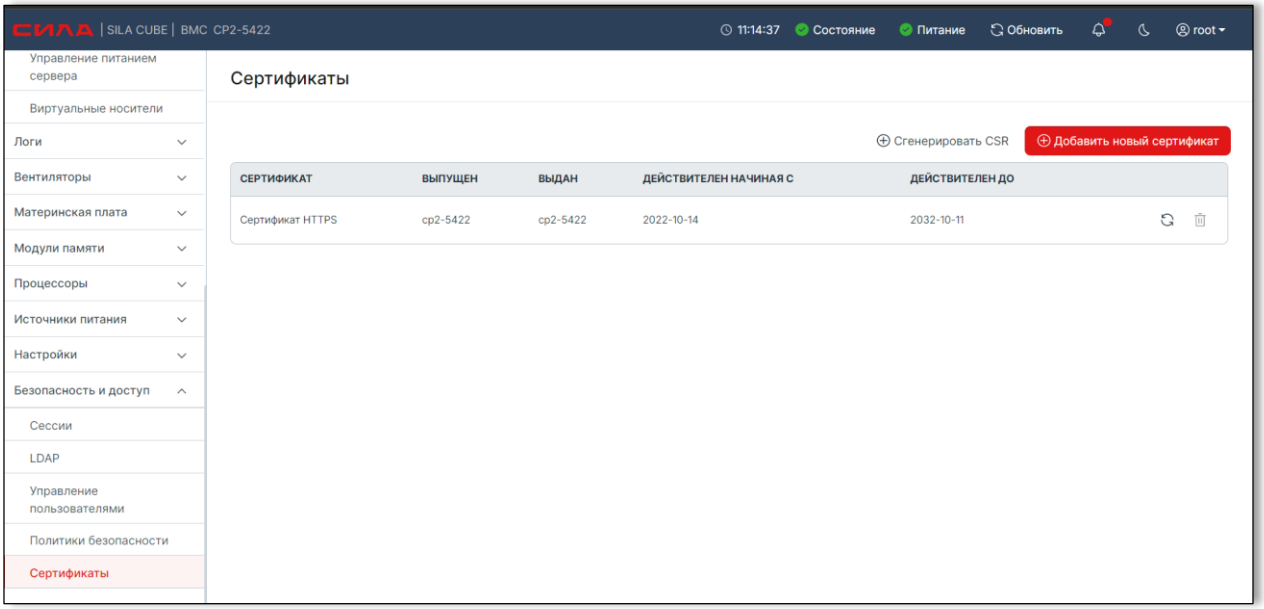

Рисунок 8. Страница «Сертификаты»

Нажать на кнопку «Сгенерировать CSR». В открывшемся окне заполнить параметры и нажать на кнопку «Сгенерировать CSR».

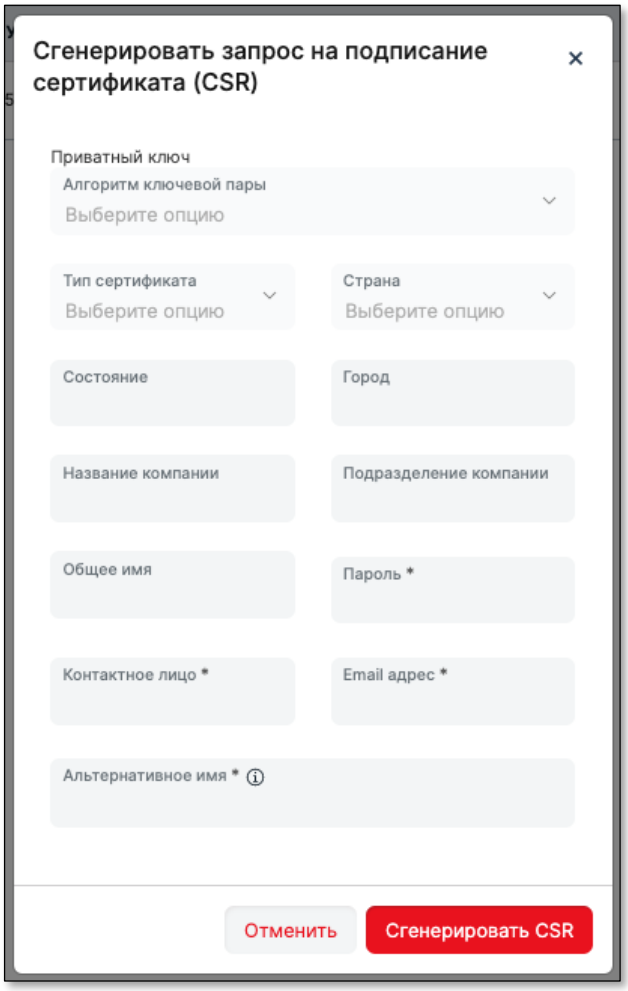

Рисунок 9. Страница «Сгенерировать CSR»

6.1.2 ЗАГРУЗКА КЛЮЧЕЙ SSH

Для загрузки ключей SSH необходимо зайти в основном меню в раздел **Безопасность и доступ -> Сертификаты**. Нажать на кнопку «Добавить новый сертификат». В открывшемся окне выбрать тип сертификата, загрузить файл сертификата и нажать на кнопку «Добавить».

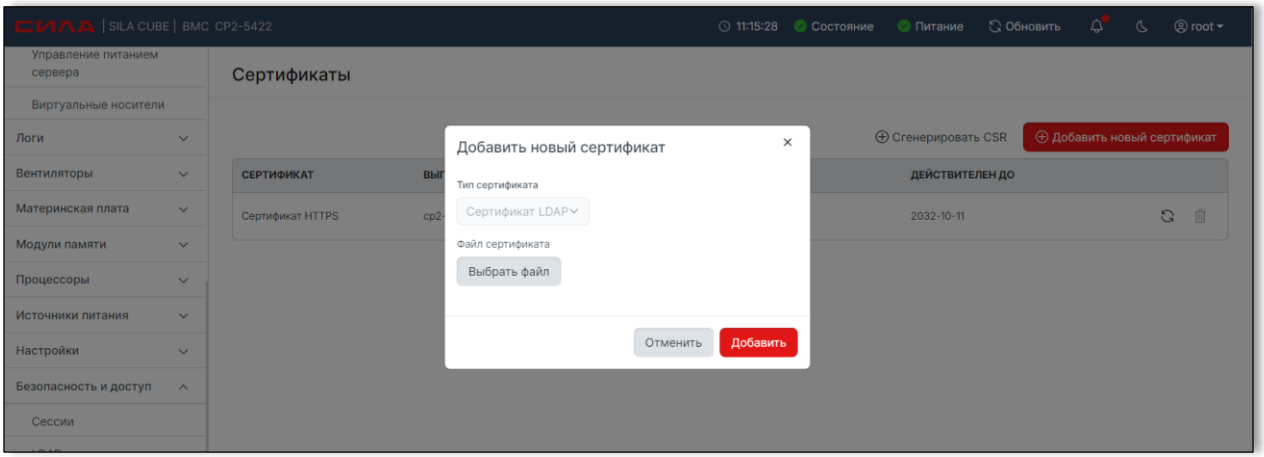

Рисунок 10. Страница «Добавить новый сертификат»

6.1.3 ОТОБРАЖЕНИЕ SSH КЛЮЧЕЙ

Для просмотра существующих SSH ключей необходимо зайти в основном меню в раздел **Безопасность и доступ -> Сертификаты**. В таблице отобразятся загруженные сертификаты.

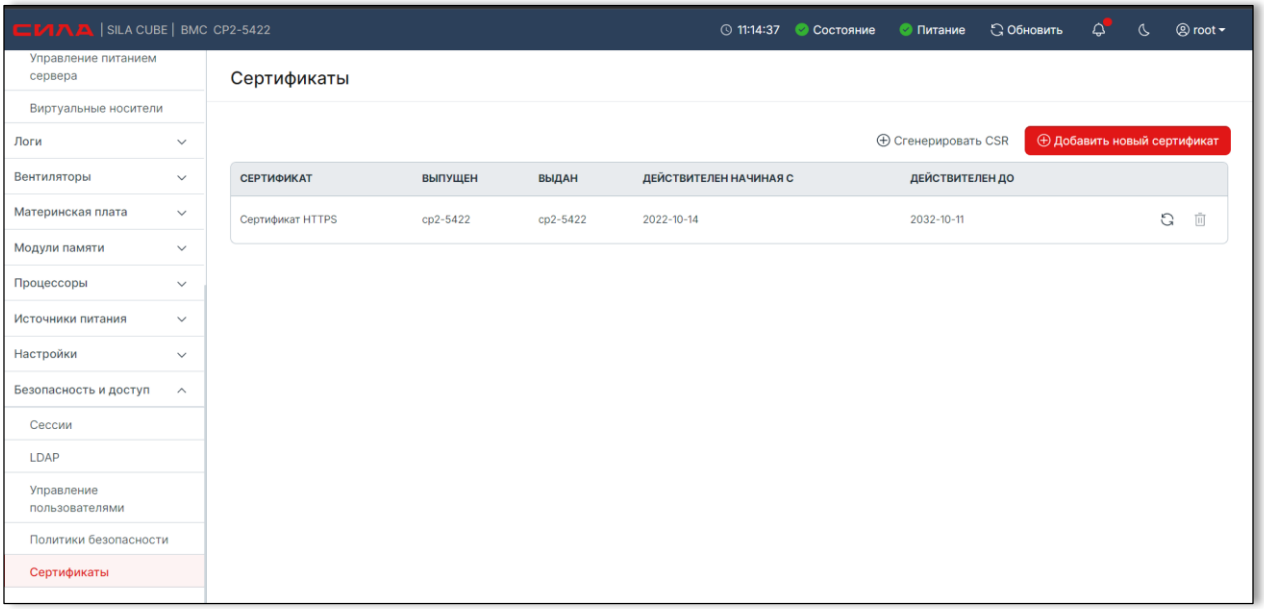

Рисунок 11. Страница «Сертификаты»

6.1.4 УДАЛЕНИЕ SSH-КЛЮЧЕЙ

Для удаления существующих SSH ключей необходимо зайти в основном меню в раздел **Безопасность и доступ -> Сертификаты**. Выбрать нужный сертификат и нажать на кнопку удаления.

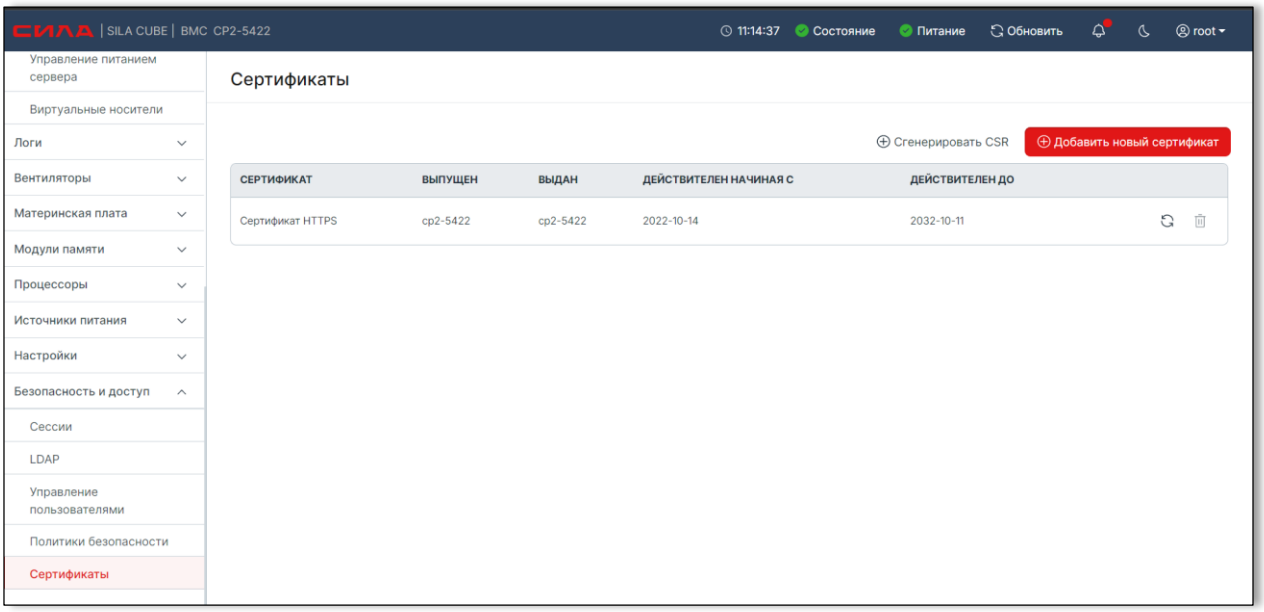

Рисунок 12. Страница «Сертификаты», кнопка удаления

6.2 ВЗАИМОДЕЙСТВИЕ С СИЛА КУБ С ПОМОЩЬЮ IPMI

Пользователю доступны следующие функции:

- конфигурация локальной сети;
- управление электропитанием шасси.

Перед тем, как подключиться с помощью ipmitool, необходимо создать пользователя через web-интерфейс Сила КУБ с паролем без спецсимволов.

ВНИМАНИЕ:

Набор параметров «**-I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST>**» необходим при доступе по сети и может быть опущен при доступе с того же сервера.

Структура команды:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> <CMD>

Где:

<USER> - логин

<PASSWORD> - пароль

<HOST> - IP адрес BMC

<CMD> - команда для выполнения

Пример команды:

ipmitool -I lanplus -C 17 -p 623 -U admin -P 0penBmc1 -H 10.0.0.135 bmc info

Конфигурация локальной сети:

Сводная информация о текущей конфигурации сети:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> lan print <CHANNEL_NUMBER>

Где:

<CHANNEL_NUMBER> - номер канала

Источник получения IP адреса:

DHCP:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> lan set <CHANNEL_NUMBER> ipsrc dhcp

Статический IP адрес:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> lan set <CHANNEL_NUMBER> ipsrc static

Настройка статической адресации:

IP адрес:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> lan set <CHANNEL_NUMBER> ipaddr <ADDRESS>

Маска подсети:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> lan set <CHANNEL_NUMBER> netmask <NETMASK>

Шлюз:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> lan set <CHANNEL_NUMBER> defgw ipaddr <ADDRESS>

Где:

<ADDRESS> - IP адрес

<NETMASK> - маска подсети

Пример команд:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> lan set <CHANNEL_NUMBER> ipaddr 192.168.0.1

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> lan set <CHANNEL_NUMBER> netmask 255.255.254.0

ВНИМАНИЕ:

При изменении конфигурации сетевых интерфейсов (например, при смене IP адреса), необходимо использовать эти настройки в структуре команды (например, параметр **-H <HOST>**).

Управление электропитанием сервера:

Сводное состояние шасси:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> chassis status

Текущее состояние питания:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> chassis power status

Включение питания:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> chassis power on

Выключение питания:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> chassis power off

Перезагрузка:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> chassis power reset

Управление политиками восстановления питания сервера:

Список доступных:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> chassis policy list

Краткое описание политик:

always-on - Всегда включено. Система всегда включается при подаче питания.

always-off - Всегда выключено. Система всегда остаётся выключенной при подаче питания.

previous - Последнее состояние. Система возвращается в своё последнее (включённое/выключенное) состояние при подаче питания.

Установить политику:

ipmitool -I lanplus -C 17 -p 623 -U <USER> -P <PASSWORD> -H <HOST> chassis policy <POWER_POLICY>

Где:

<POWER_POLICY> - политика восстановления питания

6.3 ВЗАИМОДЕЙСТВИЕ С СИЛА КУБ ЧЕРЕЗ RESTFUL API

ВНИМАНИЕ:

Поддержка базового REST API будет прекращена в будущих выпусках. Пожалуйста, используйте Redfish.

Пример запроса:

Команда получения списка датчиков температуры:

curl -u <LOGIN>:<PASSWORD> -k -s https://<BMC>/xyz/openbmc_project/sensors/temperature/list

6.4 ВЗАИМОДЕЙСТВИЕ С СИЛА КУБ ЧЕРЕЗ ПРОТОКОЛ REDFISH

DMTF публикует файлы схем для стандартных данных, применяемых Redfish.

Пример запроса:

Команда получения логов:

curl -u <LOGIN>:<PASSWORD> -k -s https://<BMC>/redfish/v1/Systems/system/LogServices/EventLog/Entries

7 НАСТРОЙКА УЧЕТНЫХ ЗАПИСЕЙ И ПРИВИЛЕГИЙ ПОЛЬЗОВАТЕЛЕЙ

7.1 ТЕКУЩИЕ СЕССИИ ПОЛЬЗОВАТЕЛЕЙ

Пользователь может посмотреть текущие сессии пользователей, перейдя в раздел основного меню **Безопасность и доступ -> Сессии.**

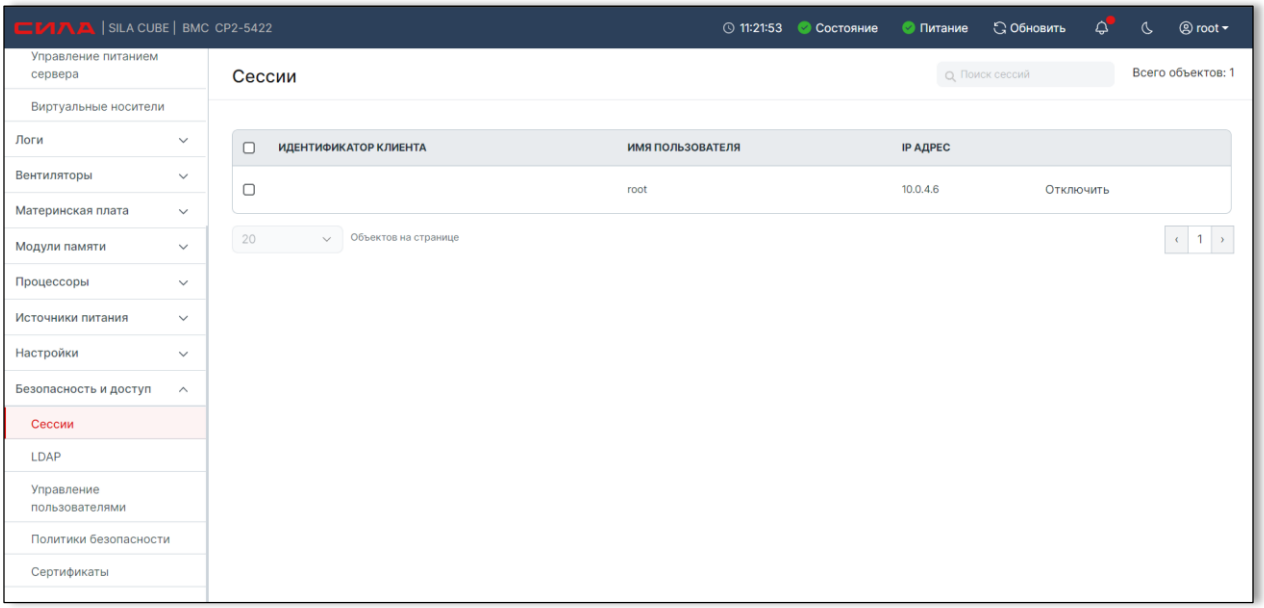

Рисунок 13. Страница «Сессии»

Администратор может отключить сессию пользователя, выбрав ее и нажав на кнопку «Отключить».

7.2 РОЛИ И ПРИВИЛЕГИИ В СИЛА КУБ

В системе предустановлены следующие роли Administrator, Operator, ReadOnly, No Access.

Описание привилегий для каждой роли пользователь может увидеть в разделе **Безопасность и доступ -> Управление пользователями** в таблице «Просмотр описаний привилегий ролей».

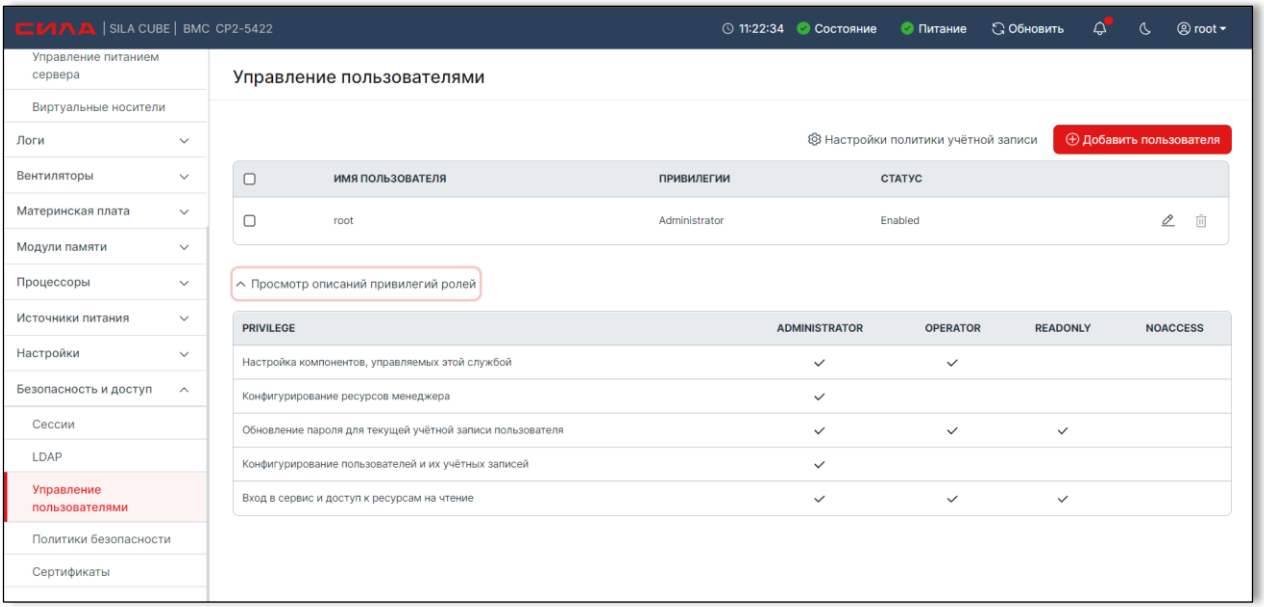

Рисунок 14. Страница «Управление пользователями» и развернутой таблицей «Просмотр описаний привилегий ролей»

7.3 РЕКОМЕНДУЕМЫЕ СИМВОЛЫ В ИМЕНАХ ПОЛЬЗОВАТЕЛЕЙ

Имя пользователя не может начинаться с цифры и не может содержать специальные символы за исключением символа подчеркивания.

7.4 НАСТРОЙКА ЛОКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ

Администратор может управлять локальными пользователями, перейдя в раздел основного меню **Безопасность и доступ -> Управление пользователями**.

Нажав на кнопку «Добавить пользователя», можно добавить пользователя.

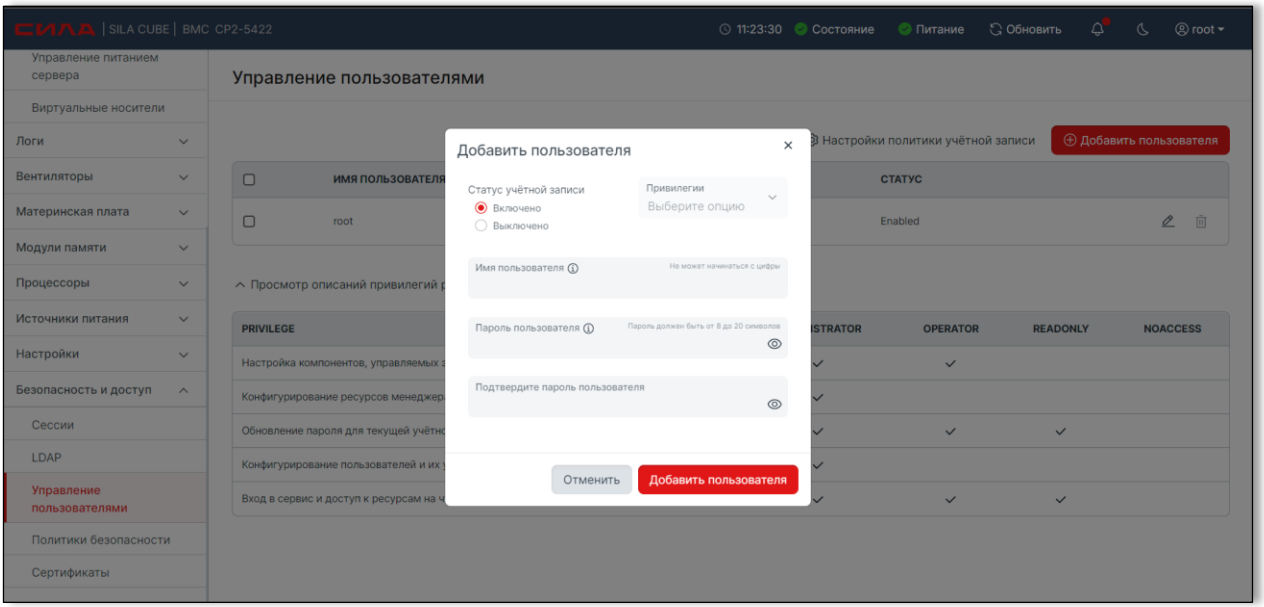

Рисунок 15. Окно добавления нового пользователя

Нажав на кнопку редактирования для выбранного пользователя, Администратор может редактировать данные пользователя.

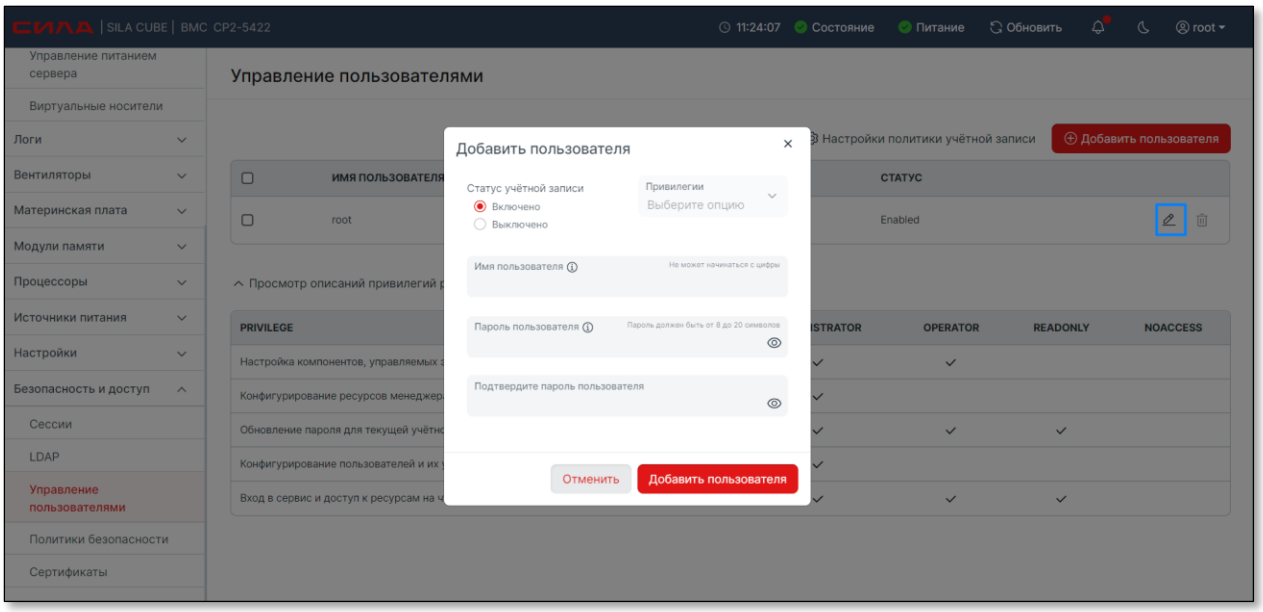

Рисунок 16. Окно редактирования существующего пользователя

Настройка общих пользователей LDAP/AD:

Администратор может настраивать LDAP, перейдя в раздел основного меню **Безопасность и доступ -> LDAP.**

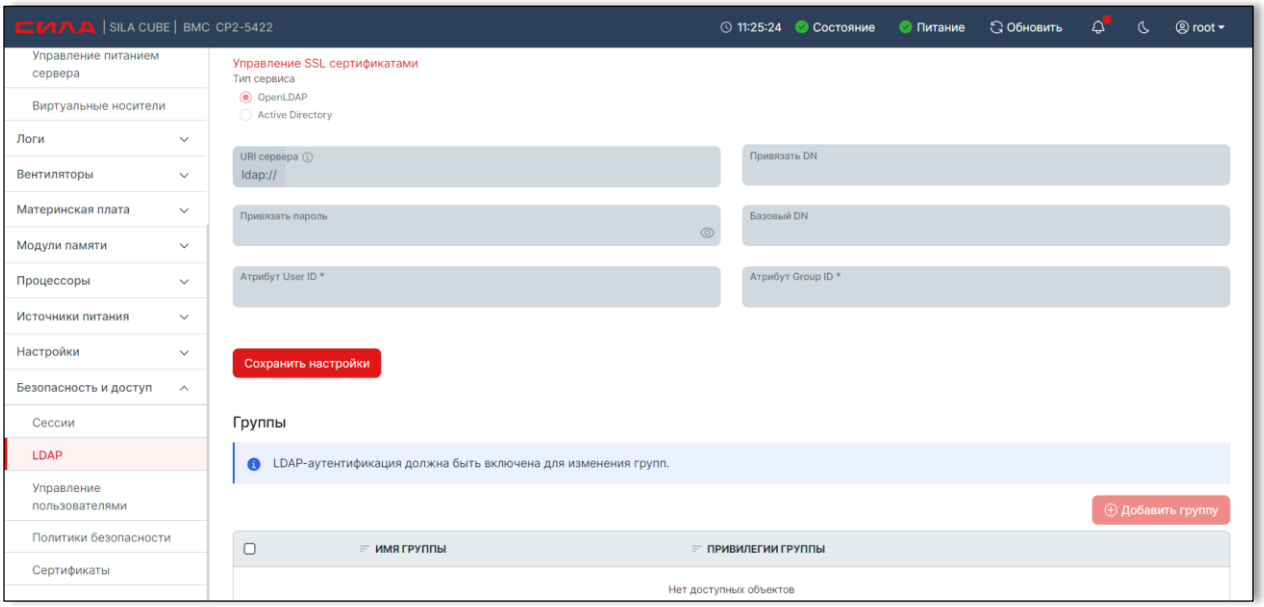

Рисунок 17. Страница «LDAP»

В данном разделе необходимо выбрать checkbox «Аутентификация LDAP» и указать LDAP сервер.

Также необходимо добавить группы ролей, созданных на LDAP сервере, под которыми будут аутентифицировать LDAP пользователи. Для этого необходимо нажать на кнопку «Добавить группу».

Пример данных для настройки подключения (для MS AD):

Server URI - 192.168.0.1

Bind DN - CN=Admin,CN=Users,DC=organisation,DC=local

Bind password - password

Base DN - CN=Users,DC=organisation,DC=local

Group name - Domain Users

Group privilege - Administrator

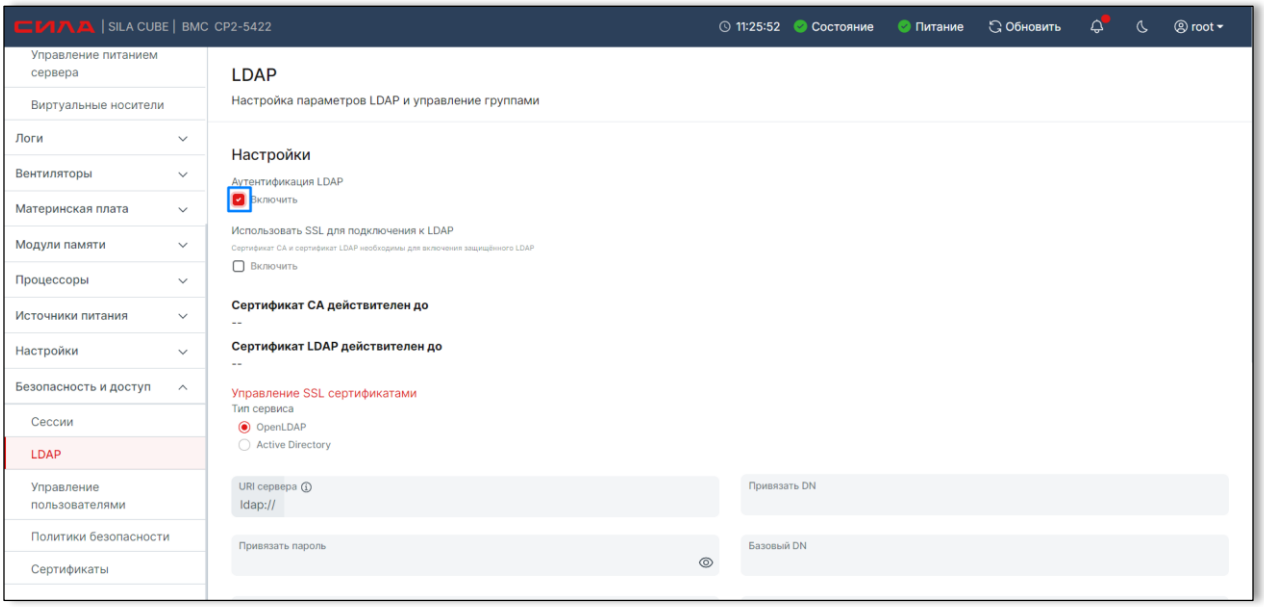

Рисунок 18. Включить аутентификацию LDAP и добавить группу

ВНИМАНИЕ, для аутентификации требуется установка как минимум CA домена AD.

7.4.1 ДОБАВЛЕНИЕ ПОЛЬЗОВАТЕЛЕЙ ЧЕРЕЗ BIOS ДЛЯ МОДЕЛЕЙ CP2-5422, CP4-5422

1. Перейти на пункт меню User ID
2. Выбрать пункт User Name. В открывшемся модальном окне ввести новое имя пользователя.
3. Выбрать пункт User Status. В открывшемся модальном окне выбрать Enabled.
4. Выбрать пункт User Password. В открывшемся модальном окне ввести пароль. Подтвердить в модальном окне сообщение о внесении изменений после нажатия Save and Exit.
5. Выбрать пункт Channel. В открывшемся модальном окне ввести 1. Нажать Enter 2 раза.
6. Выбрать пункт Privilege. В открывшемся модальном окне выбрать нужный пункт привилегий (например, Administrator).
7. Выбрать пункт Channel. В открывшемся модальном окне ввести 3. Нажать Enter 2 раза
8. Выбрать пункт Privilege. В открывшемся модальном окне выбрать нужный пункт привилегий (например, Administrator).
9. Выбрать пункт Add current settings to list. Нажать F10 для сохранения данных и выхода из BIOS (Рисунок 19).

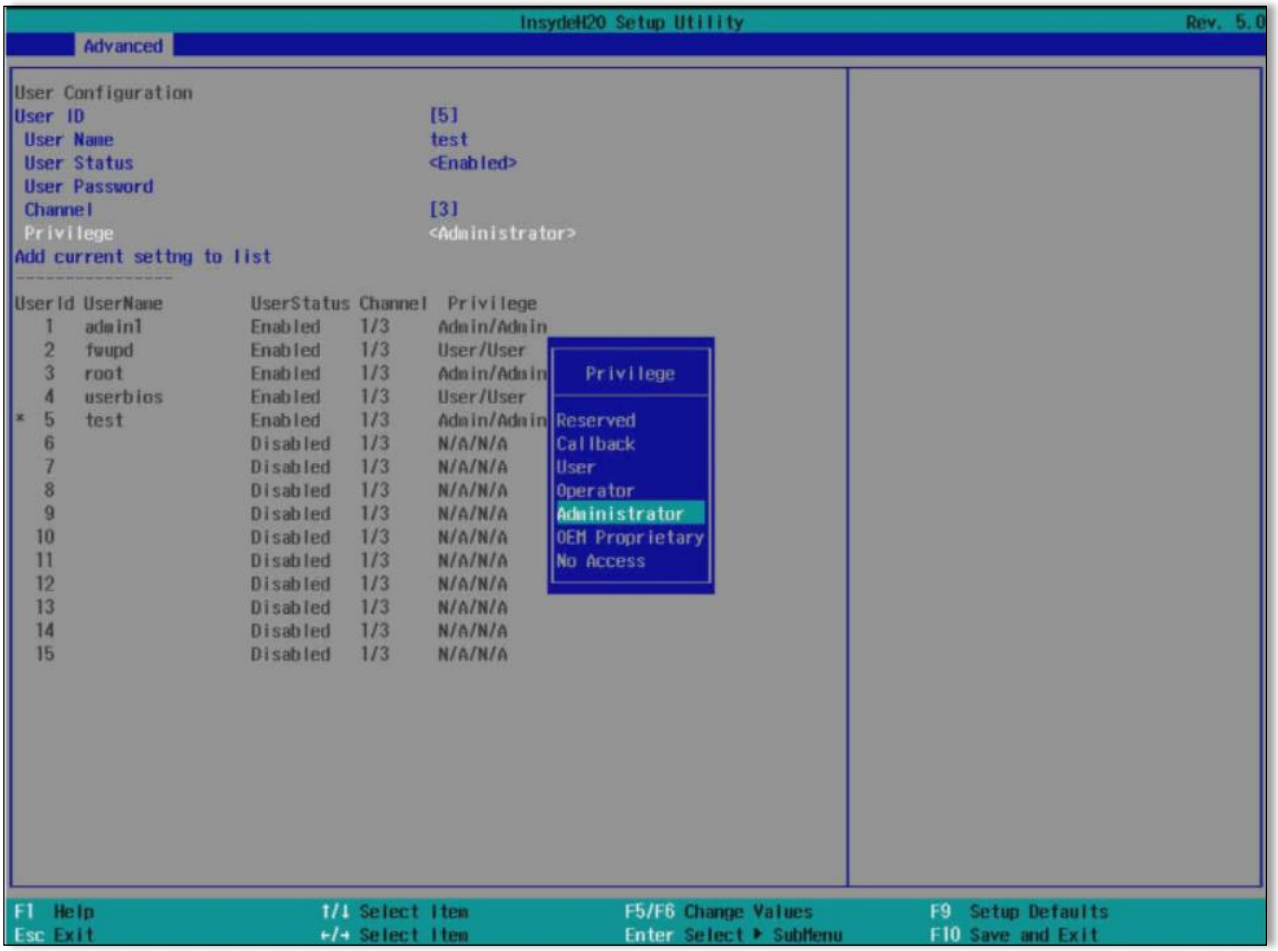

Рисунок 19 Создание пользователя в BIOS

8 ОТПРАВКА ОПОВЕЩЕНИЙ И ПРЕДУПРЕЖДЕНИЙ

8.1 НАСТРОЙКА ОТПРАВКИ ОПОВЕЩЕНИЙ И ПРЕДУПРЕЖДЕНИЙ ПО ПРОТОКОЛУ SNMP V2

В графическом интерфейсе в основном меню необходимо открыть раздел **Настройки -> Настройки передачи информации** (Рисунок 20).

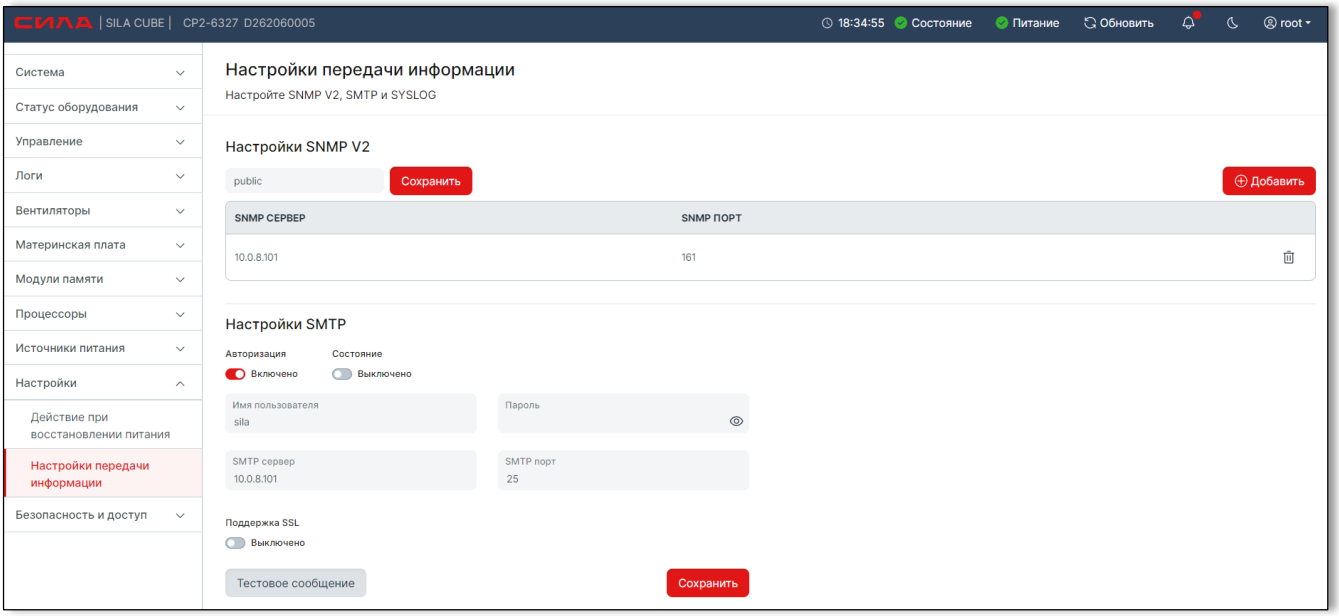

Рисунок 20. Страница «Настройка передачи информации»

Для настройки в разделе Настройки SNMP v2 пользователь может нажать кнопку «Добавить», в открывшемся диалоговом окне ввести параметры настройки (Рисунок 21).

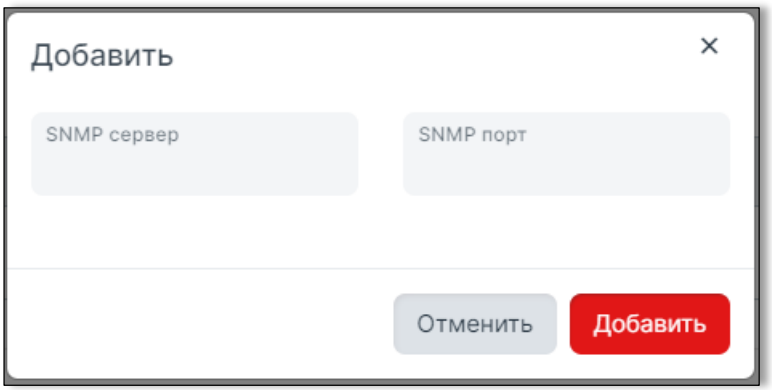

Рисунок 21. Настройки передачи по протоколу SNMP v2

8.2 НАСТРОЙКА ОТПРАВКИ ОПОВЕЩЕНИЙ И ПРЕДУПРЕЖДЕНИЙ ПО ПРОТОКОЛУ SMTP

В графическом интерфейсе в основном меню необходимо открыть раздел **Настройки -> Настройки передачи информации** (Рисунок 22).

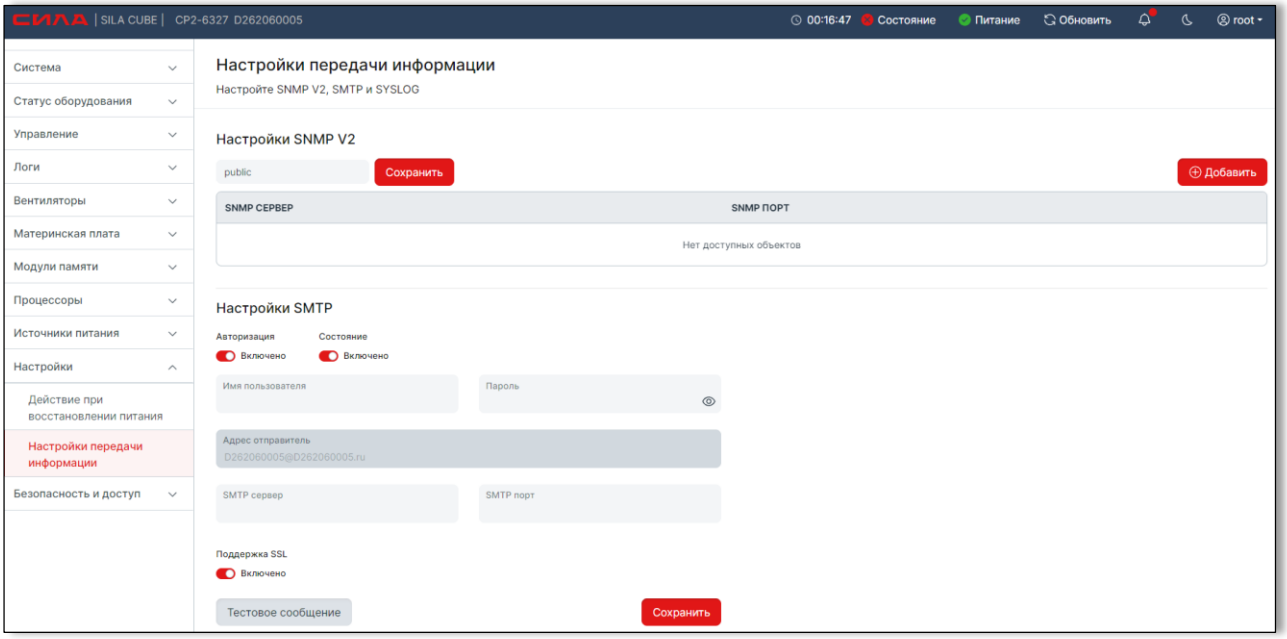

Рисунок 22. Страница «Настройка передачи информации»

В интерфейсе Сила КУБ доступно управление протоколом SMTP. Пользователь может:

- включать и отключать сервис SMTP
- включать и отключать авторизацию в сервисе SMTP
- менять адрес отправителя сообщений сервиса SMTP

8.2.1 УПРАВЛЕНИЕ СОСТОЯНИЕМ ПРОТОКОЛА SMTP

Для включения SMTP переведите соответствующий переключатель в состояние «Включено», для включения – в состояние «Выключено».

8.2.2 УПРАВЛЕНИЕ АВТОРИЗАЦИЕЙ SMTP

Для включения авторизации SMTP необходимо перевести соответствующий переключатель в состояние «Включено», а затем ввести следующие параметры:

- Имя пользователя
- Пароль
- IP-адрес SMTP-сервера
- SMTP-порт

После ввода требуется нажать кнопку «Сохранить».

Затем можно добавить email получателей, нажав кнопку «Добавить» (Рисунок 23).

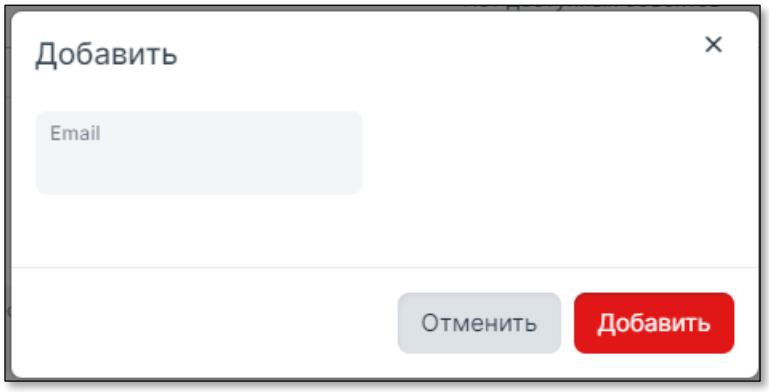

Рисунок 23. Добавление email получателей

Для проверки корректности настроек нажать кнопку «Тестовое сообщение».

8.2.3 РЕДАКТИРОВАНИЕ АДРЕСА ОТПРАВИТЕЛЯ СООБЩЕНИЙ ПО SMTP

Для редактирования адреса отправителя необходимо перевести переключатель «Авторизация» в состояние «Выключено», а затем ввести новый адрес в соответствующее поле. После ввода требуется нажать кнопку «Сохранить».

Если аутентификация SMTP включена, то письма будут приходить от отправителя ИМЯ_ХОСТА_КУБ@ИМЯ_ХОСТА_КУБ.ru.

8.3 НАСТРОЙКА ОТПРАВКИ ОПОВЕЩЕНИЙ И ПРЕДУПРЕЖДЕНИЙ ПО ПРОТОКОЛУ SYSLOG

В графическом интерфейсе в основном меню необходимо открыть раздел **Настройки -> Настройки передачи информации** (Рисунок 24).

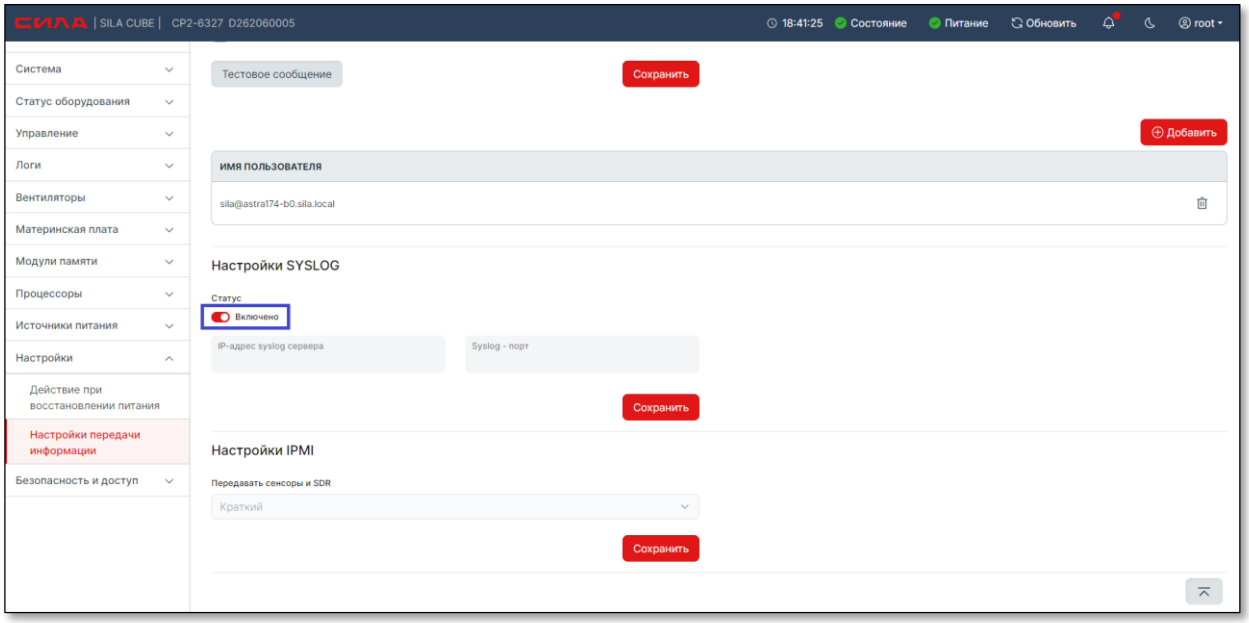

Рисунок 24. Страница «Настройка передачи информации»

Для включения SYSLOG необходимо перевести соответствующий переключатель в состояние «Включено», а затем ввести параметры:

- IP-адрес syslog-сервера
- Syslog-порт

Нажать кнопку «Сохранить».

8.4 НАСТРОЙКА ОТПРАВКИ ОПОВЕЩЕНИЙ И ПРЕДУПРЕЖДЕНИЙ ПО IPMI

В графическом интерфейсе в основном меню необходимо открыть раздел **Настройки -> Настройки передачи информации** (Рисунок 25).

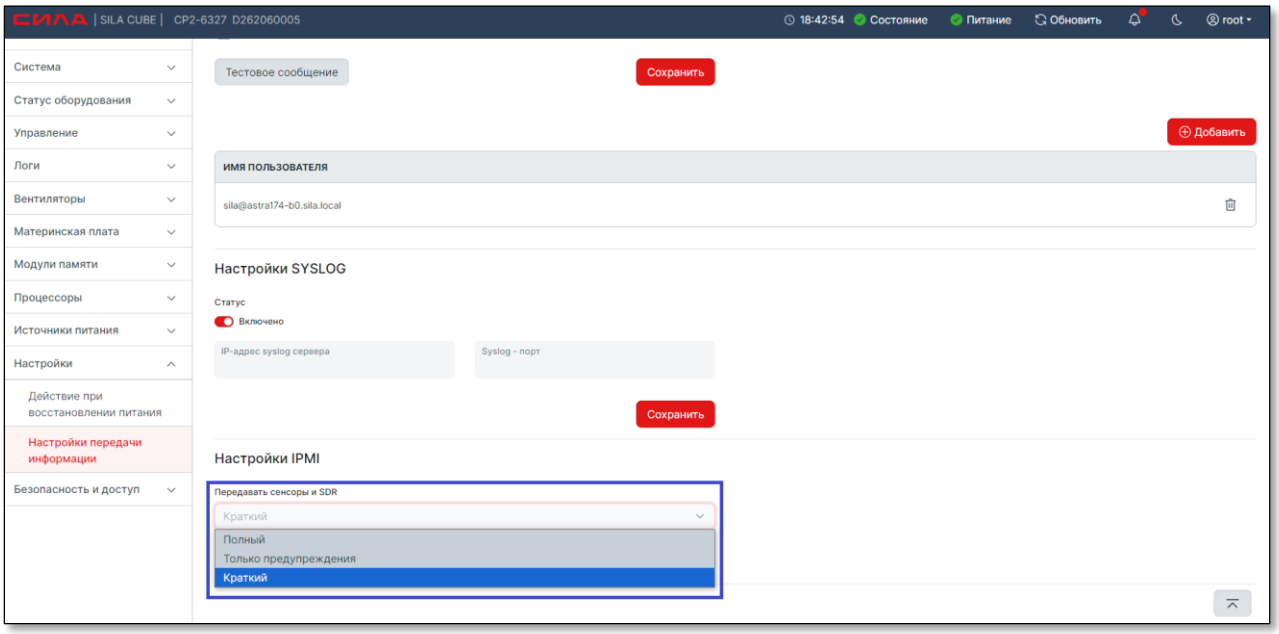

Рисунок 25 Страница «Настройка передачи информации»

Выбор варианта передачи данных о сенсорах и SDR:

- **Полный** – передавать полный набор сенсоров
- **Только предупреждения** – передавать только датчики, показания которых выходят за пороговые значения
- **Краткий** – передавать состояния групп компонентов.

8.5 ИНЫЕ СПОСОБЫ ОТПРАВКИ ОПОВЕЩЕНИЙ И ПРЕДУПРЕЖДЕНИЙ

Используйте SILA-MIB.txt с BMC и snmp утилиты (например, ManageEngine MibBrouser Free Tool) для получения данных snmp протоколу.
Файл SILA-MIB.txt можно загрузить из каталога BMC /usr/share/snmp/mibs или через https – клиент (например браузер или curl) по адресу:

https://<IP-addres-of-BMC-host>/mibs/SILA-MIB.txt

9 УПРАВЛЕНИЕ ЛОГАМИ

9.1 ОТОБРАЖЕНИЕ ЖУРНАЛА СОБЫТИЙ

ВНИМАНИЕ:

Количество записей в логах ограничено до 1024 для моделей CP1-6326 и CP2-6327.

Зайти в основном меню в раздел **Логи -> Журнал событий**.

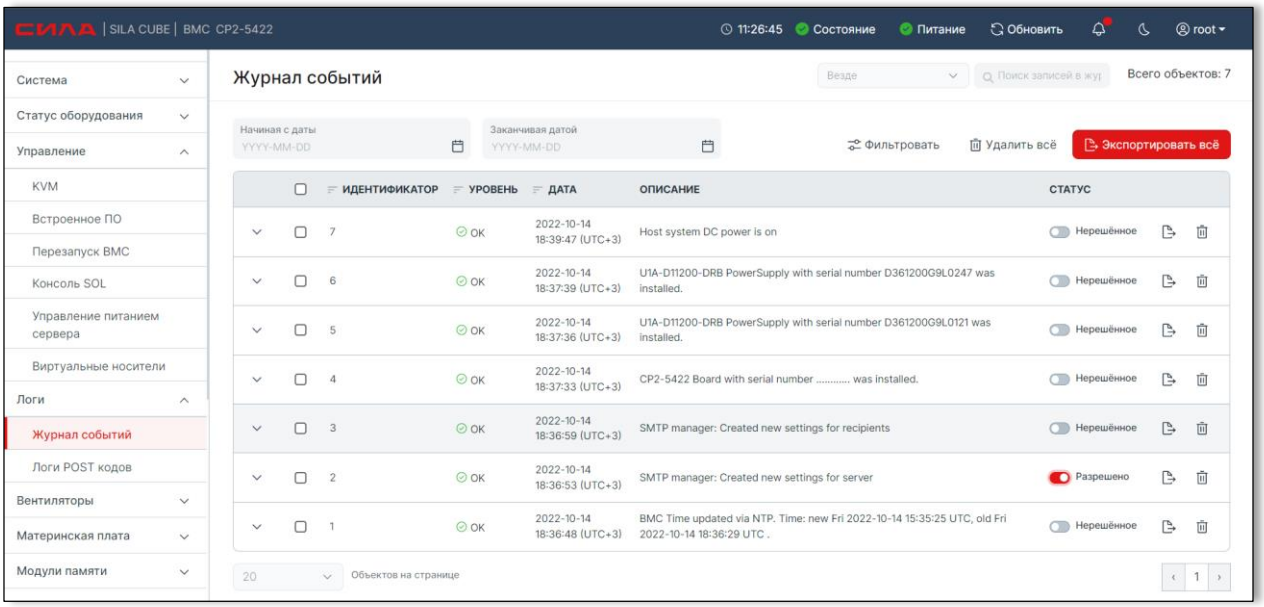

Рисунок 26. Страница «Журнал событий»

По каждому логу можно получить информацию, нажав на кнопку «Экспортировать» (элемент под цифрой 1 на Рисунок 27). Лог сохраняется на локальном компьютере в формате JSON.

Пользователь может удалить лог, нажав на соответствующий элемент (элемент под цифрой 2 Рисунок 27).

Пользователь может отметить лог как «решенный», нажав на переключатель в статусе лога (элемент под цифрой 3 на Рисунок 27).

Пользователь может управлять массово всеми логами, нажав на чекбокс в шапке таблицы (элемент под цифрой 4 на Рисунок 27).

Логи событий RAID-контроллеров и работа с ними описаны в разделе 14.9.

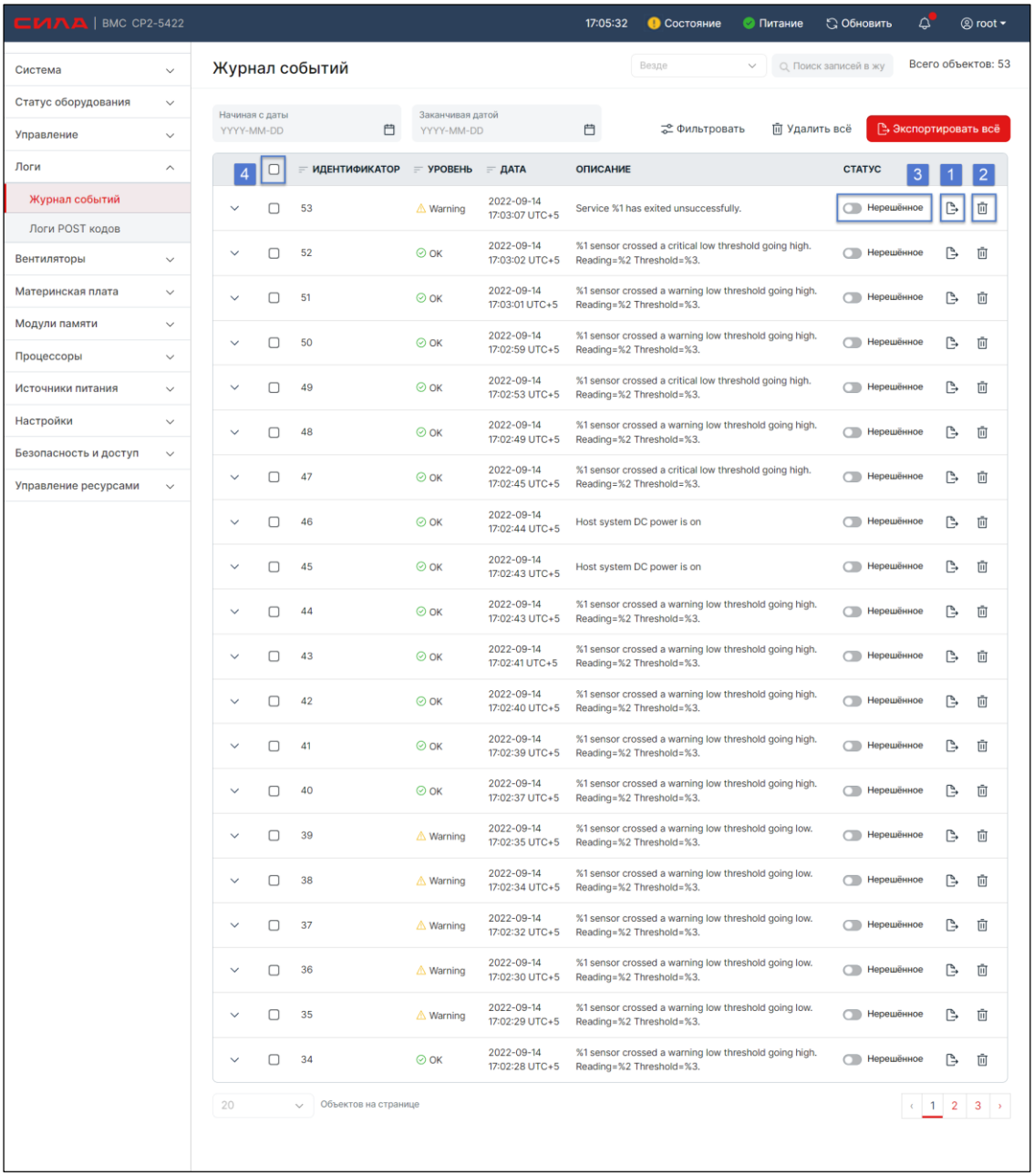

Рисунок 27. Страница «Журнал событий», массовое выделение логов

9.2 АВТОРЕШЕНИЕ СОБЫТИЙ

ВНИМАНИЕ:

Авторешение событий доступно для моделей CP1-6326 и CP2-6327.

При включении авторешения событий логи с уровнями «WARNING» и «CRITICAL» будут автоматически переводиться в статус «Решенные» после прихода соответствующего события с уровнем «OK». Если все «WARNING» и «CRITICAL» события находятся в статусе «Решенные», индикатор «Состояние» в верхней панели станет зеленым.

Пользователь может включить авторешение событий, нажав на соответствующий переключатель (Рисунок 28).

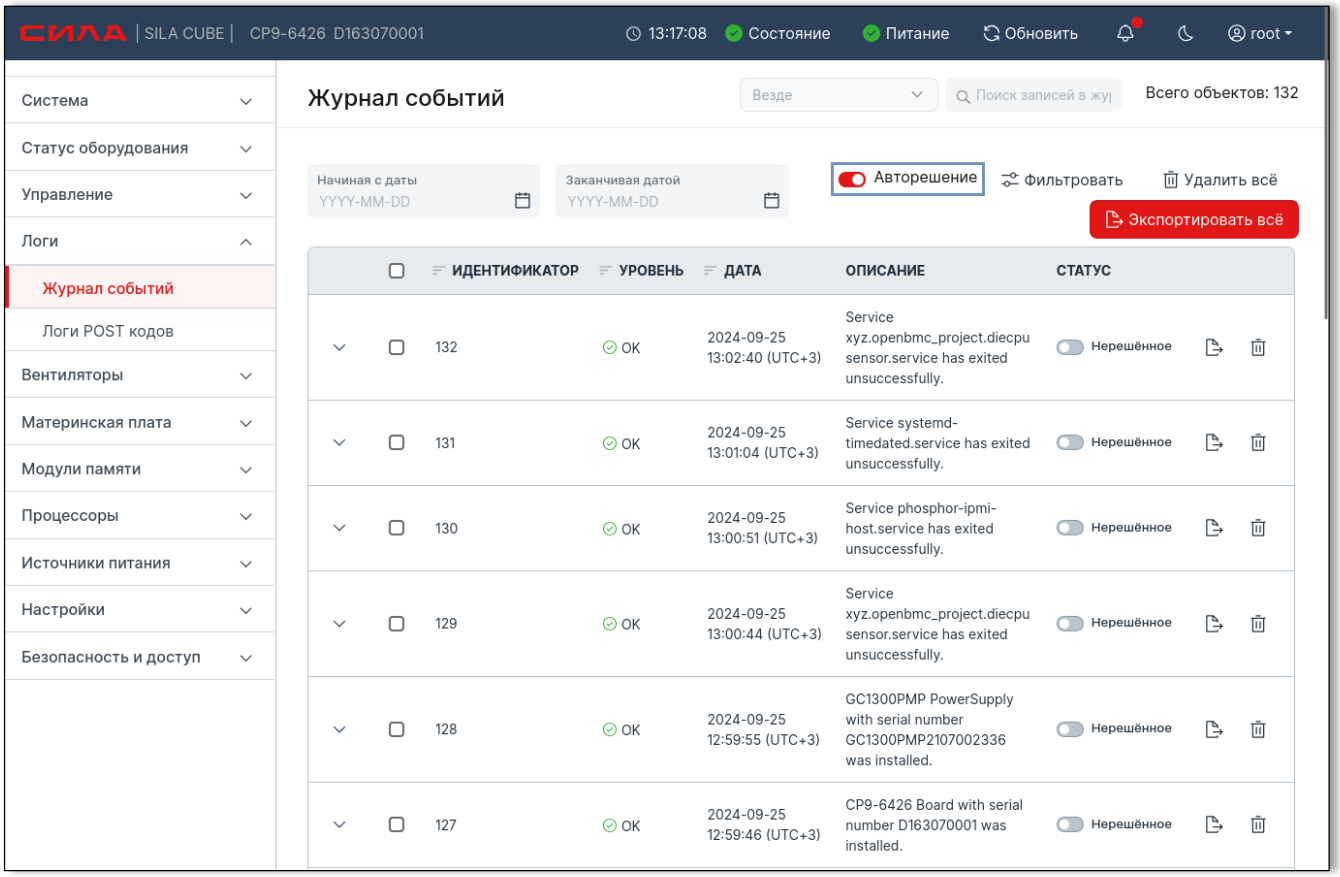

Рисунок 28. Страница «Журнал событий», авторешение событий

9.3 ВЫГРУЗКА ЛОГОВ

Помимо выгрузки каждого лога по отдельности, можно экспортировать весь журнал событий сразу также в формате JSON. Полный экспорт можно сделать на странице **Система -> Обзор**. На странице есть соответствующая кнопка, а также выбор: экспортировать все или только отфильтрованные события (Рисунок 29).

Доступные фильтры событий:

- журнал событий
- сетевые адаптеры
- RAID-контроллеры
- датчики
- информация о системе
- системные события

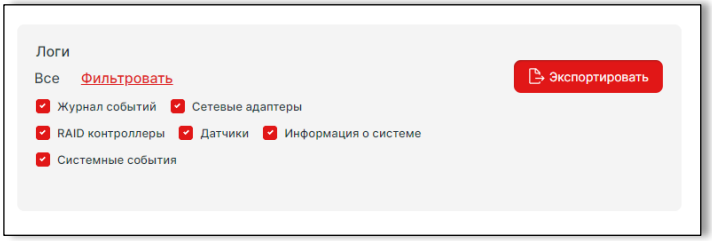

Рисунок 29. Страница «Обзор», фильтры логов

10 УПРАВЛЕНИЕ ЭЛЕКТРОПИТАНИЕМ ИЗ ИНТЕРФЕЙСА СИЛА КУБ

Пользователь может управлять электропитанием, перейдя в раздел основного меню **Управление -> Управление питанием сервера**.

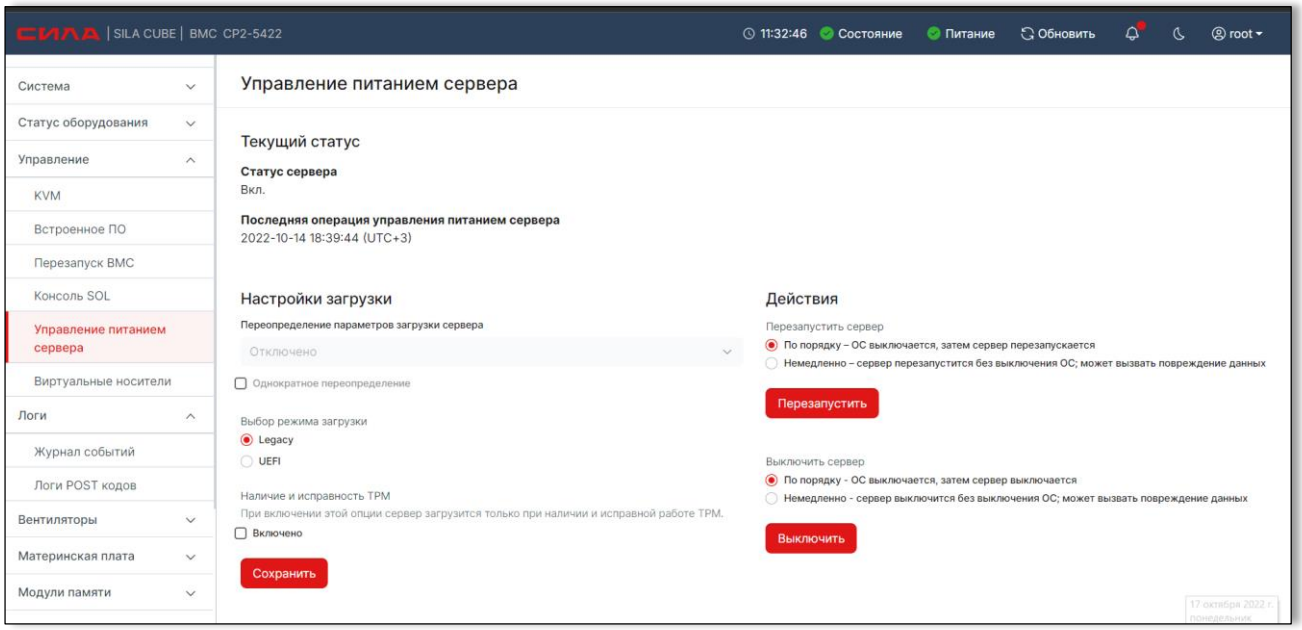

Рисунок 30. Страница «Управление питанием сервера»

Пользователь может управлять политиками питания, перейдя в раздел основного меню **Настройки - > Действие при восстановлении питания**.

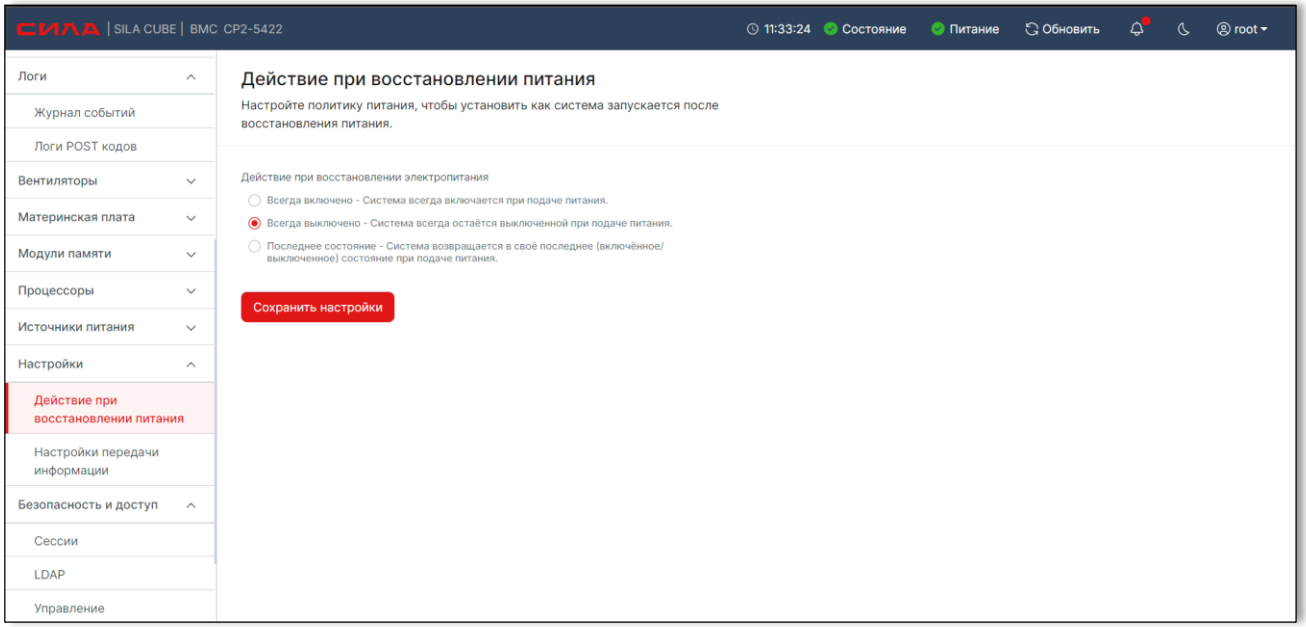

Рисунок 31. Страница «Действие при восстановлении питания»

В данном разделе меню пользователь может выбрать правило включения питания системы Сила КУБ после включения питания основного сервера.

Примечание: для корректной работы политики питания системы на серверах СР2-5422, СР4-5422 необходимо убедиться, что параметр в BIOS – Advenced – ACPI Table/Futures Control – FACP – RTC S4 Wakeup установлен в положение Disabled.

11 НАСТРОЙКА И МОНИТОРИНГ СЕТЕВЫХ ИНТЕРФЕЙСОВ BMC

Пользователь может управлять и контролировать сетевые интерфейсы, перейдя в раздел в основном меню **Система -> Сеть.**

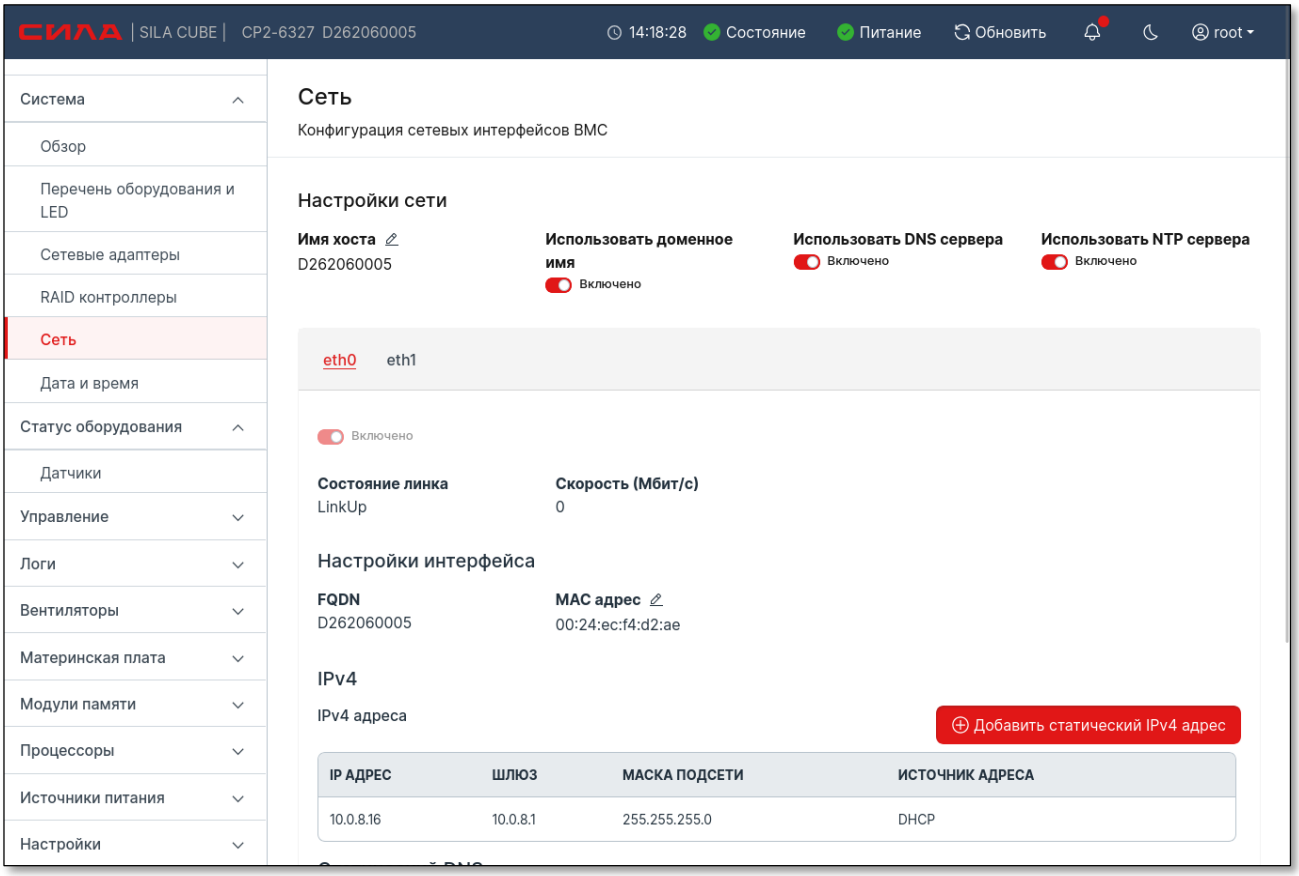

Рисунок 32. Страница «Сеть»

В настройках сети пользователь может выбрать использование доменного имени, DNS-сервера и NTP-сервера.

Для каждого сетевого интерфейса есть своя закладка (например, eth0 и eth1), где для интерфейса можно:

- добавить статический IP-адрес
- увидеть IP-адрес, назначенный DNS-сервером
- включать и выключать его с помощью переключателя (Рисунок 33)

ВНИМАНИЕ:

Выключение интерфейса eth0 недоступно в целях безопасности, так как необходимо, чтобы работал хотя бы один Ethernet-интерфейс.

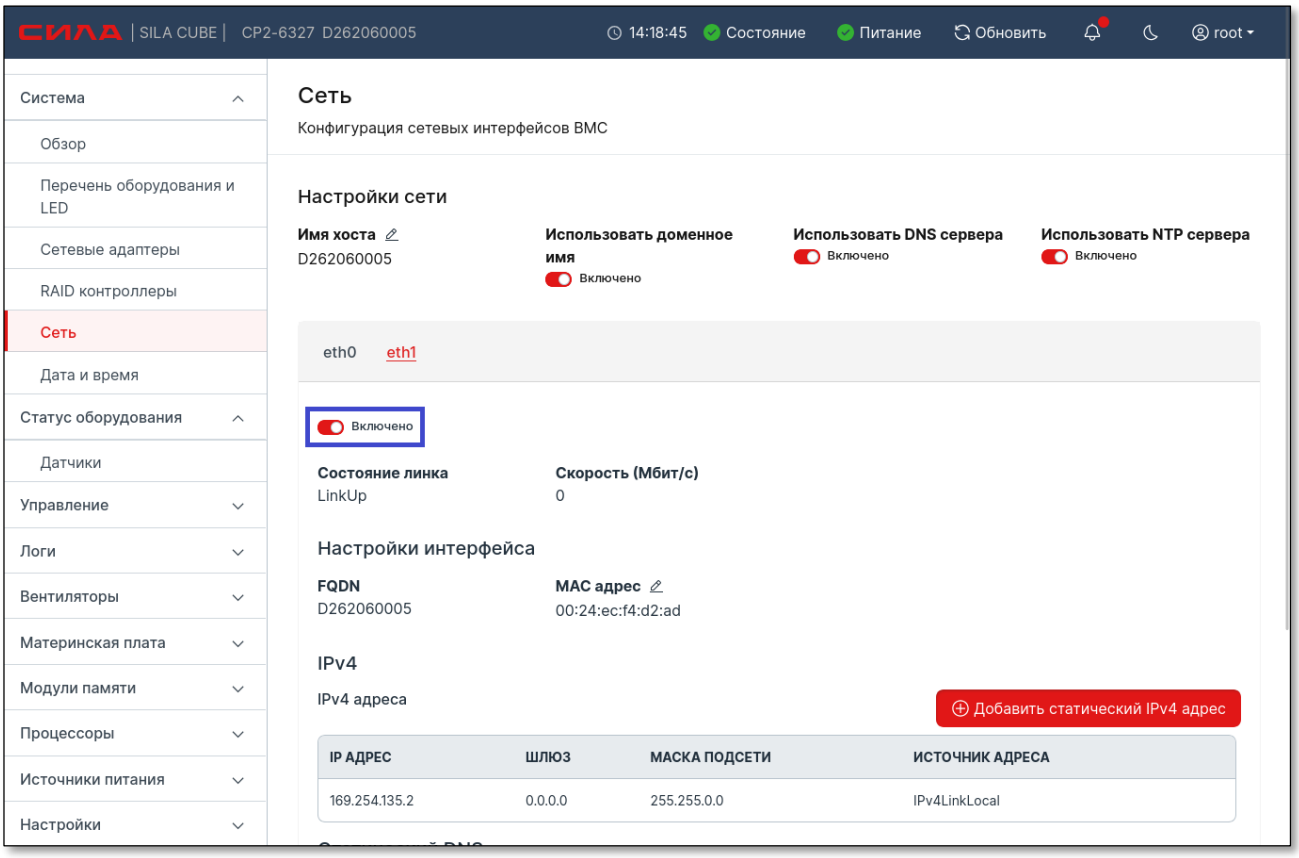

Рисунок 33. Переключатель состояния Ethernet-интерфейса

12 УПРАВЛЕНИЕ УСТРОЙСТВАМИ ХРАНЕНИЯ

Управление устройствами хранения в настоящий момент не реализовано.

13 УПРАВЛЕНИЕ ВИРТУАЛЬНЫМИ УСТРОЙСТВАМИ

Пользователь может управлять виртуальными устройствами, перейдя в раздел основного меню **Управление -> Виртуальные носители** (Рисунок 34**)**.

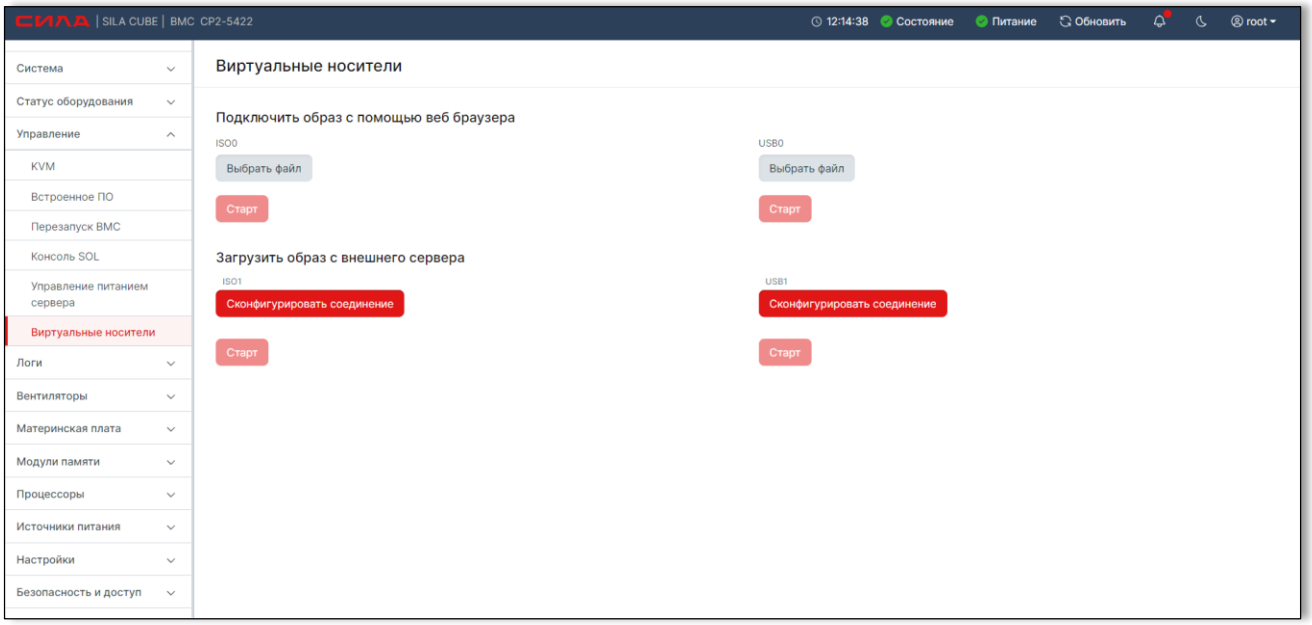

Рисунок 34. Страница «Виртуальные носители»

На странице «Виртуальные носители» пользователь может загружать/подключать образ виртуального носителя с удаленного сервера или локально со своего компьютера. Содержимое образа в виде виртуального устройства может быть прочитано в запущенной операционной системе хоста, либо операционная система может быть установлена с носителя.

13.1 РЕЖИМЫ/ПРЕДОПРЕДЕЛЁННЫЕ ТИПЫ УСТРОЙСТВ

На рисунке 34 представлены 2 типа виртуальных устройств:

- «ISOx» - для подключения файлов-образов в виртуальное «cdrom» устройство;
- «USBx» - для подключения файлов-образов в виртуальное «usb» устройство;

Для образов формата iso9660 используется тип виртуального устройства «cd-rom», для образов более современных форматов используется подключение типа «usb».

На странице так же представлены два способа подключения виртуальных устройств:

- через «web-браузер» пользователя (файл образа физически находится локально на стороне клиента, и его содержимое передаётся по установившемуся https соединению);
- с «внешнего сервера» (файл образа находится на сервере, на BMC передаётся только его адрес (URL));

Особенности режимов:

- «USBx» - предпочтительный тип (представляется как «USB Mass Storage»);
- «ISOx» - с целью поддержки носителей формата iso9660;
- «FLOPPYx» - поддержка образов/устройства не осуществляется;
- «через web-браузер» - т.к. соединение может быть нестабильным, медленным, объём носителя (файла-образа) может быть сравнительно большим, предпочтение следует отдавать варианту с образами на «внешнем сервере». Более того, поскольку источник данных находится на стороне браузера, обновление страницы приведёт к потере установившегося соединения, другими словами, к экстренному/форсированному извлечению образа из устройства. Данный метод может быть полезен для небольших, редких/случайных данных подобно дискам с драйверами устройств;
- «с внешнего сервера» - это более предпочтительный способ, т.к. он централизованный, сервер может иметь с BMC более надёжное, в отличии от браузера, соединение.

Доступ к образам на «внешнем сервере» настраивается с помощью URL.

Поддерживаемые протоколы (schema):

- "http://";
- “https://”
- "ftp://";
- "nfs://";
- "smb://";

При указании URL есть возможность указать имя пользователя и пароль (в отдельных полях формы, не URL) для авторизации BMC на сервере, а также флаг разрешения записи в файл образа, если это применимо.

Особенность: в случае "smb://" имя пользователя по умолчанию не является пустым, оно неявно задано как "OpenBmc".

13.2 ОСОБЕННОСТИ КОНТРОЛЯ УСТРОЙСТВ СО СТОРОНЫ WEB-БРАУЗЕРА

Состояние подключенных образов с внешнего сервера может быть проконтролировано путём перезагрузки страницы.

Аналогичное действительно для операции извлечения образа. Задержка операции подключения/извлечения может достигать минуты.

13.3 ЗАГРУЗКА С ВИРТУАЛЬНОГО НОСИТЕЛЯ

В Boot-Manager-е BIOS-а «USBx» устройство будет представлено как «Linux File-Stor Gadget», «ISOx» - как «Linux File-CD Gadget», например,

Рисунок 35. Окно Boot-Manager-а BIOS-а

Факт обнаружения виртуального носителя BIOS не обязательно означает возможность загрузки с него, например, некоторые форматы образов могут не поддерживаться BIOS, также некоторые образы могут работать только в одном из режимов (cd-rom/usb).

13.4 ФОРМАТ ОБРАЗА С ПОДДЕРЖКОЙ EFI ЗАГРУЗКИ

При наличии возможности загрузки с виртуального устройства в режиме EFI BIOS отдельно добавит соответствующий пункт («EFI USB Device») как на Рисунок 36.

Контроль за загрузкой в режиме EFI можно осуществить через «EFI Shell».

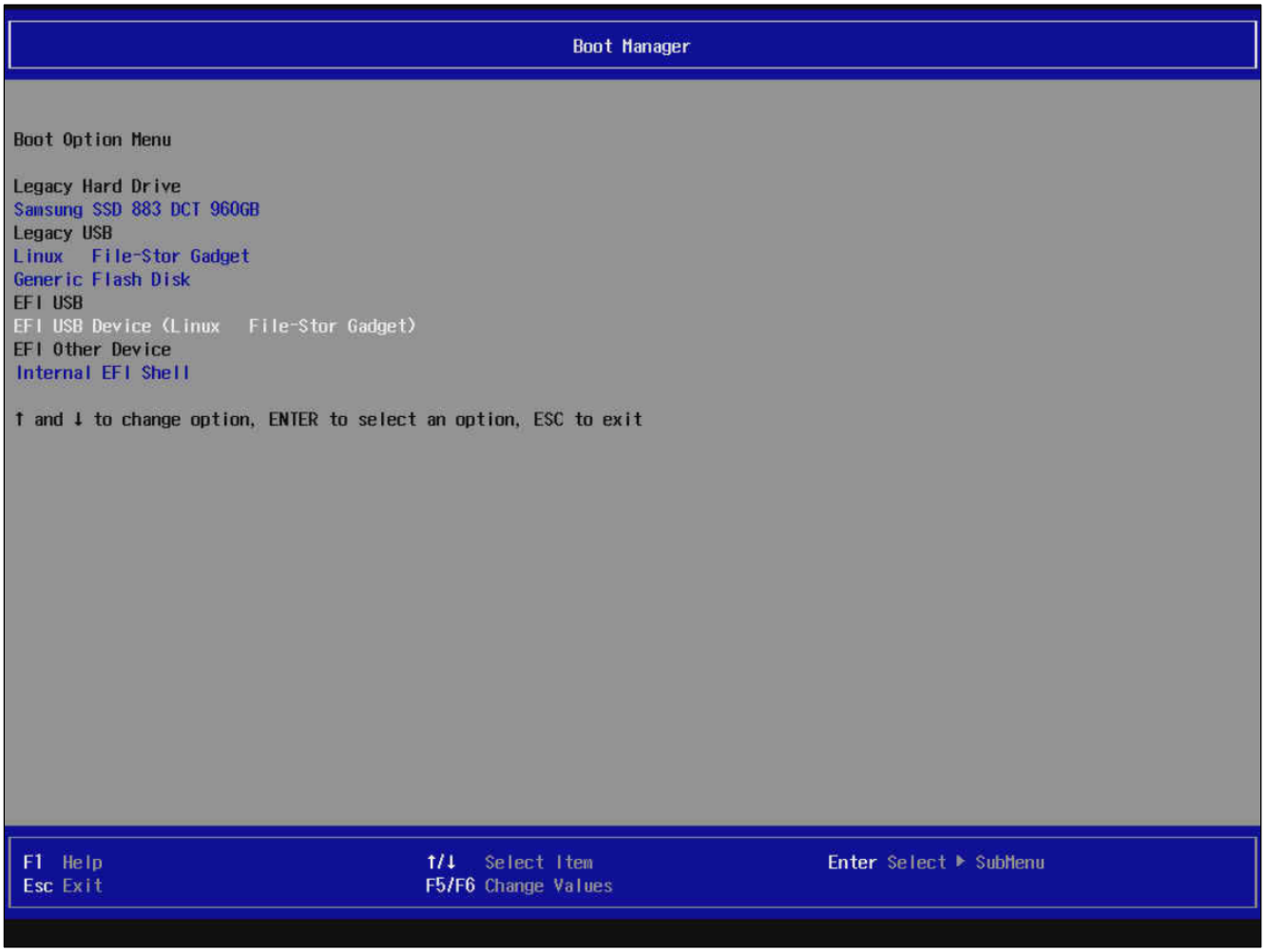

Рисунок 36. Виртуальное устройство в режиме EFI

14 УПРАВЛЕНИЕ RAID-КОНТРОЛЛЕРАМИ

ВНИМАНИЕ:

Управление RAID-контроллерами доступно для моделей CP1-6326 и CP2-6327. Некорректная работа данного функционала может быть вызвана несовместимостью ПО Сила КУБ с вашим RAID-контроллером. За актуальным списком поддерживающихся типов RAID-контроллеров обращайтесь к производителю Сервера.

В веб-интерфейсе Сила КУБ можно:

- просматривать информацию о RAID
- производить операции с физическими накопителями
- управлять дисковыми массивами
- управлять логическими накопителями

Перед работой с RAID-контроллерами убедитесь, что они обновлены до последней версии.

14.1 ОТОБРАЖЕНИЕ ИНФОРМАЦИИ О RAID

При выборе в левом основном меню раздела **Система -> RAID management** в правой части отображается информация (Рисунок 37):

- о RAID-массивах
- о физических накопителях
- о дисковых массивах
- о логических накопителях

14.1.1 ИНФОРМАЦИЯ О RAID-МАССИВАХ

Информация, которая отображается о RAID-массивах:

- имя
- статус (всегда Enabled)
- серийный номер
- шифр
- версия встроенного ПО

Каждый RAID-массив можно раскрыть, чтобы посмотреть подробную информацию.

14.1.2 ИНФОРМАЦИЯ О ФИЗИЧЕСКИХ НАКОПИТЕЛЯХ

Список физических накопителей формируется на основе вставленных дисков в переднюю панель сервера.

У физических накопителей есть:

- имя
- номер группы слотов и слота
- состояние
- серийный номер
- шифр

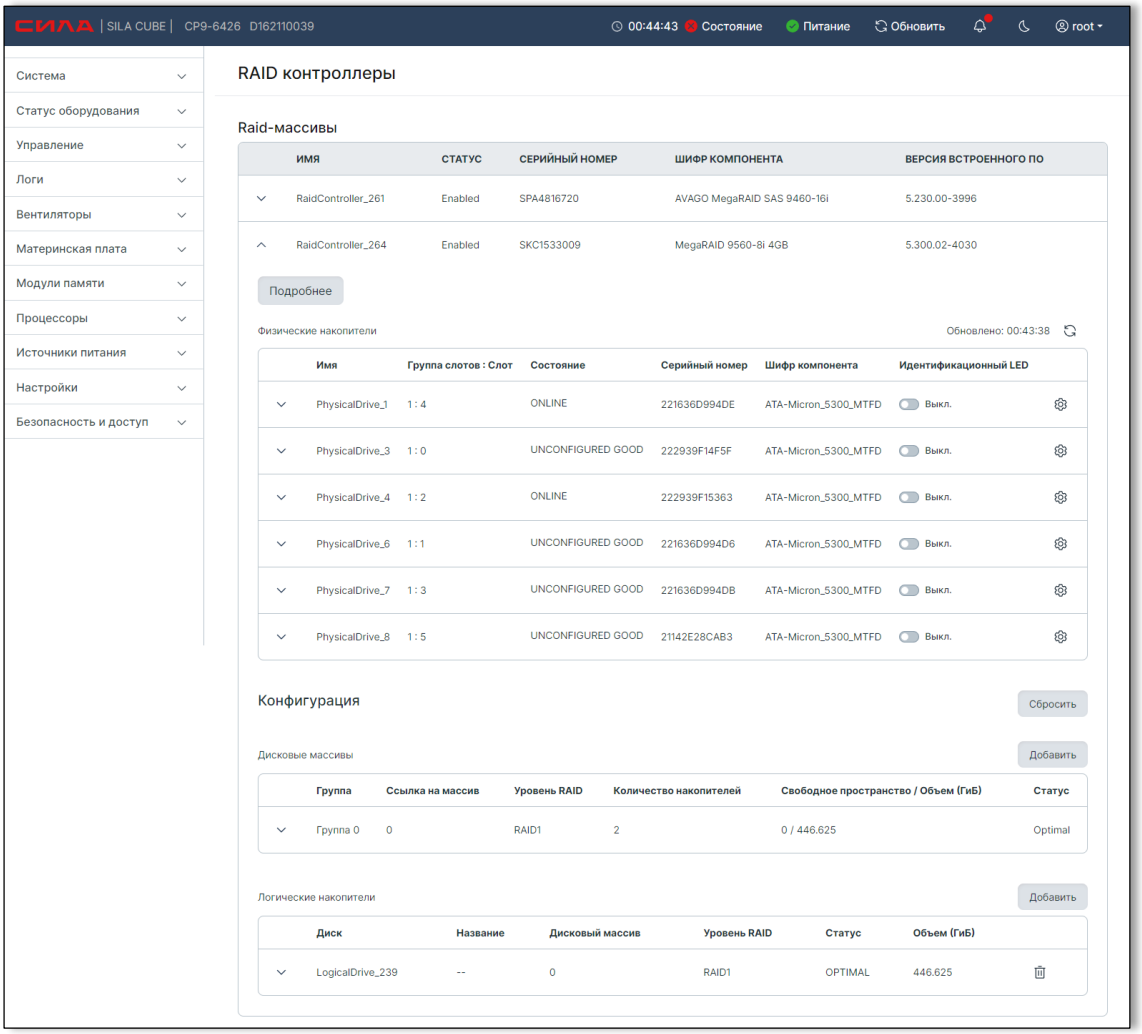

Рисунок 37. Страница «RAID контроллеры»

Состояния вставленных физических накопителей могут быть следующими:

- ONLINE (доступен для массива дисков и является частью виртуального накопителя)
- OFFLINE (содержит недопустимые данные и является частью виртуального накопителя)
- HOT SPARE (резервный накопитель)
- REBUILD (хранит данные виртуального накопителя для восстановления)
- FAILED (неустранимая ошибка накопителя, находящегося в статусе ONLINE или HOT SPARE)
- MISSING (отсутствие накопителя в статусе ONLINE в передней панели сервера)
- UNCONFIGURED GOOD (доступен для массива дисков, но не сконфигурирован как часть виртуального накопителя или резервный)
- UNCONFIGURED BAD (неустранимая ошибка неинициализированного накопителя или находящегося в статусе UNCONFIGURED GOOD)
- COPYBACK (копирование и перенос данных на накопитель)

Каждый физический накопитель можно раскрыть, чтобы посмотреть подробную информацию.

Переключение физических накопителей в различные состояния описано в разделе 14.2.

14.1.3 ИНФОРМАЦИЯ О ДИСКОВЫХ МАССИВАХ

Дисковые массивы добавляются пользователем на основе физических накопителей. Информация, которая отображается о дисковых массивах:

- номер группы
- ссылка на массив
- уровень RAID (зависит от количества дисков)
- количество накопителей в массиве
- объем свободного пространства (ГиБ)
- общий объем (ГиБ)
- статус

Статус массива дисков формируется по статусам его логических накопителей и может быть следующим:

- Optimal
- Warning

Статус «Warning» у дискового массива отображается только в том случае, если у логического накопителя, который относится к этому массиву, статус не «Optimal».

Каждый дисковый массив можно раскрыть, чтобы посмотреть подробную информацию.

14.1.4 ИНФОРМАЦИЯ О ЛОГИЧЕСКИХ НАКОПИТЕЛЯХ

Логические накопители можно добавлять на основе дисковых массивов. О логических накопителях отображается следующая информация:

- наименование диска
- номер дискового массива
- уровень RAID
- общий объем (ГиБ)
- статус

Логические диски могут иметь следующие статусы:

- Offline (диск недоступен)
- Partially Degraded (диск частично вышел из строя)
- Degraded (диск вышел из строя)
- Optimal (диск в нормальном состоянии)
- Unknown (состояние диска не определено)

Каждый логический накопитель можно раскрыть, чтобы посмотреть подробную информацию.

14.2 ПЕРЕКЛЮЧЕНИЕ РЕЖИМА RAID-КОНТРОЛЛЕРА

При просмотре подробной информации о RAID-контроллере отображается раздел «Personality» с текущим режимом работы контроллера и возможностью его сменить (Рисунок 38).

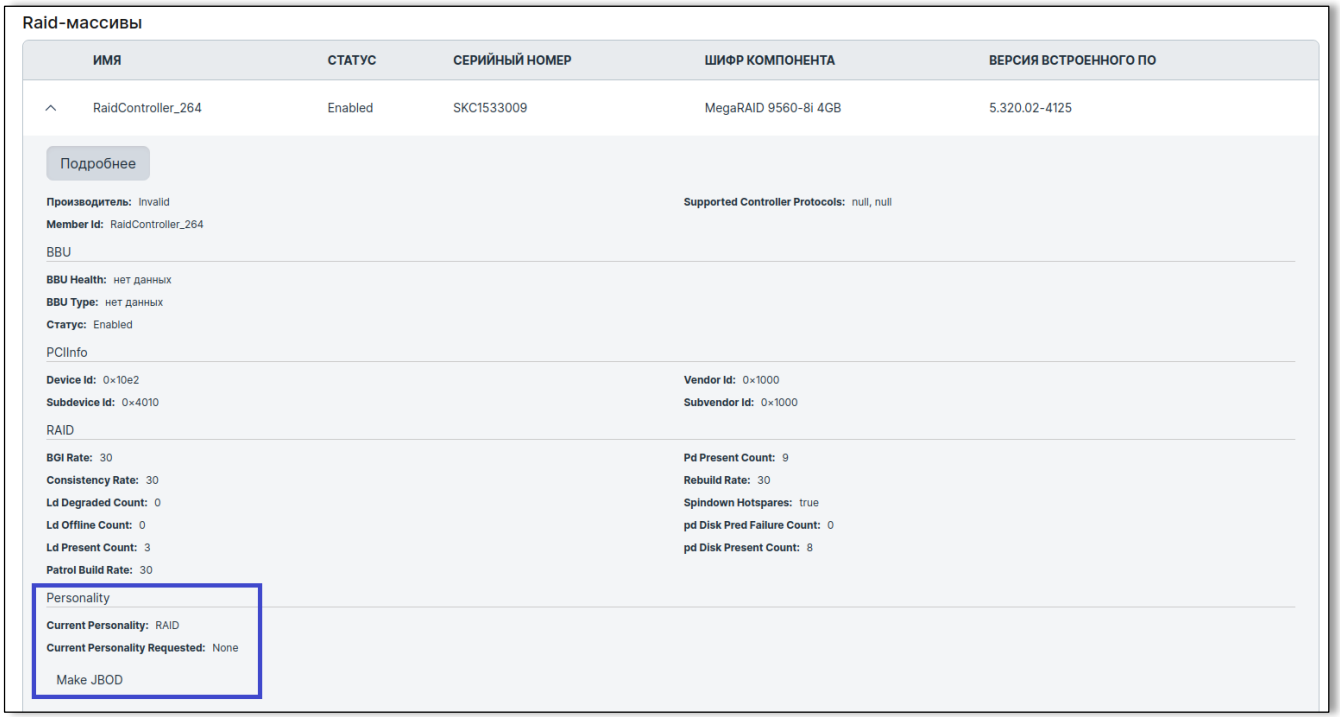

Рисунок 38. Просмотр режима работы RAID-контроллера

Если в свойстве «Current Personality» отображается «RAID», то ниже доступна кнопка «Make JBOD», которая установит JBOD-режим работы контроллера. Если в свойстве отображается «JBOD», то ниже доступна кнопка «Make RAID» для установки RAID-режима.

Для переключения режима в JBOD:

1. Нажмите кнопку «Make JBOD» в разделе «Personality» и дождитесь появления окна подтверждения смены режима (Рисунок 39).

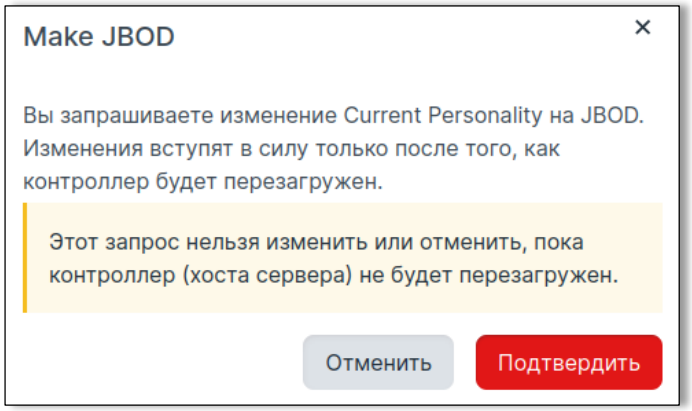

Рисунок 39. Подтверждение включения JBOD у RAID-контроллера

2. Подтвердите изменение.
3. Перезагрузите хост.

RAID-контроллер перейдет в переходное состояние. При попытке сменить режим работы в состоянии отобразится предупреждение (Рисунок 40).

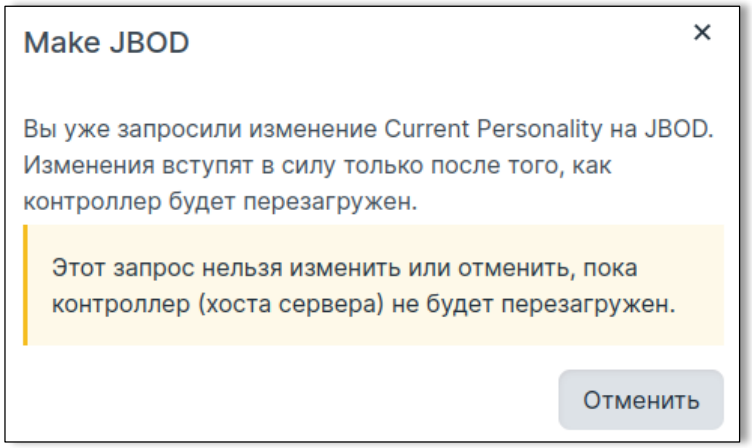

Рисунок 40. Попытка сменить режим RAID-контроллера в переходном состоянии

В режиме JBOD недоступны следующие действия (Рисунок 41):

- добавление конфигурации
- добавление логического накопителя
- операции над физическими и логическими накопителями

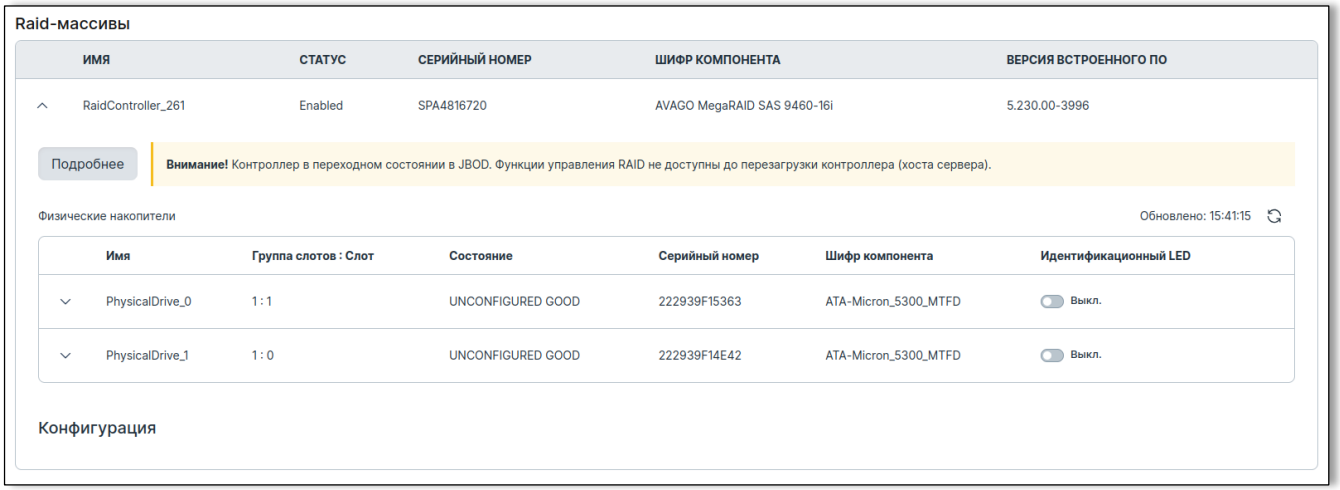

Рисунок 41. RAID-контроллер в режиме JBOD

14.3 ОПЕРАЦИИ С ФИЗИЧЕСКИМИ НАКОПИТЕЛЯМИ

Пользователь может проводить операции над физическими накопителями, среди которых управление LED-индикацией, а также те операции, которые зависят от состояния накопителя (Таблица 3).

Таблица 3. Состояния и операции над физическими накопителями

Текущее состояние	Доступные операции	Состояние после операции
UNCONFIGURED GOOD	Assign Hot Spare	HOT SPARE
	Assign Dedicated Hot Spare	HOT SPARE
	Crypto Erase	UNCONFIGURED GOOD
	Make Unconfigured Bad	UNCONFIGURED BAD
	Prepare For Removal	UNCONFIGURED GOOD
	Sanitize	UNCONFIGURED GOOD (если операция завершилась успешно или включен безопасный выход из операции в случае ошибки)
		UNCONFIGURED BAD (если операция не завершилась успешно или выключен безопасный выход из операции в случае ошибки)
	Start Erase	UNCONFIGURED GOOD
	Start Clear	UNCONFIGURED GOOD
HOT SPARE	Unassign Hot Spare	UNCONFIGURED GOOD
UNCONFIGURED BAD	Make Unconfigured Good	UNCONFIGURED GOOD
ONLINE	Make Offline	OFFLINE
OFFLINE	Make Online	ONLINE
	Mark Missing	UNCONFIGURED GOOD
	Start Rebuild	REBUILD
PREPARE FOR REMOVAL	Undo Prepare For Removal	UNCONFIGURED GOOD
REBUILD	Suspend Rebuild (если REBUILD в процессе)	REBUILD (на паузе)
	Resume Rebuild (если REBUILD на паузе)	REBUILD (в процессе)
	Stop Rebuild	UNCONFIGURED GOOD (если на RAID-контроллере установлен автоматический REBUILD)
		OFFLINE (если на RAID-контроллере не установлен автоматический REBUILD)

Текущее состояние	Доступные операции	Состояние после операции
	Make Offline	UNCONFIGURED GOOD (если на RAID-контроллере установлен автоматический REBUILD)
		OFFLINE (если на RAID-контроллере не установлен автоматический REBUILD)
COPYBACK (в процессе)	Suspend CopyBack (если COPYBACK в процессе)	COPYBACK (на паузе)
	Resume CopyBack (если COPYBACK на паузе)	COPYBACK (в процессе)

Операции, которые зависят от состояния, доступны при нажатии кнопки в строке физического накопителя (Рисунок 42).

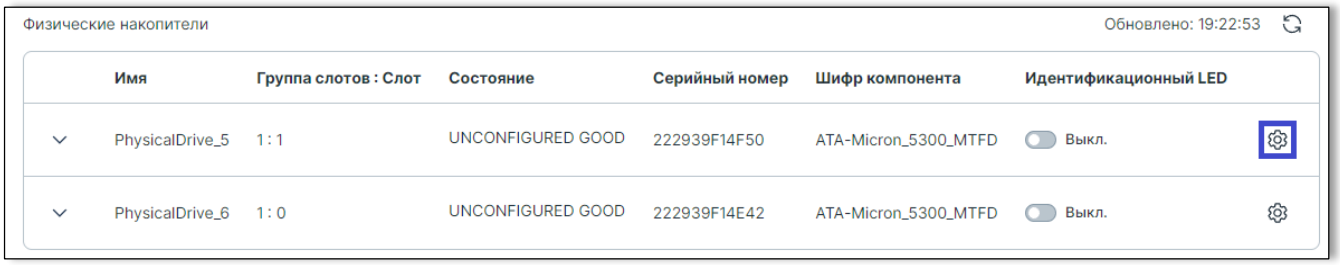

Рисунок 42. Использование операций над физическими накопителями

14.3.1 УПРАВЛЕНИЕ LED-ИНДИКАЦИЕЙ НАКОПИТЕЛЯ

Пользователь может управлять LED-индикацией накопителя. Действие доступно, если раскрыть RAID-контроллер, в котором есть физические накопители.

Для включения LED-индикации переведите переключатель «Идентификационный LED» в положение «Вкл.» в строке физического накопителя, для отключения LED-индикации – в положение «Выкл.».

Данное действие реализует операции «Start Locate» и «Stop Locate», которые подсвечивают накопители.

14.3.2 ОБНОВЛЕНИЕ ИНФОРМАЦИИ О СОСТОЯНИИ

Обновление информации происходит автоматически. После успешного выполнения операции отобразится соответствующее уведомление.

Также пользователь может нажать на соответствующую кнопку над списком накопителей для обновления информации вручную (Рисунок 43).

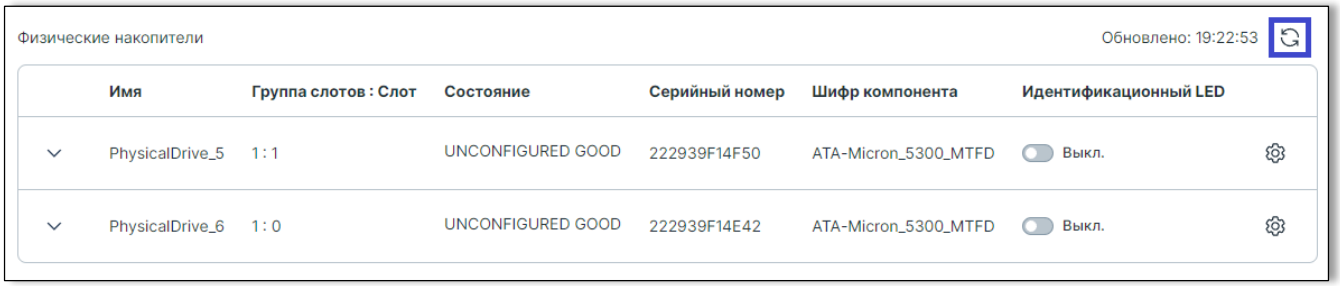

Рисунок 43. Обновление информации о физических накопителях

14.3.3 ОПЕРАЦИИ В СОСТОЯНИИ UNCONFIGURED GOOD

ВНИМАНИЕ:

Наличие некоторых операций зависит от прошивки RAID-контроллера.

Пользователь может осуществить следующие операции над физическим накопителем в состоянии UNCONFIGURED GOOD (Рисунок 44):

- Assign Hot Spare (действие переведет накопитель в состояние HOT SPARE)
- Assign Dedicated Hot Spare (действие переведет накопитель в состояние HOT SPARE и сделает его выделенным резервным накопителем для выбранной группы или групп)
- Crypto Erase (действие стирает данные на накопителе, но оставляет его в состоянии UNCONFIGURED GOOD; после операции нельзя дешифровать данные)
- Make Unconfigured Bad (действие переведет накопитель в состояние UNCONFIGURED BAD)
- Prepare For Removal (действие подготавливает накопитель к удалению и переводит его в состояние UNCONFIGURED GOOD)
- Sanitize (действие стирает данные на накопителе и переводит его в состояние UNCONFIGURED GOOD или UNCONFIGURED BAD)
- Start Erase (действие начинает стирать данные на накопителе, но оставляет его в состоянии UNCONFIGURED GOOD)
- Start Clear (действие начинает инициализацию данных на накопителе, но оставляет его в состоянии UNCONFIGURED GOOD)

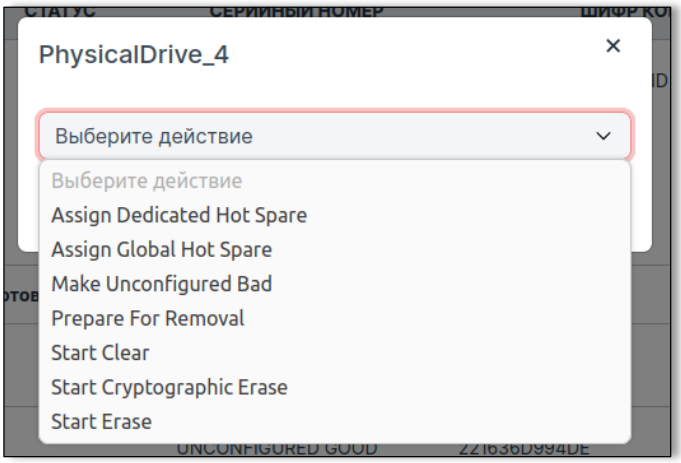

Рисунок 44. Операции для состояния UNCONFIGURED GOOD

При выборе операции «Assign Dedicated Hot Spare» необходимо выбрать группу или несколько групп, которым будет назначен выделенный накопитель (Рисунок 45).

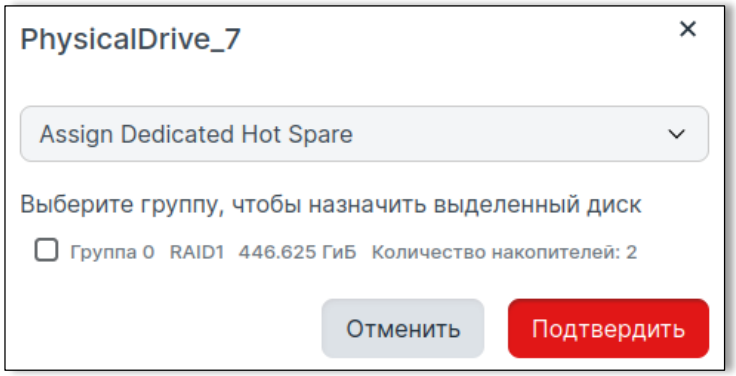

Рисунок 45. Операция «Assign Dedicated Hot Spare» для физического накопителя

Во время операции «Assign Dedicated Hot Spare» можно получить сообщение о текущем состоянии при нажатии на кнопку (Рисунок 46).

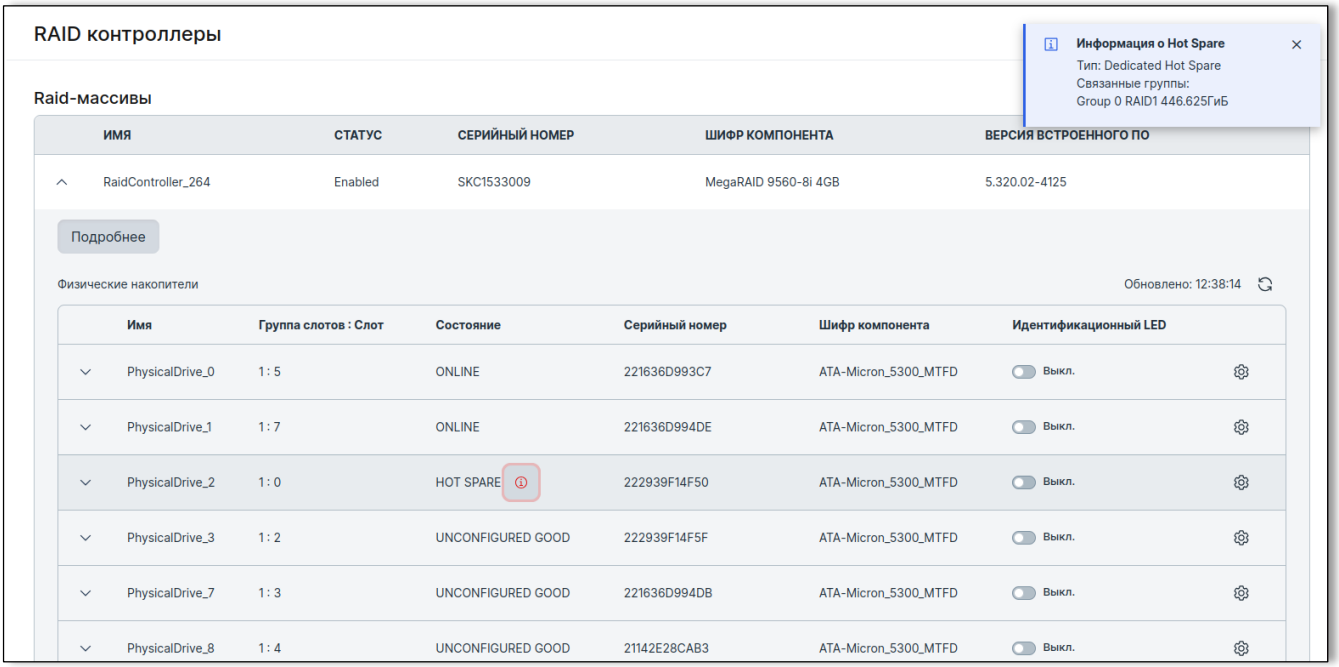

Рисунок 46. Получение информации о текущем состоянии HOT SPARE физического накопителя

При выборе операции «Sanitize» необходимо выбрать режим (Рисунок 47):

- Cryptographic (после операции нельзя дешифровать данные)
- Overwrite (перезаписывание данных для HDD-накопителей)
- Block (блочная очистка данных для SSD-накопителей)

Также можно включить разрешение на безопасный выход из операции в случае ошибки – от этого зависит состояние накопителя.

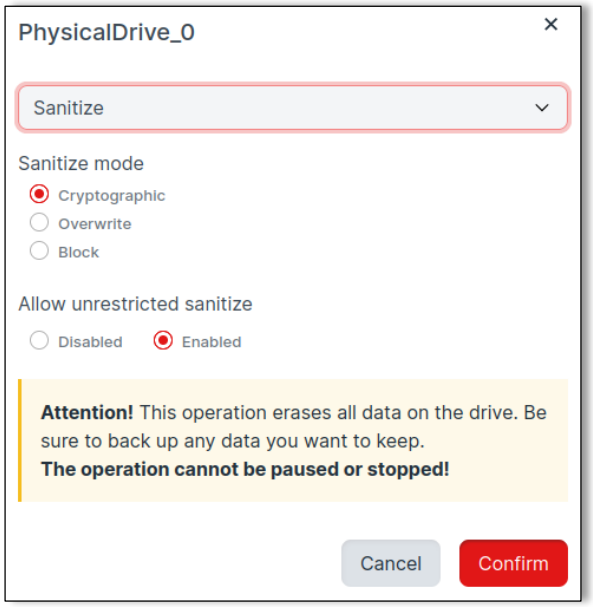

Рисунок 47. Операция «Sanitize» для физического накопителя

При выборе операции «Start Erase» необходимо выбрать режим (Рисунок 48):

- Simple – удаление данных одним проходом, при котором на место старых данных записывается один постоянный шаблон. Самый быстрый режим, но низкий по надежности, так как данные остаются доступны для восстановления.
- Normal – удаление данных тремя проходами, при котором на место старых данных записывается три разных шаблона. Более надежный режим, так как данные сложнее восстановить.
- Thorough – удаление данных девятью проходами (стирание данных трижды). Самый надежный режим, так как после него восстановление данных практически невозможно.

Также во время операций «Start Erase» и «Start Clear» отображается индикатор с процентом выполнения.

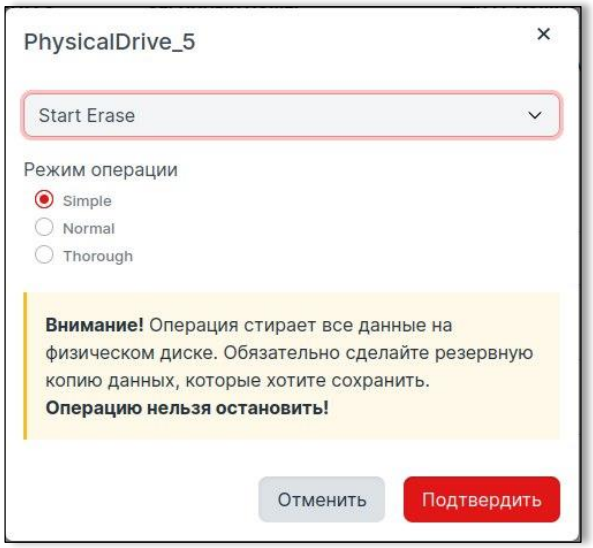

Рисунок 48. Операция «Start Erase» для физического накопителя

14.3.4 ОПЕРАЦИИ В СОСТОЯНИИ HOT SPARE

Пользователь может осуществить операцию «Unassign Hot Spare» над физическим накопителем в состоянии HOT SPARE. Данная операция переведет накопитель в состояние UNCONFIGURED GOOD.

14.3.5 ОПЕРАЦИИ В СОСТОЯНИИ UNCONFIGURED BAD

Пользователь может осуществить операцию «Make Unconfigured Good» над физическим накопителем в состоянии UNCONFIGURED BAD. Данная операция переведет накопитель в состояние UNCONFIGURED GOOD или UNCONFIGURED GOOD (FOREIGN), если у накопителя FOREIGN-конфигурация.

14.3.6 ОПЕРАЦИИ В СОСТОЯНИИ ONLINE

Пользователь может осуществить операцию «Make Offline» над физическим накопителем в состоянии ONLINE. Данная операция переведет накопитель в состояние OFFLINE.

14.3.7 ОПЕРАЦИИ В СОСТОЯНИИ OFFLINE

Пользователь может осуществить следующие операции над физическим накопителем в состоянии OFFLINE:

- Make Online (действие переведет накопитель в состояние ONLINE или в состояние REBUILD, если он был добавлен на место накопителя в состоянии MISSING)
- Mark Missing (действие удаляет накопитель из дискового массива и переводит его в состояние UNCONFIGURED GOOD)
- Start Rebuild (действие доступно только для того накопителя, который был добавлен на место накопителя в состоянии MISSING; переведет накопитель в состояние REBUILD)

14.3.8 ОПЕРАЦИИ В СОСТОЯНИИ PREPARE FOR REMOVAL

Пользователь может осуществить операцию «Undo Prepare For Removal» над физическим накопителем в состоянии PREPARE FOR REMOVAL. Данная операция переведет накопитель в состояние UNCONFIGURED GOOD.

14.3.9 ОПЕРАЦИИ В СОСТОЯНИИ REBUILD

«Rebuild» – операция по восстановлению физического накопителя. Во время выполнения данной операции у накопителя отображается состояние REBUILD.

ВНИМАНИЕ:

Объем накопителя, для которого проводится операция «Rebuild», должен быть больше или равен минимальному объему накопителя в дисковом массиве.

Пользователь может осуществить следующие операции над накопителем в состоянии REBUILD:

- Suspend Rebuild (действие доступно во время восстановления накопителя и приостанавливает его)
- Resume Rebuild (действие доступно во время приостановки восстановления накопителя и возобновляет его)

- Stop Rebuild (действие останавливает восстановление накопителя; переводит накопитель в состояние UNCONFIGURED GOOD, если на RAID-контроллере включено автоматическое восстановление; переводит накопитель в состояние OFFLINE, если на RAID-контроллере отключено автоматическое восстановление)
- Make Offline (действие переводит накопитель в состояние UNCONFIGURED GOOD, если на RAID-контроллере включено автоматическое восстановление; переводит накопитель в состояние OFFLINE, если на RAID-контроллере отключено автоматическое восстановление)

ВНИМАНИЕ:

Если операция «Stop Rebuild» выполняется для накопителя, на RAID-контроллере которого включено автоматическое восстановление, RAID-контроллер автоматически начнет операцию «Rebuild» на любом другом доступном накопителе. Если доступные накопители отсутствуют, то накопитель, на котором выполняется операция, перейдет в состояние MISSING.

Также во время операции «Rebuild» отображается индикатор с процентом выполнения.

14.3.10 ОПЕРАЦИИ В СОСТОЯНИИ COPYBACK

«CopyBack» – операция копирования и переноса данных на физический накопитель. Во время выполнения данной операции у накопителя отображается состояние COPYBACK. Пользователь может осуществить следующие операции над физическим накопителем в состоянии COPYBACK:

- Suspend CopyBack (действие доступно во время копирования и переноса данных на накопитель в состоянии COPYBACK и приостанавливает операцию)
- Resume CopyBack (действие доступно во время приостановки копирования и переноса данных на накопитель в состоянии COPYBACK и возобновляет операцию)

Во время операции «CopyBack» отображается индикатор с процентом выполнения.

14.3.11 ОПЕРАЦИЯ ЗАМЕНЫ ОТСУТСТВУЮЩИХ НАКОПИТЕЛЕЙ

«ReplaceMissing» – операция замены отсутствующего накопителя в дисковом массиве. Операция доступна, если в дисковом массиве есть уведомление об отсутствии накопителя.

ВНИМАНИЕ:

Объем накопителя, который указывается в качестве замены, должен быть больше или равен объему отсутствующего накопителя.

Для замены отсутствующего накопителя:

1. Нажмите кнопку «Replace Missing» в дисковом массиве (Рисунок 49) и дождитесь появления окна выбора накопителей для замены.
2. Отметьте накопитель, который заменит отсутствующий.

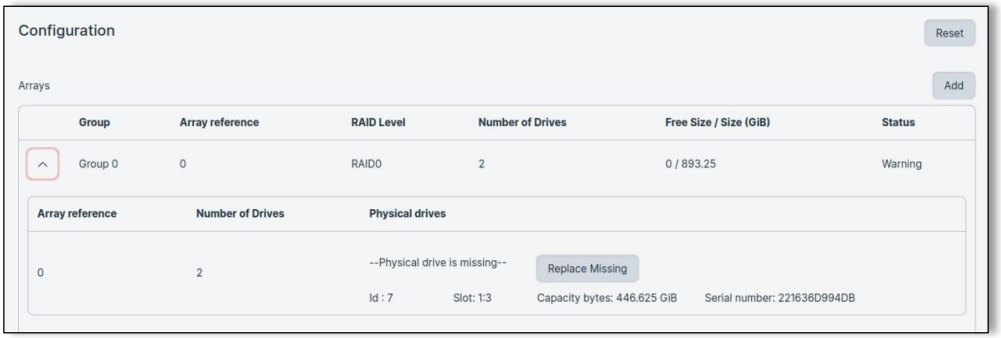

Рисунок 49. Замена отсутствующего физического накопителя в дисковом массиве

14.3.12 УПРАВЛЕНИЕ FOREIGN-КОНФИГУРАЦИЯМИ

FOREIGN-конфигурации – те конфигурации физических накопителей, которые были созданы на другом RAID-контроллере. Такие накопители при вставке в RAID-контроллер получают состояние UNCONFIGURED BAD. После операции «Make Unconfigured Good» они перейдут в состояние UNCONFIGURED GOOD (FOREIGN).

На накопителях в состоянии UNCONFIGURED GOOD (FOREIGN) нельзя создавать конфигурации для дисковых массивов и логических накопителей, поэтому следует очистить накопитель от FOREIGN-конфигурации.

Для удаления FOREIGN-конфигурации у физического накопителя нажмите кнопку «Clear Foreign Config». Накопитель перейдет в состояние UNCONFIGURED GOOD.

ВНИМАНИЕ:

Просмотр и импорт FOREIGN-конфигураций на данный момент не реализован.

14.4 ДОБАВЛЕНИЕ ДИСКОВОГО МАССИВА

Пользователь может добавлять дисковые массивы. Действие доступно, если раскрыть RAID-контроллер с физическими накопителями, которые:

- в состоянии UNCONFIGURED GOOD
- не находятся в состоянии PREPARE FOR REMOVAL
- над которыми в данный момент не выполняются никакие операции

Параметры добавления дисков в RAID различаются в зависимости от уровня RAID:

- RAIDx – уровни RAID с одной цифрой (например, 0, 1, 5, 6)
- RAIDxx – уровни RAID с двумя цифрами (например, 00, 10, 50, 60)

14.4.1 ДОБАВЛЕНИЕ ДИСКОВОГО МАССИВА УРОВНЯ RAIDX

Для добавления дискового массива уровня RAIDx:

1. Нажмите кнопку «Добавить» напротив раздела «Дисковые массивы» и дождитесь появления окна добавления конфигурации (Рисунок 50).

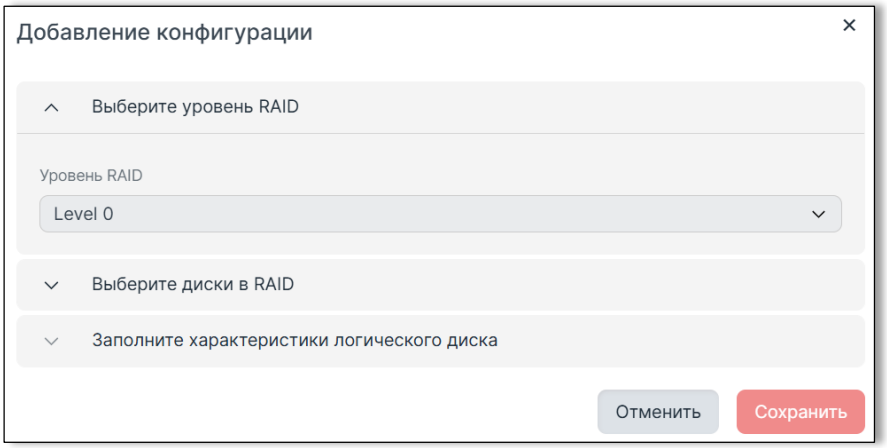

Рисунок 50. Выбор уровня RAIDx для массива дисков

2. Выберите уровень RAID, который содержал бы одну цифру в номере уровня.
3. Отметьте физические накопители, которые войдут в массив (Рисунок 51).

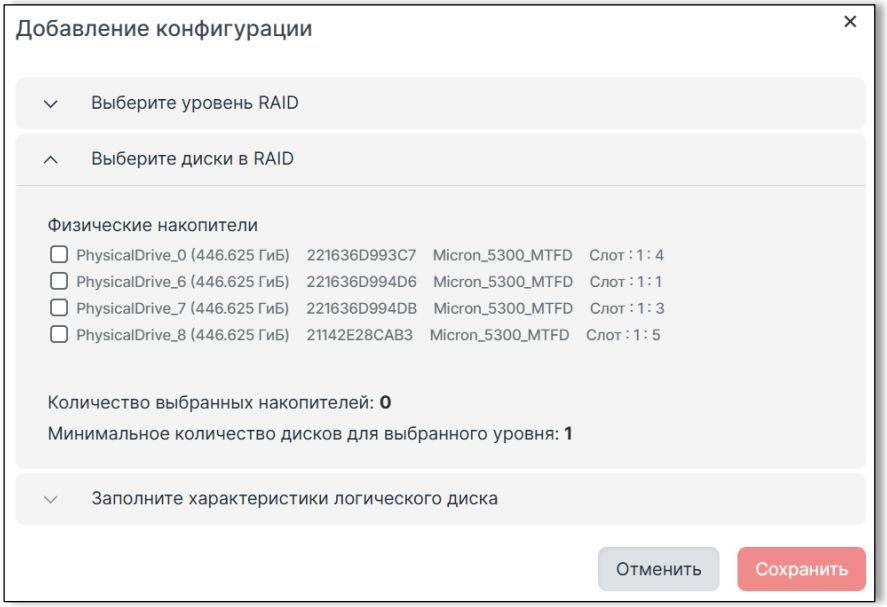

Рисунок 51. Выбор дисков в RAIDx для массива

4. Заполните характеристики логического диска (Рисунок 52).

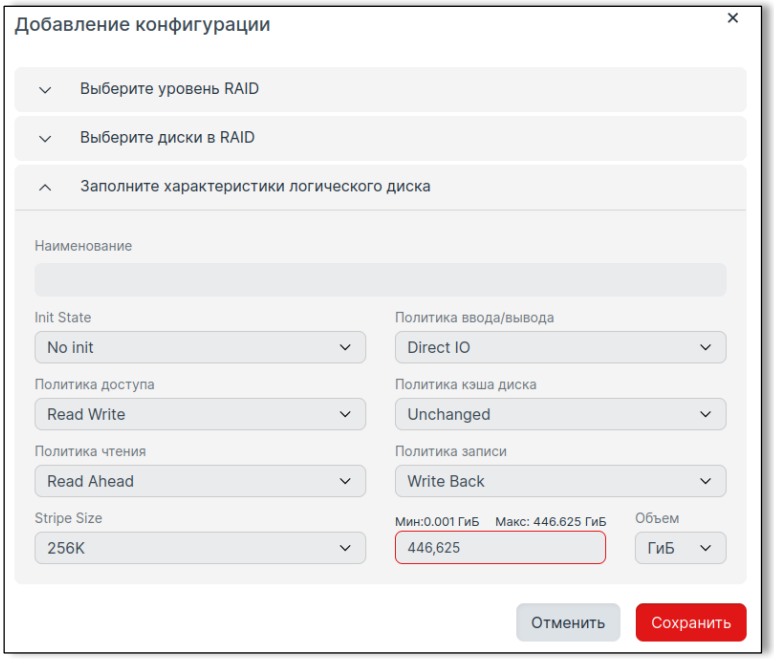

Рисунок 52. Заполнение характеристик логического диска в массиве

5. Нажмите кнопку «Сохранить».

После добавления массив появится в списке дисковых массивов.

14.4.2 ДОБАВЛЕНИЕ ДИСКОВОГО МАССИВА УРОВНЯ RAIDXX

Для добавления дискового массива уровня RAIDxx:

1. Нажмите кнопку «Добавить» напротив раздела «Дисковые массивы» и дождитесь появления окна добавления конфигурации (Рисунок 53).

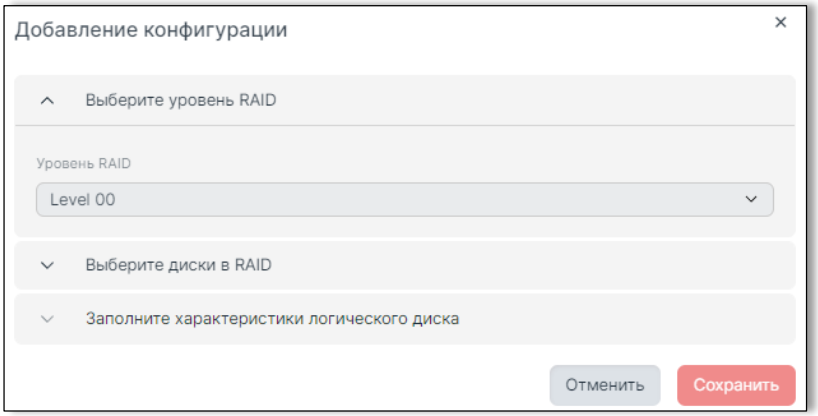

Рисунок 53. Выбор уровня RAIDxx для массива дисков

2. Выберите уровень RAID, который содержал бы две цифры в номере уровня.
3. Отметьте физические накопители, которые войдут в массив (Рисунок 54). При необходимости можно добавлять группы дисков нажатием на кнопку «Добавить группу». При этом количество дисков в каждой группе должно быть одинаковым. Групп может быть не более 8.

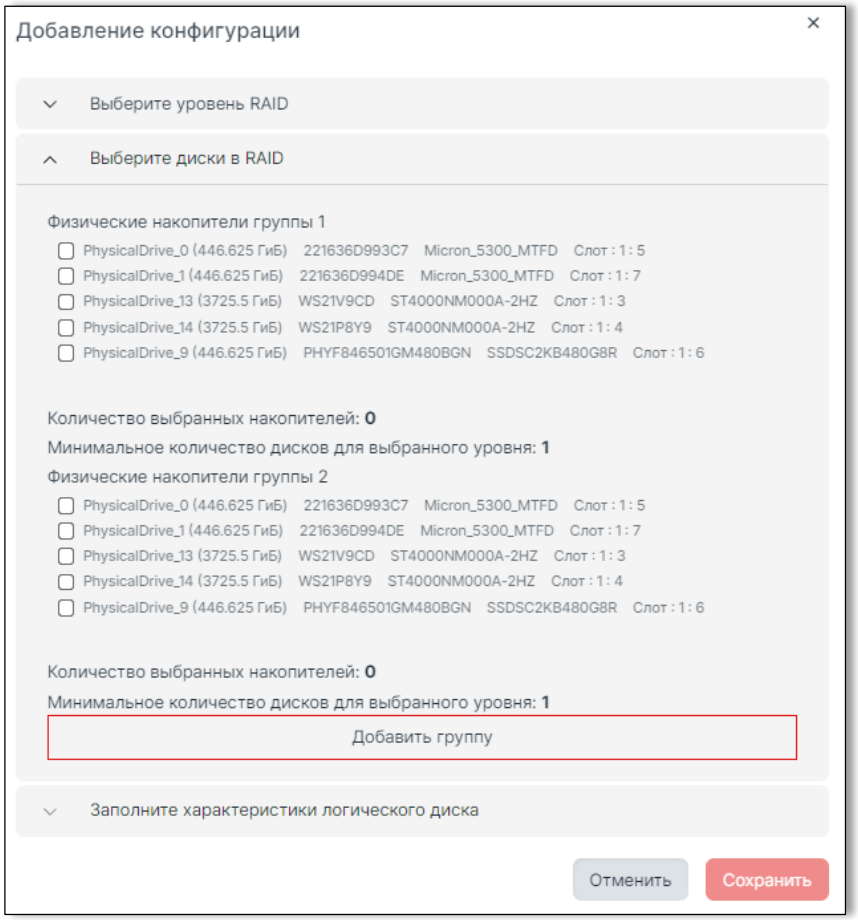

Рисунок 54. Выбор дисков в RAIDxx для массива

4. Заполните характеристики логического диска (Рисунок 52).
5. Нажмите кнопку «Сохранить».

После добавления массив появится в списке дисковых массивов.

14.5 ДОБАВЛЕНИЕ ЛОГИЧЕСКОГО НАКОПИТЕЛЯ

Пользователь может добавлять логические накопители. Действие доступно, если раскрыть RAID-контроллер, в котором есть хотя бы один дисковый массив.

Для добавления логического накопителя:

1. Нажмите кнопку «Добавить» напротив раздела «Логические накопители» и дождитесь появления окна добавления логического диска (Рисунок 55).
2. Выберите группу массивов в списке.
3. Заполните характеристики логического накопителя.
4. Нажмите кнопку «Сохранить»

После сохранения нужно дождаться уведомления об успешном сохранении, затем добавленный логический накопитель появится в списке.

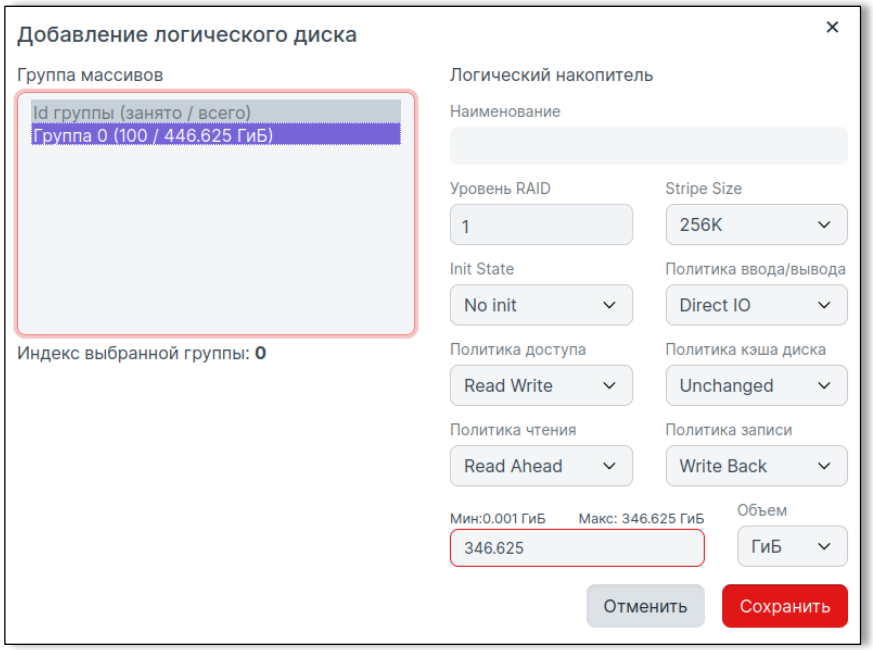

Рисунок 55. Добавление логического диска в RAID

14.5.1 СЕГМЕНТАЦИЯ СВОБОДНОГО ПРОСТРАНСТВА В RAID

После удаления логического накопителя из дискового массива, если он не был последним, RAID-контроллер освободит пространство на массиве, но не объединит его с оставшимся пространством. В окне добавления логического диска можно увидеть эти сегменты в свободном пространстве группы (Рисунок 56). Эти сегменты также можно выбрать для создания логического накопителя.

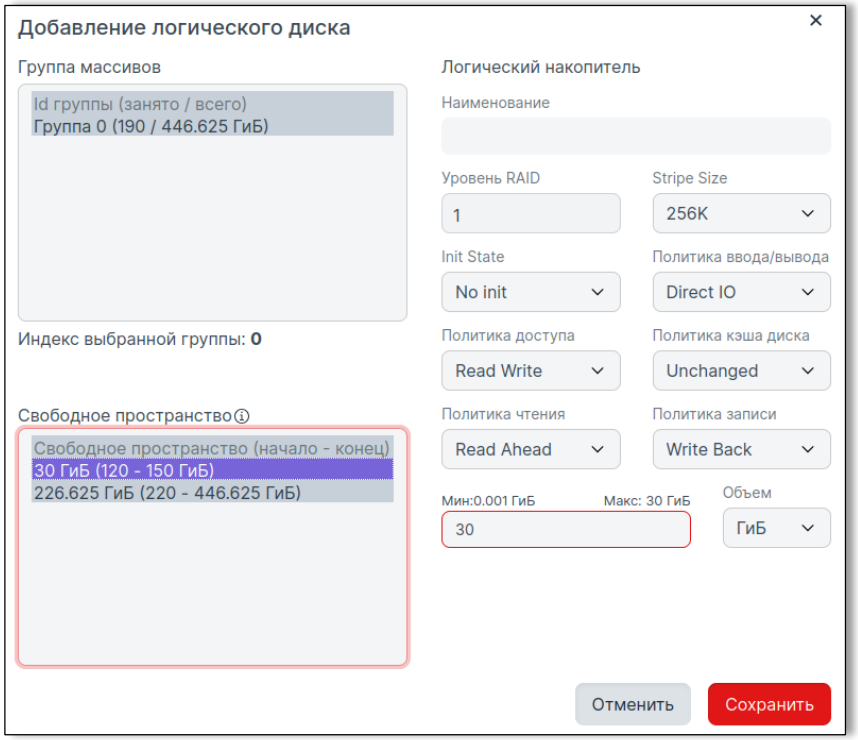

Рисунок 56. Сегменты свободного пространства при добавлении логического накопителя

14.6 УДАЛЕНИЕ ЛОГИЧЕСКОГО НАКОПИТЕЛЯ

Пользователь может удалять логические накопители. Действие доступно, если раскрыть RAID-контроллер, в котором есть логические накопители.

Для удаления логического накопителя нажмите отмеченную кнопку у логического накопителя в списке (Рисунок 57) и подтвердите удаление во всплывшем окне.

После удаления нужно дождаться уведомления об успешном удалении, затем удаленный накопитель исчезнет из списка.

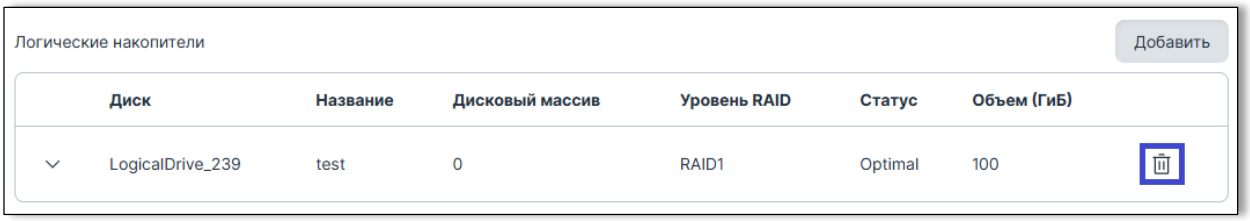

Рисунок 57. Удаление логического накопителя из RAID

14.7 ОПЕРАЦИИ С ЛОГИЧЕСКИМИ НАКОПИТЕЛЯМИ

Пользователь может проводить операции над логическими накопителями, среди которых управление LED-индикацией, а также те операции, которые зависят от статуса накопителя (Таблица 4).

Таблица 4. Статусы и операции над логическими накопителями

Текущий статус	Тип	Операции	Примечание
Любой, кроме статуса во время выполнения операций модификации	Операции видимости	Hide Drive Group	
		Unhide Drive Group	
		Hide Virtual Drive	
		Unhide Virtual Drive	
Optimal	Операции проверки целостности данных	Check Consistency	
		Suspend Check Consistency	
		Resume Check Consistency	
		Stop Check Consistency	
	Операции инициализации	Fast Initialization	
		Full Initialization	

Текущий статус	Тип	Операции	Примечание
		Stop Initialization	
		Suspend Background Init	Доступны во время фоновой операции Background Init
		Resume Background Init	
		Stop Background Init	
	Операции модификации	Expand	Доступны при наличии только одного логического диска в дисковом массиве
		Reconfigure	
	Операции очистки	Start Erase	
		Stop Erase	

Операции, которые зависят от состояния, доступны при нажатии кнопки в строке логического накопителя (Рисунок 58).

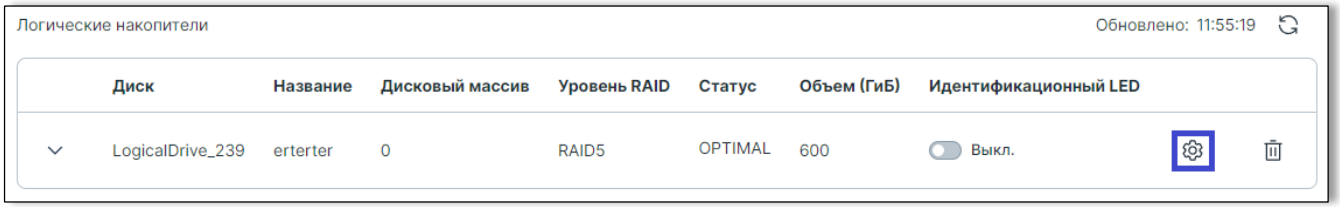

Рисунок 58. Использование операций над логическими накопителями

Список доступных операций различается при наличии только одного логического накопителя в дисковом массиве (Рисунок 59) или нескольких (Рисунок 60).

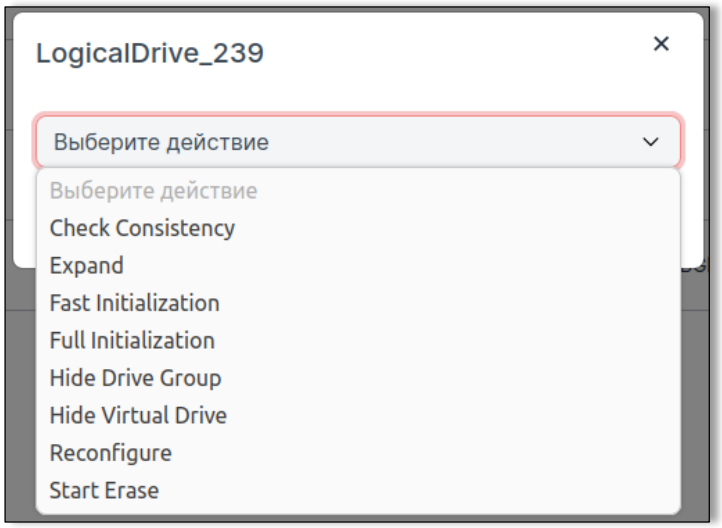

Рисунок 59. Операции для одного логического накопителя в дисковом массиве

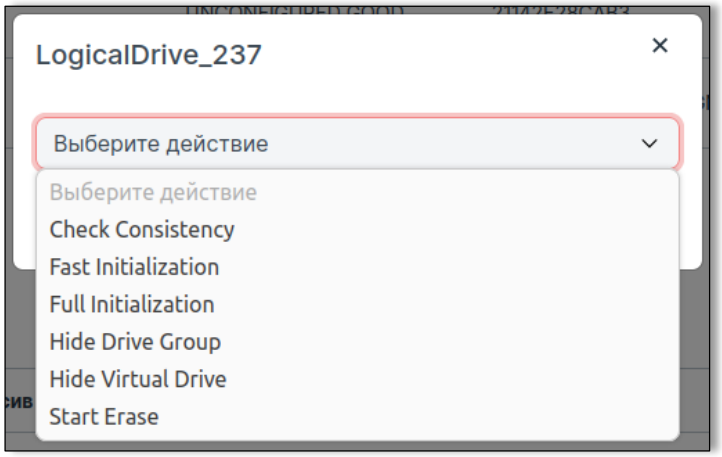

Рисунок 60. Операции для нескольких логических накопителей в дисковом массиве

14.7.1 УПРАВЛЕНИЕ LED-ИНДИКАЦИЕЙ НАКОПИТЕЛЯ

Пользователь может управлять LED-индикацией логического накопителя. Действие доступно, если раскрыть RAID-контроллер, в котором есть логические накопители.

Для включения LED-индикации переведите переключатель «Идентификационный LED» в положение «Вкл.» в строке логического накопителя. Данное действие включит LED-индикацию у физических накопителей, которые входят в состав логического диска, при этом ее нельзя отключить, пока она активна у логического накопителя. Также действие включит индикацию у тех логических накопителей дискового массива, которые созданы на тех же физических дисках.

Для отключения LED-индикации переведите переключатель «Идентификационный LED» в положение «Выкл.» в строке логического накопителя. Данное действие выключит LED-индикацию у физических накопителей, которые входят в состав логического диска. Также действие выключит индикацию у тех логических накопителей дискового массива, которые созданы на тех же физических дисках.

14.7.2 ОБНОВЛЕНИЕ ИНФОРМАЦИИ О СОСТОЯНИИ

Обновление информации происходит автоматически. После успешного выполнения операции отобразится соответствующее уведомление.

Также пользователь может нажать на соответствующую кнопку над списком накопителей для обновления информации вручную (Рисунок 61).

Рисунок 61. Обновление информации о логических накопителях

14.7.3 ОПЕРАЦИИ ВИДИМОСТИ НАКОПИТЕЛЕЙ

Пользователь может осуществить следующие операции видимости над логическим накопителем:

- Hide Drive Group (действие скрывает все логические накопители группы от ОС, параметр «AccessPolicy» принимает значение «Hidden»)
- Unhide Drive Group (действие возвращает видимость группы логических накопителей для ОС, параметр «AccessPolicy» принимает исходное значение)
- Hide Virtual Drive (действие скрывает логический накопитель от ОС параметр «AccessPolicy» принимает значение «Hidden»)
- Unhide Virtual Drive (действие возвращает видимость логического накопителя для ОС, параметр «AccessPolicy» принимает исходное значение)

14.7.4 ОПЕРАЦИИ ПРОВЕРКИ ЦЕЛОСТНОСТИ ДАННЫХ НАКОПИТЕЛЕЙ

«Check Consistency» – операция по проверке корректности и целостности данных на логическом накопителе.

ВНИМАНИЕ:

Операция «Check Consistency» недоступна для уровней RAID0 и RAID00.

Пользователь может осуществить следующие операции над логическим накопителем, если выполняется операция «Check Consistency»:

- Suspend Check Consistency (действие доступно во время проверки целостности данных накопителя и приостанавливает ее)
- Resume Check Consistency (действие доступно во время приостановки проверки целостности данных накопителя и возобновляет ее)
- Stop Check Consistency (действие останавливает проверку целостности данных накопителя).

Также во время операции «Check Consistency» отображается индикатор с процентом выполнения.

14.7.5 ОПЕРАЦИИ ИНИЦИАЛИЗАЦИИ НАКОПИТЕЛЕЙ

Пользователь может осуществить следующие операции инициализации логического накопителя:

- Fast Initialization (действие выполняет быструю инициализацию данных на логическом накопителе; отображается как «Fast Init»)
- Full Initialization (действие выполняет полную инициализацию данных на логическом накопителе; отображается как «Full Init»)
- Stop Initialization (действие останавливает любую – «Fast» или «Init» – операцию инициализации данных)

Также операцией инициализации данных на логическом накопителе является «Background Init». Она выполняется в фоновом режиме и начинается спустя 5 минут после создания виртуального накопителя. Эта операция похожа на «Check Consistency», так как проверяет накопитель на ошибки, но отличается тем, что принудительно запускается только для новых виртуальных накопителей.

Пользователь может осуществить следующие операции над логическим накопителем, если выполняется операция «Background Init»:

- Suspend Background Init (действие доступно во время фоновой проверки целостности данных накопителя и приостанавливает ее)
- Resume Background Init (действие доступно во время приостановки фоновой проверки целостности данных накопителя и возобновляет ее)
- Stop Background Init (действие останавливает фоновую проверку целостности данных накопителя)

Во время операций инициализации отображается индикатор с процентом выполнения. При этом выполнение операций «Fast Initialization» и «Full Initialization» зависит от информации на диске: их индикатор может не отображаться, если операция выполняется слишком быстро.

14.7.6 ОПЕРАЦИИ МОДИФИКАЦИИ НАКОПИТЕЛЕЙ

Пользователь может осуществить следующие операции модификации над логическим накопителем:

- Expand (действие увеличивает объем логического накопителя)
- Reconfigure (действие позволяет изменить уровень RAID и количество физических накопителей на логическом накопителе)

Операции модификации доступны при наличии только одного логического накопителя в дисковом массиве.

При выборе операции «Expand» необходимо указать процент расширения (Рисунок 62).

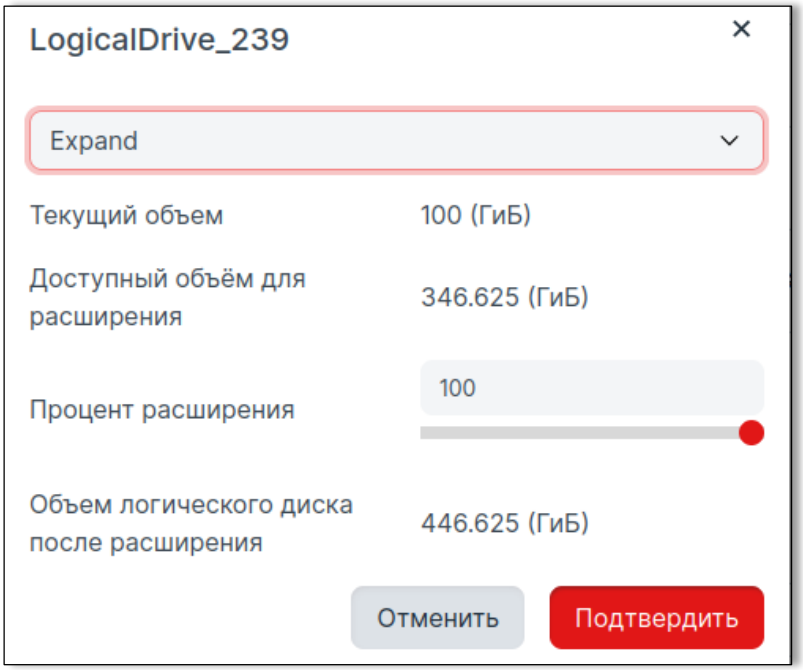

Рисунок 62. Операция «Expand» для логического накопителя

При выборе операции «Reconfigure» необходимо указать уровень RAID и тип операции (Рисунок 63).

Типы Reconfigure-операций, которые можно выбрать:

- без изменений
- добавить диски (требуется выбрать физические накопители, которые нужно добавить; после добавления физические накопители получат состояние ONLINE)
- убрать диски (требуется выбрать физические накопители, которые нужно убрать; после удаления физические накопители получат состояние UNCONFIGURED GOOD)

ВНИМАНИЕ:

Во время процесса реконструкции на RAID-контроллере недоступно создание конфигурации или логических накопителей. При открытии модальных окон создания конфигурации или логических накопителей отображается соответствующее сообщение.

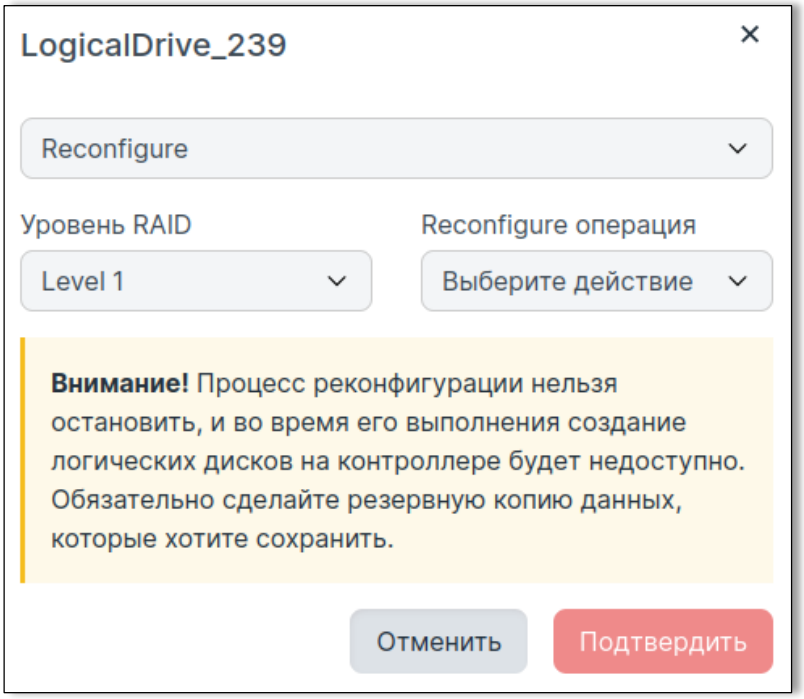

Рисунок 63. Операция «Reconfigure» для логического накопителя

Во время операций модификации можно получить сообщение о текущем состоянии реконструкции при нажатии на кнопку (Рисунок 64).

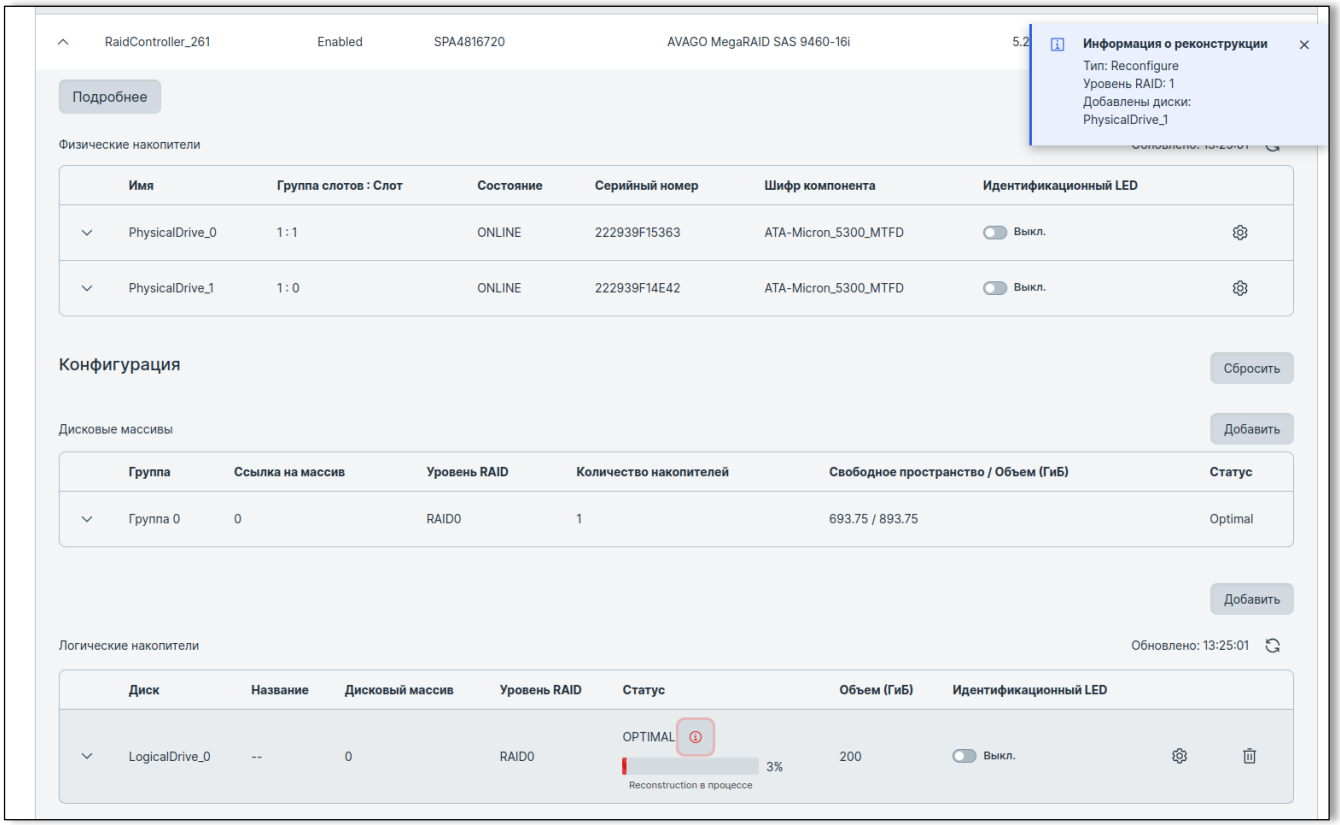

Рисунок 64. Получение информации о текущем состоянии реконструкции логического накопителя

Также во время операции модификации отображается индикатор с процентом выполнения и типом «Recon», так как «Expand» и «Reconfigure» к нему относятся.

14.7.7 ОПЕРАЦИИ ОЧИСТКИ НАКОПИТЕЛЕЙ

«Start Erase» – операция по очистке данных на логическом накопителе. Очистку накопителя можно остановить операцией «Stop Erase».

При выборе операции «Start Erase» необходимо выбрать режим (Рисунок 65):

- Simple – удаление данных одним проходом, при котором на место старых данных записывается один постоянный шаблон. Самый быстрый режим, но низкий по надежности, так как данные остаются доступны для восстановления.
- Normal – удаление данных тремя проходами, при котором на место старых данных записывается три разных шаблона. Более надежный режим, так как данные сложнее восстановить.
- Thorough – удаление данных девятью проходами (стирание данных трижды). Самый надежный режим, так как после него восстановление данных практически невозможно.

Также можно включить удаление логического накопителя после очистки.

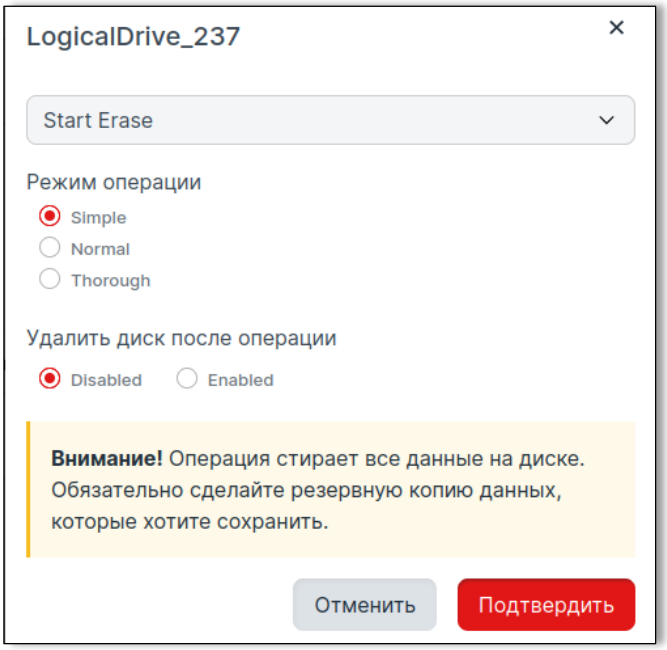

Рисунок 65. Операция «Start Erase» для логического накопителя

Во время операции «Start Erase» отображается индикатор с процентом выполнения. При этом скорость выполнения зависит от информации на диске: индикатор может не отображаться, если операция выполняется слишком быстро.

14.8 СБРОС КОНФИГУРАЦИИ

Пользователь может сбросить конфигурацию дисковых массивов и логических накопителей. Действие доступно, если раскрыть RAID-контроллер.

Для сброса конфигурации дисковых массивов и логических накопителей нажмите кнопку «Сбросить» напротив раздела «Конфигурация» и подтвердите сброс во всплывшем окне.

После сброса из RAID-контроллера удалятся все логические накопители и дисковые массивы, а физические накопители получат состояние UNCONFIGURED GOOD.

14.9 ЛОГИРОВАНИЕ СОБЫТИЙ RAID

В журнале событий Сила КУБ отображаются логи изменений в RAID-контроллерах. Логи формируются для следующих событий:

- создание, изменение, удаление RAID-массивов, физических и логических накопителей
- переход физического накопителя из состояния ONLINE в любое другое
- переход физического накопителя из состояния UNCONFIGURED GOOD в любое другое
- переход логического накопителя из статуса Optimal в любое другое

События для физических и логических накопителей могут появиться в журнале со статусом «WARNING» – такие события необходимо удалить или отметить как решенные (см. раздел 9) после завершения настройки RAID.

15 РАБОТА С ОСНОВНЫМИ ФУНКЦИЯМИ В РАЗДЕЛЕ «ИНФОРМАЦИЯ О СЕРВЕРЕ»

15.1 СТАТИЧЕСКАЯ ИНФОРМАЦИЯ О КОНФИГУРАЦИИ СЕРВЕРА

При выборе в основном меню раздел **Система -> Перечень оборудования и LED** в правой части отображается Перечень оборудования и LED (Рисунок 66).

При нажатии в разделе «Быстрые ссылки к компонентам оборудования» на ссылку «Источники питания» отобразится раздел «Источники питания».

СИЛА | SILA CUBE | CP2-6327 D262060005 14:25:08 Состояние Питание Обновить root

Система
Статус оборудования
Управление
Логи
Вентиляторы
Материнская плата
Модули памяти
Процессоры
Источники питания
Настройки
Безопасность и доступ

Перечень оборудования и LED

Управление LED

Состояние питания
Вкл.

Идентификационный LED системы
Выкл.

Быстрые ссылки к компонентам оборудования

Система
BMC
Шасси
Слоты DIMM
Вентиляторы
Источники питания
Процессоры
PCI-устройства

Система

ИДЕНТИФИКАТОР	ТИП ОБОРУДОВАНИЯ	СОСТОЯНИЕ	НОМЕР ПОЗИЦИИ	ИДЕНТИФИКАЦИОННЫЙ LED
system	system	OK	--	Выкл.

BMC

ИДЕНТИФИКАТОР	СОСТОЯНИЕ	НОМЕР ПОЗИЦИИ	ИДЕНТИФИКАЦИОННЫЙ LED
bmc	OK	--	--

Шасси

ИДЕНТИФИКАТОР	СОСТОЯНИЕ	НОМЕР ПОЗИЦИИ	ИДЕНТИФИКАЦИОННЫЙ LED
SILA_Baseboard	OK	--	--
SILA_CPUs	OK	--	--
SILA_DIMM	OK	--	--
SILA_Fans	OK	--	--
SILA_PSUs	OK	--	--
chassis	OK	--	--

Слоты DIMM

Поиск Всего объектов: 32

ИДЕНТИФИКАТОР	STATUS (STATE)	НОМЕР ПОЗИЦИИ	ОБЪЁМ МИБ
dimm0	Warning	CPU0_DIMM_A1	0
dimm1	Absent	CPU0_DIMM_A2	0
dimm2	OK	CPU0_DIMM_B1	16384

Вентиляторы

Поиск Всего объектов: 4

ИДЕНТИФИКАТОР	СОСТОЯНИЕ	ШИФР КОМПОНЕНТА	СЕРИЙНЫЙ НОМЕР
System Fan 1	OK	--	--
System Fan 2	OK	--	--
System Fan 3	OK	--	--
System Fan 4	OK	--	--

Источники питания

Поиск Всего объектов: 2

ИДЕНТИФИКАТОР	СОСТОЯНИЕ	НОМЕР ПОЗИЦИИ	ИДЕНТИФИКАЦИОННЫЙ LED
GC1600PMP_PSU1	OK	--	--
GC1600PMP_PSU2	OK	--	--

Процессоры

Поиск Всего объектов: 2

ИДЕНТИФИКАТОР	СТАТУС (СОСТОЯНИЕ)	СОСТОЯНИЕ	НОМЕР ПОЗИЦИИ	ИДЕНТИФИКАЦИОННЫЙ LED
CPU_0	Enabled	OK	CPU0	--
CPU_1	Absent	OK	CPU1	--

Установленые PCI-устройства

ИМЯ	СОСТОЯНИЕ	КЛАСС УСТРОЙСТВА	ТИП УСТРОЙСТВА	ПРОИЗВОДИТЕЛЬ
I350 Gigabit Network Connection	OK	NetworkController	MultiFunction	Intel Corporation
AST1150 PCI-to-PCI Bridge	OK	--	SingleFunction	ASPEED Technology, Inc.
ASPEED Graphics Family	OK	--	SingleFunction	--
MegaRAID 12GSAS/PCIe Secure SAS39xx	OK	--	SingleFunction	Broadcom / LSI

Рисунок 66. Страница «Перечень оборудования и LED»

15.2 ИНФОРМАЦИЯ ОБ УСТАНОВЛЕННЫХ ПРОЦЕССОРАХ И МАТЕРИНСКОЙ ПЛАТЕ, И ИХ СОСТОЯНИИ

При выборе в левом основном меню раздела **Система -> Перечень оборудования и LED**, в правой части отображается Перечень оборудования и LED (Рисунок 66).

При нажатии в разделе «Быстрые ссылки к компонентам оборудования» на ссылку «Процессоры» отобразится раздел «Процессоры (Рисунок 67).

При раскрытии раздела отобразится подробная информация.

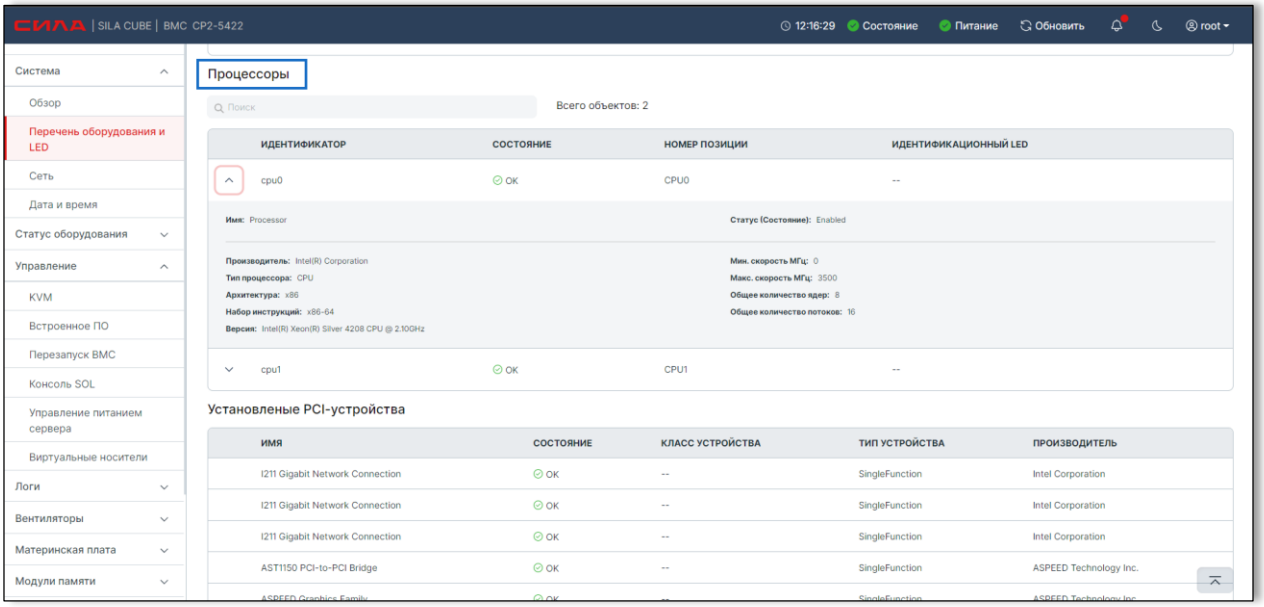

Рисунок 67. Страница «Перечень оборудования и LED», раздел «Процессоры»

15.3 ОБНОВЛЕНИЕ МИКРОКОДА BMC И BIOS

При выборе в левом основном меню раздела **Управление -> Встроенное ПО**, в правой части отображается информация о встроенном ПО (Рисунок 68):

- BMC
- Хост
- Раздел «Обновить встроенное ПО»

При нажатии «Выбрать файл» отобразится окно для выбора файла с компьютера.

При выборе файла и нажатии «Открыть» окно закрывается.

При нажатии на кнопку «Начать обновление» происходит обновление встроенного ПО.

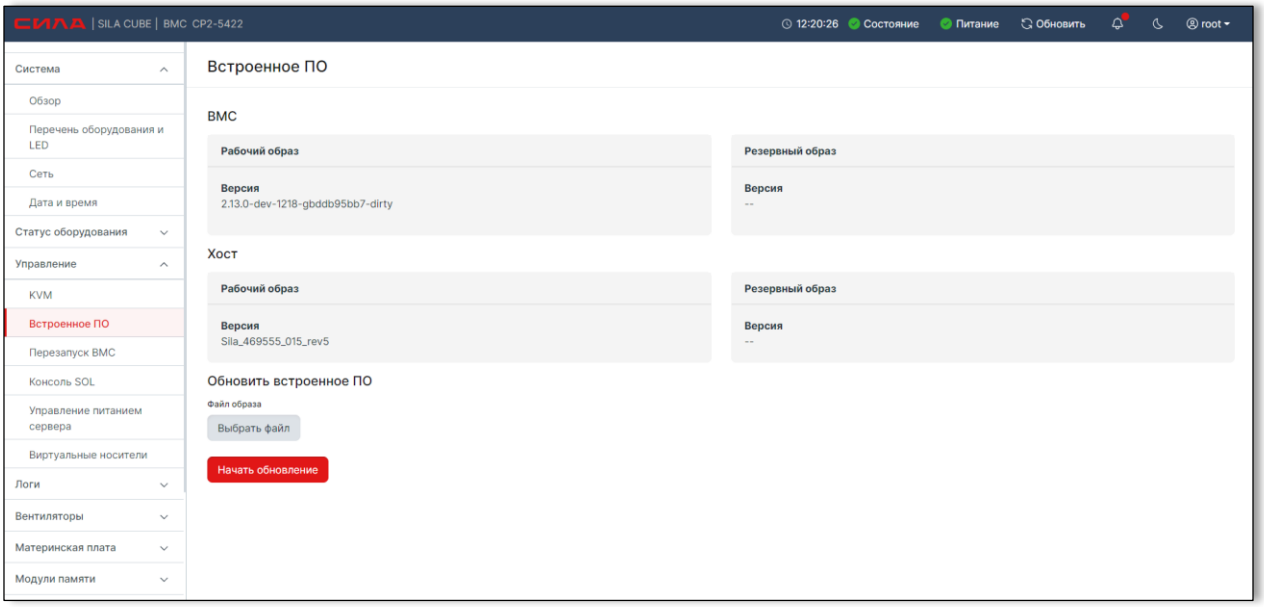

Рисунок 68. Страница «Встроенное ПО»

15.4 ОТОБРАЖЕНИЕ ФУНКЦИИ УПРАВЛЕНИЯ ОС И СЕРВЕРА, ПРОВЕРКИ ВЫКЛЮЧЕНИЯ СЕРВЕРА

При выборе в левом основном меню раздела **Управление -> Управление электропитанием и ОС сервера** в правой части отображается раздел об управлении электропитанием и ОС сервера (Рисунок 69).

Отображается:

- Текущий статус
- Раздел Действия
- Настройки загрузки

В разделе «Действия» отображается:

- Перезапуск сервера:
  - по порядку – сначала ОС, потом сервер
  - немедленно – сервер перезагружается без перезагрузки ОС
- Выключение сервера:
  - по порядку – сначала ОС, потом сервер
  - немедленно – сервер выключается без выключения ОС

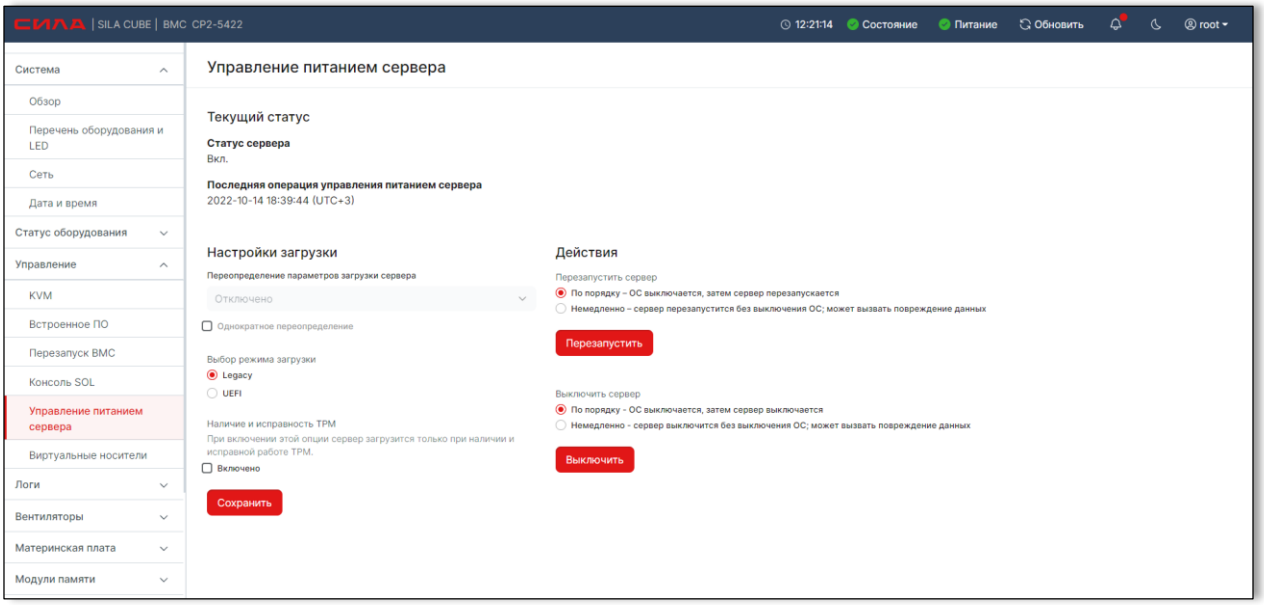

Рисунок 69. Страница «Управление питанием и ОС сервера»

При выборе способа перезапуска и нажатии кнопки «Перезапустить» отображается окно с запросом подтверждения перезапуска (Рисунок 70).

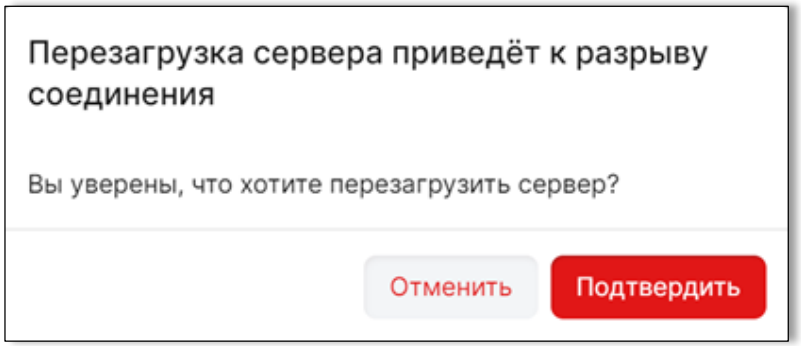

Рисунок 70. Всплывающее окно «Перезапустить сервер»

При выборе способа выключения и нажатии кнопки «Выключить» отображается окно с запросом подтверждения выключения. После подтверждения выключения в статусе сервера отображается «Выключен».

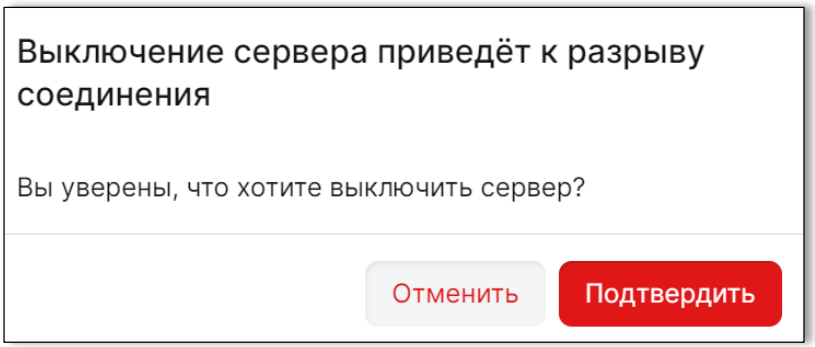

Рисунок 71. Всплывающее окно «Выключить сервер»

При выключенном сервере в разделе «Управление» отображается кнопка «Включить».

При нажатии на кнопку «Включить» отображается окно «Включить сервер».

При подтверждении включения и нажатии «Включить» сервер включается. Отображается статус сервера «Включен» (Рисунок 72).

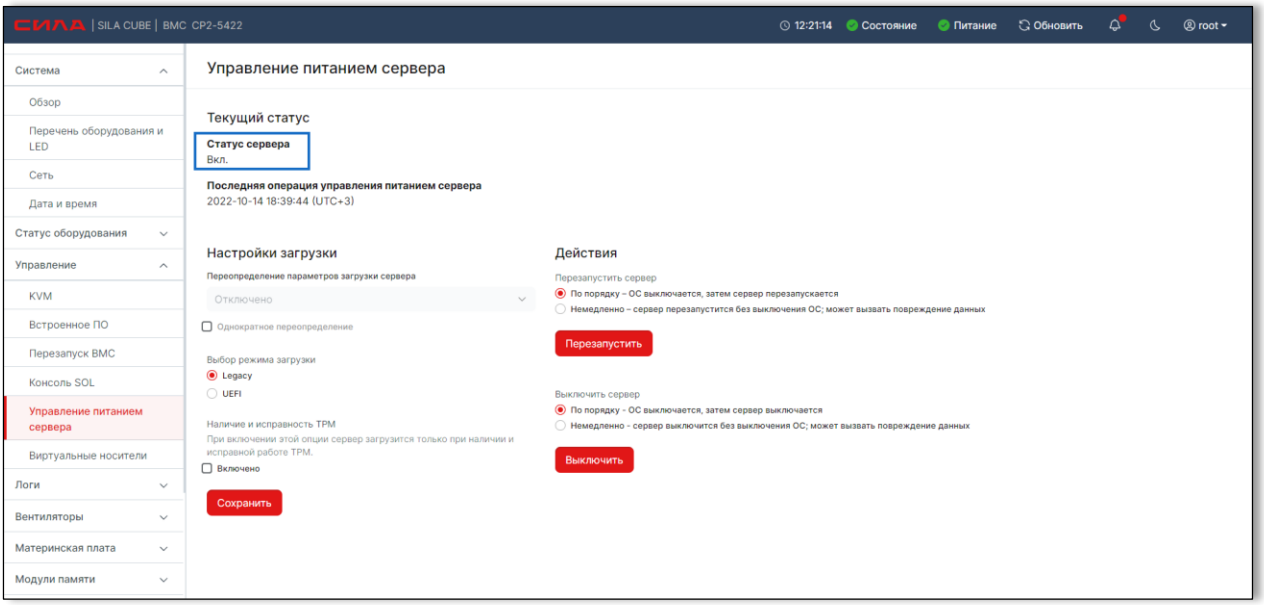

Рисунок 72. Страница «Управление питанием и ОС сервера», статус сервера «Включен»

16 РАБОТА С ОТДЕЛЬНЫМИ РАЗДЕЛАМИ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА

16.1 РАЗДЕЛ «СИСТЕМА»

16.1.1 ОТОБРАЖЕНИЕ ИНФОРМАЦИИ О СЕТЕВЫХ АДАПТЕРАХ

ВНИМАНИЕ:

Отображение информации о сетевых адаптерах доступно для моделей CP1-6326 и CP2-6327 только для ограниченного количества конфигураций.

При выборе в левом основном меню раздела **Система -> Сетевые адаптеры** в правой части отображается информация о сетевых адаптерах (Рисунок 73).

Рисунок 73. Страница «Сетевые адаптеры»

Список сетевых адаптеров формируется на основе подключенных к серверу сетевых карточек.

Состояние портов каждого адаптера меняется в зависимости от состояния линка и вставленных сетевых кабелей в сервер.

Состояние линка может быть:

- Up (активен)
- Down (неактивен)
- Unavailable (недоступен)

16.1.2 ОТОБРАЖЕНИЕ НАСТРОЕК ДАТЫ И ВРЕМЕНИ, НАСТРОЕК ПАРАМЕТРОВ СЕТИ

При выборе в левом основном меню раздела **Система -> Дата и время** в правой части отображается информация о настройке даты и времени (Рисунок 74).

По умолчанию дата, время берутся с host-машины.

Для отображения даты, времени в интерфейсе можно выбрать «Часовой пояс»

При выборе «NTP», вводе Сервера и нажатии «Сохранить настройки» отобразится дата и время с NTP-сервера.

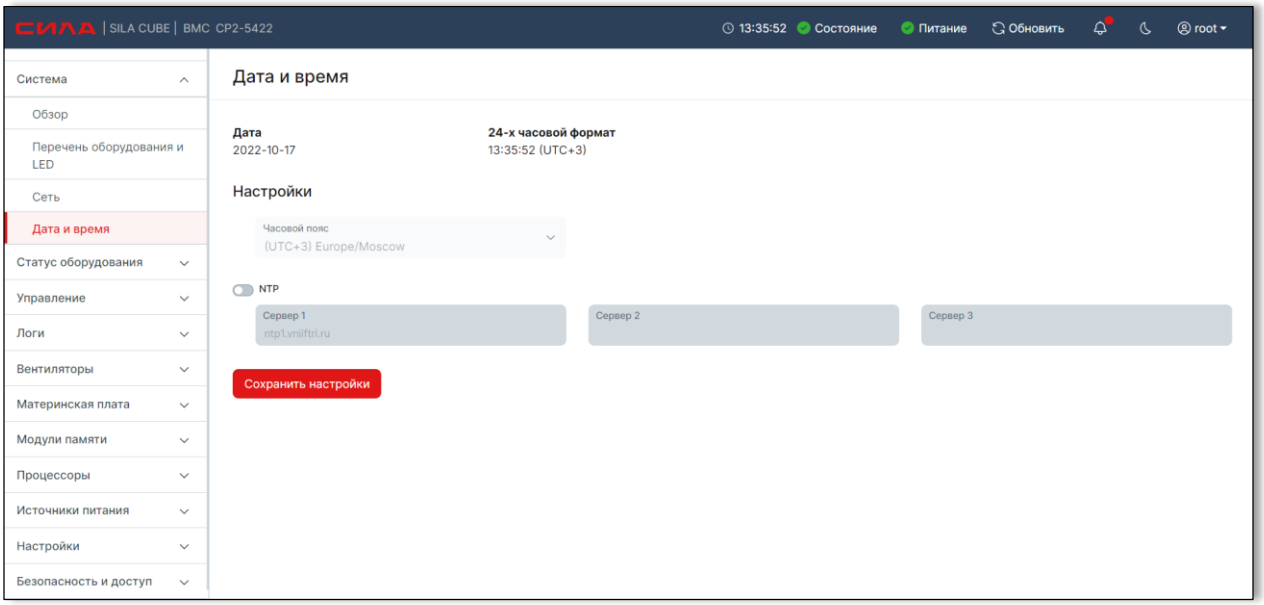

Рисунок 74. Страница «Дата и время»

16.2 РАЗДЕЛ «СТАТУС ОБОРУДОВАНИЯ»

16.2.1 ПРОСМОТР ПЕРЕЧНЯ ДАТЧИКОВ

При нажатии на раздел в основном меню **Статус оборудования -> Датчики** отобразится страница, где можно просмотреть перечень датчиков в BMC (Рисунок 75).

СИЛА | SILA CUBE | CP2-6327 D262060005 11:15:22 Состояние Питание Обновить root

Система
Статус оборудования
Датчики
Управление
Логи
Вентиляторы
Материнская плата
Модули памяти
Процессоры
Источники питания
Настройки
Безопасность и доступ

Датчики

Поиск датчиков

Всего объектов: 44

Фильтровать Экспортировать всё

ИМЯ	СТАТУС	МИН. КРИТ. ЗНАЧЕНИЕ	МИН. ЗНАЧЕНИЕ	ТЕКУЩЕЕ ЗНАЧЕНИЕ	МАКС. ЗНАЧЕНИЕ	МАКС. КРИТ. ЗНАЧЕНИЕ
PSU1 Fan Speed 1	OK	100 RPM	-- RPM	5568 RPM	-- RPM	0 RPM
PSU2 Fan Speed 1	OK	100 RPM	-- RPM	5256 RPM	-- RPM	0 RPM
Pwm PSU1 Fan 1	OK	-- Percent	-- Percent	30 Percent	-- Percent	-- Percent
Pwm PSU2 Fan 1	OK	-- Percent	-- Percent	30 Percent	-- Percent	-- Percent
PCH Temp	OK	0 °C	5 °C	-- °C	98 °C	103 °C
PSU1 Temperature	OK	-- °C	-- °C	22.031 °C	62 °C	65 °C
PSU2 Temperature	OK	-- °C	-- °C	22.125 °C	62 °C	65 °C
PhysicalDrive 6	OK	-- °C	-- °C	17 °C	-- °C	-- °C
PhysicalDrive 7	OK	-- °C	-- °C	18 °C	-- °C	-- °C
PhysicalDrive 8	OK	-- °C	-- °C	14 °C	-- °C	-- °C
RaidController 264	OK	-- °C	-- °C	36 °C	-- °C	-- °C
m2nvme1	OK	-- °C	-- °C	0 °C	60 °C	70 °C
m2nvme2	OK	-- °C	-- °C	0 °C	60 °C	70 °C
A P12V PSU SCALED	OK	10.616 V	10.945 V	12.082 V	13.101 V	13.494 V
P105 PCH AUX	OK	0.966 V	0.995 V	1.058 V	1.106 V	1.139 V
P12V AUX	OK	10.616 V	10.945 V	12.117 V	13.101 V	13.494 V
P1V8 PCH	OK	1.648 V	1.699 V	1.837 V	1.904 V	1.961 V
P3V3	OK	2.974 V	3.066 V	3.358 V	3.541 V	3.647 V
PSU1 Input Voltage	OK	207 V	210 V	230.5 V	250 V	253 V
PSU1 Output Voltage	OK	10.8 V	11.4 V	11.896 V	12.6 V	13.2 V
PSU2 Input Voltage	OK	207 V	210 V	230.5 V	250 V	253 V
PSU2 Output Voltage	OK	10.8 V	11.4 V	11.984 V	12.6 V	13.2 V
PVCCIN CPU1	OK	1.376 V	1.418 V	1.836 V	2.088 V	2.151 V
PVCCIO CPU1	OK	0.729 V	0.752 V	1.037 V	1.155 V	1.19 V
PVDQ ABC CPU1	OK	1.104 V	1.138 V	1.246 V	1.263 V	1.301 V
PVDQ DEF CPU1	OK	1.104 V	1.138 V	1.246 V	1.263 V	1.301 V
PVNN PCH AUX	OK	0.783 V	0.807 V	1.007 V	1.049 V	1.081 V
Pwm 2	OK	-- Percent	-- Percent	100 Percent	-- Percent	-- Percent
Pwm 4	OK	-- Percent	-- Percent	100 Percent	-- Percent	-- Percent
Pwm 7	OK	-- Percent	-- Percent	100 Percent	-- Percent	-- Percent
Pwm 8	OK	-- Percent	-- Percent	100 Percent	-- Percent	-- Percent
System Fan 1	OK	100 RPM	-- RPM	15115 RPM	-- RPM	0 RPM
System Fan 2	OK	100 RPM	-- RPM	14841 RPM	-- RPM	0 RPM
PSU1 Input Current	OK	-- A	-- A	0.733 A	-- A	-- A
PSU1 Output Current	OK	-- A	-- A	12.296 A	145 A	165 A
PSU2 Input Current	OK	-- A	-- A	0.611 A	-- A	-- A
PSU2 Output Current	OK	-- A	-- A	10.703 A	145 A	165 A
PSU1 Input Power	OK	-- W	-- W	166.25 W	1700 W	1900 W
PSU1 Output Power	OK	-- W	-- W	146.75 W	-- W	-- W
PSU2 Input Power	OK	-- W	-- W	140.25 W	1700 W	1900 W
PSU2 Output Power	OK	-- W	-- W	129 W	-- W	-- W
System Airflow	OK	-- cft_i/min	-- cft_i/min	47.878 cft_i/min	-- cft_i/min	-- cft_i/min

Рисунок 75. Страница «Датчики»

В данном перечне представлена информация о:

- датчиках температуры;
- датчиках скорости вентиляторов;
- датчиках напряжения;
- датчиках тока;
- датчиках мощности.

ВНИМАНИЕ:

Датчики температуры RAID-контроллеров и физических накопителей доступны только для моделей CP1-6326 и CP2-6327.

В перечне для каждого датчика указаны:

- статус, отображающий состояние датчика;
- минимальное критическое значение;
- минимальное значение;
- текущее значение;
- максимальное значение;
- максимальное критическое значение.

Значение датчиков указаны с единицами измерения.

Статус датчика может быть:

- OK
- Warning
- Critical

При нажатии на кнопку «Экспортировать всё» перечень датчиков экспортируется в JSON-формате в выбранную папку.

16.3 РАЗДЕЛ «УПРАВЛЕНИЕ»

16.3.1 ПРОВЕРКА ОТОБРАЖЕНИЯ ПЕРЕЗАГРУЗКИ BMC

При выборе в основном меню раздела **Управление -> Перезапуск BMC** в правой части экрана отобразится информация о последнем перезапуске BMC и кнопка «Перезапустить BMC» (Рисунок 76).

При нажатии на кнопку «Перезапустить BMC» отображается всплывающее окно «Перезагрузка BMC».

При подтверждении перезагрузки происходит перезагрузка BMC.

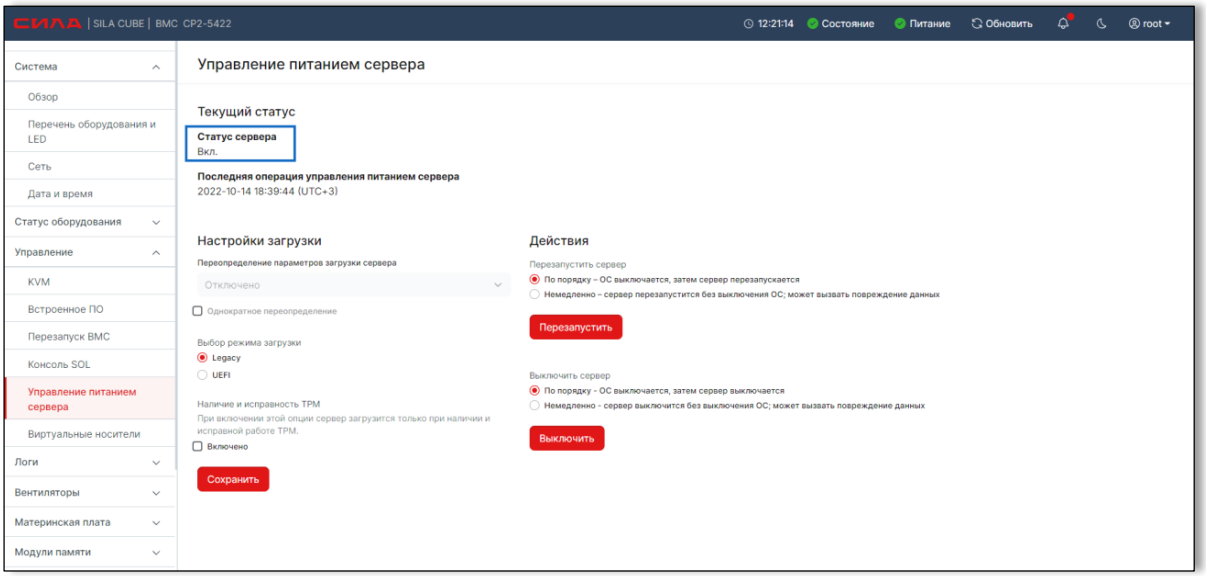

Рисунок 76. Вкладка «Перезапуск BMC»

16.4 АНАЛИТИЧЕСКАЯ ПАНЕЛЬ «МОДУЛЬ ПАМЯТИ»

16.4.1 ОТОБРАЖЕНИЕ ДИНАМИЧЕСКОЙ ИНФОРМАЦИИ О СОСТОЯНИИ МОДУЛЕЙ ПАМЯТИ

При нажатии на раздел в основном меню **Модули памяти -> Динамическая информация** отобразится страница, где находится аналитическая панель с информацией о состоянии температуры модулей памяти (Рисунок 77).

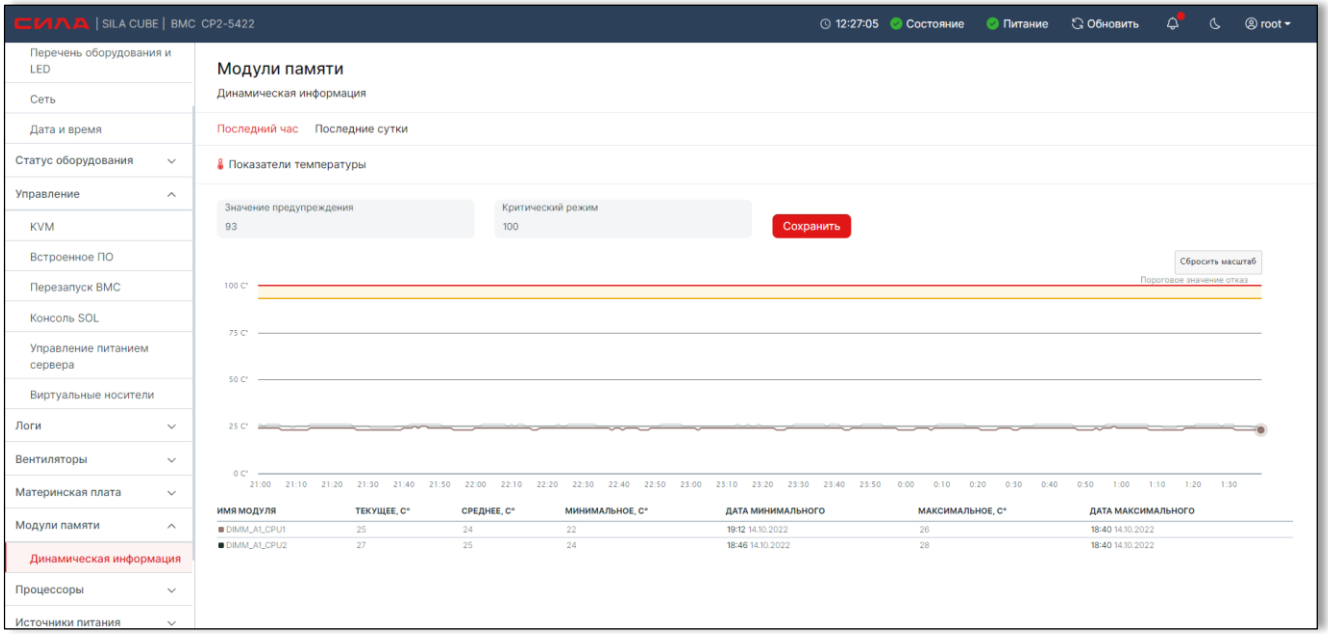

Рисунок 77. Страница «Модуль памяти. Динамическая информация»

При работе с панелью можно выбрать период, за который вы хотите получить информацию о состоянии температуры модулей памяти. Также реализована возможность увеличения масштаба выбранного участка графика. Для это необходимо левой кнопкой мыши выделить на графике интересуемый участок. Для возврата масштаба графика в исходное состояние необходимо нажать на кнопку «Сбросить масштаб».

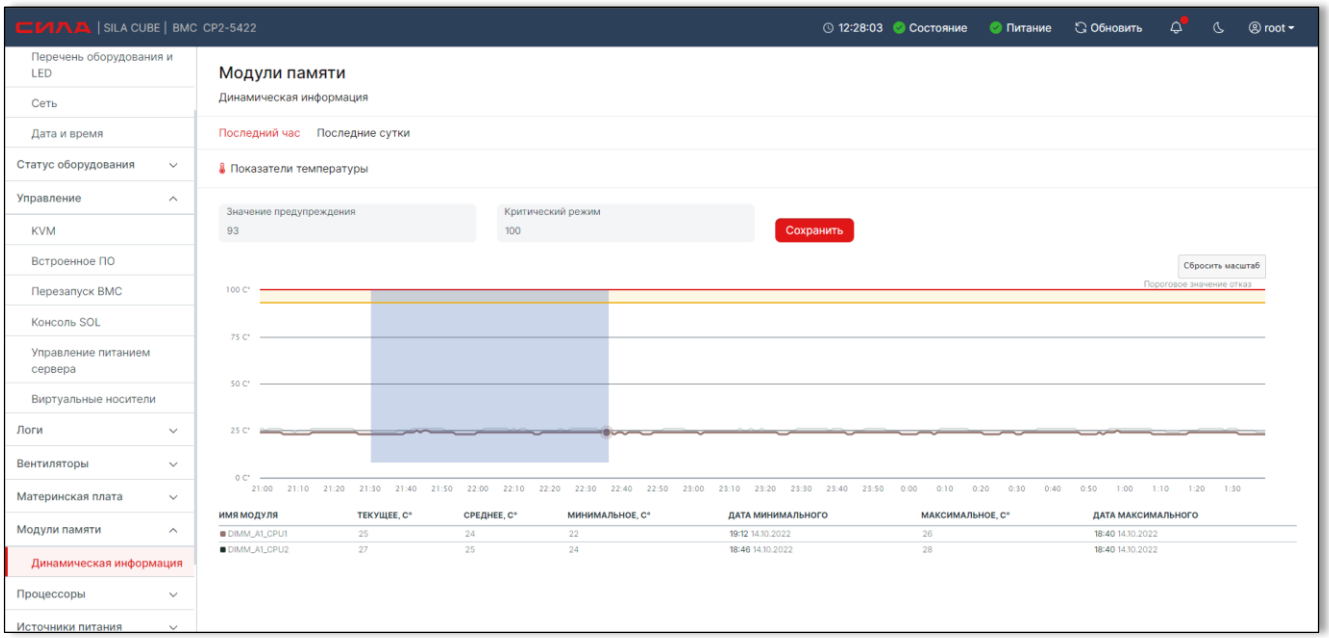

Рисунок 78. Страница «Модуль памяти. Динамическая информация». Выделение участка графика

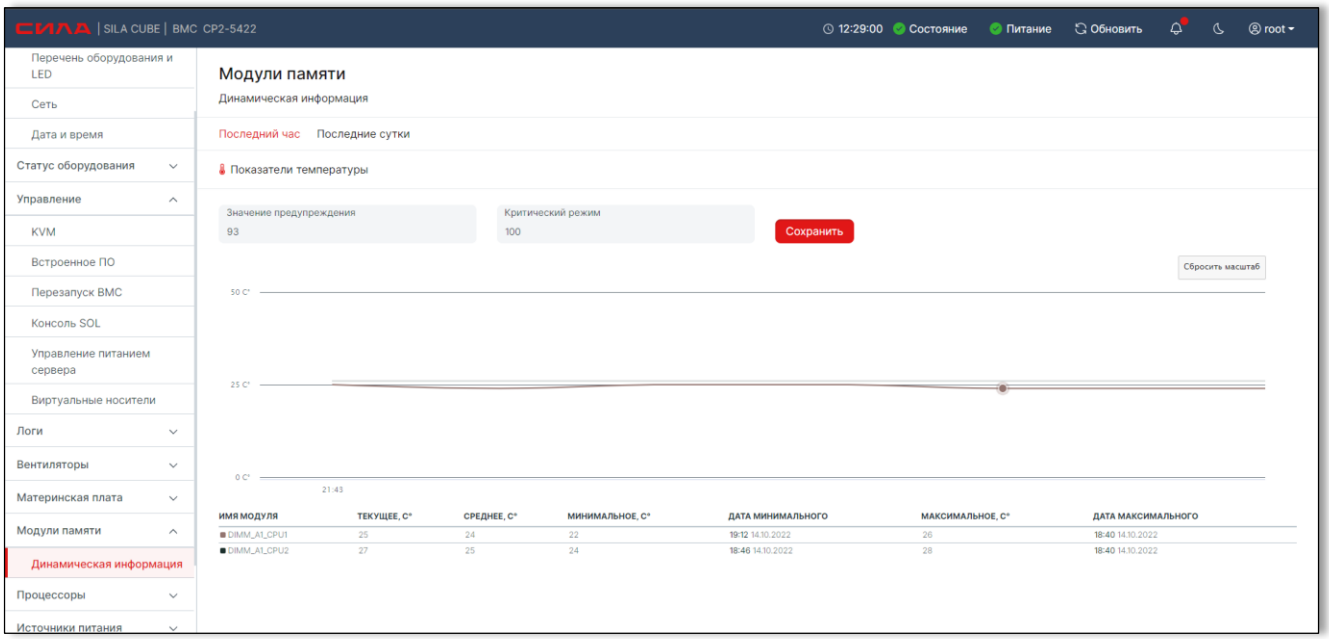

Рисунок 79. Страница «Модуль памяти. Динамическая информация». Увеличенный масштаб выбранного участка графика

16.5 АНАЛИТИЧЕСКАЯ ПАНЕЛЬ «ВЕНТИЛЯТОРЫ»

16.5.1 ПЕРЕЧЕНЬ ОТОБРАЖАЕМОЙ ДИНАМИЧЕСКОЙ ИНФОРМАЦИИ О ТЕКУЩЕМ СОСТОЯНИИ ВЕНТИЛЯТОРОВ

При выборе в левом основном меню раздела **Вентиляторы -> Динамическая информация** отобразится аналитическая панель с информацией о показателях скорости работы вентиляторов.

Примечание: наличие и типы вентиляторов могут отличаться в зависимости от конфигурации системы.

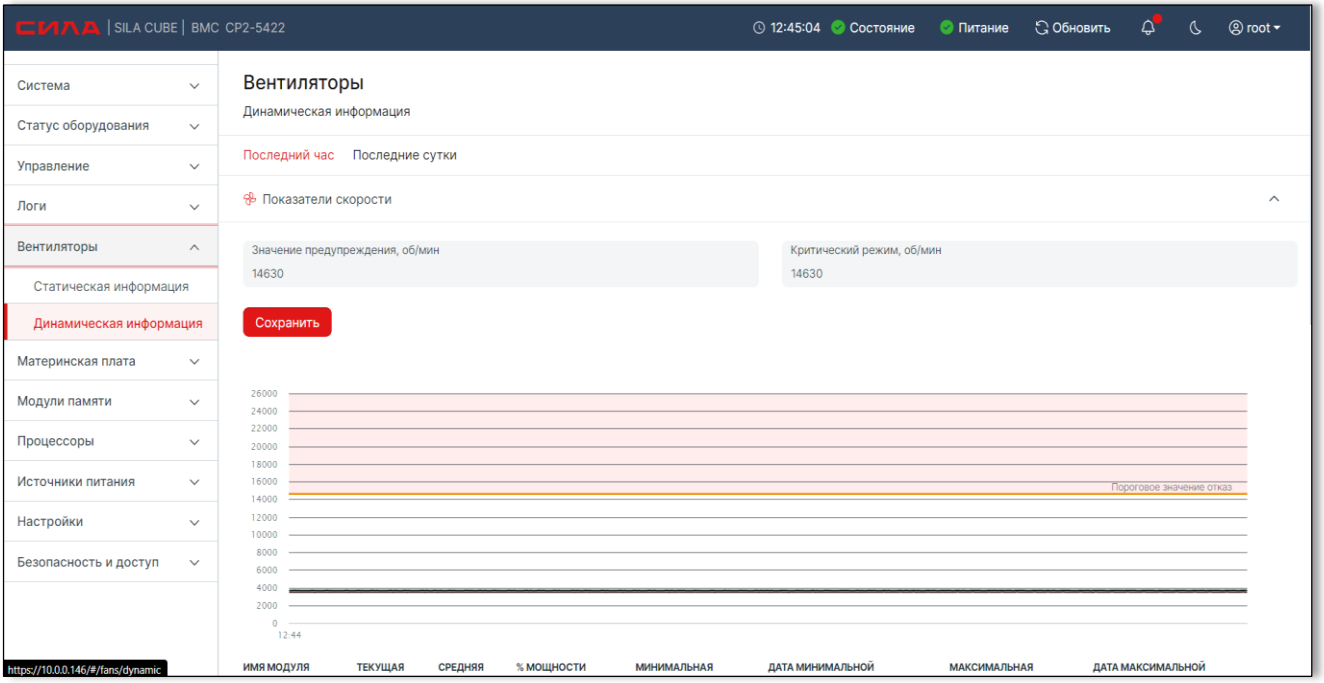

Рисунок 80. Страница «Вентиляторы. Динамическая информация»

При работе с панелью можно выбрать период, за который вы хотите получить информацию о показателях вентиляторов. Также реализована возможность увеличения масштаба выбранного участка графика. Для это необходимо левой кнопкой мыши выделить на графике интересуемый участок. Для возврата масштаба графика в исходное состояние необходимо нажать на кнопку «Сбросить масштаб».

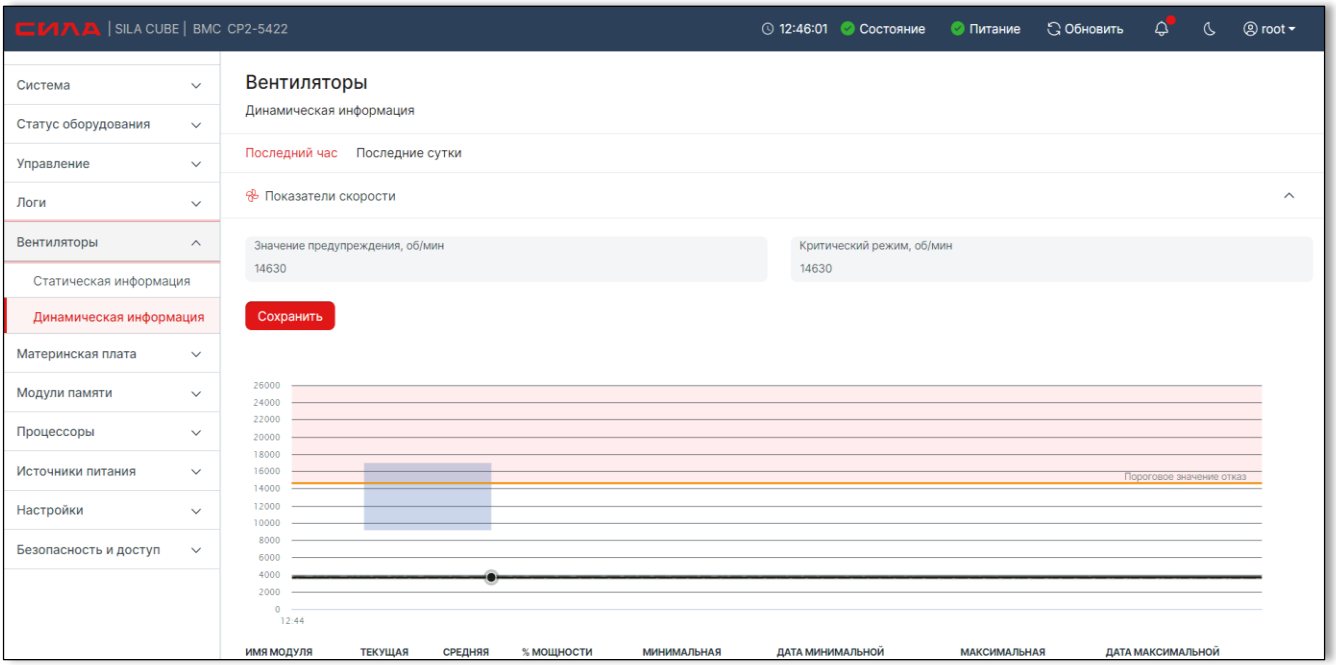

Рисунок 81. Страница «Вентиляторы. Динамическая информация». Выделение участка графика

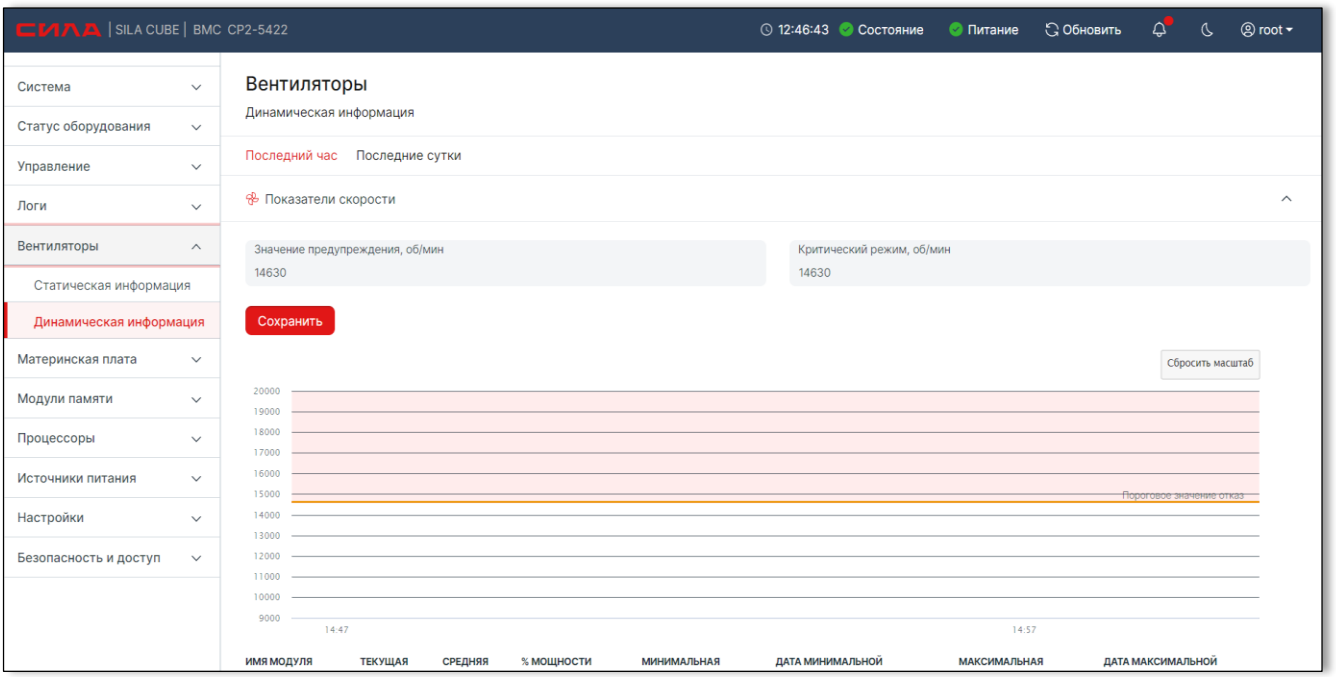

Рисунок 82. Страница «Вентиляторы. Динамическая информация». Увеличенный масштаб выбранного участка графика

16.6 АНАЛИТИЧЕСКАЯ ПАНЕЛЬ «МАТЕРИНСКАЯ ПЛАТА»

16.6.1 ОТОБРАЖЕНИЕ ДИНАМИЧЕСКОЙ ИНФОРМАЦИИ О СОСТОЯНИИ МАТЕРИНСКОЙ ПЛАТЫ

При выборе в левом основном меню раздела **Материнская плата -> Динамическая информация**, где находится аналитическая панель с информацией о состоянии температуры материнских плат.

При работе с панелью можно выбрать период, за который вы хотите получить информацию о состоянии температуры материнских плат. Также вы можете выбрать пороговое значения предупреждения об критической ситуации. Для увеличения масштаба выбранного участка графика. Для это необходимо левой кнопкой мыши на графике выделить интересуемый участок. Для возврата масштаба графика в исходное состояние необходимо нажать на кнопку «Сбросить масштаб».

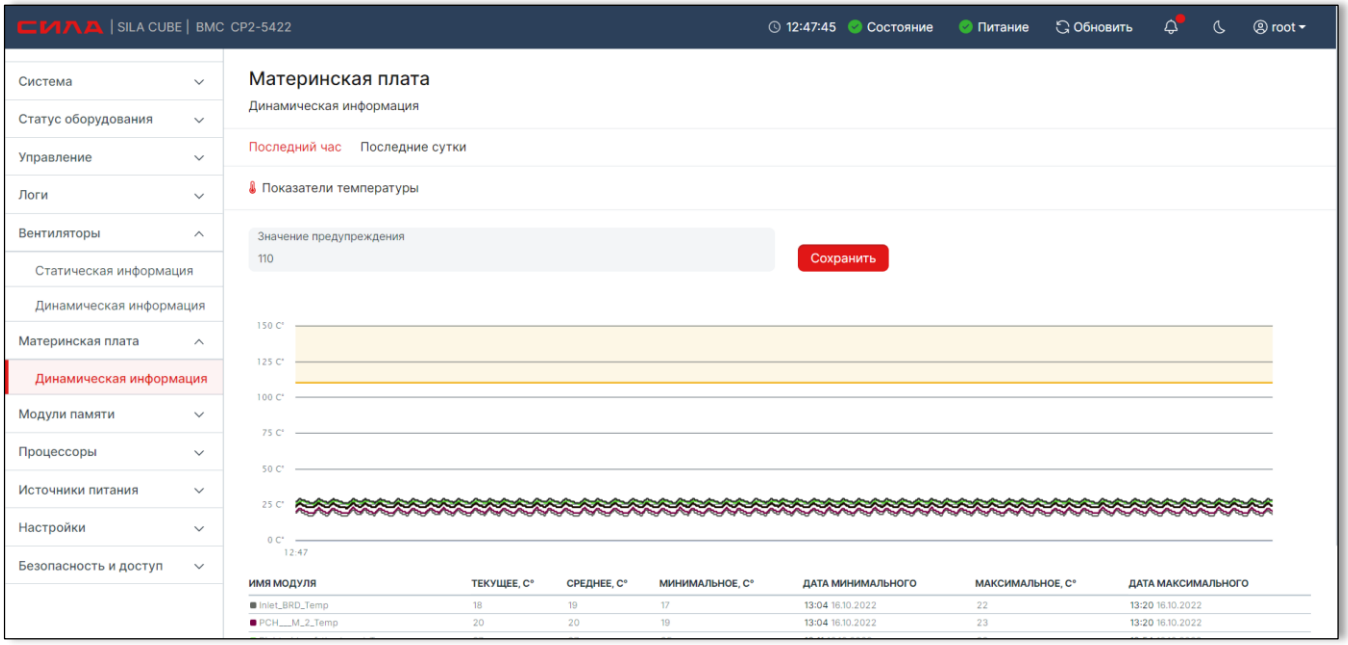

Рисунок 83. Страница «Материнская плата. Динамическая информация»

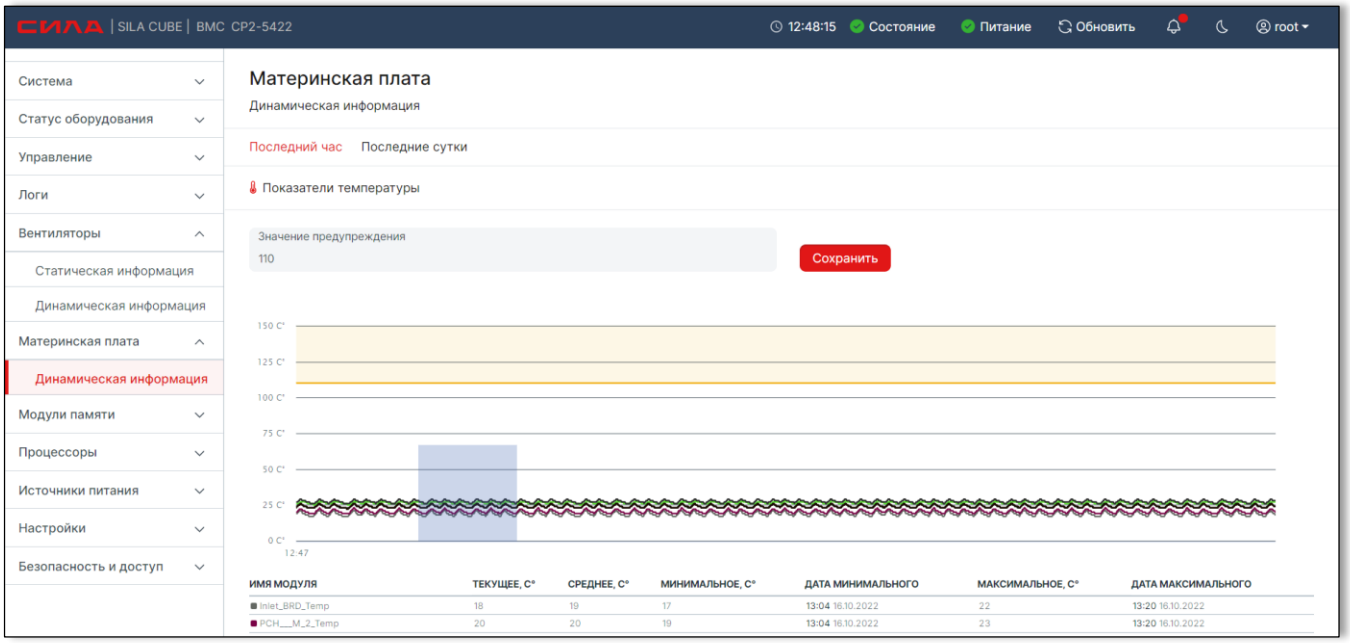

Рисунок 84. Страница «Материнская плата. Динамическая информация» Выделение участка графика

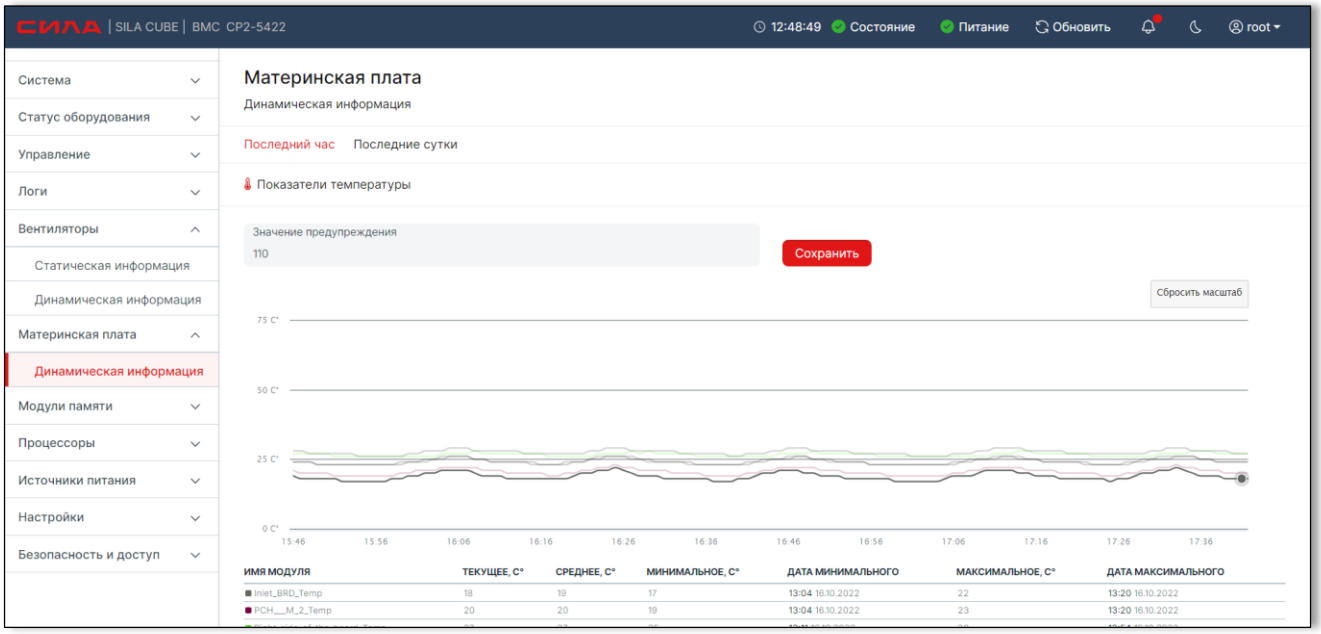

Рисунок 85. Страница «Материнская плата. Динамическая информация» Увеличенный масштаб выбранного участка графика

16.7 АНАЛИТИЧЕСКАЯ ПАНЕЛЬ «ПРОЦЕССОРЫ»

16.7.1 ОТОБРАЖЕНИЕ ДИНАМИЧЕСКОЙ ИНФОРМАЦИИ О СОСТОЯНИИ ПРОЦЕССОРОВ

При выборе в левом основном меню раздела **Процессоры -> Динамическая информация**, где находится аналитическая панель с информацией о состоянии температуры процессоров.

При работе с панелью можно выбрать период, за который вы хотите получить информацию о состоянии температуры процессоров или потребляемой мощности. Также вы можете выбрать пороговое значения предупреждения об критической ситуации. Для увеличения масштаба выбранного участка графика. Для это необходимо левой кнопкой мыши на графике выделить интересуемый участок. Для возврата масштаба графика в исходное состояние необходимо нажать на кнопку «Сбросить масштаб»

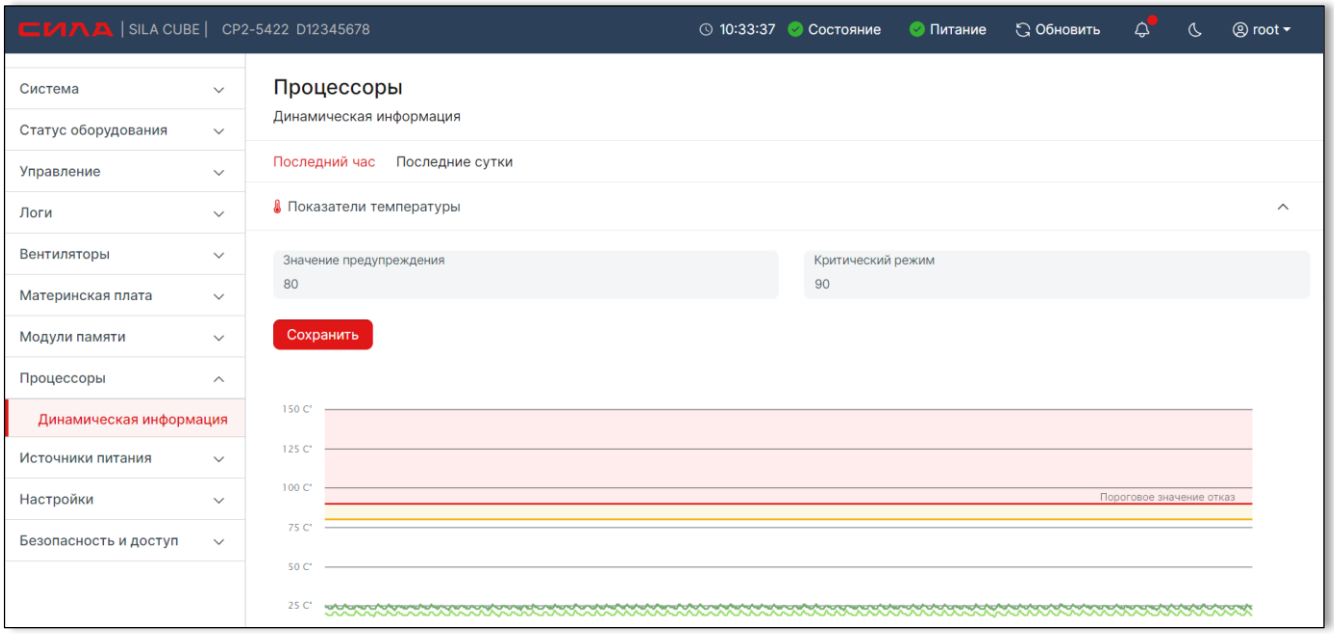

Рисунок 86 Страница «Процессоры. Динамическая информация»

16.8 АНАЛИТИЧЕСКАЯ ПАНЕЛЬ «ИСТОЧНИКИ ПИТАНИЯ»

16.8.1 ОТОБРАЖЕНИЕ ДИНАМИЧЕСКОЙ ИНФОРМАЦИИ О СОСТОЯНИИ ИСТОЧНИКОВ ПИТАНИЯ

При выборе в левом основном меню раздела **Источники питания -> Динамическая информация**, где находится аналитическая панель с информацией о состоянии температуры источников питания и других показателях.

При работе с панелью можно выбрать период, за который вы хотите получить информацию о состоянии температуры источников питания или других показателях. Также вы можете выбрать пороговое значения предупреждения об критической ситуации. Для увеличения масштаба выбранного участка графика. Для это необходимо левой кнопкой мыши на графике выделить интересуемый участок. Для возврата масштаба графика в исходное состояние необходимо нажать на кнопку «Сбросить масштаб».

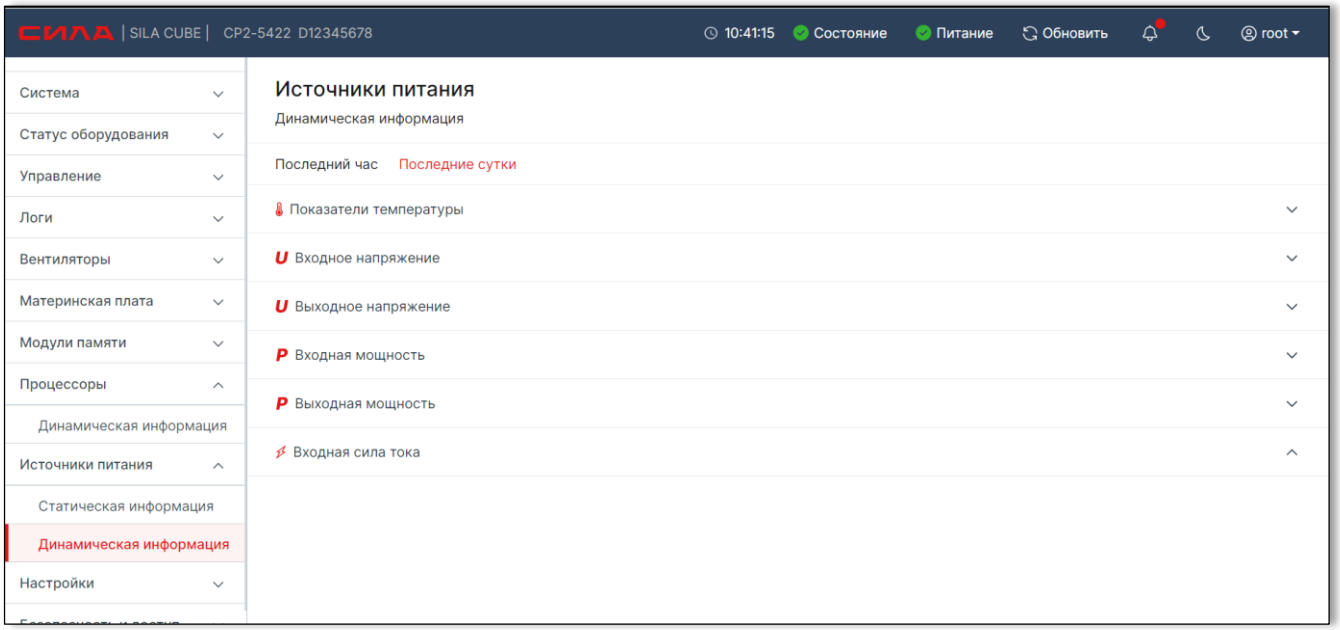

Рисунок 87 Страница «Источники питания. Динамическая информация»

16.9 ОТДЕЛЬНЫЕ ЭЛЕМЕНТЫ УПРАВЛЕНИЯ

Для просмотра списка сообщений и перехода к журналу нужно нажать кнопку «Уведомления».

Для перевода к журналу событий нужно кликнуть на уведомление из списка (Рисунок 88).

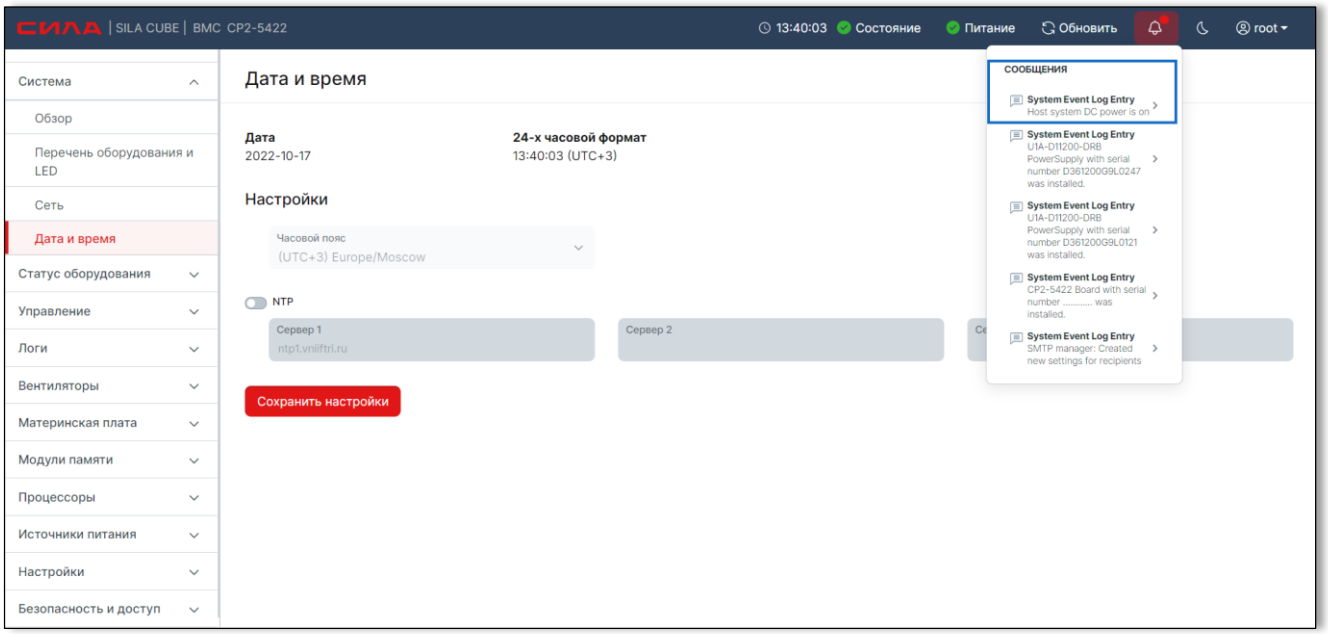

Рисунок 88. Список сообщений

Для переключения интерфейс в «ночной режим» нажмите кнопку (Рисунок 89).

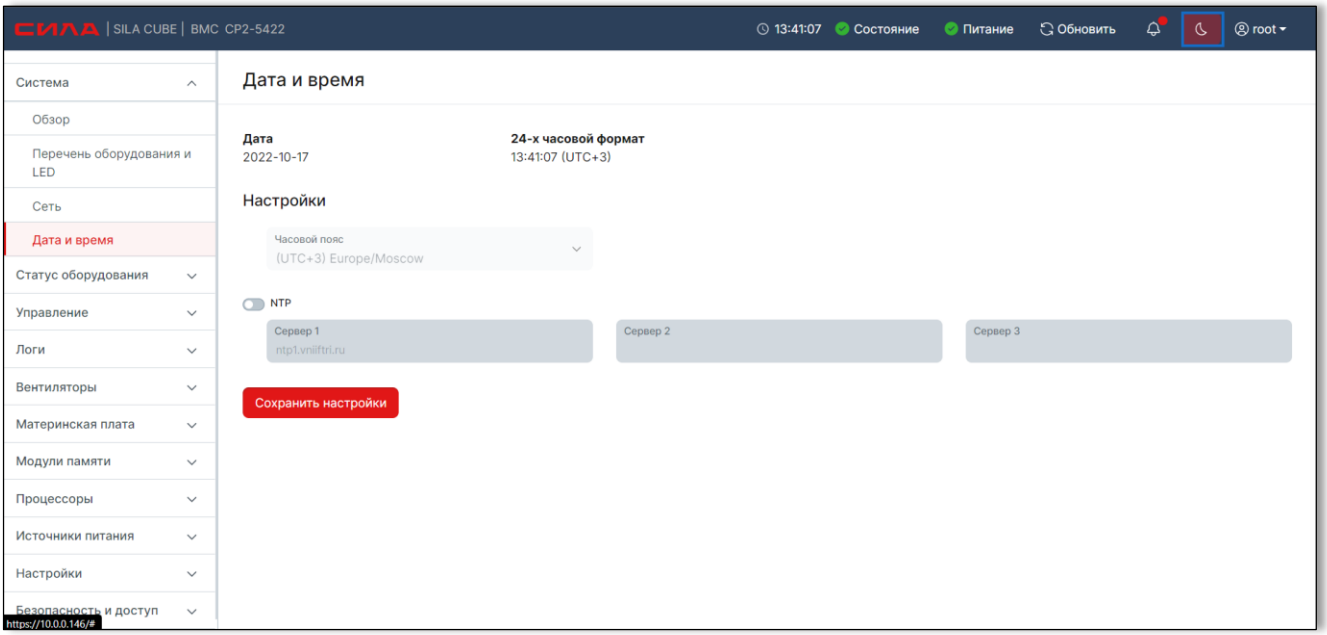

Рисунок 89. Переключение в ночной режим

После переключения интерфейс будет выглядеть, как показано на Рисунок 90.

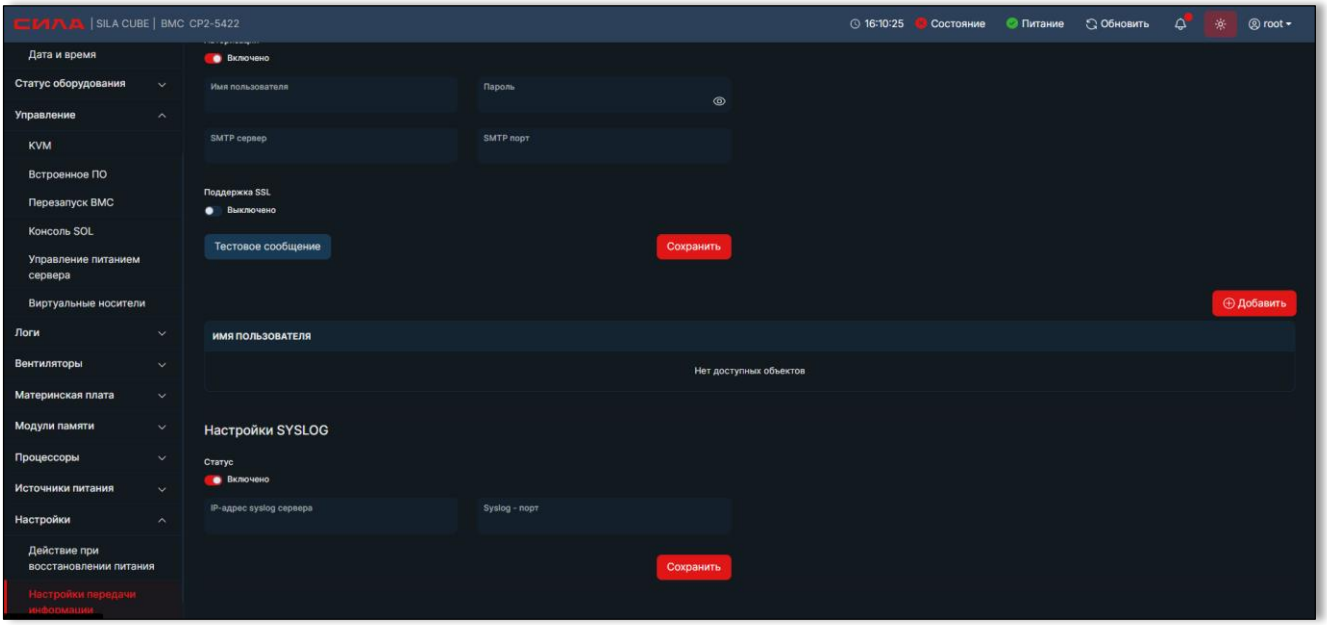

Рисунок 90. Ночной режим интерфейса

17 ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

17.1 СООБЩЕНИЯ ОБ ОШИБКАХ

Таблица 5. Сообщения об ошибках

Проблема / Код ошибки	Решение
ESXi отображает сообщение «Alert» по сенсорам, у которых нет граничных значений.	Состояние сенсоров, возвращаемых по протоколу IPMI, не содержащих корректной размерности (размерность unspecified) и пороговых значений (threshold), приводятся справочно. Использовать их для определения состояния системы не рекомендуется.
Сообщение в журнале событий: «Service systemd-networkd-wait-online.service has exited unsuccessfully»	При возникновении данного сообщения в журнале событий его можно пометить как разрешенное или удалить. Данное событие не сигнализирует о неисправности.
Сообщение в журнале событий: «Service phosphor-ipmi-host.service has exited unsuccessfully»	Для СР2-5422, СР4-5422: При возникновении данного сообщения в журнале событий следует проверить работоспособность. Например, из операционной системы сервера выполнить: **#ipmitool power status.** В случае, если локальный протокол IPMI работоспособен или операционная система сервера не использует локальный протокол IPMI, событие можно пометить как разрешенное или удалить. В случае, если локальный протокол IPMI неработоспособен, и операционная система сервера использует локальный протокол IPMI, рекомендуется перезагрузить сервер. После чего проверить работоспособность связи сервера с BMC по локальному протоколу IPMI. Для серверов СР1-6326, СР2-6327, СР9-6426: При возникновении данного сообщения в журнале событий следует перезагрузить СИЛА Куб. После перезагрузки СИЛА Куб необходимо перезагрузить сервер

17.2 ОСОБЕННОСТИ СИСТЕМ

17.2.1 ДОСТУП К IPMI

Для доступа к IPMI по протоколу lanplus используется набор шифров 17 (например, **ipmitool -I lanplus -C 17…)**.

Выделенный сетевой интерфейс для сервера CP2-5422 может быть доступен по протоколу IPMI как каналы 1 и 3. Например:

- **ipmitool lan print**
- **ipmitool lan print 1**
- **ipmitool lan print 3**

Выделенный сетевой интерфейс для серверов CP1-6326, CP2-6327, CP9-6426 доступен по протоколу IPMI как канал 1. Например:

- **ipmitool lan print**
- **ipmitool lan print 1**

По протоколу REDFISH и через Web-интерфейс выделенный сетевой интерфейс для серверов СИЛА именуется – «eth0».

Сетевой интерфейс совмещенный с LOM-портом для серверов CP1-6326, CP2-6327, CP9-6426 доступен по протоколу IPMI как канал 3. Например, **ipmitool lan print 3.**

По протоколу REDFISH и через Web-интерфейс сетевой интерфейс совмещенный с LOM-портом для серверов CP1-6326, CP2-6327, CP9-6426 именуется – «eth1»

17.3 РЕКОМЕНДАЦИИ

17.3.1 ДЛЯ СЕРВЕРА CP2-5422, CP4-5422

- При инсталляции версии, начиная с 01.07 рекомендуется обновление BIOS до версии 8.4.
- Зарегистрированные серийные номера серверов всегда содержат в начале символ D.
- Если серийный номер не задан, например: в системе СИЛА Куб виден как NEED TO SET или в операционной системе команда

```
dmidecode -t 1 | grep Serial | grep D
```

ничего не возвращает, тогда

– Запросить в Службе Поддержки архив ***tar zvfbios_8_X_linux_update.tgz,***

где X – версия BIOS

– Распаковать архив

– Перейти в каталог,

– Выполнить команду:

```
./set_dmi.sh <Серийный номер сервера> <Серийный номер платформы>
```

– Серийный номер восстановлен.

17.3.2 ДЛЯ СЕРВЕРОВ CP1-6326, CP2-6327, CP9-6426

- При инсталляции версии, начиная с 01.07 рекомендуется обновление BIOS до версии 9.3.
- При добавлении пользователя через BIOS в меню Add user после установки пароля может возникнуть ошибка "Set User Access Command Failed!!!", но пароль устанавливается корректно. Обходные пути: управлять пользователями через Web-интерфейс СИЛА Куб или после возникновения этой ошибки продолжить настройку пользователя в BIOS в подменю Change User Settings. Для изменения прав доступа, необходимо выбрать 3 канал и выставить на нем соответствующий уровень доступа.

КОНТАКТНАЯ ИНФОРМАЦИЯ

Техническая поддержка

+7 (495) 662-10-52 для звонков из Москвы

+7 (800) 600-96-22 для звонков из регионов

support@sila.ru

Если Вам требуется квалифицированная помощь, позвоните на телефон «горячей линии поддержки», напишите письмо или воспользуйтесь другими способами обращения в техническую поддержку:

- система учета заявок Service Desk: https://support.sila.ru/
- форма регистрации заявки на сайте: https://sila.ru/ru/contacts

СИЛА

КОНТАКТЫ

125167, г. Москва,
Ленинградский пр-т, д. 37А, корп. 4

+7 (495) 933-37-01
info@sila.ru
www.sila.ru