# Руководство пользователя

# Системы управления и мониторинга V-Sense

2025 год

Оглавление

**1. ВВЕДЕНИЕ** ..... 4
**2. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ** ..... 4
**3. ПОДГОТОВКА К РАБОТЕ** ..... 4
**4. РАБОТА С ПО** ..... 4
**4.1. Вход в ПО** ..... 4
**4.2. Основная страница** ..... 7
**4.3. Сеть** ..... 8
4.3.1. Дашборды ..... 8
4.3.2. Устройства ..... 9
4.3.3. Версия ПО ..... 12
4.3.4. Серийные номера ..... 13
4.3.5. Шаблоны устройств ..... 14
4.3.6. Группа хостов ..... 15
**4.4. Логирование** ..... 18
**4.5. Радиус** ..... 19
**4.6. Модуль событий** ..... 23
**4.7. Почта** ..... 24
4.7.1. Модуль Почты ..... 24
4.7.2. Модуль Рассылки ..... 25
4.7.3. Статистика Почты ..... 25
4.7.4. Настройка Команд ..... 26
4.7.5. Настройка Отчетов ..... 27
4.7.6. Телеграм ..... 28
**4.8. Администрирование** ..... 30
4.8.1. Настройка Логирования ..... 31
4.8.2. Модуль Конфигурационных Файлов ..... 31
4.8.3. Сохранить / Загрузить БД ..... 33
4.8.4. TFTP ..... 33
4.8.5. NTP ..... 35
4.8.6. Модуль Хранения ..... 35

**4.9. Пользователи** ..... 37
**4.10. Терминал** ..... 39
**4.11. Лицензия** ..... 45
**5. ТРЕБОВАНИЯ ПО** ..... 48
**5.1. Требования квалификации персонала** ..... 48
**5.2. Требования к АРМ** ..... 48
**5.3. Требования к серверной части** ..... 49
**6. СПИСОК СОКРАЩЕНИЙ** ..... 50

# 1. ВВЕДЕНИЕ

Настоящее руководство пользователя распространяется на программное обеспечение – систему управления и мониторинга V-Sense. ПО V-Sense является системой мониторинга и управления оборудования Вектор Технологии, а также прочего оборудования информационных технологий. Руководство пользователя содержит технические характеристики, описание программного обеспечения, принципы взаимодействия пользователя с программным обеспечением и указания, необходимые для правильной и безопасной его эксплуатации.

# 2. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

Система управления и мониторинга V-Sense предназначена для управления и мониторинга сетевого оборудования. Основными протоколами сбора информации и управления являются SNMP (v2/v3) и SSH(v2).

ПО представляет собой WEB-ориентированную платформу, состоящую из клиентской и серверной части. Клиентская часть является веб-приложением, визуализирующим функционал серверной части. В серверную часть входят функции хранения и обработки информации.

# 3. ПОДГОТОВКА К РАБОТЕ

Для начала работы с ПО V-Sense на автоматизированном рабочем месте должен быть предустановлен один из предложенных WEB – браузеров: Яндекс.Браузер, Google Chrome, Microsoft Edge, Mozilla Firefox, Opera или другой аналогичный, с установленными обновлениями не позднее 2020 года.

Для доступа к системе V-Sense требуется подключение к сети, в которой доступен вычислительный ресурс, где установлена СУИМ.

# 4. РАБОТА С ПО

## 4.1. Вход в ПО

ПО V-Sense поставляется в виде виртуальной машины.

Для входа в ПО необходимо в адресной строке браузера ввести IP-адрес, например, как на рис. 4.1.1 (где XXX.XXX.XXX.XXX – IP-адрес, YYYYY - порт). По умолчанию порт можно не указывать.

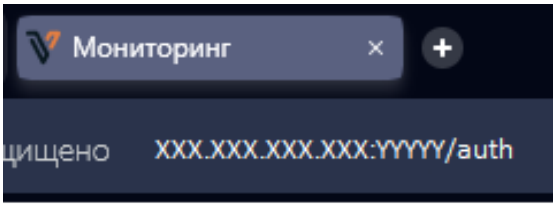



Рисунок 4.1.1 – Ввод IP-адреса

Пользователь переадресовывается на страницу авторизации ПО V-Sense (рис. 4.1.2).

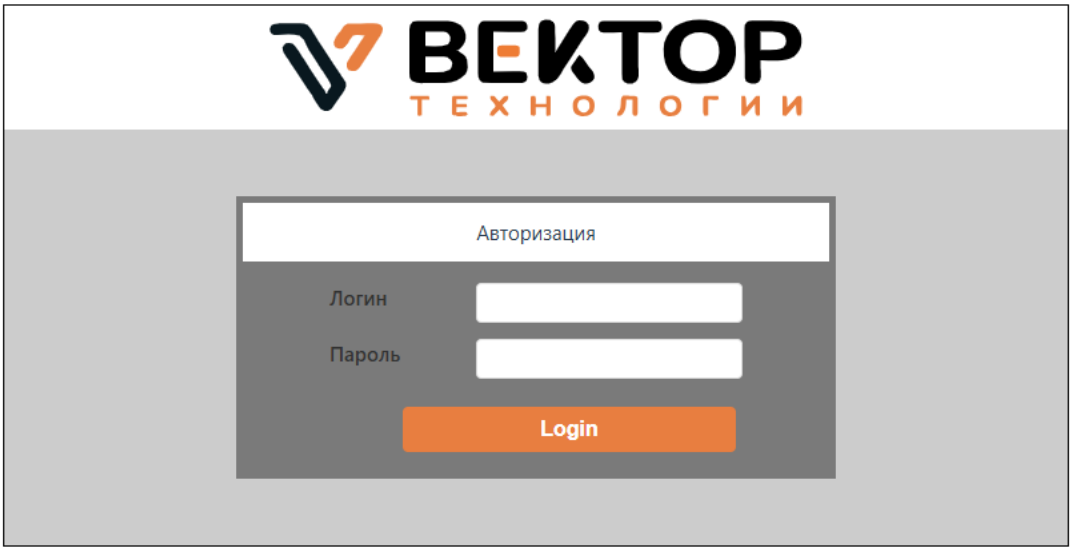



Рисунок 4.1.2 – Авторизация пользователя

Для получения доступа к данным необходимо выполнить авторизацию: указать логин и пароль, а затем нажать кнопку «*Login*». По умолчанию доступны следующие наборы логинов\паролей:

– user\user;
– admin\admin;
– superadmin\superadmin.

При неправильном вводе логина или пароля появляется сообщение об ошибке (рис. 4.1.3).

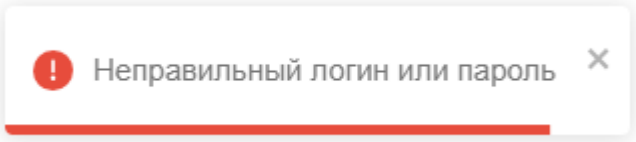



Рисунок 4.1.3 – Ошибка авторизации пользователя

### 4.2. Основная страница

После авторизации в ПО вы попадаете на основную страницу (рис. 4.2.1).

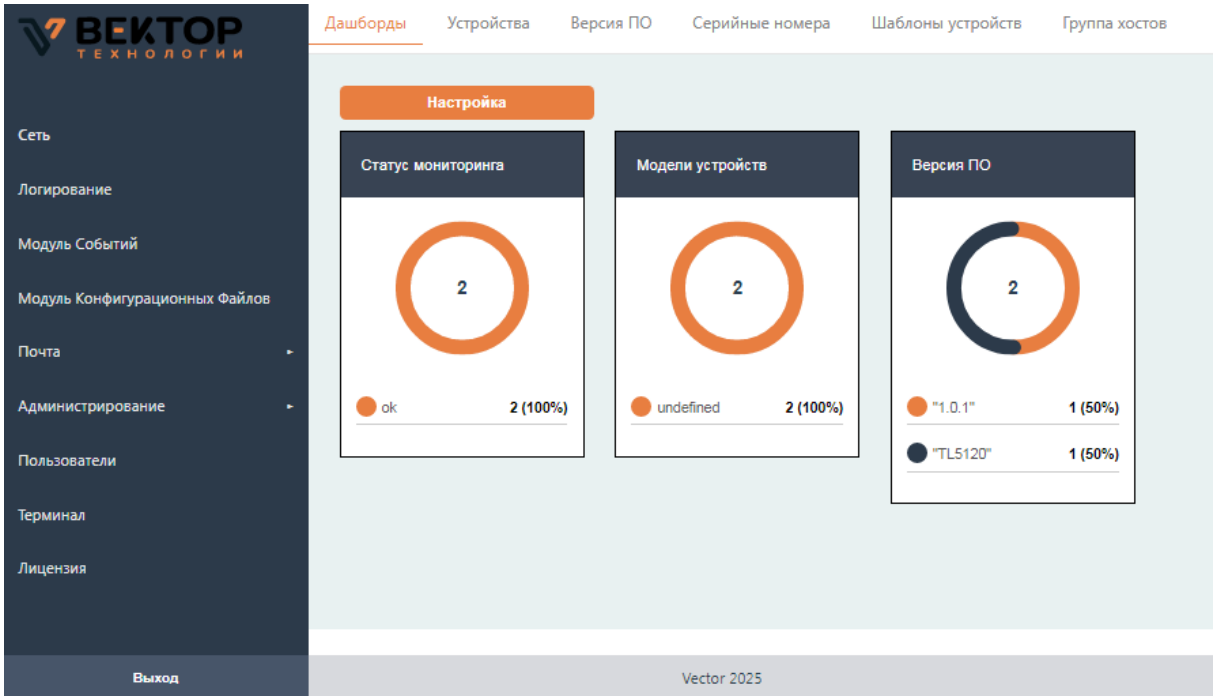



Рисунок 4.2.1 – Основная страница

На основной странице ПО V-Sense представлено меню со следующими вкладками:

1. Сеть;
2. Логирование;
3. Радиус;
4. Модуль событий;
5. Почта;
6. Администрирование;
7. Пользователи;
8. Терминал;
9. Лицензия.

## 4.3. Сеть

В данном окне представлены основные элементы системы мониторинга:

– Дашборды;

– Устройства;

– Версия ПО;

– Серийные номера;

– Шаблоны устройств;

– Группа хостов.

### 4.3.1. Дашборды

Модуль отвечает за предоставление графической информации о текущем состоянии устройств, находящихся в мониторинге (рис. 4.3.1.1). В данном модуле отражены основные показатели в различных графических вариантах, такие как:

– состояние оборудования онлайн/оффлайн;

– актуальность версий ПО;

– состояния архивирования конфигурация устройств;

– последние события в сети;

– показатели устройств с наивысшими параметрами: загрузка CPU, температура.

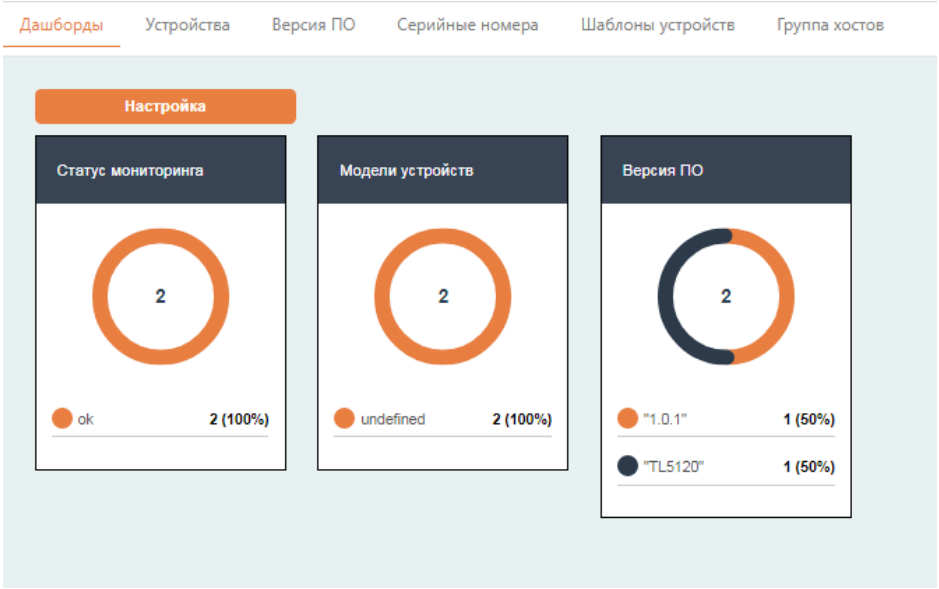



Рисунок 4.3.1.1 – Окно «Дашборды»

В системе мониторинга можно создавать пользовательские дашборды. Для добавления нового дашборда необходимо заполнить следующие поля (рис. 4.3.1.2):

– ***название дашборда*** – краткое описание дашборда;

– ***тип диаграммы*** – выбор графического представления дашборда (круговая диаграмма);

– ***позиция*** – положение в окне мониторинга;

– ***опрашиваемый OID*** – параметр мониторинга, по которому будет строиться дашборд.

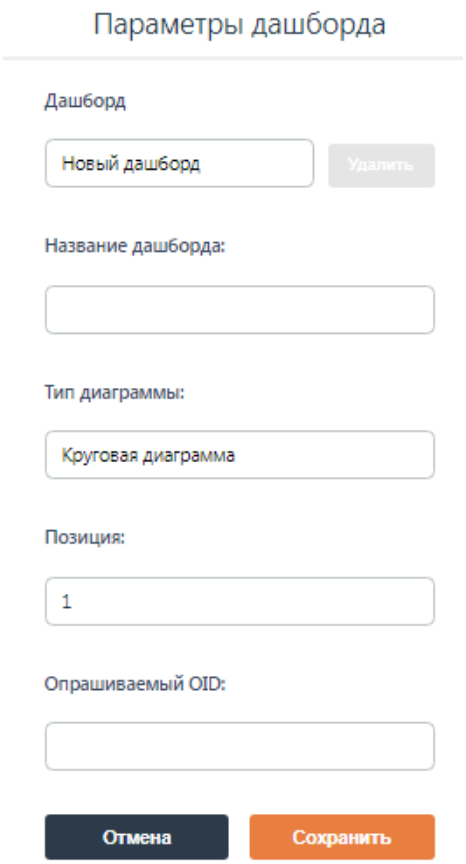



Рисунок 4.3.1.2 – Настройка дашбордов

4.3.2. Устройства

При открытии вкладки отображается список устройств, которые находятся в мониторинге, в «Режиме таблицы» (рис. 4.3.2.1). Также список устройств может быть представлен в графическом виде в «Режиме карты». Для

переключения режимов, соответственно, нужно нажать на кнопки «*Режим карты*» или «*Режим таблицы*».

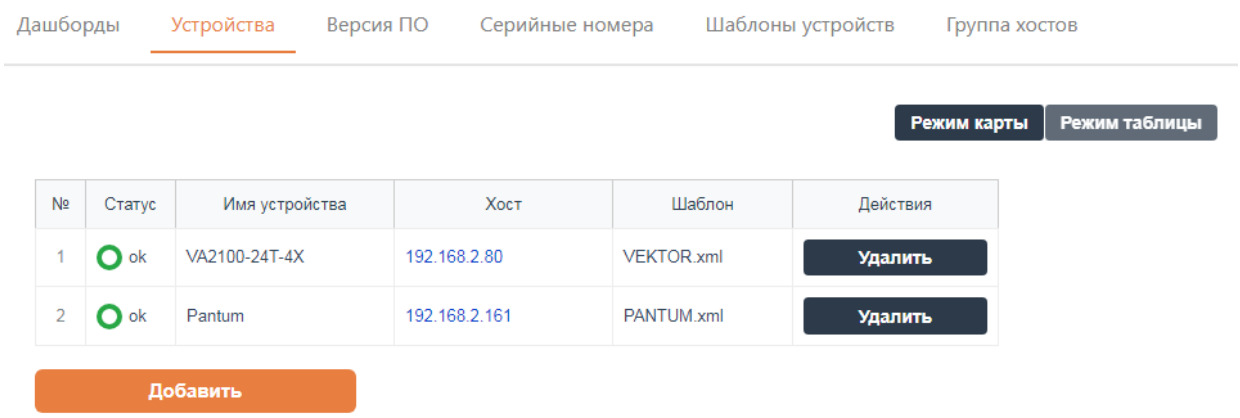



Рисунок 4.3.2.1 – Окно «Устройства»

В «Режиме таблицы» список устройств представлен в табличном виде со следующими полями:

– ***Статус*** – состояние устройства в системе мониторинга, значение данного поля может принимать значения «ok» или «fail»;

– ***Имя устройства*** - имя устройства в системе мониторинга;

– ***Хост*** – IP-адрес устройства;

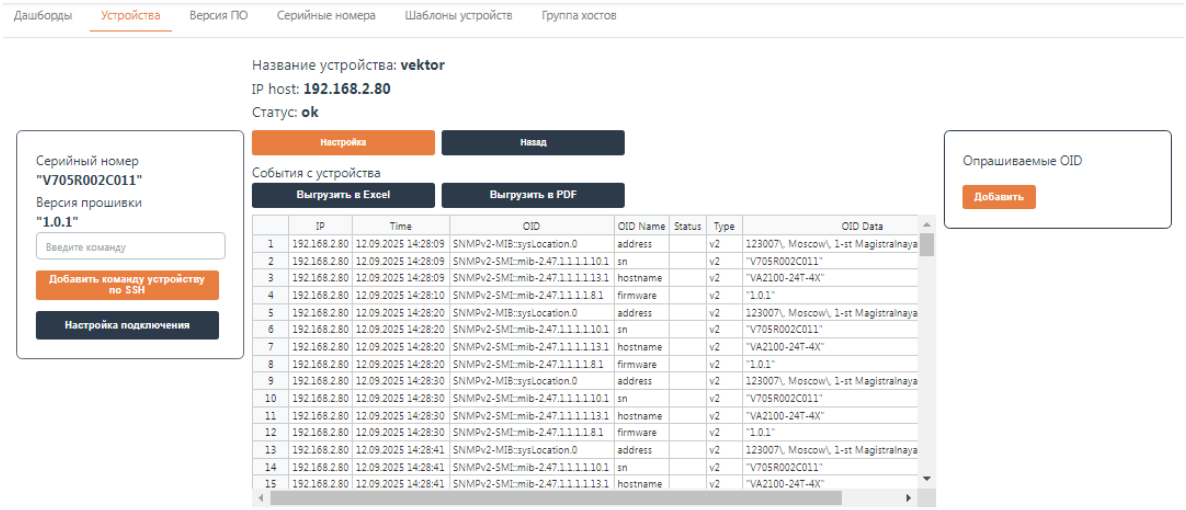
– ***Шаблон*** – список OID для опроса, который соответствует типу устройств;

– ***Действия*** – удаление устройства из системы мониторинга.

Перед добавлением нового устройства нужно создать схему. Схема – это набор устройств. Схема создается в «Режиме карты».

«Режим карты» – это визуальное схематичное представление того, как подключены устройства в сети. На карте можно разместить блок, привязанный к IP-адресу устройства, двигать его (зажав на клавиатуре клавишу «Ctrl») и протягивать связи между блоками (зажав на клавиатуре клавишу «Shift»).

По двойному щелчку мыши на блок в «Режиме карты» открывается окно с информацией об устройстве (рис. 4.3.2.2).




| | IP | Time | OID | OID Name | Status | Type | OID Data |
|---|---|---|---|---|---|---|---|
| 1 | 192.168.2.80 | 12.09.2025 14:28:09 | SNMPv2-MIB::sysLocation.0 | address | | v2 | 123007\, Moscow\, 1-st Magistralnaya |
| 2 | 192.168.2.80 | 12.09.2025 14:28:09 | SNMPv2-SMI::mib-2.47.1.1.1.1.10.1 | sn | | v2 | "V705R002C011" |
| 3 | 192.168.2.80 | 12.09.2025 14:28:09 | SNMPv2-SMI::mib-2.47.1.1.1.1.13.1 | hostname | | v2 | "VA2100-24T-4X" |
| 4 | 192.168.2.80 | 12.09.2025 14:28:10 | SNMPv2-SMI::mib-2.47.1.1.1.1.8.1 | firmware | | v2 | "1.0.1" |
| 5 | 192.168.2.80 | 12.09.2025 14:28:20 | SNMPv2-MIB::sysLocation.0 | address | | v2 | 123007\, Moscow\, 1-st Magistralnaya |
| 6 | 192.168.2.80 | 12.09.2025 14:28:20 | SNMPv2-SMI::mib-2.47.1.1.1.1.10.1 | sn | | v2 | "V705R002C011" |
| 7 | 192.168.2.80 | 12.09.2025 14:28:20 | SNMPv2-SMI::mib-2.47.1.1.1.1.13.1 | hostname | | v2 | "VA2100-24T-4X" |
| 8 | 192.168.2.80 | 12.09.2025 14:28:20 | SNMPv2-SMI::mib-2.47.1.1.1.1.8.1 | firmware | | v2 | "1.0.1" |
| 9 | 192.168.2.80 | 12.09.2025 14:28:30 | SNMPv2-MIB::sysLocation.0 | address | | v2 | 123007\, Moscow\, 1-st Magistralnaya |
| 10 | 192.168.2.80 | 12.09.2025 14:28:30 | SNMPv2-SMI::mib-2.47.1.1.1.1.10.1 | sn | | v2 | "V705R002C011" |
| 11 | 192.168.2.80 | 12.09.2025 14:28:30 | SNMPv2-SMI::mib-2.47.1.1.1.1.13.1 | hostname | | v2 | "VA2100-24T-4X" |
| 12 | 192.168.2.80 | 12.09.2025 14:28:30 | SNMPv2-SMI::mib-2.47.1.1.1.1.8.1 | firmware | | v2 | "1.0.1" |
| 13 | 192.168.2.80 | 12.09.2025 14:28:41 | SNMPv2-MIB::sysLocation.0 | address | | v2 | 123007\, Moscow\, 1-st Magistralnaya |
| 14 | 192.168.2.80 | 12.09.2025 14:28:41 | SNMPv2-SMI::mib-2.47.1.1.1.1.10.1 | sn | | v2 | "V705R002C011" |
| 15 | 192.168.2.80 | 12.09.2025 14:28:41 | SNMPv2-SMI::mib-2.47.1.1.1.1.13.1 | hostname | | v2 | "VA2100-24T-4X" |

Рисунок 4.3.2.2 – Окно с информацией об устройстве

Для добавления нового устройства на вкладке «Режим таблицы» нужно (рис. 4.3.2.3):

– выбрать ***схему***;

– выбрать ***тип устройства***;

– указать ***название устройства***;

– указать ***хост*** - IP-адрес, по которому можно обратиться к устройству в сети;

– указать ***порт*** - порт, по которому SNMP-протокол обращается к устройству (по умолчанию – «161»);

– выбрать ***шаблон*** – набор OID, которые запрашиваются по SNMP-протоколу у устройства;

– указать ***версию SNMP-протокола***, по которому обращаемся к устройству;

– ***SNMP community*** (по умолчанию – «public»);

– указать ***порт SSH*** – необязательное поле, по умолчанию – «22»;

– указать ***логин SSH*** – необязательное поле, логин для подключения;

– указать ***пароль SSH*** – необязательное поле, пароль для подключения.

Функционал кнопки «*Добавить блок*» кроме таблицы добавляет устройство также визуальным блоком на карту.

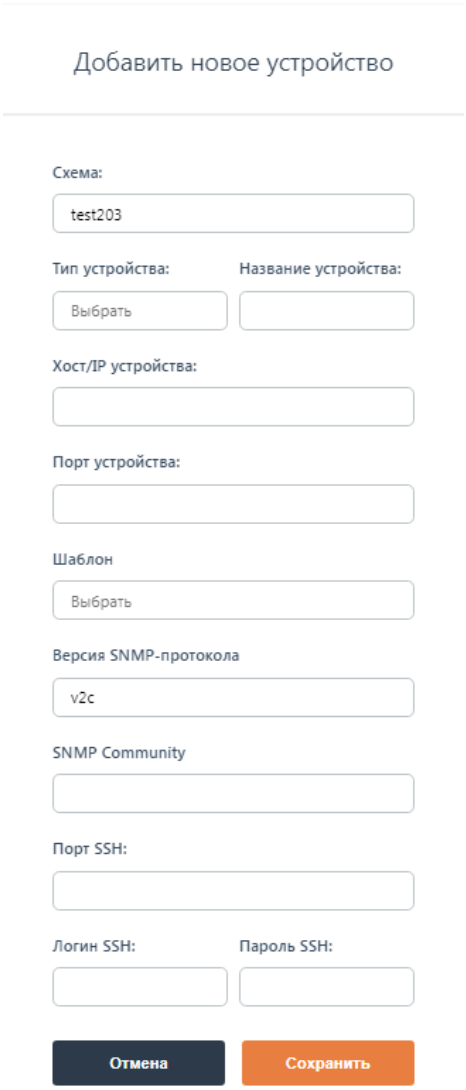



Рисунок 4.3.2.3 – Добавление нового устройства

Функционал кнопки «*Сохранить схему*» сохраняет текущие изменения на выбранной схеме.

4.3.3. Версия ПО

Модуль версий ПО отвечает за проверку версии ПО на устройстве, которое находится в мониторинге, а также обновление устройств (рис. 4.3.3.1). Для каждой отдельной модели устанавливается «актуальная» версия ПО Пользователем, после чего система управления сверяет модель и ПО и выводит информацию об актуальности ПО.

Обновление ПО производится отправкой команд на оборудование по SSH и использованием TFTP-сервера, функционал которого предусмотрен в рамках системы мониторинга.

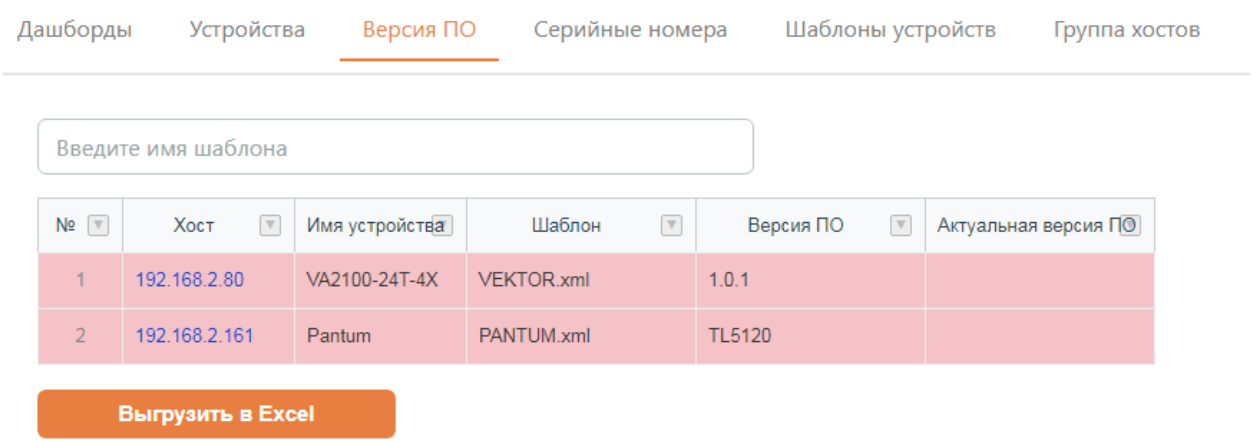



Рисунок 4.3.3.1 – Окно «Версия ПО»

Получить список версий ПО в виде файла таблицы можно, нажав на кнопку «*Выгрузить в Excel*».

4.3.4. Серийные номера

Функционал данного модуля считывает серийные номера с оборудования для учета у клиента (рис. 4.3.4.1).

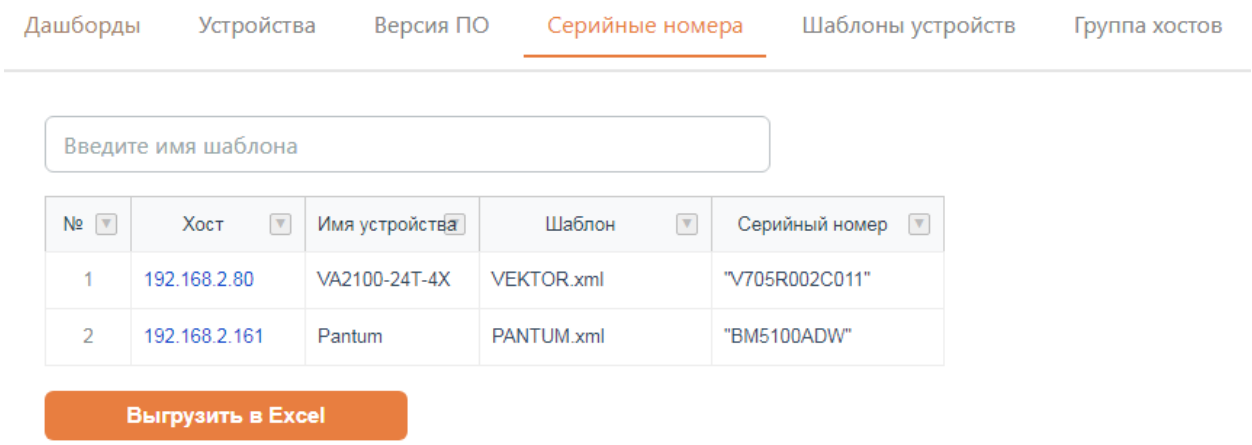



Рисунок 4.3.4.1 – Окно «Серийные номера»

В окне представлены серийные номера устройств мониторинга, в табличном виде со следующими полями:

– ***Хост*** – IP-адрес устройства;

– ***Имя устройства*** - имя устройства в системе мониторинга;

– ***Шаблон*** – список OID для опроса, который соответствует типу устройств;

– ***Серийный номер*** – серийный номер устройства.

Получить список серийных номеров устройств в виде файла таблицы можно, нажав на кнопку «*Выгрузить в Excel*».

4.3.5. Шаблоны устройств

Данный модуль позволяет создавать шаблоны устройств для мониторинга, указывать их OID и название (рис. 4.3.5.1).

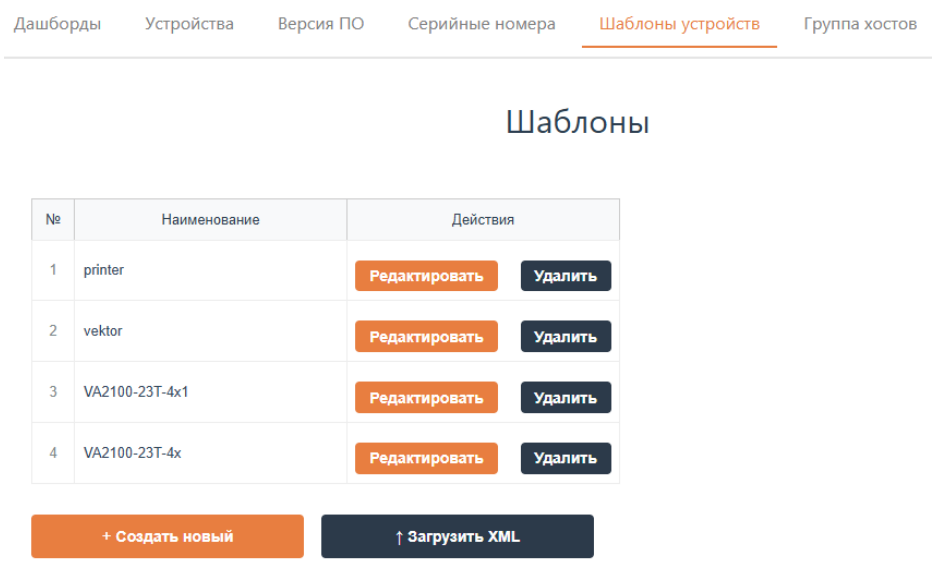



Рисунок 4.3.5.1 – Окно «Шаблоны устройств»

Для добавление нового шаблона необходимо нажать на кнопку «*Создать новый*» и заполнить следующие поля (рис. 4.3.5.2):

– ***Наименование*** – имя OID для идентификации внутри системы мониторинга (например, «firmware»);

– ***Команда*** – порядковый номер OID (например, «1.3.6.1.2.1.1.4.0»);

– ***Параметр*** – выбрать GET или WALK;

– ***Описание*** – описание OID, расшифровка наименования (например, «версия прошивки оборудования»);

– ***Тип данных*** – как правило, STRING (текстовая строка) или INT32 (числовая переменная).

Если выбран протокол SSH, можно указать интервал (в секундах), через который будут отправляться команды.

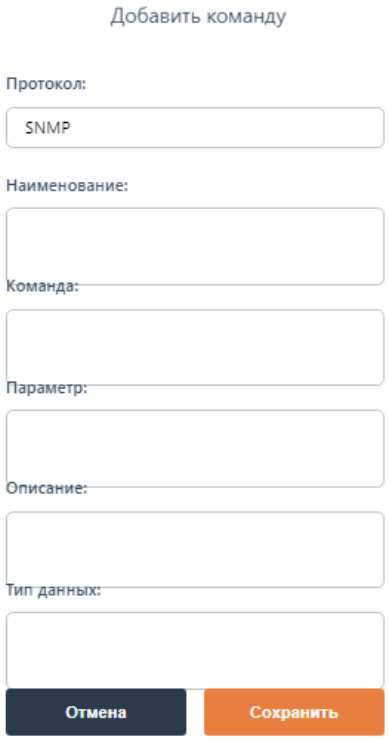



Рисунок 4.3.5.2 – Создание нового шаблона

Редактирование/удаление готового шаблона позволяет редактировать или удалить существующие OID, либо добавить новые.

4.3.6. Группа хостов

Модуль позволяет сгруппировать однотипное оборудования, назначить актуальную версию ПО для него, указать файл актуальной прошивки и назначить команду для обновления оборудования (рис. 4.3.6.1).

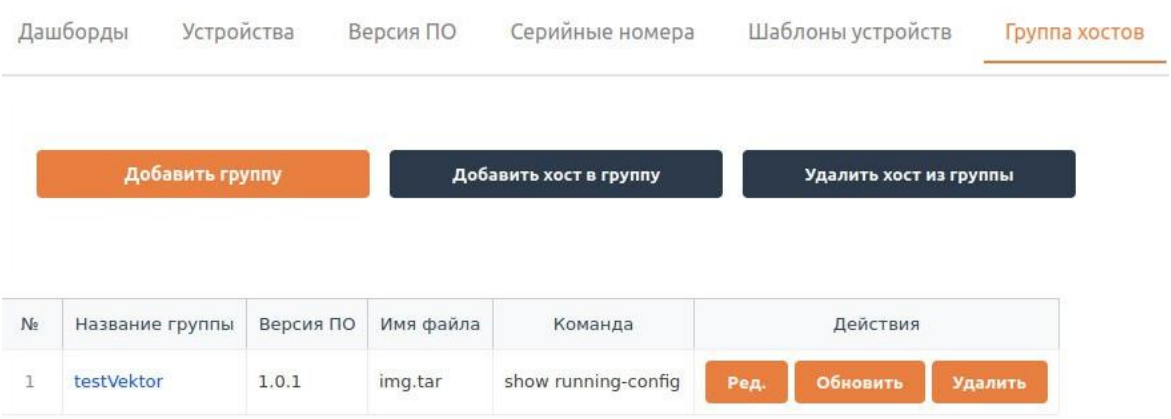



Рисунок 4.3.6.1 – Окно «Группа хостов»

Для добавления новой группы хостов необходимо нажать кнопку «*Добавить группу*» и заполнить следующие поля (рис. 4.3.6.2):

– ***Название группы*** – наименование новой группы;

– ***Версия ПО*** – отражается на вкладке «Версия ПО»;

– ***Имя файла*** – не используется;

– ***Команда*** – действие, которое будет выполняться удаленно по SSH при нажатии кнопки «*Обновить*».

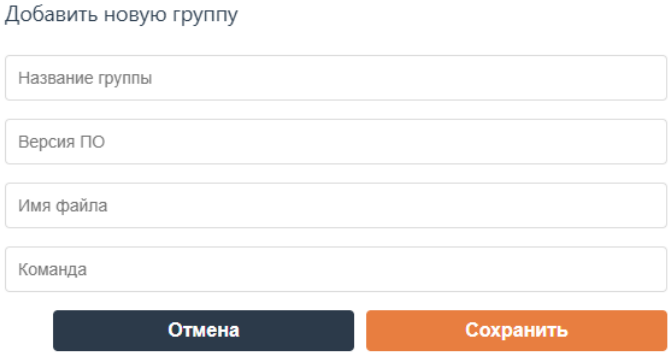



Рисунок 4.3.6.2 – Добавление новой группы хостов

Для добавления хоста в группу необходимо нажать на кнопку «*Добавить хост в группу*», выбрать из списка группу и хост, нажать кнопку «*Добавить*» (рис. 4.3.6.3).

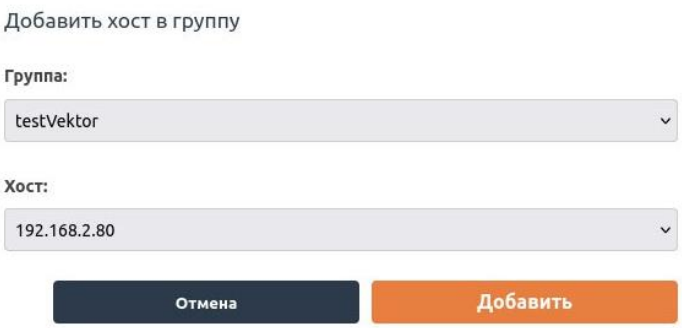



Рисунок 4.3.6.3 – Добавление хоста в группу

Для удаления хоста из группы нужно нажать на кнопку «*Удалить*» в столбце «Действие» в таблице в окне «Группа хостов» (рис. 4.3.6.4 и рис. 4.3.6.5).




Рисунок 4.3.6.4 – Удаление хоста из группы (хост не в группе)




Рисунок 4.3.6.5 – Удаление хоста из группы (хост в группе)

Редактирование группы хостов выполняется в форме, аналогичной добавлению группы (рис. 4.3.6.6).

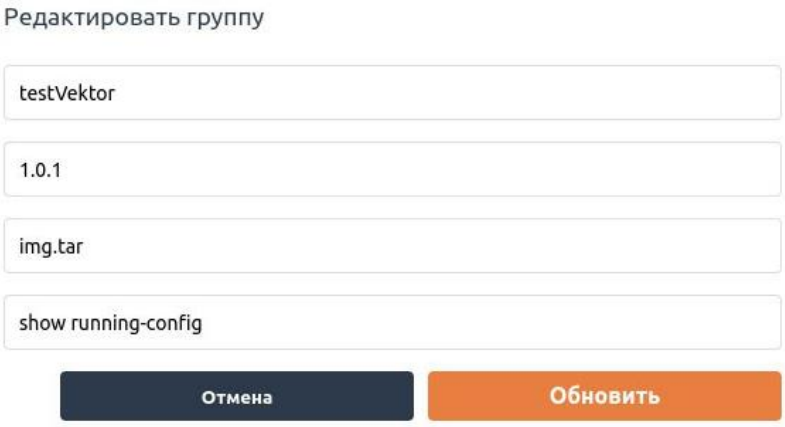



Рисунок 4.3.6.6 – Редактирование хоста

### 4.4. Логирование

При переходе на вкладку «Логирование» из основного меню открывается вкладка «Текущие логи» (рис. 4.4.1). В ней отображаются логи с удаленных устройств.

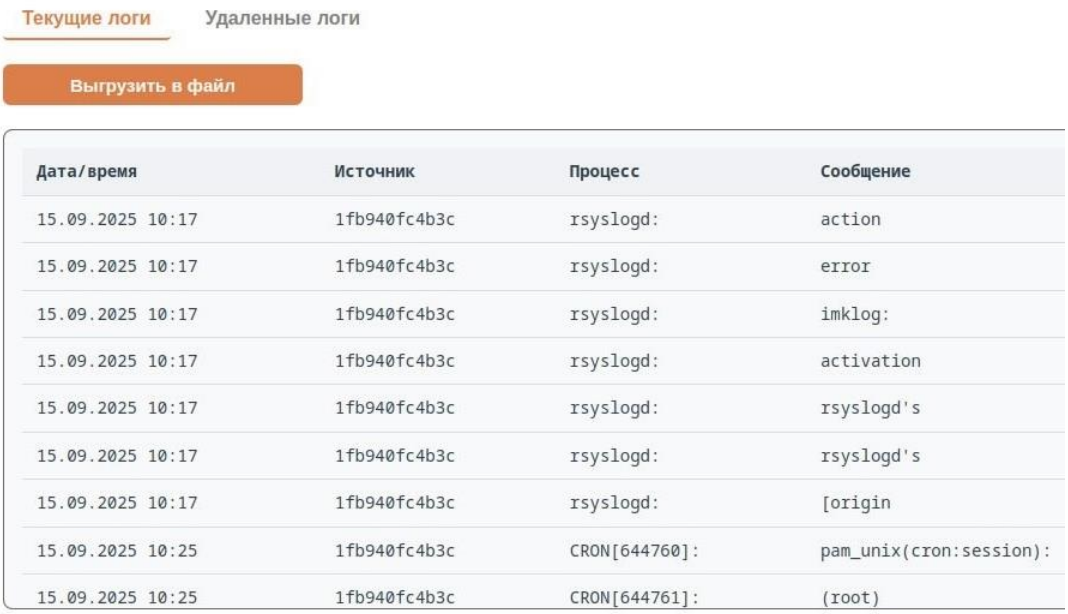



Рисунок 4.4.1 – Окно «Удаленные логи»

Вкладка «Удаленные логи» для просмотра логов на удаленных хостах (рис. 4.4.2).

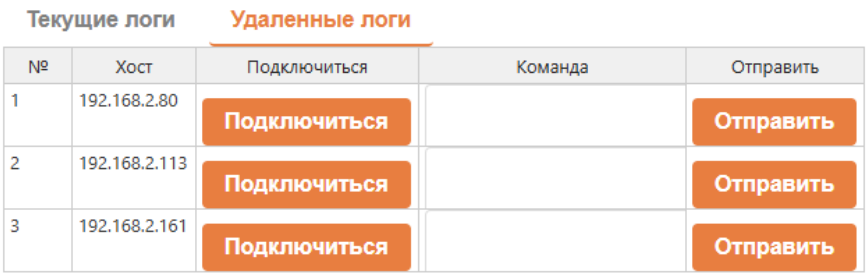



Рисунок 4.4.2 – Окно «Удаленные логи»

По нажатию на кнопку «*Подключиться*» переходим в терминал, где автоматически происходит подключение к устройству, и выполняется команда для получения логов. Данные для подключения берутся из данных, которые вводятся при создании устройства для мониторинга.

Получить список логов в виде файла можно, нажав на кнопку «*Выгрузить в файл*».

### 4.5. Радиус

С помощью RADIUS сервера добавляются новые пользователи в систему, настраивается их уровень доступа к оборудованию, а оборудование настраивается на авторизацию.

При переходе на вкладку «Радиус» из основного меню открывается окно «Управление RADIUS сервером» (рис. 4.5.1).

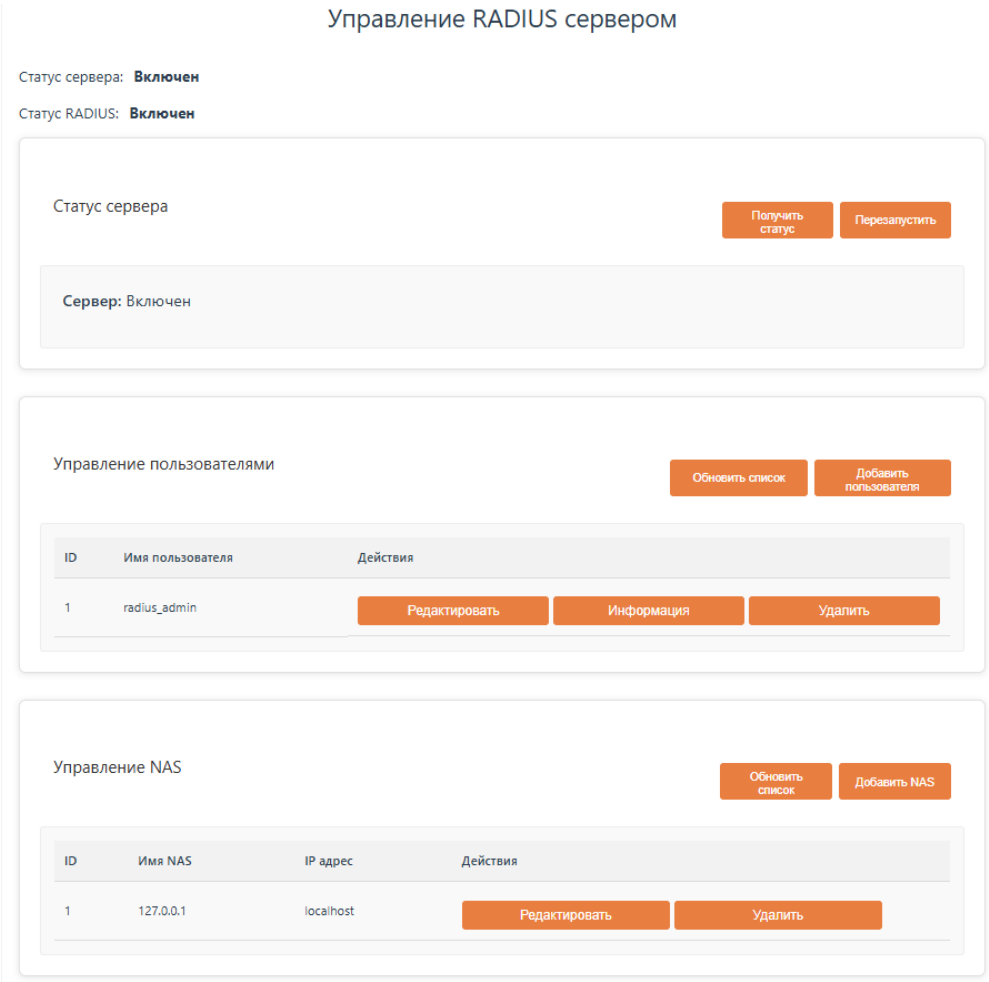



Рисунок 4.5.1 – Окно «Управление RADIUS сервером»

Вкладка «Радиус» имеет следующий функционал:

– для получения текущего статуса работы RADIUS сервера, нажмите кнопку «*Получить статус*» (рис. 4.5.2);

– для перезапуска RADIUS сервера нажмите кнопку «*Перезапустить*» (рис. 4.5.2);

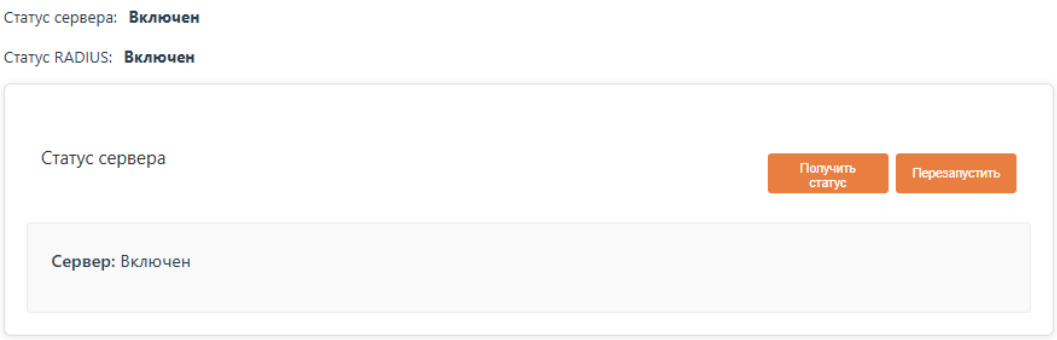



Рисунок 4.5.2 – Статус сервера

– для добавления нового пользователя, нажмите кнопку «*Добавить пользователя*» (рис. 4.5.3);

– чтобы редактировать информацию о пользователе нажмите кнопку «*Редактировать*» (рис. 4.5.3);

– для просмотра информации о пользователе нажмите кнопку «*Информация*» (рис. 4.5.3);

– чтобы удалить пользователя нажмите кнопку «*Удалить*» (рис. 4.5.3);

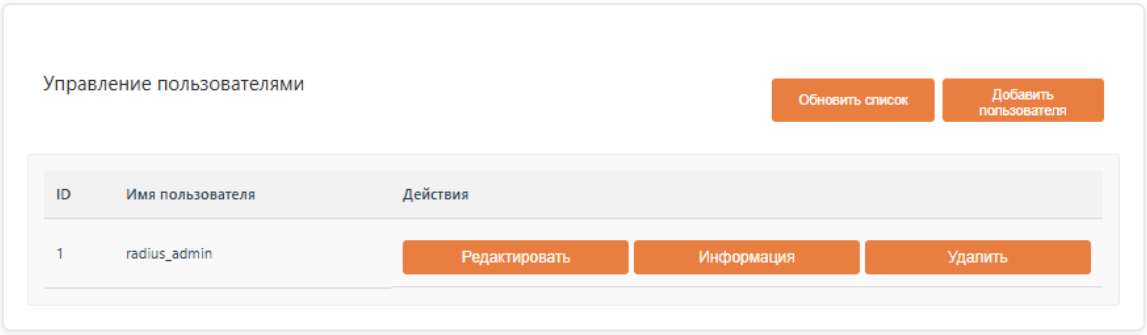



Рисунок 4.5.3 – Управление пользователями

Для добавления нового пользователя необходимо нажать на кнопку «*Добавить пользователя*». В появившемся окне заполнить поля «Имя пользователя» и «Пароль» и нажать кнопку «*Сохранить*» (рис. 4.5.4).

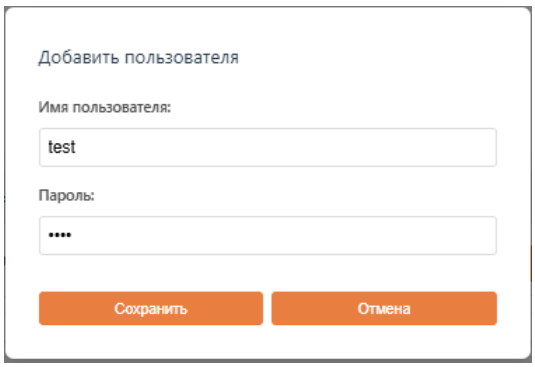



Рисунок 4.5.4 – Добавление нового пользователя

При успешном добавлении пользователя в системе, информация о нем появится в таблице (рис. 4.5.5).

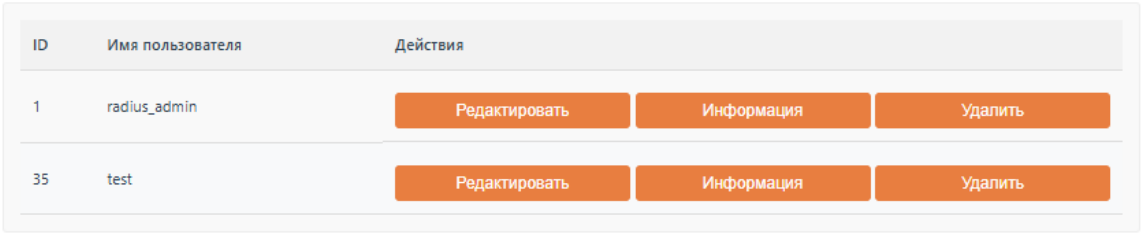



Рисунок 4.5.5 – Таблица пользователей

Для того, чтобы отредактировать пароль пользователя, необходимо нажать на кнопку «*Редактировать*», заполнить поле «Пароль» и нажать кнопку «*Сохранить*» (рис. 4.5.6).

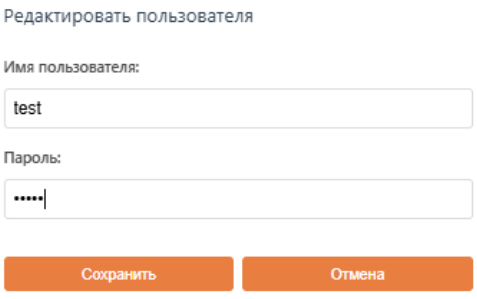



Рисунок 4.5.6 – Редактирование пользователя

Для удаления пользователей нужно нажать на кнопку «*Удалить*» в таблице пользователей, в строке с выбранным пользователем, после этого в браузере во всплывающем окне подтвердить действие, нажав кнопку «*Ок*» (рис. 4.5.7).

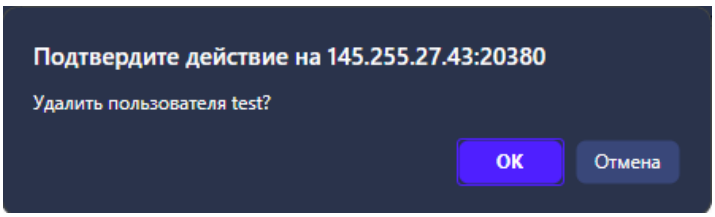



Рисунок 4.5.7 – Подтверждение удаления пользователя

NAS (Network Access Server) — это сервер или устройство, которое управляет доступом пользователей к сети. Он выступает в роли клиента RADIUS, запрашивая аутентификацию у FreeRADIUS (рис. 4.5.8).

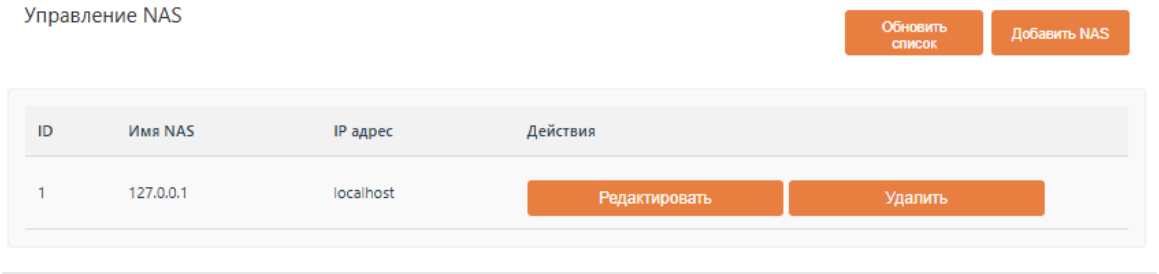



Рисунок 4.5.8 – Управление NAS-сервером

Примеры NAS:

– Wi-Fi роутеры (например, MikroTik, Ubiquiti, Cisco);
– VPN-серверы (OpenVPN, PPTP, L2TP/IPsec);
– Серверы доступа (DSL-концентраторы, коммутаторы).

### 4.6. Модуль событий

В данном модуле выводятся сообщения, полученные от оборудования по SNMP-протоколу, и отчеты по работе системы мониторинга (рис. 4.6.1).




Рисунок 4.6.1 – Окно «Модуль событий»

## 4.7. Почта

Модуль почты необходим для отправки отчетов и сообщений о работе системы мониторинга и состоит из следующих пунктов (рис. 4.7.1):

– Модуль Почты;
– Модуль Рассылки;
– Статистика Почты;
– Настройка Команд;
– Настройка Отчетов;
– Телеграм.

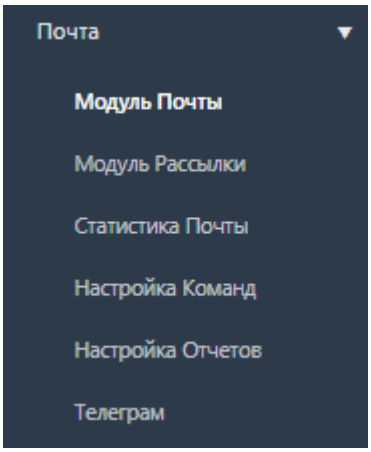



Рисунок 4.7.1 – Подменю вкладки «Почта»

### 4.7.1. Модуль Почты

При переходе на вкладку «Модуль Почты» из подменю открывается окно «Настройка почты» (рис. 4.7.1.1).

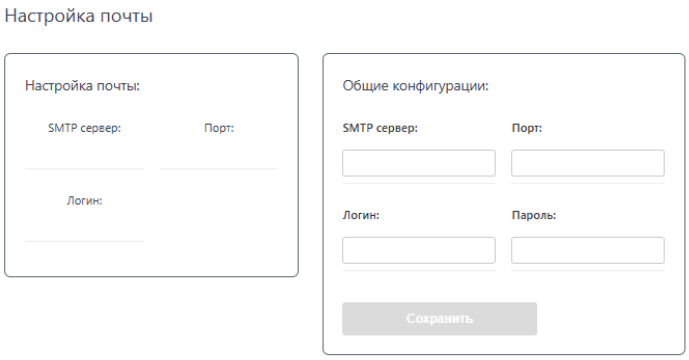



Рисунок 4.7.1.1 – Окно «Настройка почты»

В данном окне настраивается почта отправителя отчетов, прописываются следующие поля:

– SMTP-сервер;

– порт SMTP-сервера;

– логин и пароль для SMTP-сервера.

При нажатии на кнопку «*Сохранить*» данные записываются в систему.

4.7.2. Модуль Рассылки

При переходе на вкладку «Модуль Рассылки» из подменю открывается окно «Управление списком рассылки» (рис. 4.7.2.1).

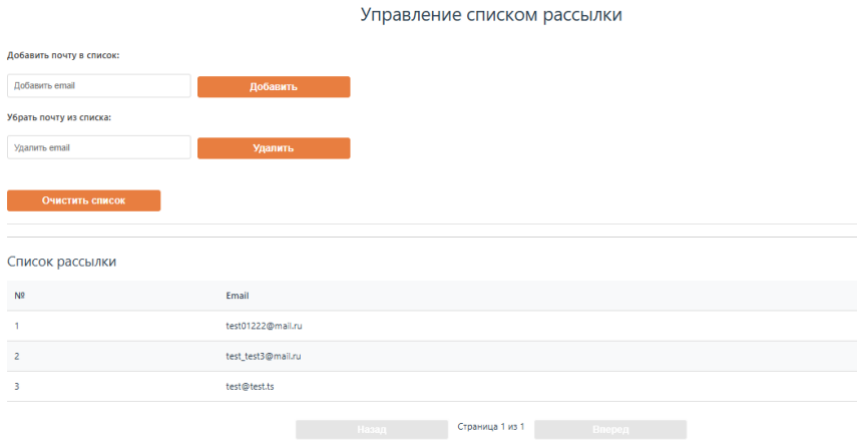



Рисунок 4.7.2.1 – Окно «Управление списком рассылки»

Функционал данного окна позволяет добавить электронную почту в список рассылки, либо удалить почту из списка. Список рассылки – список электронных почт, куда массово отправляются отчеты.

Для добавления электронного адреса пропишите его в поле «Добавить e-mail» и нажмите кнопку «*Добавить*».

Для удаления почты из списка, аналогично, заполните поле «Удалить e-mail» и нажмите кнопку «*Удалить*».

4.7.3. Статистика Почты

При переходе на вкладку «Статистика Почты» из подменю открывается окно «История отправленных писем» (рис. 4.7.3.1).

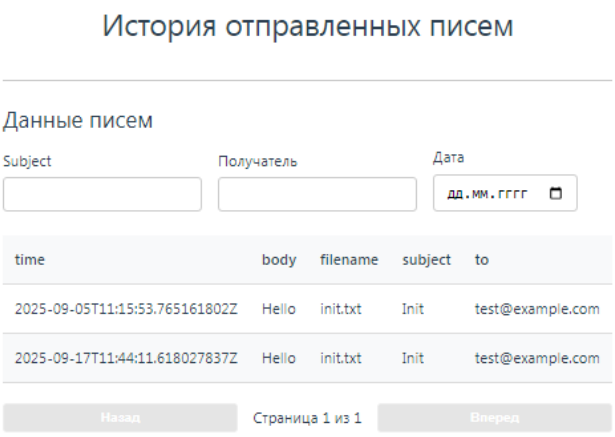



Рисунок 4.7.3.1 – Окно «История отправленных писем»

В данном окне содержится информация о том, какие отчеты были высланы, с указанием времени, файла отправки и получателя.

Есть возможность отфильтровать таблицу по объекту, получателю и дате отправки письма.

4.7.4. Настройка Команд

При переходе на вкладку «Настройка Команд» из подменю открывается окно «Настройка команд» (рис. 4.7.4.1).

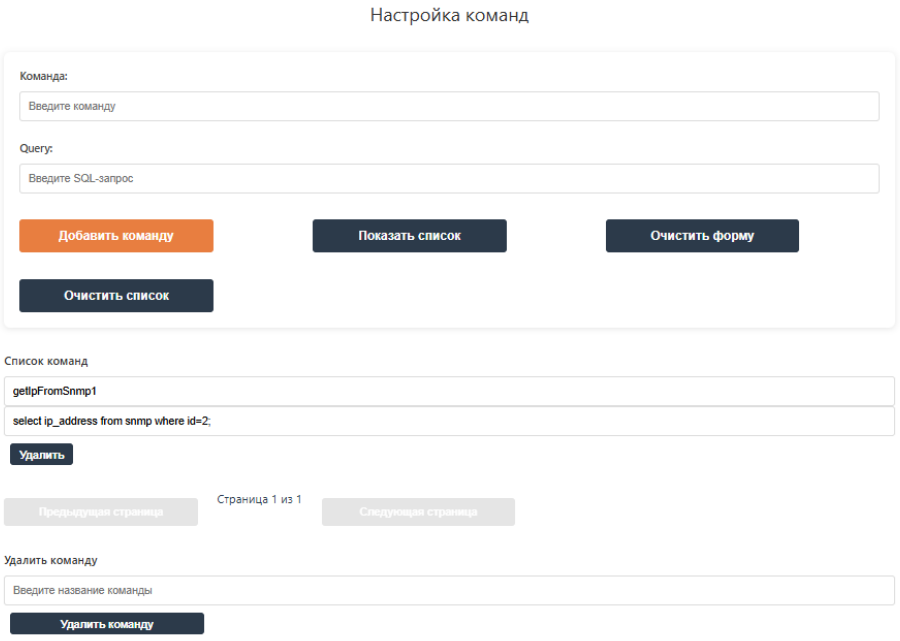



Рисунок 4.7.4.1 – Окно «Настройка команд»

Функционал позволяет настроить команду, которая будет выполняться каждый раз при отправке отчета.

4.7.5. Настройка Отчетов

При переходе на вкладку «Настройка Отчетов» из подменю открывается окно «Настройка отчетов» (рис. 4.7.5.1).

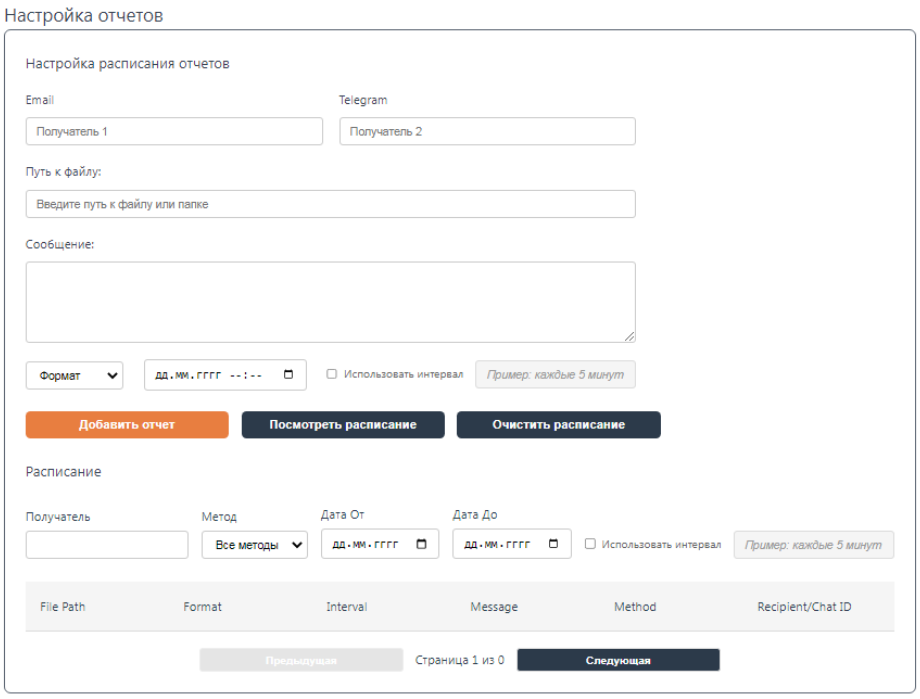



Рисунок 4.7.5.1 – Окно «Настройка отчетов»

В данном окне можно:

– настроить данные получателя (почта, Телеграм или и то, и другое) (рис. 4.7.5.2);

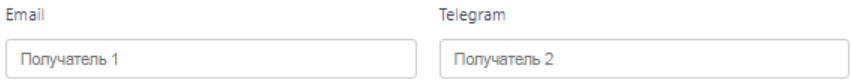



Рисунок 4.7.5.2 – Данные получателя

– выбрать точную дату отправки отчета, либо промежуток периодичности отправки (например, «Каждые 5 минут») (рис. 4.7.5.3);

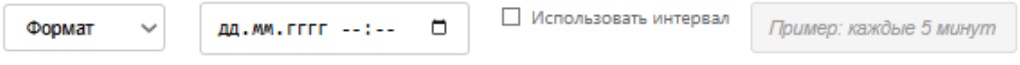



Рисунок 4.7.5.3 – Периодичность отправки отчетов

– выбрать тип файла и указать ссылку на файл на сервере (рис. 4.7.5.4);




Рисунок 4.7.5.4 – Файл для отправки

– ввести текст письма, который будет отправляться вместе с отчетом (рис. 4.7.5.5);

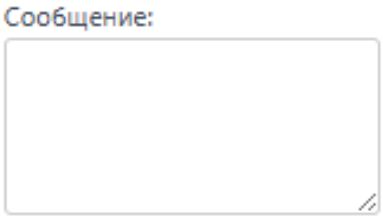



Рисунок 4.7.5.5 – Текст письма для отправки

– также можно настроить расписание, в котором указать получателя, период и интервал отправки отчета (рис. 4.7.5.6).

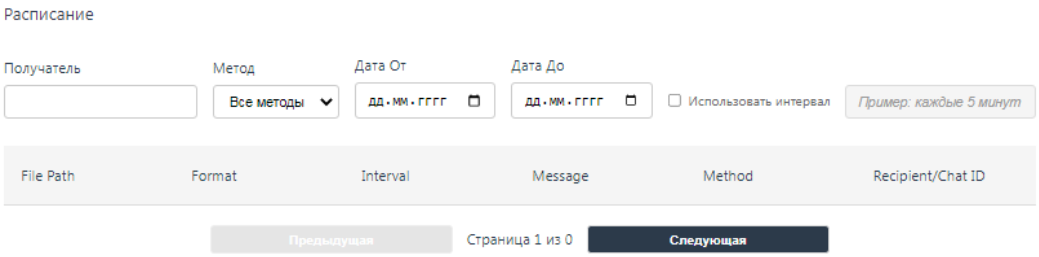



Рисунок 4.7.5.6 – Настройка интервалов отправки

4.7.6. Телеграм

При переходе на вкладку «Телеграм» из подменю открывается окно «Настройка Telegram бота» (рис. 4.7.6.1).

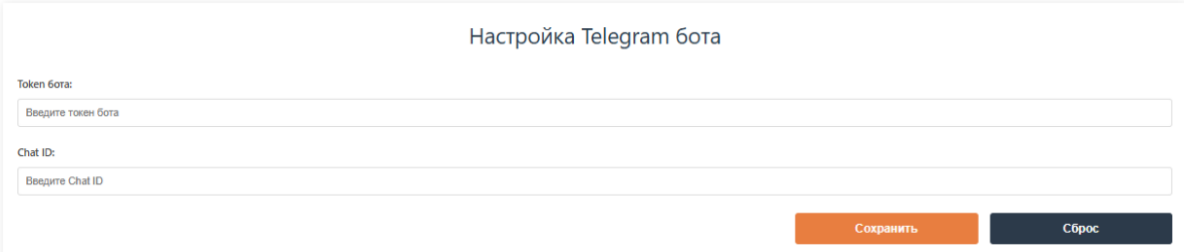



Рисунок 4.7.6.1 – Окно «Настройка Telegram бота»

Данный функционал позволяет указать токен бота, который будет слать отчет, а также id чата или диалога с пользователем, куда будет присылаться отчет.

### 4.8. Администрирование

Модуль администрирования сервера представляет из себя модуль, с помощью которого Пользователь изменяет параметры функционирования ПО, такие как:

– профили данных для использования с оборудованием: логины, пароли, community для SNMP;

– данные по авторизации пользователей ПО: создание, модификация и удаление Пользователей ПО, используя пару логин/пароль, хранящиеся локально на ПО.

При нажатии на вкладку «Администрирование» из основного меню открывается подменю (рис. 4.8.1):

– Настройка Логирования;

– Модуль Конфигурационных Файлов;

– Сохранить / Загрузить БД;

– TFTP;

– NTP;

– Модуль Хранения.

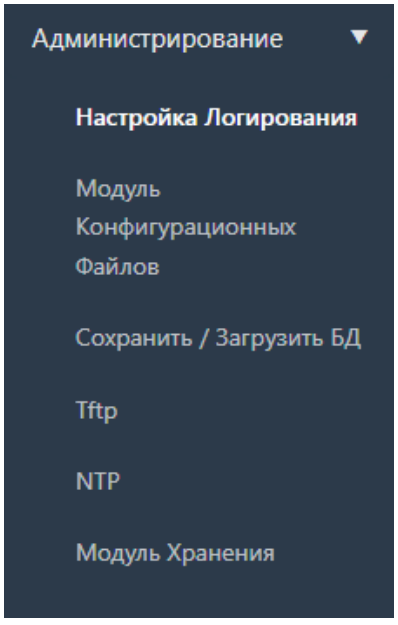



Рисунок 4.8.1 – Подменю вкладки «Администрирование»

4.8.1. Настройка Логирования

В системе мониторинга развернут Syslog-сервер для сбора логов.

В настройках пользователь должен указать (рис. 4.8.1.1):

– ***порты***, которые открываются для приема пакетов с логами;

– ***уровень логов***, которые будет принимать сервер (остальные логи будут удаляться);

– ***размер файла с логами***.

Файл с логами пишется циклически: более старые логи заменяются новыми.

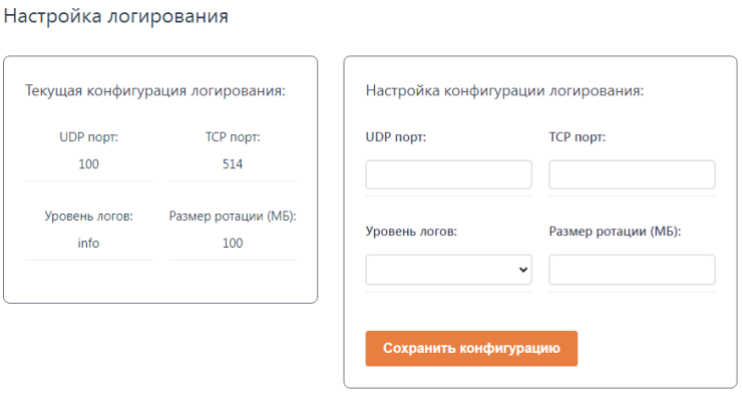



Рисунок 4.8.1.1 – Окно «Настройка логирования»

4.8.2. Модуль Конфигурационных Файлов

Данный модуль предназначен для загрузки и сохранения конфигурационных файлов проекта мониторинга (рис. 4.8.2.1).

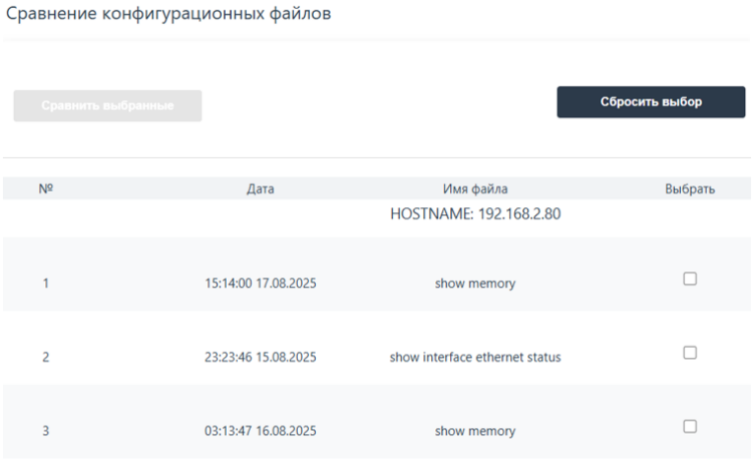



Рисунок 4.8.2.1 – Окно «Сравнение конфигурационных файлов»

Для сравнения конфигурационных файлов выберите 2 из них, нажав галочки в соответствующих строках таблицы, и нажмите кнопку «*Сравнить выбранные*» (рис. 4.8.2.2).

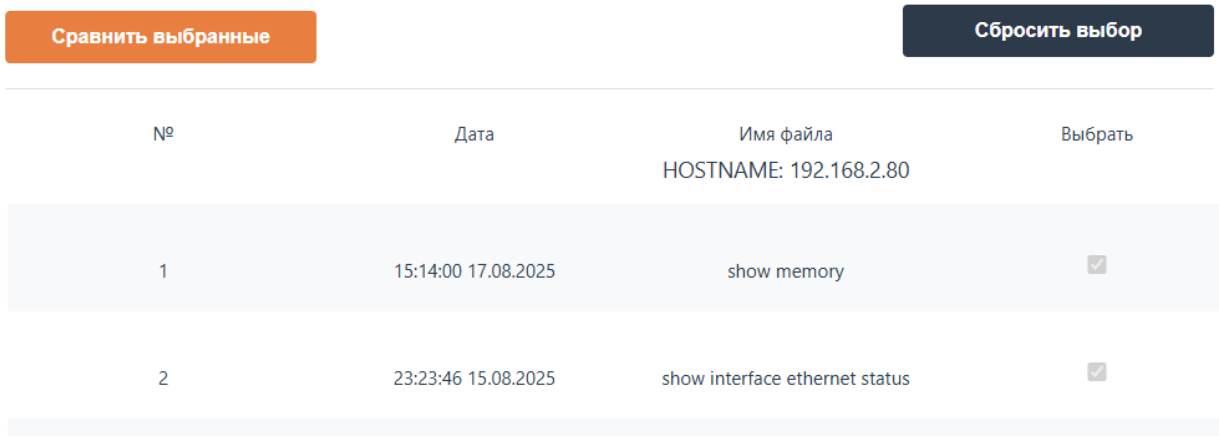



Рисунок 4.8.2.2 – Сравнение файлов

После выполнения команды в следующем окне сравниваются тексты двух выбранных файлов конфигурации (рис. 4.8.2.3).

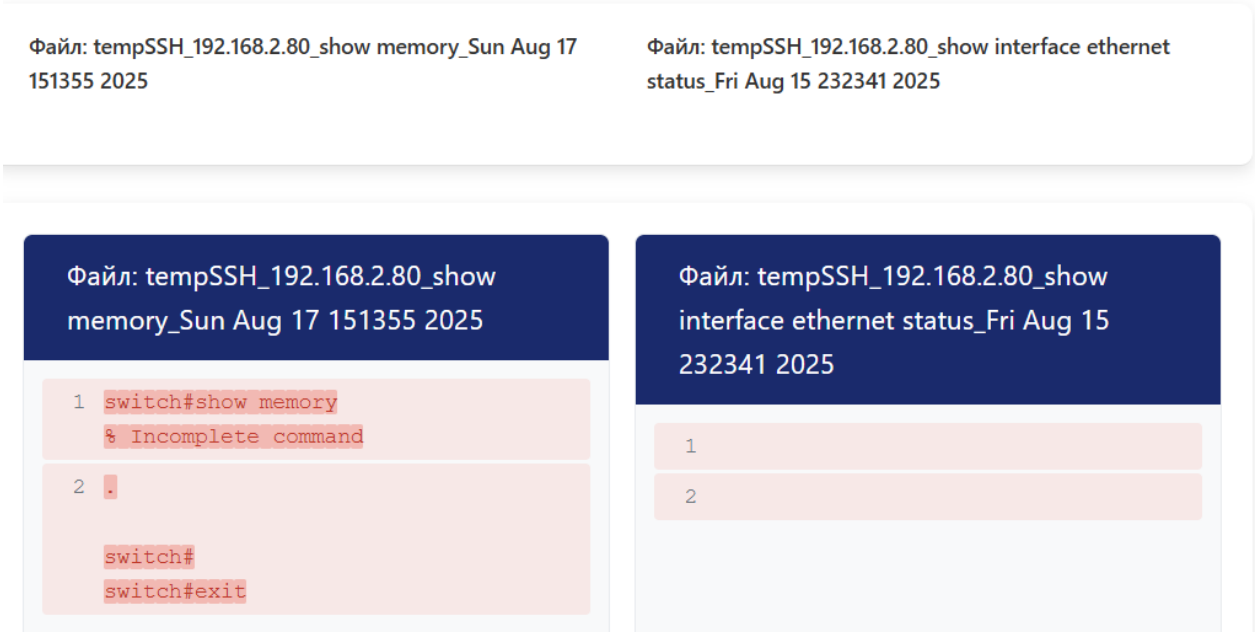



Рисунок 4.8.2.3 – Окно сравнения

В столбце «Действия» доступен функционал скачать файл конфигурации, либо удалить его (рис. 4.8.2.4).

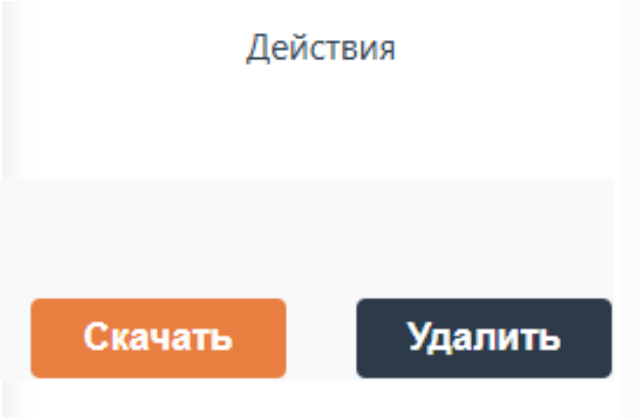



Рисунок 4.8.2.4 – Действия с файлом конфигурации

4.8.3. Сохранить / Загрузить БД

Функционал данной вкладки позволяет сохранить проект в текстовый файл, а также загрузить проект из файла (рис. 4.8.3.1).

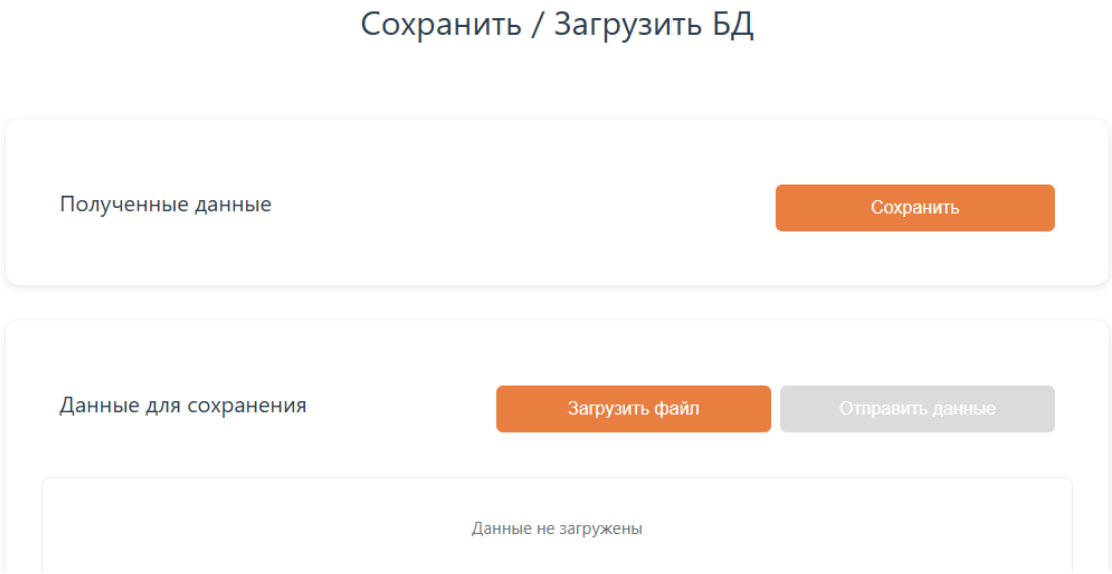



Рисунок 4.8.3.1 – Окно «Сохранить / Загрузить БД»

4.8.4. TFTP

TFTP-сервер развернут на сервере мониторинга. На данный сервер можно загружать файлы, а также использовать для обновления.

Пользователь имеет следующие возможности работы с TFTP-сервером:

– настройка имени пользователя, рабочей директории, порта и дополнительных опций (рис. 4.8.4.1);

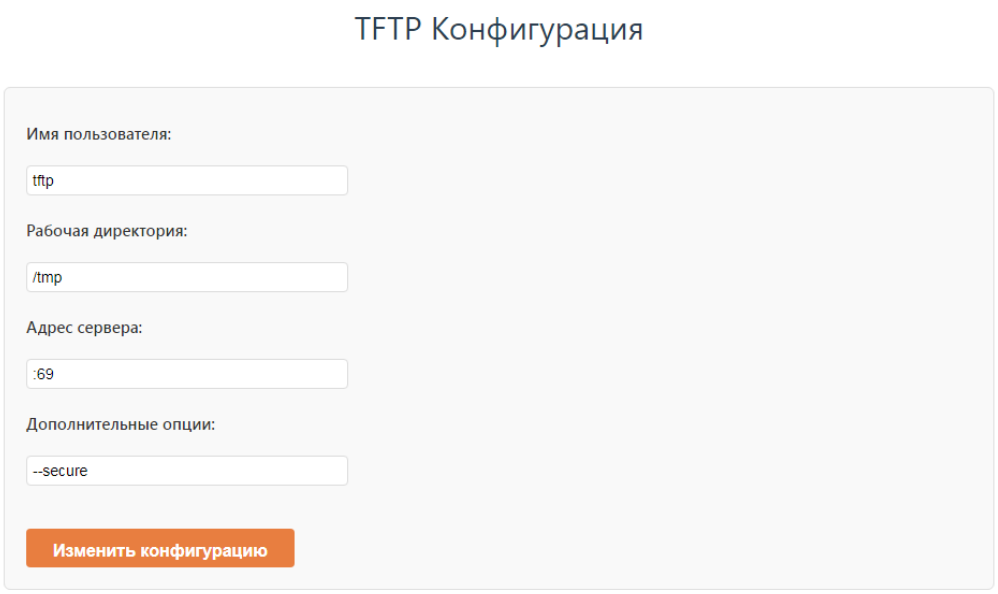



Рисунок 4.8.4.1 – Конфигурация TFTP-сервера

– просмотр текущей конфигурации сервера (рис. 4.8.4.2);

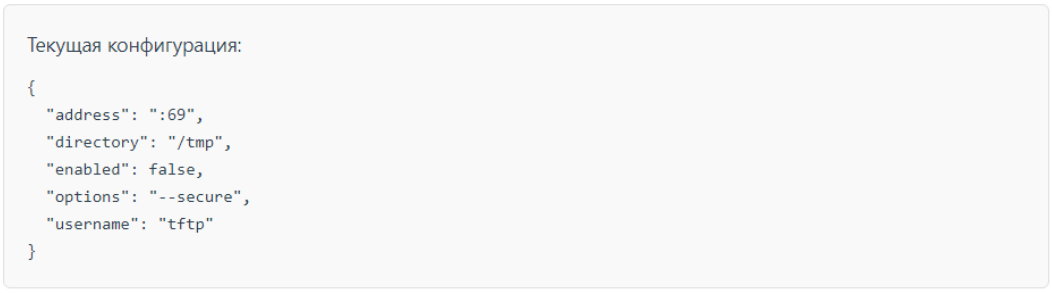



Рисунок 4.8.4.2 – Текущая конфигурация TFTP-сервера

– просмотр текущих файлов на TFTP-сервере (рис. 4.8.4.3);

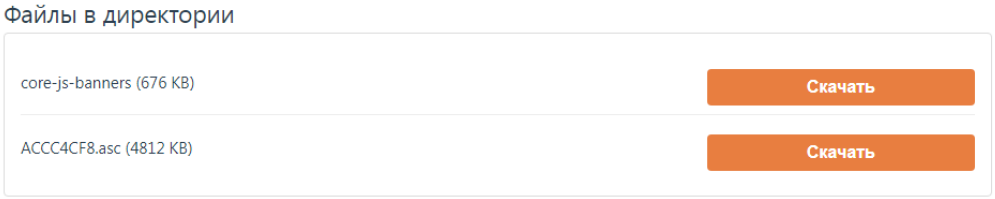



Рисунок 4.8.4.3 – Текущие файлы на TFTP-сервере

– загрузка файла на TFTP-сервер (рис. 4.8.4.4);

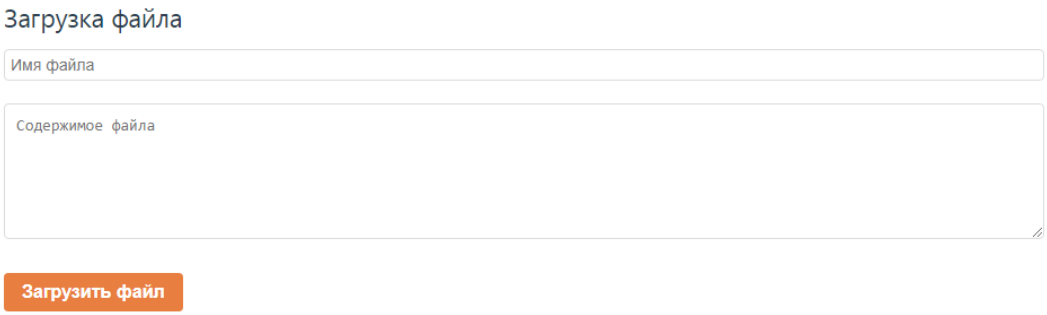



Рисунок 4.8.4.4 – Загрузка файла на TFTP-сервер

– удаление файла с TFTP-сервера (рис. 4.8.4.5).

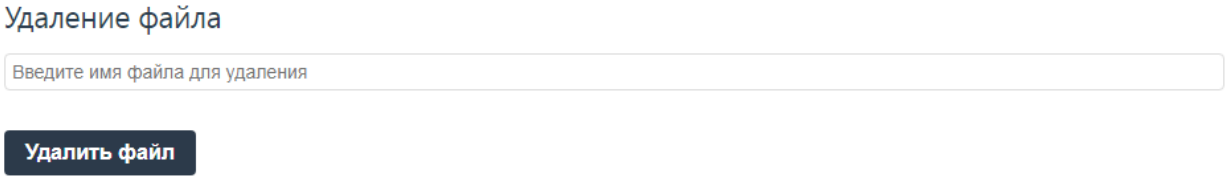



Рисунок 4.8.4.5 – Удаление файла с TFTP-сервера

4.8.5. NTP

NTP-сервер используется для раздачи времени в локальной сети (рис. 4.8.5.1).

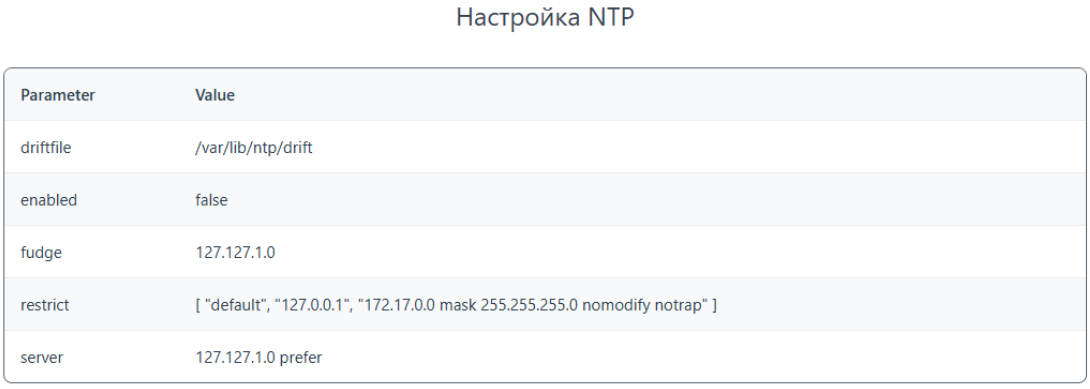



Рисунок 4.8.5.1 – Окно «Настройка NTP»

4.8.6. Модуль Хранения

Модуль имеет возможность задавать интервалы хранения данных, чтобы не допускать разрастания базы данных мониторинга. Каждый интервал сжимает данные в 2 раза. При накоплении данных для сжатия предыдущая таблица очищается, и накопление данных начинается заново.

Например, при установленном интервале – 1 день, данные накапливаются в течение 1 дня, после этого перемещаются в созданную таблицу. Предыдущая таблица при этом очищается, и в нее начинают копиться новые данные. Данные же хранятся в сжатом виде.

Существует возможность настроить неограниченное количество интервалов хранения: например, 1 день, 1 неделя, 1 месяц, 1 год (рис. 4.8.6.1).

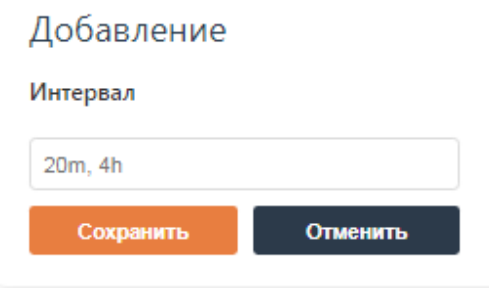



Рисунок 4.8.6.1 – Создание интервалов хранения

## 4.9. Пользователи

При переходе на вкладку «Пользователи» из основного меню открывается окно «Пользователи» (рис. 4.9.1).

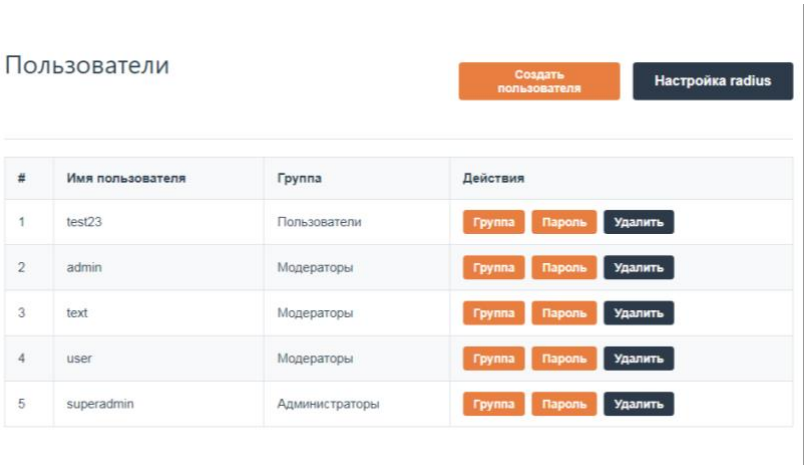



Рисунок 4.9.1 – Окно «Пользователи»

При нажатии на кнопку «*Создать пользователя*» открывается форма для добавления нового пользователя (рис. 4.9.2).

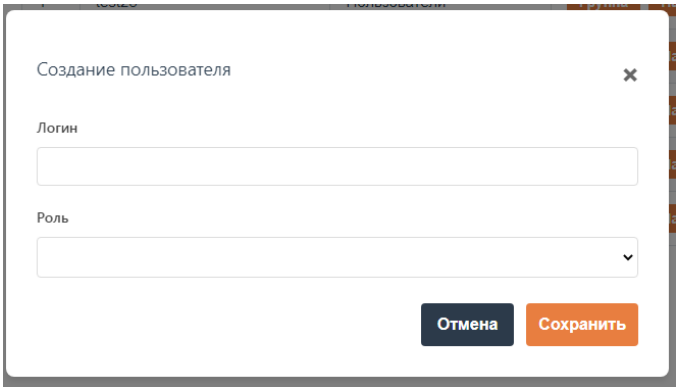



Рисунок 4.9.2 – Форма «Создать пользователя»

Требования для паролей:

– длина пароля – 8 символов;
– наличие одной заглавной буквы;
– наличие одной цифры;
– для пользователя пароль всегда совпадает с логином.

При нажатии на кнопку «*Настройка radius*» открывается окно «Настройка RADIUS» (рис. 4.9.3).

В данном окне можно настроить RADIUS сервер. Через RADIUS можно авторизовываться в ПО для администрирования устройств, а также добавлять новых пользователей.

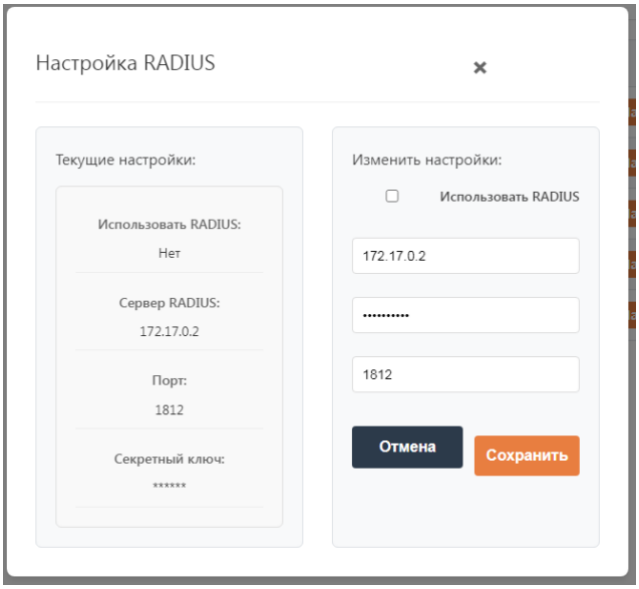



Рисунок 4.9.3 – Окно «Настройка RADIUS»

## 4.10. Терминал

При переходе на вкладку «Терминал» из основного меню открывается окно «Terminal Interface» (рис. 4.10.1).

Функционал данной вкладки позволяет подключиться к устройству по протоколу SSH, для выполнения команд на удаленном оборудовании.




Рисунок 4.10.1 – Окно «Terminal Interface»

Для подключения к устройству необходимо заполнить данные (например, как на рис. 4.10.2):

– SSH Host;
– SSH User;
– SSH Password;
– SSH Port.

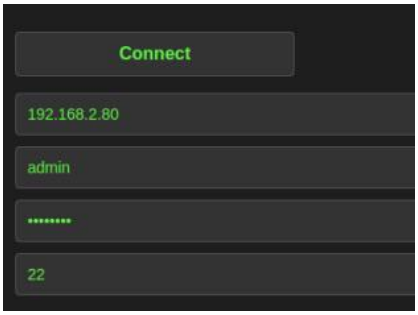



Рисунок 4.10.2 – Данные для подключения к устройству

После нажатия на кнопку «*Подключиться*» в терминале отобразятся сообщения о подключении к устройству.

При успешном подключении в терминале появится сообщение об успешном подключении (рис. 4.10.3).

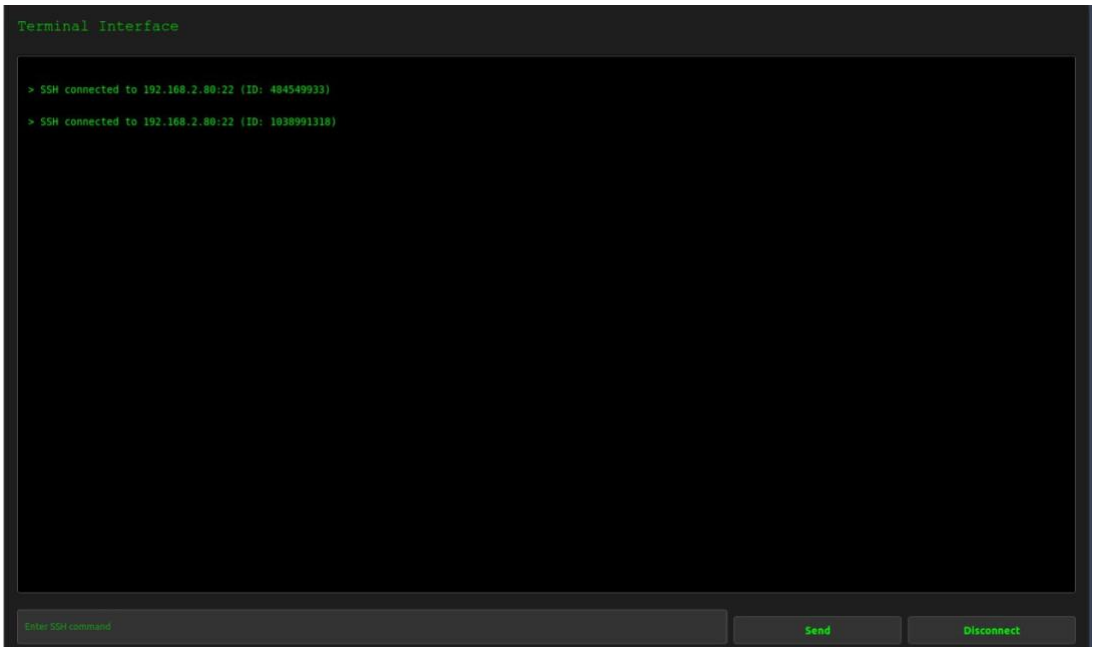



Рисунок 4.10.3 – Успешное подключение к устройству

При ошибке подключения в терминале отобразится сообщение об ошибке (рис. 4.10.4).

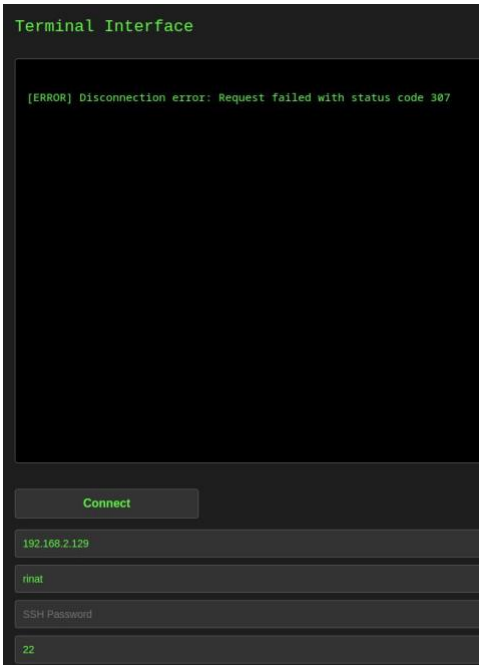



Рисунок 4.10.4 – Ошибка подключения к устройству

После успешного подключения можно взаимодействовать с устройством, отправляя на него команды (рис. 4.10.5). Список доступных команд находятся в Руководстве пользователя для устройств.




Рисунок 4.10.5 – Пример отправки команд на устройство

Ответ на выполнение команды выводится в терминал (рис. 4.10.6).

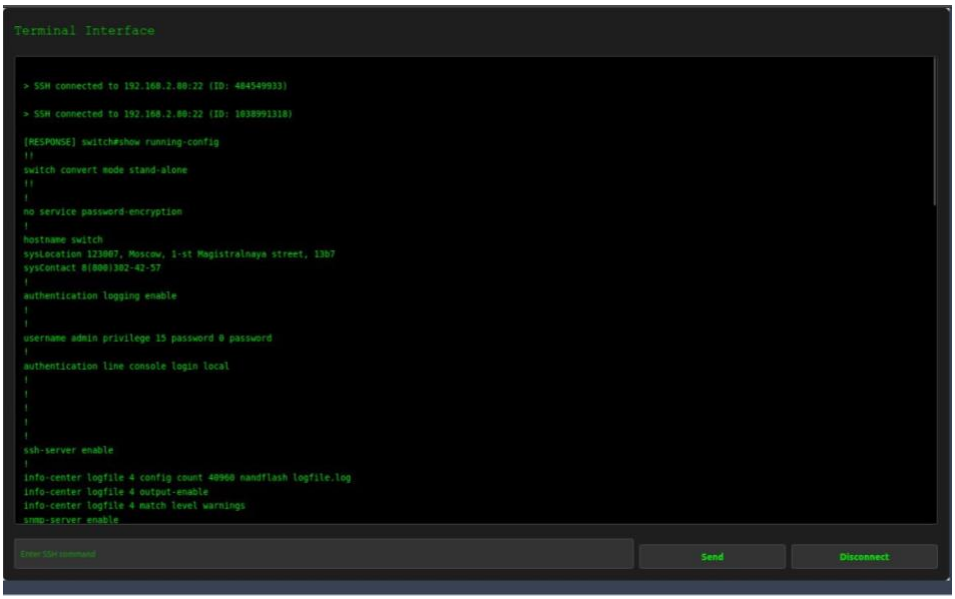



Рисунок 4.10.6 – Ответ на выполнение команды

Чтобы отключиться от устройства нажмите кнопку «*Отключиться*» (рис. 4.10.7).

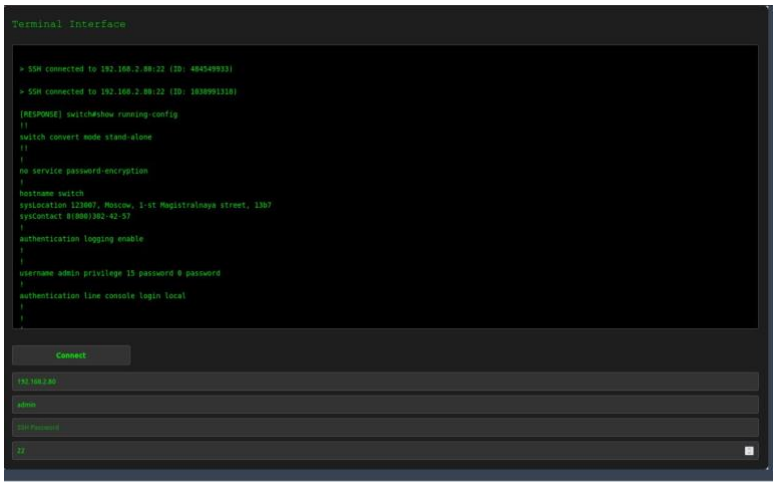



Рисунок 4.10.7 – Отключение от устройства

При отправке команд на устройство могут возникать и другие ошибки, они отображаются в терминале (рис. 4.10.8).




Рисунок 4.10.8 – Ошибки при выполнении команд

Ошибки делятся на два типа:

– ошибки соединения (таблица 1);

– ошибки при выполнении удаленных команд.

Таблица 1. Ошибки соединения

| Тип ошибки | Описание ошибки | Причины | Способ устранения |
|---|---|---|---|
| Ошибки подключения | Connection refused (Соединение отклонено) | SSH-сервер не запущен или заблокирован брандмауэром | Проверьте статус SSH-сервера, убедитесь, что он запущен, и настройте брандмауэр для разрешения SSH-соединений |
| | Connection timed out (Время ожидания истекло) | Сервер недоступен или сетевые настройки неверны | Проверьте доступность сервера, убедитесь в правильности сетевых настроек и попробуйте подключиться снова |
| | Network is unreachable | Проблемы с сетью или | Проверьте сетевые настройки и |

| | | | |
|---|---|---|---|
| | (Сеть недоступна) | неправильные сетевые настройки | убедитесь, что сеть работает правильно |
| Ошибки аутентификации | Authentication failed (Аутентификация не удалась) | Неправильный пароль или отсутствие необходимых прав доступа | Проверьте правильность пароля, убедитесь, что у вас есть права доступа к серверу |
| | Permission denied (publickey) (Доступ запрещен (публичный ключ)) | Ключ SSH не настроен или неверно настроен | Проверьте настройки ключей SSH, убедитесь, что публичный ключ добавлен на сервер и корректно настроен |
| | Key exchange failed (Сбой обмена ключами) | Проблемы с обменом ключами между клиентом и сервером | Проверьте настройки SSH-сервера и клиента, убедитесь, что они поддерживают один и тот же алгоритм обмена ключами |
| Ошибки ключей | Host key verification failed (Сбой проверки ключа хоста) | Изменился ключ хоста, или он не совпадает с сохраненным в базе | Удалите старый ключ хоста из known_hosts и подтвердите новый ключ |
| | No such identity (Такой ключ не найден) | Неправильно указан путь к ключу или ключ отсутствует | Укажите правильный путь к ключу или добавьте ключ в SSH-агент |
| Другие ошибки | Resource temporarily unavailable (Ресурс временно недоступен) | Сервер перегружен, не хватает ресурсов для обработки подключения | Подождите некоторое время и повторите попытку, обратитесь к администратору сервера |

| | | | |
|---|---|---|---|
| | Invalid user (Недопустимый пользователь) | Имя пользователя, указанное при подключении, не существует на сервере | Укажите правильное имя пользователя |

В случае возникновения ошибок при выполнении удаленных команд обратитесь к руководству пользователя на устройство, к которому подключаетесь.

## 4.11. Лицензия

Модуль лицензирования обеспечивает контроль за количеством управляемых устройств. Лицензия передается в виде уникального лицензионного ключа на определенное количество устройств.

При переходе на вкладку «Лицензия» из основного меню открывается окно «Управление лицензиями» (рис. 4.11.1).

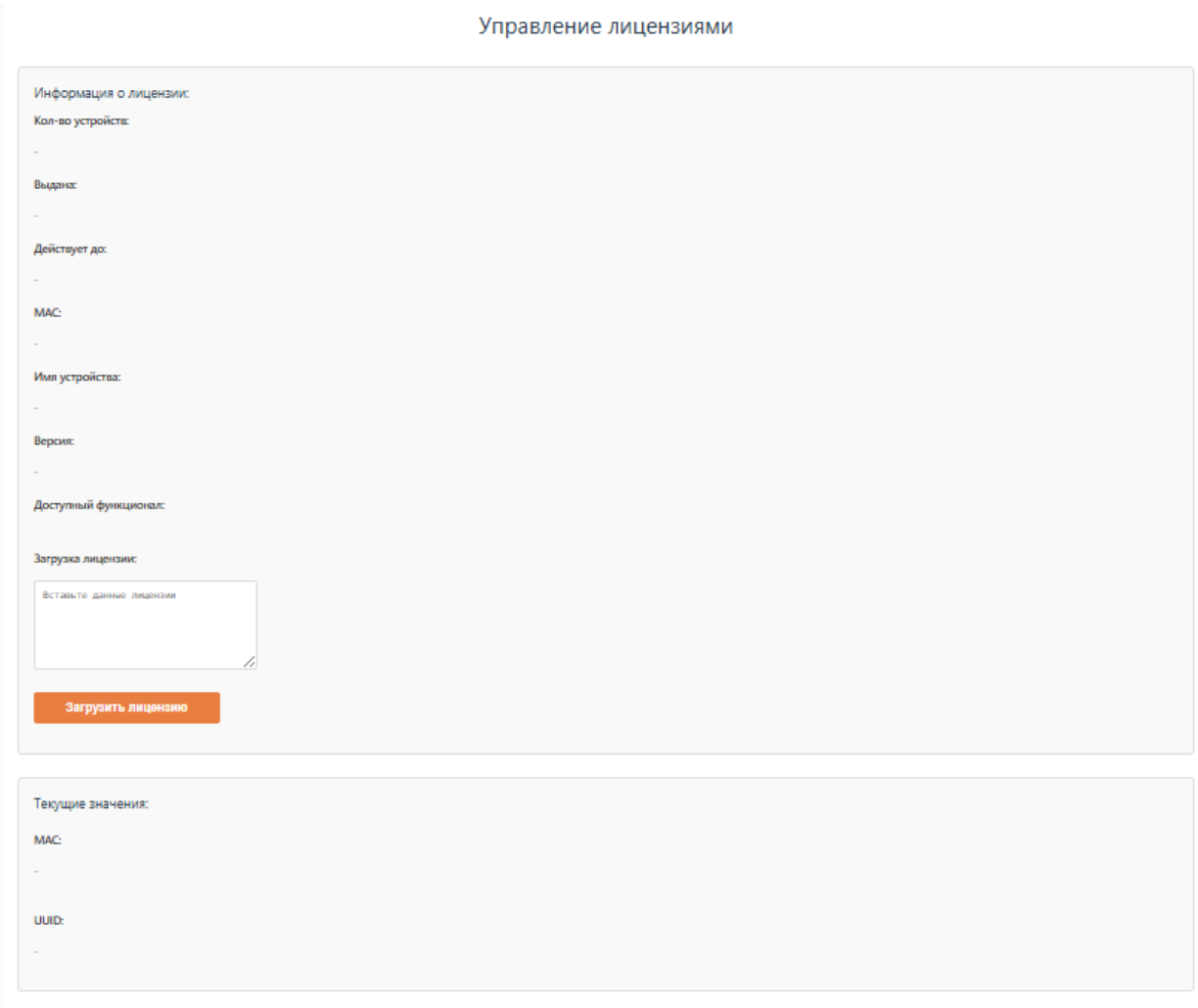



Рисунок 4.11.1 – Окно «Управление лицензиями»

Количество блоков и функционал определяется лицензией. Для получения лицензии необходимо связаться с обладателем.

В окне «Управление лицензиями» находится:

– информация о наличии, либо отсутствии лицензии;

– количество устройств, которые могут использоваться по данной лицензии (рис. 4.11.2);

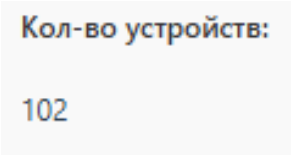



Рисунок 4.11.2 – Информация о количестве устройств

– срок действия лицензии (рис. 4.11.3);

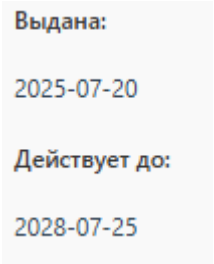



Рисунок 4.11.3 – Информация о сроке лицензии

– в поле «Доступный функционал» отображаются лицензии по конкретным модулям (рис. 4.11.4);

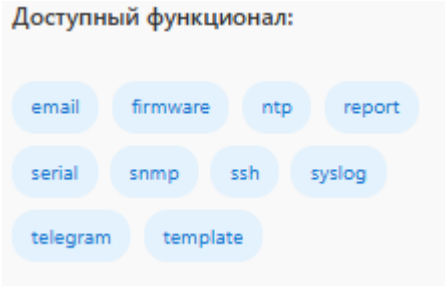



Рисунок 4.11.4 – Поле «Доступный функционал»

– в поле «Текущие значения» отображаются значения MAC и UUID, необходимые для генерации лицензии (рис. 4.11.5);

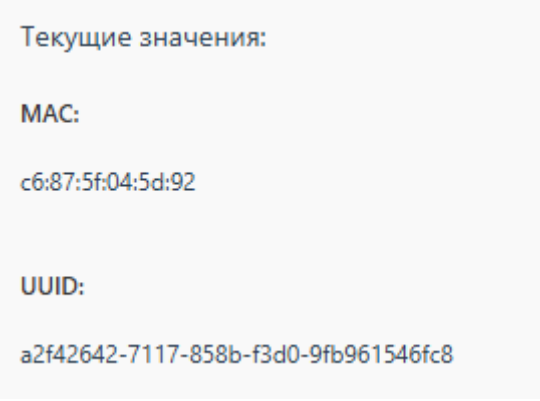



Рисунок 4.11.5 – Поле «Текущие значения»

Для установки лицензии необходимо вставить полученную лицензию в поле «Загрузка лицензии» и нажать кнопку «*Загрузить лицензию*» (рис 4.11.6).

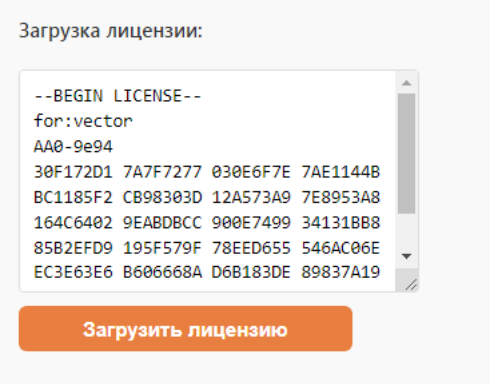



Рисунок 4.11.6 – Поле «Загрузка лицензии»

При успешной загрузке лицензии обновится информация о лицензии (рис. 4.11.7).

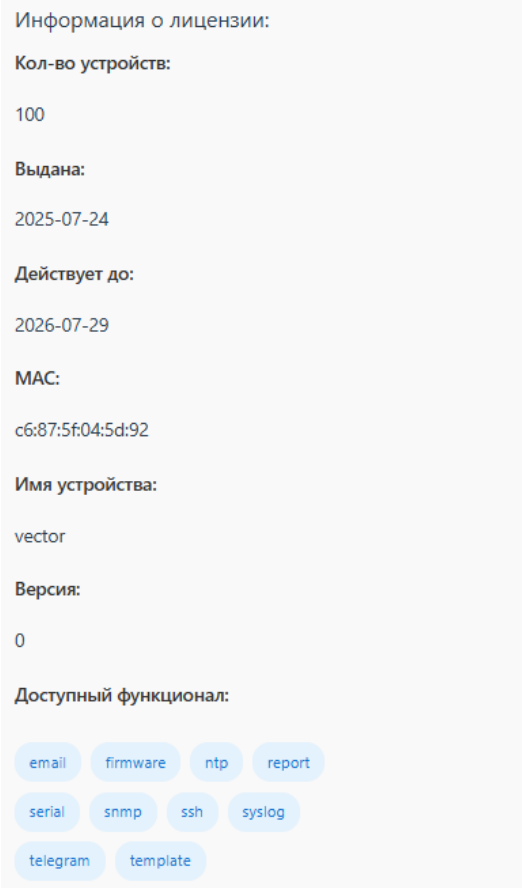



Рисунок 4.11.7 – Информация о лицензии после загрузки ключа

# 5. ТРЕБОВАНИЯ ПО

## 5.1. Требования квалификации персонала

Для обеспечения ввода программного обеспечения в действие персонал, должен изучить эксплуатационную документацию на ПО V-Sense и знать и уметь работать со следующими технологиями: Linux: уверенное знание и пользование терминалом, навыки и понимания работы с сетевыми службами, установка и администрирование приложений; Docker: понимание принципов работы технологии, навыки работы с контейнерами (запуск, остановка, мониторинг, конфигурация).

Для использования программного обеспечения персонал должен изучить эксплуатационную документацию на ПО V-Sense и овладеть навыками работы с ПО.

Пользователи системы должны владеть навыками работы с Интернет-браузерами (Яндекс.Браузер, Google Chrome, Microsoft Edge, Mozilla Firefox, Opera).

## 5.2. Требования к АРМ

АРМ должно быть с предустановленной операционной системой (Windows, Linux, Astra Linux, РЕД ОС, ALT Linux и аналоги), установлен интернет-браузер (Яндекс.Браузер, Google Chrome, Microsoft Edge, Mozilla Firefox, Opera или аналогичные), средства работы с файлами формата: pdf, doc, xls.

Технические требования к АРМ:

– процессор: 1 гигагерц (ГГц) или быстрее с двумя или более ядрами на совместимом 64-разрядном процессоре;

– ОЗУ: 4 гигабайта (ГБ) или больше; ПЗУ: 1 ГБ или больше свободного места на диске;

– графическая карта: совместим с DirectX 12 или более поздней версии с драйвером WDDM 2.0;

– дисплей: дисплей с высоким разрешением (720p), монитор с разрешением 9 дюймов или более, 8 бит на цветовой канал;

– устройства ввода: клавиатура, компьютерная мышь.

### 5.3. Требования к серверной части

Минимальная конфигурация сервера для запуска и устойчивой работы системы управления и мониторинга:

– операционная система Linux с поддержкой Docker;

– процессор, поддерживающий виртуализацию и имеющий минимум 4 ядра, рекомендуемое количество – 8 ядер;

– минимальный объем оперативной памяти от 8 ГБ, рекомендуемый 16 ГБ;

– минимальный объем свободного места на жестком диске 200 ГБ, рекомендуемый 1ТБ;

– наличие сетевого интерфейса 1 Гбит/с.

# 6. СПИСОК СОКРАЩЕНИЙ

| | | |
|---|---|---|
| ПО | - | программное обеспечение |
| АРМ | - | автоматизированное рабочее место |
| ОЗУ | - | оперативное запоминающее устройство |
| ПЗУ | - | постоянное запоминающее устройство |
| СУИМ | - | Система управления и мониторинга |
| ООО | - | Общество с ограниченной ответственностью |
| SNMP | - | Simple Network Management Protocol |
| ОИТ | - | Оборудование информационных технологий |
| IP | - | Уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP. |