СОГЛАСОВАНО
ООО «Энткор-Е»

_____И.О. Корявченко
«___»_____ 2025 г.

УТВЕРЖДАЮ
ООО «Энткор-Е»

_____М.Ю. Сухарь
«___»_____ 2025 г.

Программное обеспечение e-node

Руководство пользователя

Чита, 2025

Содержание

1. Введение

e-node – универсальный программный комплекс мониторинга и управления сетевой и серверной инфраструктурой, инженерным оборудованием, оборудованием АСУ, АСУ ТП, информационными системами и другими типами оборудования и программного обеспечения Заказчика, а также средство контроля, управления и обеспечения безопасности сетевой, серверной и облачной инфраструктуры.

Система может использоваться как самостоятельный, законченный продукт, так и встраиваться во внешние (существующие или разрабатываемые) информационные системы Заказчиков.

Система обеспечивает:

- быстрое внедрение за счёт существующего набора описанных устройств, включая российское оборудование;
- прозрачный технический учёт (инвентаризацию) физических и логических ресурсов технологических сетей связи, ИТ-инфраструктуры и инженерных систем, а также мониторинг их состояния;
- замену множества систем мониторинга оборудования на единую платформу;
- полное понимание структуры информационных потоков в сетях;
- возможность выделения сетевого взаимодействия, относящегося к определенным сервисам и приложениям, обеспечение безопасности на уровне информационных потоков;
- помощь оператору в определении критических уровней ошибок в сети и принятию оптимальных решений по устранению угроз, локализации аварийных событий и сопровождению аварийно-восстановительных и ремонтных работ, учёт и контроль планового обслуживания;

- уведомление о событиях посредством электронного (диспетчерского) журнала, СМС-рассылки, мессенджеров и электронной почты;
- возможность управления конфигурациями и техническим учётом;
- ситуационное управление оборудованием, ресурсами технологических сетей связи, ИТ-инфраструктуры и инженерных систем;
- повышение наблюдаемости и контролируемости инфраструктуры.

Со стороны серверной части Система обеспечивает возможность:

- выбора базовой операционной системы из широкого перечня систем семейства Linux (Ubuntu, Astra Linux, ALT Linux);
- установки на виртуальные машины;
- резервирования программных узлов;
- создания сложных геораспределенных систем мониторинга и управления.

Со стороны клиентской части Система необходима для:

- технического учёта физических и логических ресурсов технологических сетей связи, ИТ-инфраструктуры и инженерных систем, а также мониторинга их состояния;
- помощи оператору в принятии оптимальных решений по устранению угроз, оперативного предоставления причин отказов, а также предиктивного анализа объектов контроля;
- ситуационного управления ресурсами технологических сетей связи, ИТ-инфраструктуры и инженерных систем;
- повышения наблюдаемости и контролируемости инфраструктуры.

Для выполнения поставленных задач программа оснащена оконным пользовательским интерфейсом, содержащим: меню выбора подсистемы, меню вкладок, панель статусов, меню пользователя, панель навигации в левой части экрана и рабочую область экрана в виде окна.

Система предназначена для решения следующих задач:

- Мониторинг состояния объектов мониторинга:
  - опрос объектов с использованием различных протоколов;
  - формирование статуса объектов на основе пороговых значений;
  - построение зависимости объектов на основе иерархии с автоматическим наследованием статуса.
- Безопасность и контроль сетевых взаимодействий и глубокий анализ сетевого трафика:
  - визуализация сетевых потоков в гибридных средах (традиционные ЦОД, облака, Kubernetes, Docker);
  - диагностирование аномалий сетевого трафика, анализ поведения информационных систем;
  - блокировка несанкционированных связей на основе политик «белых списков».
- Распределенный программный межсетевой экран:
  - пакетная фильтрация;
  - блокировка/разрешение трафика по IP-адресам, портам и протоколам (TCP/UDP/ICMP);
  - Stateful Inspection;
  - контроль состояния соединений (отслеживание сессий);
  - защита от подмены пакетов и атак типа «подделка соединений»;
  - централизованное управление политиками;
  - автоматизированное реагирование (блокировка атакующих IP на основе данных от подсистемы мониторинга, подсистемы инвентаризации сетевых пакетов);
  - единая система протоколирования событий безопасности.
- Визуализация состояния объектов мониторинга:
  - настраиваемые сводные панели (dashboard) с консолидированной информацией;

  - топология сети с географической привязкой;
  - иерархическое отображение объектов с наследованием состояния;
  - автоматическое и ручное добавление объектов;
  - отображение объектов с детальным состоянием их компонентов;
  - встроенные фильтры для отображения объектов по различным признакам.
- Инвентаризация объектов:
  - хранение различной инвентарной информации объектов, включая данные об обслуживании, с возможностью поиска;
  - загрузка и привязка документов к объектам.
- Контроль производительности:
  - формирование графического представления метрик, собираемых с объектов.
- Управление оборудованием:
  - встроенные средства создания сценариев конфигурирования объектов с помощью различных протоколов (SSH, NETCONF, SNMP);
  - наличие готовых коннекторов для управления объектов;
  - возможность заказа разработки специализированных коннекторов для объектов.
- Управление конфигурациями:
  - импорт, экспорт и хранение конфигураций оборудования с контролем версий;
  - отслеживание изменений конфигурации;
  - встроенные средства редактирования конфигурации.
- События и оповещение:
  - регистрация событий с формированием журнала по всем объектам;

  - встроенный сервер SYSLOG;
  - экспорт событий по протоколу SYSLOG;
  - отправка оповещений по электронной почте, интеграция с мессенджерами;
- Отчетность:
  - шаблоны отчетов с возможностью редактирования;
  - шаблоны представления для экспорта вывода данных из консоли управления.
- Контроль доступа:
  - ролевая модель доступа;
  - разделение доступа на уровне отдельных объектов и групп иерархии.

2. Основные требования для работы с Системой

2.1. Требования к пользователям

Для успешной и комфортной работы с программным комплексом пользователи должны:

- Обладать навыками работы с компьютерами и периферийными устройствами:
  - самостоятельно включать / отключать оборудования от электропитания;
  - запускать ОС;
  - производить набор данных на клавиатуре;
  - использовать манипулятор «мышь» для активизации визуальных элементов управления на экране монитора.
- Уметь пользоваться средствами операционной системы и оперировать ими через стандартные интерфейсы:
  - самостоятельно производить авторизацию пользователя;
  - запускать программы на исполнение;
  - использовать базовые функции оконного интерфейса, позволяющего изменять размер окна программы и перемещать его на экране монитора;
  - переключаться между окнами;
  - уметь работать с веб-браузером.
- Иметь знания и выполнять установленные для пользователя меры по защите информации;
- Знать основы сетевых технологий и соответствую терминологию.

2.2. Требования к аппаратному обеспечению

Минимальные требования к рабочему месту пользователя:

- взаимодействие пользователя с Системой должно осуществляться посредством интернет-браузера *(Firefox, Safari, Google Chrome*, Яндекс.Браузер) без применения дополнительного ПО, устанавливаемого на рабочем месте пользователя;
- компьютер для организации рабочего места (предоставляется Заказчиком);
- подключение к сети интернет (обеспечивается силами Заказчика);
- для подключения должно применяться полностью определённое имя домена (*FQDN - Fully Qualified Domain Name*) сопоставленное с внешним ip-адресом сервера приложений.

2.3. Требования к программному обеспечению

Требования к конфигурации программного обеспечения клиентской части:

- Операционная система: *Linux, Windows* или *Mac OS X*.
- Интернет-браузер (один из браузеров): *Safari; Mozilla Firefox; Google Chrome*; *Яндекс.Браузер*.

3. Архитектура и основные модули Системы

Архитектура Системы включает в себя следующие модули:

- Модуль мониторинга состояния объектов (Fault Management);
- Модуль визуализации состояния объектов;
- Модуль инвентаризации объектов (NRI);
- Модуль управления объектами;
- Модуль управления конфигурациями объектов (Configuration Management);
- Модуль контроля параметров устойчивого функционирования;
- Модуль отображения событий и оповещения и управления заявками (Notification and order management);
- Программный агент сбора информации с узлов контроля;
- Модуль инвентаризации сетевых потоков;
- Модуль межсетевого экрана;
- Модуль формирования отчетов.

Система построена на базе микросервисной архитектуры и может функционировать в среде Docker, Kubernetes.

3.1. Модуль мониторинга состояния объектов (Fault Management)

Данный модуль позволяет пользователю создать иерархию объектов, которая соответствует реальной топологии инфраструктуры предприятия, например – «здание по адресу – этаж – комната – стойка – объект – компонент объекта».

Также данный модуль позволяет:

- проводить мониторинг объектов с использованием протоколов SNMP, HTTP, ModBus, МЭК 60870-5-104, WMI, SQL, MQTT;
- формировать статус объектов на основе пороговых значений;
- строить зависимости объектов на основе иерархии с автоматическим наследованием статус;

- настраивать индивидуальные параметры опроса для каждого устройства;
- фильтровать и выгружать основные события Системы в формате PDF или CSV.

3.2. Модуль визуализации состояния объектов

Данный модуль позволяет:

- настраивать сводные панели (dashboard) с консолидированной информацией;
- отображать топологию сети с географической привязкой (а также в виде графа с отображением статусов связи между объектами);
- отображать объекты согласно иерархии с возможностью наследования состояния;
- автоматически и вручную добавлять объекты;
- автоматически строить сети на основе протокола LLDP;
- отображать объекты с детальным состоянием их компонентов;
- использовать встроенные фильтры для отображения объектов по различным признакам.

3.3. Модуль инвентаризации объектов (NRI)

Данный модуль позволяет:

- автоматически собирать и хранить инвентарную информацию об объекте, включая данные об обслуживании, с возможностью поиска;
- формировать события на основе указания даты проведения обслуживаний;
- загружать и привязывать документы к объектам;
- указывать у объектов владельца, обслуживающую организацию и тип системы;
- визуализировать телекоммуникационные стойки;

- сканировать объекты мониторинга по расписанию на предмет изменения встраиваемых модулей (в разработке);
- произвести интеграцию с внешними CMDB и системами управления заявок.

3.4. Модуль управления объектами

Данный модуль позволяет:

- использовать встроенные средства создания сценариев конфигурации объектов с помощью различных протоколов (SSH, SNMP);
- осуществлять обновления программного обеспечения устройств;
- использовать готовые коннекторы для управления объектами;
- заказывать разработку специализированных коннекторов для управления объектами;
- использовать модуль ZTP (Zero-Touch Provisioning) для первоначальной настройки оборудования в автоматическом режиме;
- использовать встроенную консоль SSH для управления объектами.

3.5. Модуль управления конфигурациями объектов (Configuration Management)

Данный модуль позволяет:

- производить импорт, экспорт и хранение конфигураций оборудования с контролем версий;
- отслеживать изменений конфигураций;
- использовать встроенные средства сравнения и редактирования конфигураций.

3.6. Модуль контроля параметров устойчивого функционирования

Модуль является средством (инструментом), предоставляющим возможность комплексной оценки объектов в КИИ, с целью определения рисков, возникновение которых может привести к снижению устойчивости функционирования объекта.

Модуль обеспечивает возможность расчета фактических свойств объекта, включающий в себя функциональность, надежность как для комплекса в целом, так и для отдельных его компонентов.

3.7. Модуль отображения событий и оповещения

Данный модуль позволяет:

- регистрировать события и формировать журнал по всем объектам;
- использовать встроенный сервер SYSLOG для приёма событий от объектов;
- экспортировать события по протоколу SYSLOG;
- отправлять оповещения по электронной почте и производить интеграцию с мессенджерами.

3.8. Программный агент сбора информации с узлов контроля;

Данный модуль позволяет представляет собой микросервис, устанавливаемый на целевые узлы для выполнения задач мониторинга. Передача конфигураций модулю производится через систему распределенных конфигураций. Все метрики и события передаются в централизованную систему управления.

Также данный модуль позволяет:

- выполнять сбор метрик о работе операционной системы (процессы, загрузка, использование ресурсов);
- выполнять сбор метрик о работе каналов связи: точка – точка, качество, количество сбоев, задержки, пропускная способность;

- выполнять сбор информации о всех сетевых пакетах на всех интерфейсах;
- применять правила межсетевого экрана;
- выполнять сбор информации о системах виртуализации;
- реализовывать функции Policy Based Routing на уровне eBPF;
- осуществлять мониторинг состояния сетевых интерфейсов.

3.9. Модуль инвентаризации сетевых потоков

Данный модуль позволяет:

- выполнять визуализацию сетевых потоков в гибридных средах (традиционные ЦОД, облака, Kubernetes, Docker);
- диагностировать аномалии сетевого трафика, осуществлять анализ поведения информационных систем;
- выполнять блокировку несанкционированных связей на основе политик «белых списков».

3.10. Модуль межсетевого экрана

Данный модуль позволяет:

- выполнять пакетную фильтрацию трафика посредством статических правил межсетевого экрана на основе IP-адресов и портов источника и назначения, а также используемых интерфейсов;
- выполнять пакетную фильтрацию трафика посредством динамических правил, формируемых во время работы Системы на основе анализа сетевых потоков;
- осуществлять контроль состояния соединений (отслеживание сессий);
- осуществлять защиту от подмены пакетов и атак типа «подделка соединений»;

- выполнять автоматизированное реагирование на инциденты сетевой безопасности (блокировка атакующих IP на основе данных от подсистемы мониторинга, подсистемы инвентаризации сетевых пакетов);
- осуществлять централизованное управление правилами межсетевого экрана, выполнять их редактирование, активацию/деактивацию, в т.ч. по определенным условиям;
- обеспечивать комплексное протоколирование событий безопасности.

3.11. Модуль формирования отчетов

Данный модуль позволяет формировать необходимые отчеты, в частности:

- статистику по типам узлов;
- отчет по созданию новых потоков;
- топ узлов источников (по количеству трафика);
- топ узлов назначения (по количеству трафика);
- топ потоков (по количеству трафика);
- топ узлов назначения (по количеству трафика по потокам).

4. Начало работы с Системой

Для начала работы с **e-node** выполните одно из следующих действий:

- введите в адресной строке веб-браузера адрес для доступа к Системе;
- откройте ярлык **e-node** на рабочем столе;
- перейдите по сохранённой ссылке в веб-браузере.

После выполнении одного из этих действий откроется окно авторизации (Рисунок 4.1).

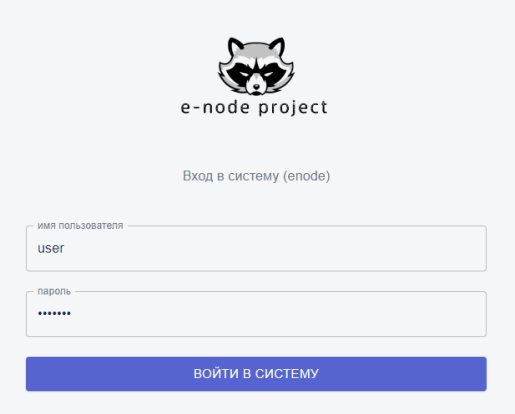


Рисунок 4.1 – Авторизация пользователя в системе e-node

Введите ваше имя пользователя и пароль, затем нажмите кнопку «Войти». Если данные введены корректно, вы попадёте на главную страницу системы **e-node**, где будет активна вкладка Dashboard (Рисунок 4.2).

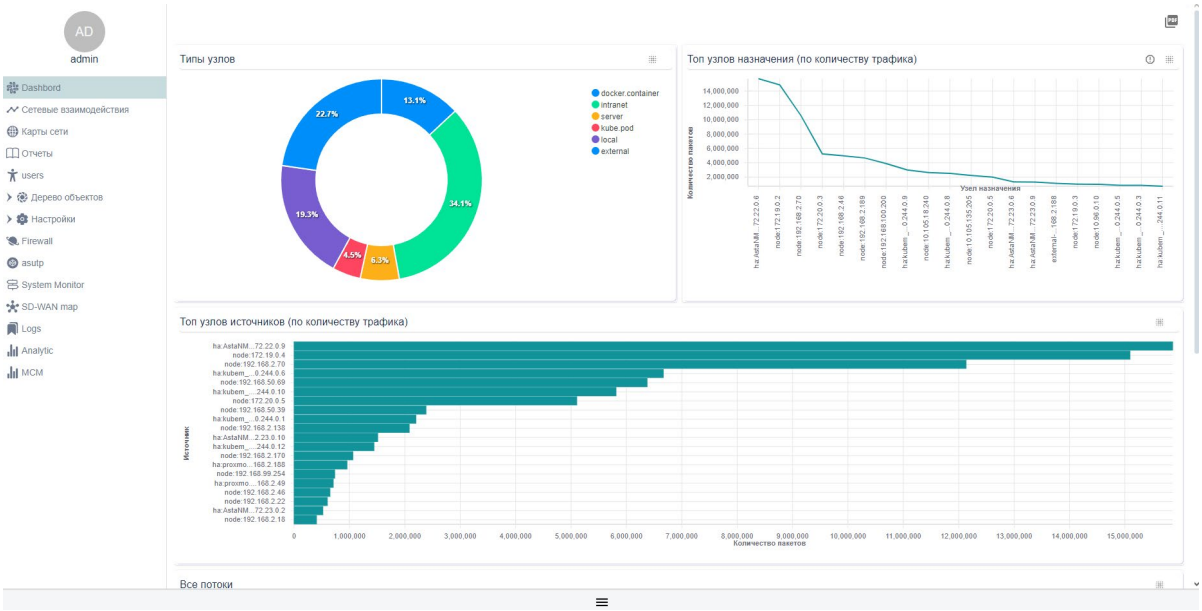


Рисунок 4.2 – Главная страница Системы (вкладка Панель приборов)

5. Описание интерфейса и выполняемых функций Системы

Пользовательский интерфейс системы разделён на три основные части (Рисунок 5.1):

- **Панель навигации** (верхняя левая часть экрана) включает в себя вкладки: «Dashboard», «Сетевые взаимодействия», «Карты сети», «Отчеты», «Пользователи», «Дерево объектов», «Firewall» и другие;
- **Панель событий** (нижняя левая часть экрана) состоит из вкладок: «События», «Задачи», «Потоки» и «Правила».
- **Панель рабочей области** (центральная часть экрана) является основным пространством для отображения данных.

Рисунок 5.1– Основные части пользовательского интерфейса

5.1. Вкладка Dashboard

Данная вкладка представляет собой аналитическую панель, в которой отображаются основные показатели и ключевые метрики Системы в виде графиков, диаграмм и таблиц.

На круговой диаграмме «**Типы узлов**» (рис. 5.2) отображено процентное соотношение всех типов узлов, которые смогла обнаружить система. При

наведении курсора мыши на любой сегмент круговой диаграммы будет показана информация о количестве узлов, которые относятся к данному типу. Например, при наведении курсора мыши на сегмент *external* появится информация, о количестве узлов данного типа (рис. 5.3):

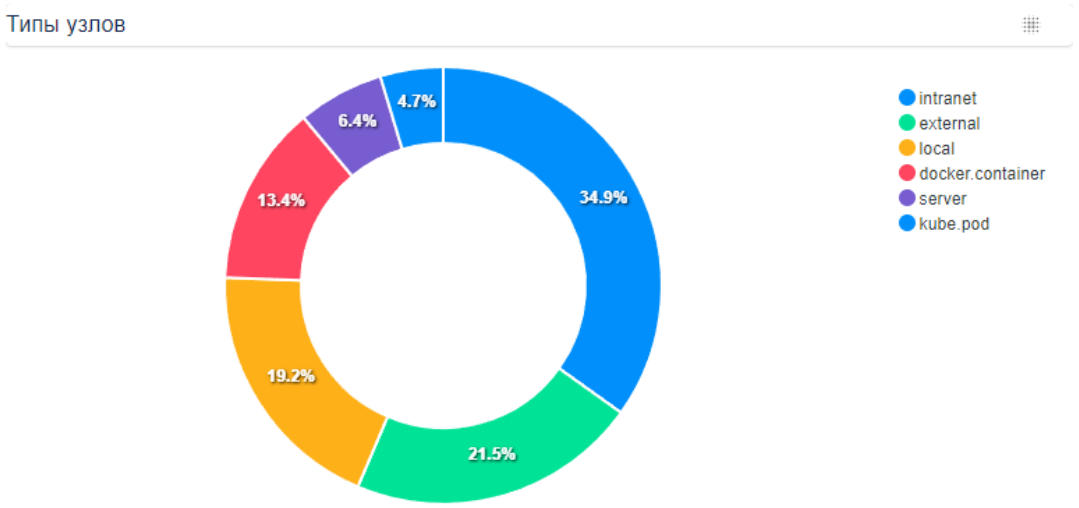


Рисунок 5.2 – Круговая диаграмма «Типы узлов»

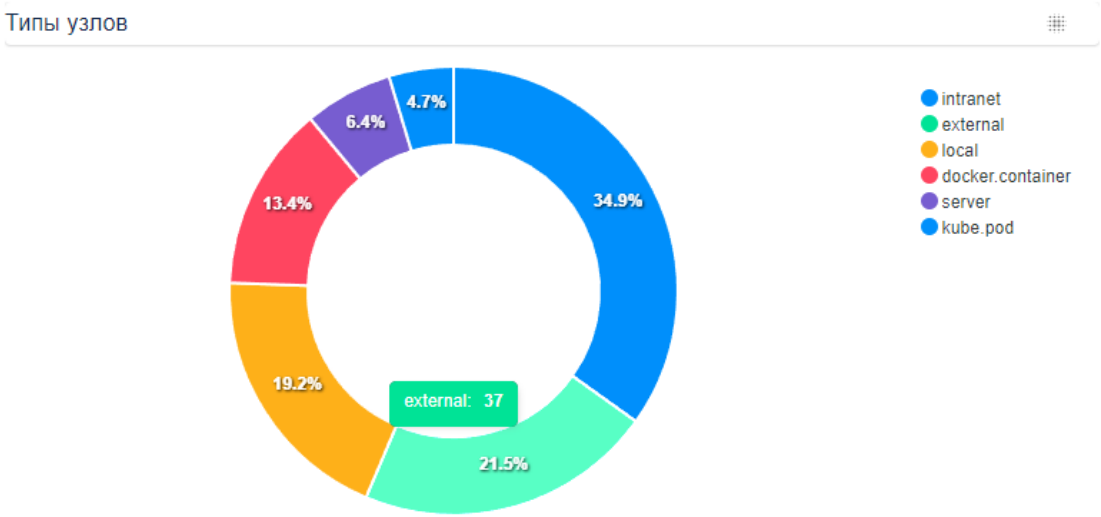


Рисунок 5.3 – Информация о количестве узлов данного типа

При нажатии на кнопку откроется выпадающее окно (рис.5.4), в котором можно выбрать внешний вид отображения типов узлов: в виде круговой диаграммы (рис.5.4) или таблицы (рис. 5.5).

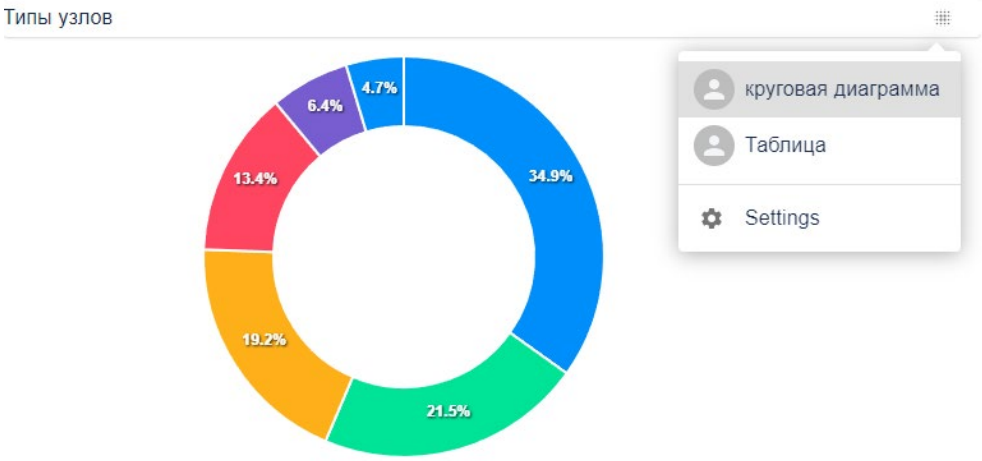


Рисунок 5.4 – Выпадающее окно с выбором вида отображения типов узлов

Типы узлов

Тип узла	Количество узлов
intranet	60
external	37
local	33
docker.container	23
server	11
kube.pod	8

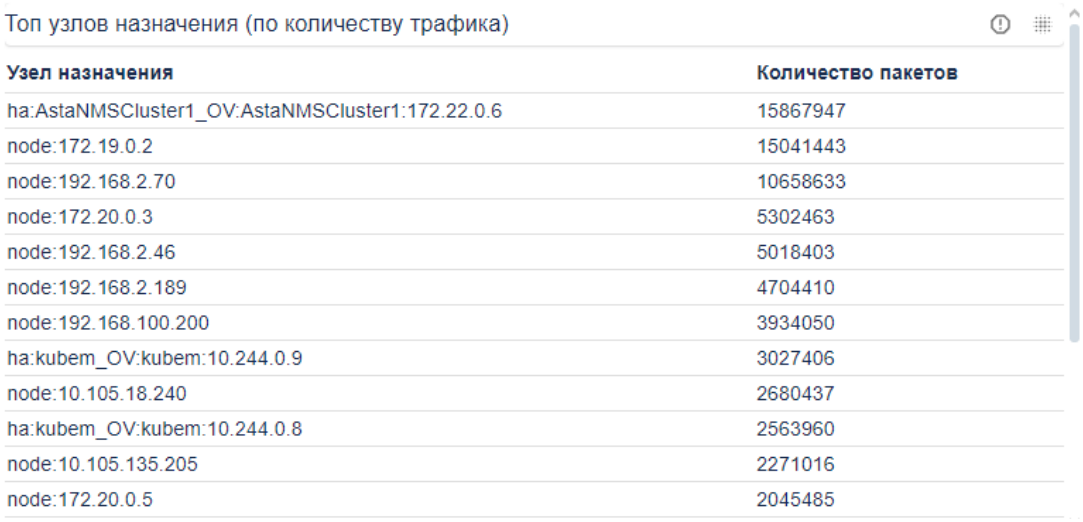
Рисунок 5.5 – Таблица «Типы узлов»

На линейном графике «**Топ узлов назначения (по количеству трафика)**» (рис. 5.6) отображены узлы с наибольшим количеством полученного трафика за 2 суток. На оси ординат указано количество пакетов, на оси абсцисс узел назначения.

Рисунок 5.6 – Линейный график "Топ узлов назначения"

При нажатии на кнопку  откроется выпадающее окно (рис. 5.6), в котором можно выбрать внешний вид отображения топ узлов назначения: в виде линейной диаграммы (рис. 5.5) или таблицы (рис. 5.7).

Рисунок 5.6 – Выпадающее окно с выбором вида отображения топ узлов назначения


Топ узлов назначения (по количеству трафика)

Узел назначения	Количество пакетов
ha:AstaNMSCluster1_OV:AstaNMSCluster1:172.22.0.6	15867947
node:172.19.0.2	15041443
node:192.168.2.70	10658633
node:172.20.0.3	5302463
node:192.168.2.46	5018403
node:192.168.2.189	4704410
node:192.168.100.200	3934050
ha:kubem_OV:kubem:10.244.0.9	3027406
node:10.105.18.240	2680437
ha:kubem_OV:kubem:10.244.0.8	2563960
node:10.105.135.205	2271016
node:172.20.0.5	2045485

Рисунок 5.7 – Таблица «Топ узлов назначения»

При нажатии на кнопку появится информационное окно с дополнительной информацией (рис. 5.8).

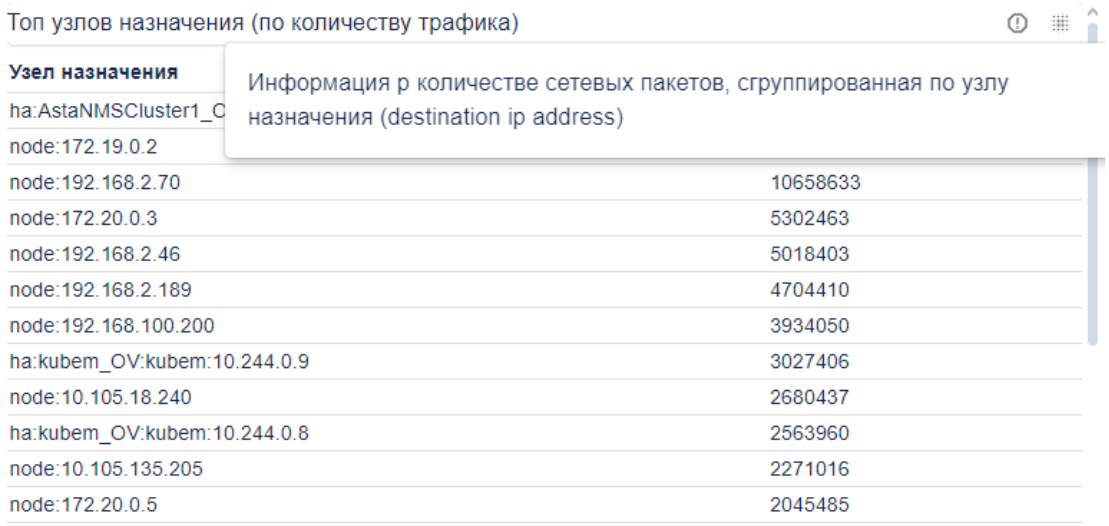


Рисунок 5.8 – Информационное окно с дополнительной информацией

На горизонтальной гистограмме «**Топ узлов источников (по количеству трафика)**» (рис.5.9) отображены узлы с наибольшим количеством отправленного трафика за 2 суток. На оси ординат указаны источники, на оси абсцисс количество пакетов.

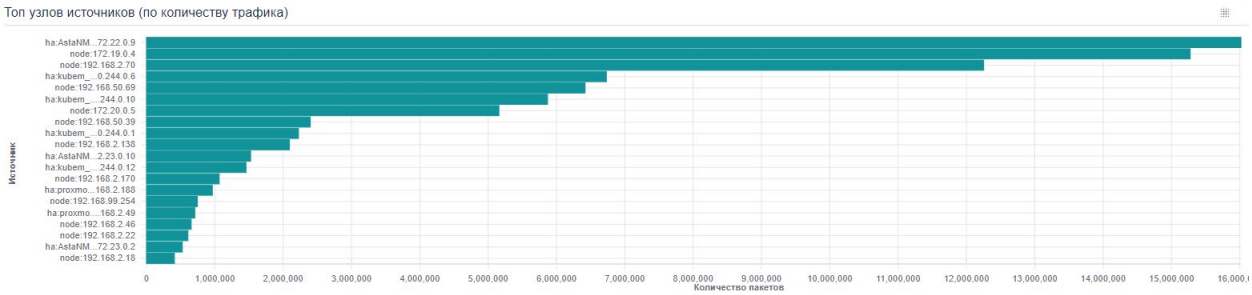


Рисунок 5.9 – Горизонтальная гистограмма "Топ узлов источников"

При нажатии на кнопку  откроется выпадающее окно (рис. 5.10), в котором можно выбрать внешний вид отображения топ узлов источников: в виде горизонтальной гистограммы (рис.5.9) или таблицы (рис. 5.11).

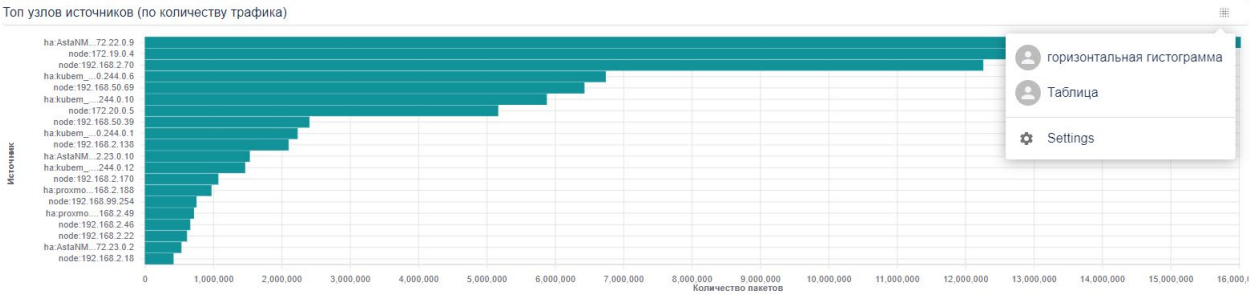


Рисунок 5.10 – Выпадающее окно с выбором вида отображения топ узлов источников

Топ узлов источников (по количеству трафика)

Источник	Количество пакетов
ha:AstaNMSCluster1_OV:AstaNMSCluster1:172.22.0.9	16017427
node:172.19.0.4	15274453
node:192.168.2.70	12252239
ha:kubem_OV:kubem:10.244.0.6	6730473
node:192.168.50.69	6419064
ha:kubem_OV:kubem:10.244.0.10	5869173
node:172.20.0.5	5157013
node:192.168.50.39	2397503
ha:kubem_OV:kubem:10.244.0.1	2224647
node:192.168.2.138	2092877
ha:AstaNMSCluster1_OV:AstaNMSCluster1:172.23.0.10	1523971
ha:kubem_OV:kubem:10.244.0.12	1456004

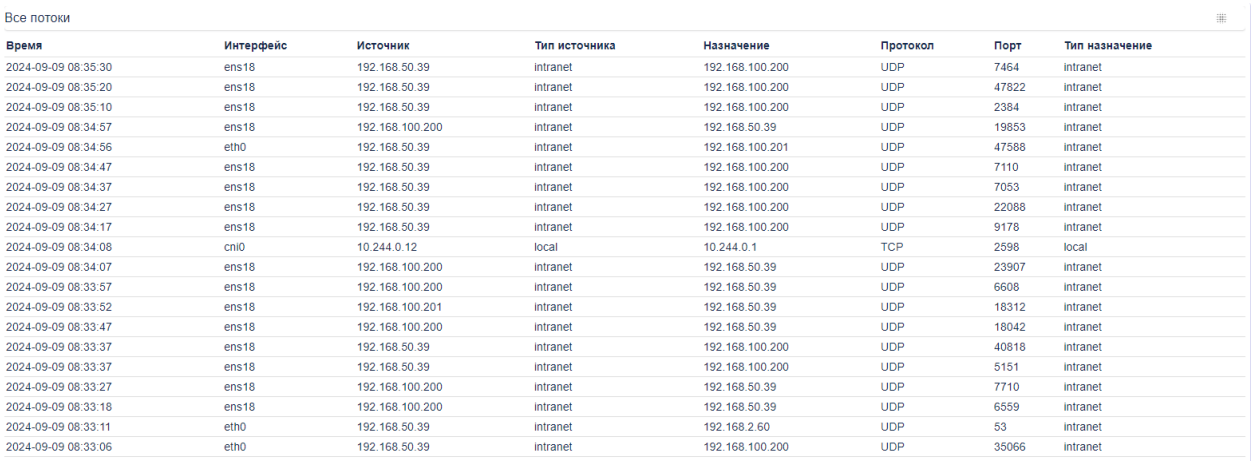
Рисунок 5.11 – Таблица «Топ узлов источников»

Внизу страницы располагается таблица «**Все потоки**» (рис. 5.12), в которой есть следующие столбцы:

- время – время обнаружение потока;

- интерфейс – сетевой интерфейс устройства, через который обнаружен поток;
- источник – *ip* адрес сетевого устройства, который является источником потока;
- тип источника – категория, под которую попадает устройство, формирующее поток;
- назначение – *ip* адрес сетевого устройства, который является назначением потока;
- протокол – транспортный протокол потока;
- порт – сетевой порт назначения;
- тип назначения – категория, под которую попадает устройство, принимающее поток.

Данные представлены за последние 48 часов.



Все потоки

Время	Интерфейс	Источник	Тип источника	Назначение	Протокол	Порт	Тип назначение
2024-09-09 08:35:30	ens18	192.168.50.39	intranet	192.168.100.200	UDP	7464	intranet
2024-09-09 08:35:20	ens18	192.168.50.39	intranet	192.168.100.200	UDP	47822	intranet
2024-09-09 08:35:10	ens18	192.168.50.39	intranet	192.168.100.200	UDP	2384	intranet
2024-09-09 08:34:57	ens18	192.168.100.200	intranet	192.168.50.39	UDP	19853	intranet
2024-09-09 08:34:56	eth0	192.168.50.39	intranet	192.168.100.201	UDP	47588	intranet
2024-09-09 08:34:47	ens18	192.168.50.39	intranet	192.168.100.200	UDP	7110	intranet
2024-09-09 08:34:37	ens18	192.168.50.39	intranet	192.168.100.200	UDP	7053	intranet
2024-09-09 08:34:27	ens18	192.168.50.39	intranet	192.168.100.200	UDP	22088	intranet
2024-09-09 08:34:17	ens18	192.168.50.39	intranet	192.168.100.200	UDP	9178	intranet
2024-09-09 08:34:08	cni0	10.244.0.12	local	10.244.0.1	TCP	2598	local
2024-09-09 08:34:07	ens18	192.168.100.200	intranet	192.168.50.39	UDP	23907	intranet
2024-09-09 08:33:57	ens18	192.168.100.200	intranet	192.168.50.39	UDP	6608	intranet
2024-09-09 08:33:52	ens18	192.168.100.201	intranet	192.168.50.39	UDP	18312	intranet
2024-09-09 08:33:47	ens18	192.168.100.200	intranet	192.168.50.39	UDP	18042	intranet
2024-09-09 08:33:37	ens18	192.168.50.39	intranet	192.168.100.200	UDP	40818	intranet
2024-09-09 08:33:37	ens18	192.168.50.39	intranet	192.168.100.200	UDP	5151	intranet
2024-09-09 08:33:27	ens18	192.168.100.200	intranet	192.168.50.39	UDP	7710	intranet
2024-09-09 08:33:18	ens18	192.168.100.200	intranet	192.168.50.39	UDP	6559	intranet
2024-09-09 08:33:11	eth0	192.168.50.39	intranet	192.168.2.60	UDP	53	intranet
2024-09-09 08:33:06	eth0	192.168.50.39	intranet	192.168.100.200	UDP	35066	intranet

Рисунок 5.12 – Таблица «Все потоки»

В правом верхнем углу страницы размещена кнопка , при нажатии на которую можно скачать в формате *pdf* всю информацию с данной страницы.

При нажатии на кнопку в самом низу страницы откроется Панель событий и задач (рис. 5.13).

Рисунок 5.13 - Панель событий и задач

Вкладка «**События**» показывает события, которые происходят в системе, а именно:

- когда появляется новый поток (потоки обнаруживает хост агент);
- происходит изменение конфигураций;
- срабатывает *firewall* по потоку (если в хост агенте включена роль *firewall*).

Вкладка «**События**» (рис. 5.13) состоит из следующих столбцов:

- время события – время, когда произошло событие;
- пользователь – кто ответственен за создание события, либо система (например, когда появился новый поток), либо пользователь, который использует еНОД (в данном случае отобразится его имя);
- описание – описание события;
- критичность – в зависимости от события присваивается её степень (предупреждение, сообщение, авария).

Вкладка «**Задачи**» показывает информацию, связанную с установкой хост агентов (рис. 5.14), а именно:

- задача – отображается имя пользователя, производившего установку хост агента, и адрес машины, куда производилась установка агента;
- время задачи – начало установки хост агента;
- время окончания – время окончания установки хост агента;
- сообщение – отображается успешно или нет была закончена установка хост агента;

- статус – отображаются шаги установки хост агента. В случае успешной установки появился значок ✓ , указывающий на успешную установку хост агента, при нажатии на него появятся окно с шагами установки (рис. 5.15). В случае неспешной установки агента появится ⓘ, при нажатии на которую можно проследить шаги установки и понять на каком шаге произошла ошибка (рис. 5.16).

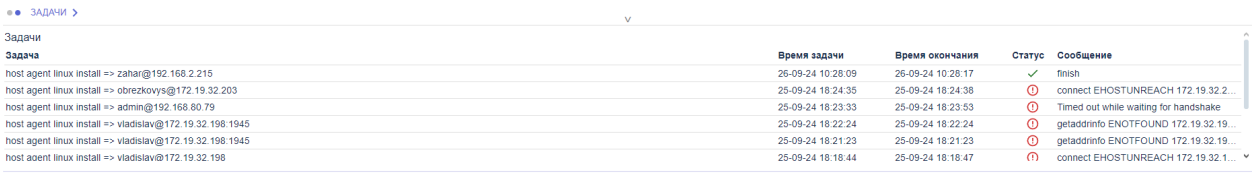


Рисунок 5.14 – Вкладка «Задачи»

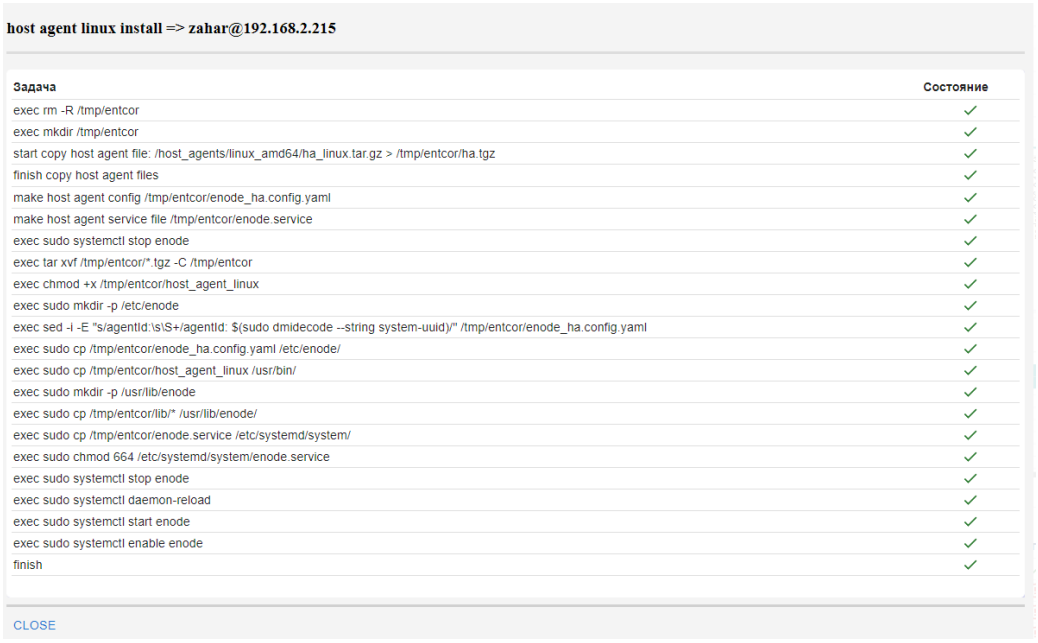


Рисунок 5.15 – Окно с шагами успешной установки хост агента

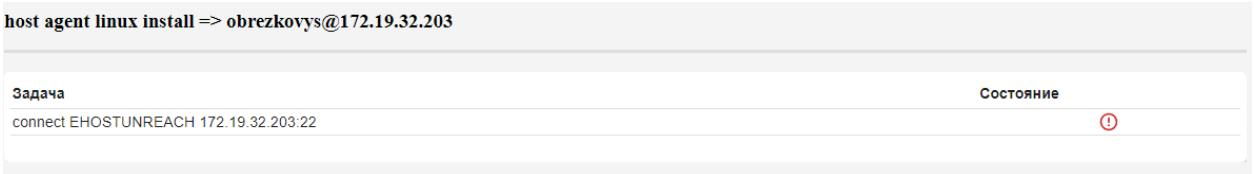


Рисунок 5.16 – Окно с ошибкой во время установки хост агента

5.2. Вкладка Сетевые взаимодействия

Данная вкладка показывает все потоки, обнаруженные программные агентами в виде таблицы «**Типы узлов**». Данная таблица состоит из следующих колонок:

- протокол – транспортный протокол потока;
- адрес источника – *ip* адрес сетевого устройства, который является источником потока;
- порт источника – источник, формирующий поток;
- порт назначения – *ip* адрес сетевого устройства, который является назначением потока;
- порт назначения – получатель сформированного потока;
- количество пакетов – количество пакетов, зарегистрированных в текущем потоке;
- объём данных – размер проходящих данных в байтах.

В верхней правой части экрана представлены основные кнопки, предназначенные для изменения визуального представления таблицы и работе с ней (рис 6.1)

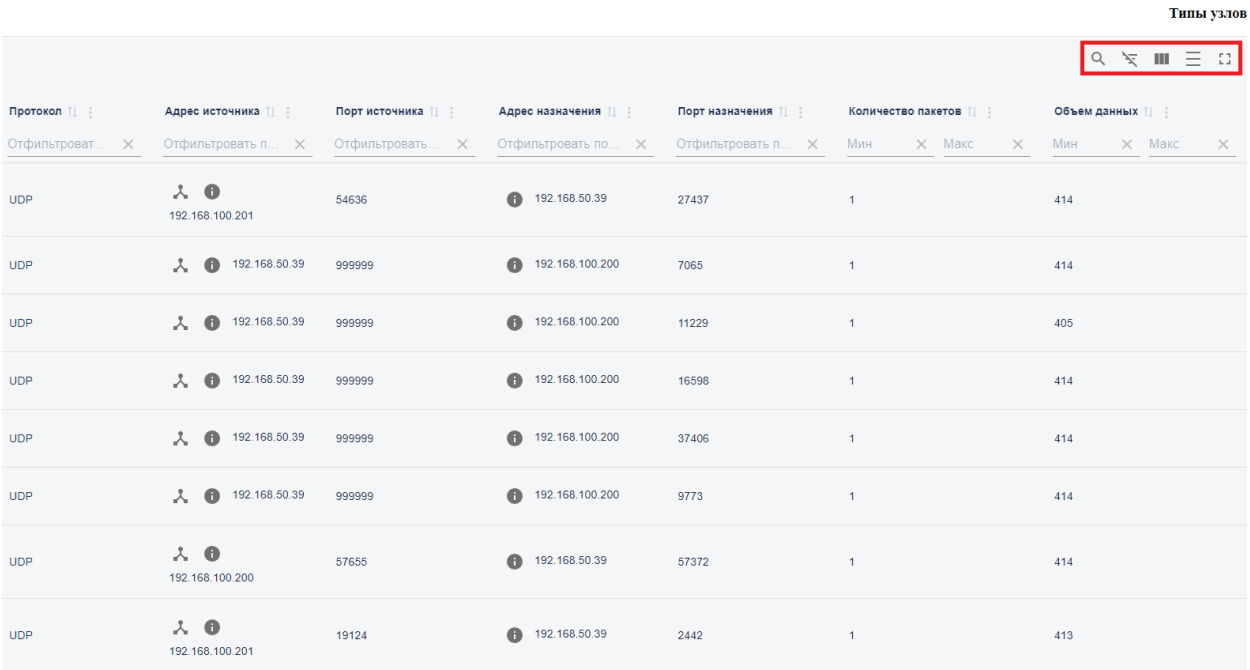


Рисунок 5.17 – Основные кнопки для работы с таблицей "Типы узлов"

Кнопка  предназначена для того, чтобы скрыть или показать строку поиска по таблице (рис 6.2).

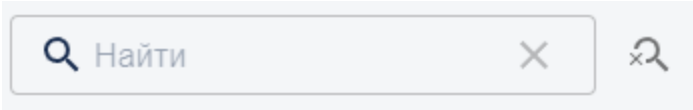


Рисунок 5.18 – Поиск по таблице "Типы узлов"

Кнопка  предназначена для того, чтобы скрыть или показать фильтры таблицы, которые расположены под заголовками столбцов (рис 6.3).

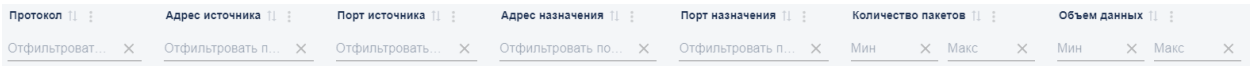


Рисунок 5.19 – Фильтры таблицы "Типы узлов"

Кнопка  предназначена для того, чтобы скрыть или показать колонки таблицы (рис. 6.4). Также имеется возможность скрыть или показать все имеющиеся колонки таблицы.

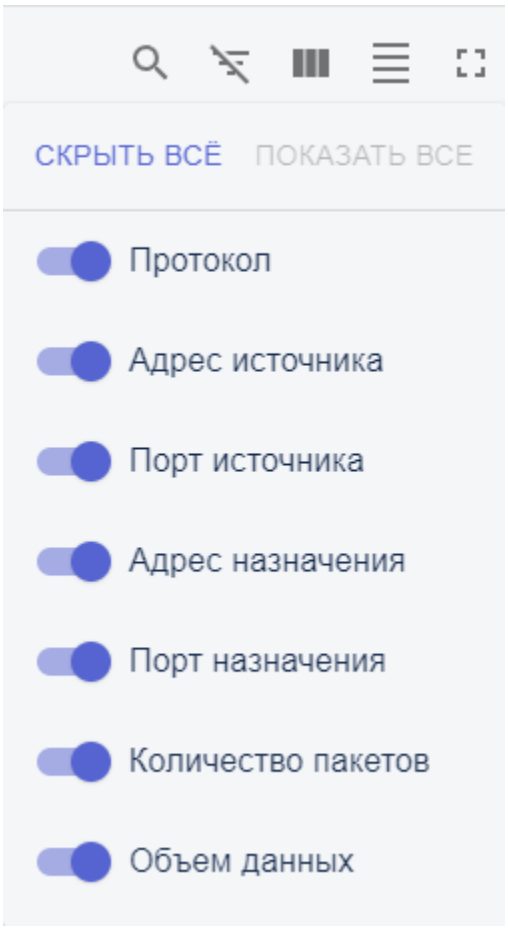


Рисунок 5.20 – Настройка отображения колонок таблицы "Типы узлов"

Кнопка предназначена для того, чтобы изменять плотность строк в таблице. Всего можно выбрать 3 плотности строк в таблице.

Кнопка предназначена для того, чтобы зайти или выйти из полноэкранного режима.

Рядом с каждым заголовком столбца есть две кнопки:

позволяет произвести сортировку данных по возрастанию или убыванию;

позволяет произвести основные действия над колонкой, а именно: очистить сортировку, сортировать по возрастанию или убыванию, очистить

фильтр или произвести фильтрацию, произвести группировку по колонке, скрыть колонку или показать все колонки (рис 6.5).

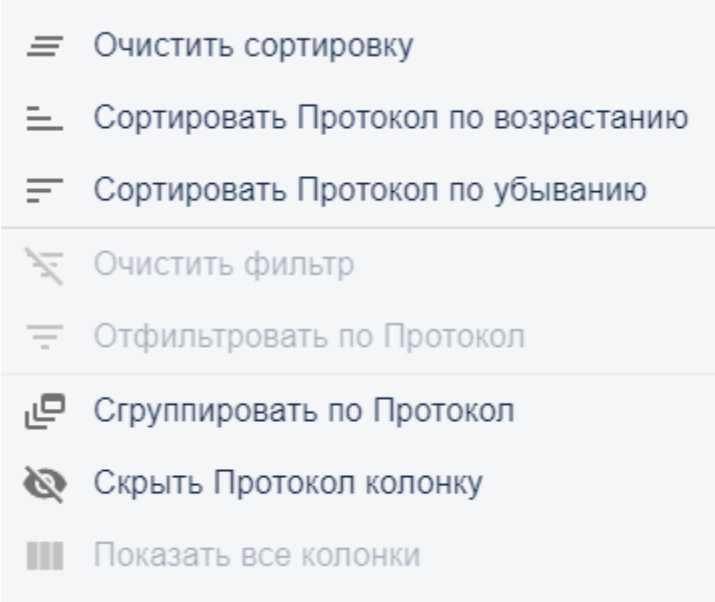


Рисунок 5.21 – Основные действия, которые можно совершить с колонкой

При нажатии на кнопку  в колонке «**Адрес источника**» откроется окно с информацией о потоке (рис. 6.6).

В правом верхнем углу окна размещена кнопка  , при нажатии на которую можно скачать в формате *pdf* всю информацию с данного окна.

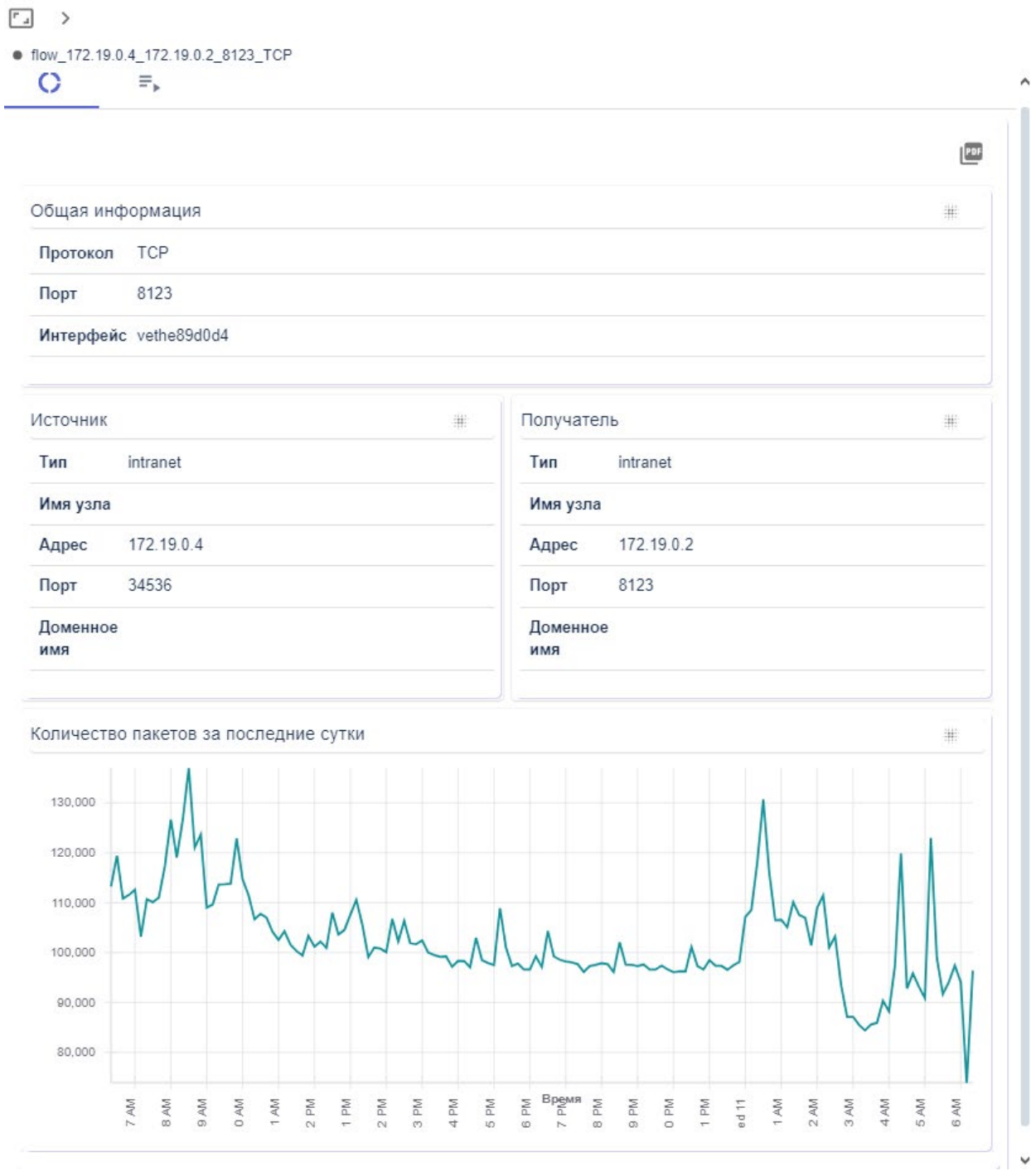


Рисунок 5.22 – Информация о выбранном потоке

Таблица «**Общая информация**» состоит из:

- протокол – транспортный протокол потока;
- порт – сетевой порт назначения;
- интерфейс – сетевой интерфейс устройства, через который обнаружен поток.

Таблица «**Источник**» показывает информацию об источнике формирования потока и состоит из:

- тип – категория, под которую попадает устройство, формирующее поток;
- имя узла – наименование устройства, формирующего поток;
- адрес – *ip* адрес сетевого устройства, которое является источником потока;
- порт – источник, формирующий поток;
- доменное имя – доменное имя устройства, которое является источником потока.

Таблица «**Получатель**» показывает информацию об устройстве назначения сформированного потока и состоит из:

- тип – категория, под которую попадает устройство, принимающее поток;
- имя узла – наименование устройства, принимающее поток;
- адрес – *ip* адрес сетевого устройства, которое является получателем потока;
- порт – получатель, сформированного потока;
- доменное имя – доменное имя устройства, которое является получателем потока.

На линейной диаграмме «**Количество пакетов за последние сутки**» представлена зависимость количества пакетов от времени. При нажатии на кнопку можно изменить вид линейной диаграммы на табличный (рис 6.7).

Количество пакетов за последние сутки

Время	Количество пакетов
10-09-24 06:20:00	113236
10-09-24 06:30:00	119440
10-09-24 06:40:00	110817
10-09-24 06:50:00	111546
10-09-24 07:00:00	112618
10-09-24 07:10:00	103229
10-09-24 07:20:00	110662
10-09-24 07:30:00	110111
10-09-24 07:40:00	111014
10-09-24 07:50:00	117267
10-09-24 08:00:00	126674
10-09-24 08:10:00	119092

Рисунок 5.23 – Таблица «Количество пакетов за последние сутки»

При нажатии на кнопку вверху окна с информацией о потоке откроется второе окно, в котором представлена информация о потоке в виде *json* (рис.6.8).

Рисунок 5.24 – Информация о потоке в виде *json*

При нажатии на кнопку  в колонке «**Адрес источника**» или «**Адрес назначения**» откроется окно с информацией об узле. На данный момент представлено 5 типов узлов: *local, intranet, external, docker* и *server*.

Тип узла *local* – узел, находящийся непосредственно на машине (программа, установленная на компьютере). При нажатии на кнопку «**Информация об узле**» появится окно (рис. 6.9) со следующими данными:

- *ID* узла – идентификатор узла в системе (узел:*ip* адрес);
- *IP*-адрес – *ip* адрес узла;
- интерфейс – название сетевого интерфейса;
- интерфейс – имя внутренней сети;
- наименование сети – идентификатор хост агента, который отследил поток;
- хост-агент владелец – имя хост агента (по умолчанию идентификатор);
- домены – домены внутри этой сети;
- параметры – дополнительные параметры, которые можно вручную настроить или добавить в настройках.

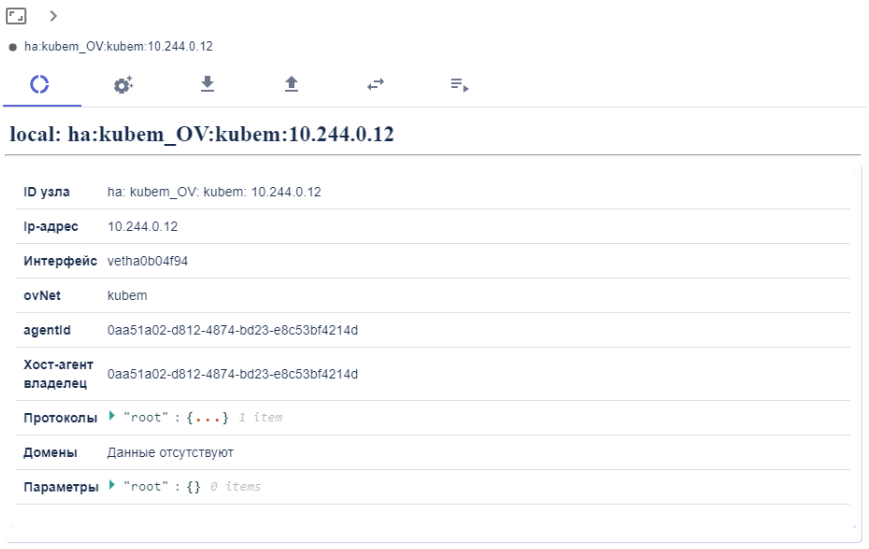


Рисунок 5.25 – Информация об узле типа *local*

Тип узла *intranet* – узел, находящийся во внутренней сети (компьютер из локальной сети, который имеет доступ к сети интернет). При нажатии на кнопку «**Информация об узле**» появится окно (рис. 6.10) со следующими данными:

- *ID* узла – идентификатор узла в системе (узел:*ip* адрес);
- *IP*-адрес – *ip* адрес узла;
- интерфейс – название сетевого интерфейса;
- *agentid* – идентификатор хост агента, который отследил поток;

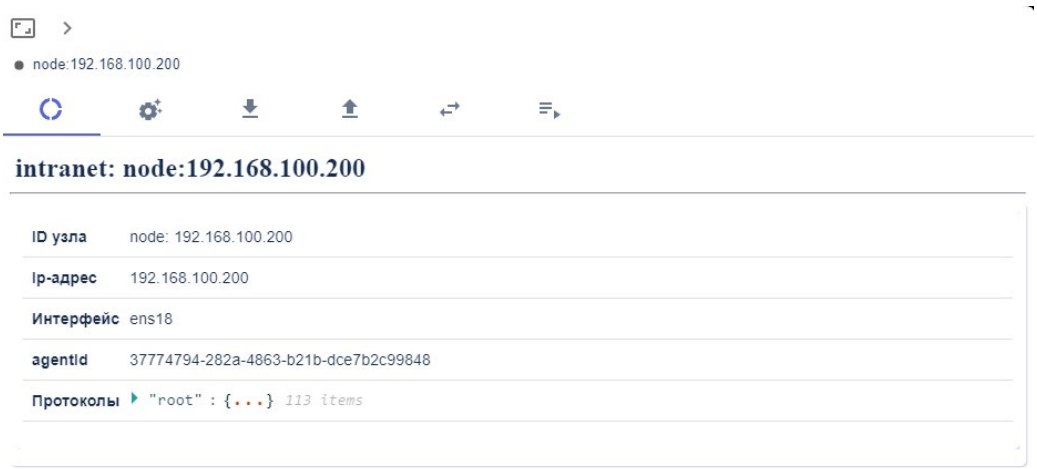


Рисунок 5.26 – Информация об узле типа *intranet*

Тип узла *external* – узел, находящийся во внешней сети (источник потоков, находящийся за пределами локального периметра в сети интернет). При нажатии на кнопку «**Информация об узле**» появится окно (рис. 6.11) со следующими данными:

- *id* – идентификатор узла в системе (узел:*ip* адрес);
- адрес – *ip* адрес, по которому было обращение;
- домен(ы) – домен(ы), к которым обращались;
- протокол – протокол, который использовался;
- время – дата и время, когда было зарегистрировано обращение;

- последнее обращение – идентификатор, показывающий когда последний раз обращались.

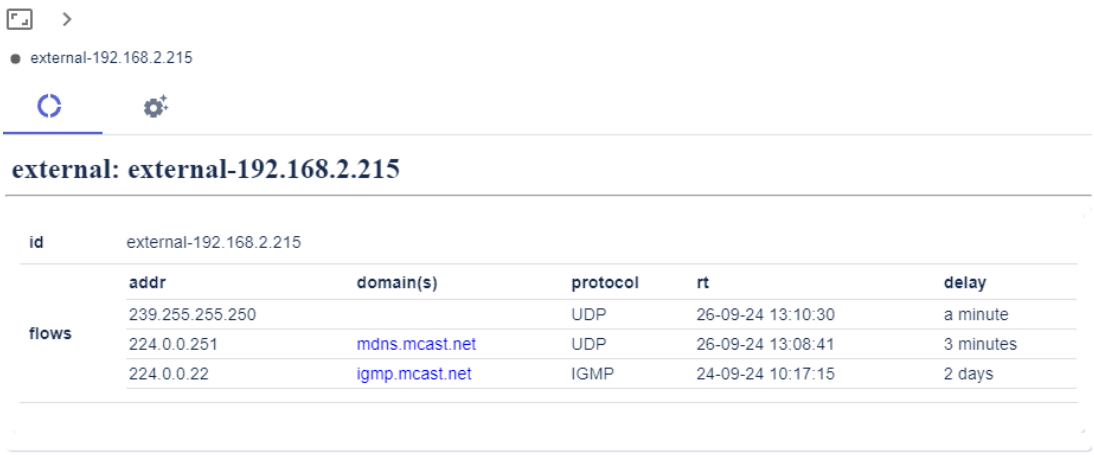


Рисунок 5.27 – Информация об узле типа *external*

Тип узла *docker* – докер контейнер, находящийся на устройстве во внутренней сети. При нажатии на кнопку «**Информация об узле**» появится окно (рис. 6.12) со следующими данными:

- наименование – наименование контейнера;
- владелец (ОС) ;
- владелец (*host*);
- путь – оболочка для запуска контейнера;
- аргументы – параметры, переданные в оболочку для запуска контейнера (файл для запуска);
- статус – запущен или остановлен контейнер;
- создано – дата и время создания контейнера;
- время запуска – время запуска контейнера;
- метки – дополнительная информация об контейнере (откуда запущен, образ контейнера и т.д.)
- сетевые настройки – сетевые настройки контейнера в виде json;
- *agentid* – идентификатор хост агента, который отследил поток;

Рисунок 5.28 – Информация о выбранном узле типа *docker*

Тип узла *server* – сервер или любое устройство, на котором находится хост агент. При нажатии на кнопку «**Информация об узле**» появится окно (рис. 6.13) со следующими данными:

- операционная система – установленная операционная система;
- архитектура – архитектура центрального процессора;
- имя хоста – доменное имя сервера (задаётся при установке операционной системы);
- процессы – список запущенных процессов, где:
  - *pid* – идентификатор процесса;
  - протокол – протокол используемый процессом;
  - порт – порт используемый или прослушиваемый процессом;
  - адрес – адрес, который слушает этот процесс;
  - имя – имя процесса;
  - *cpu* – нарузка процесса;
- ссылки – список сетевых интерфейсов, где:

- интерфейс – сетевой интерфейс;
- тип – тип интерфейса;
- mac – mac адрес интерфейса;
- адрес – *ip* адрес интерфейса (*ipV4*/маска и *ipV6*/маска);

- докер контейнеры – список работающих на сервере *docker* контейнеров;
- ресурсы – ресурсы операционной системы, где:
  - загрузка процессора – загрузка серверного процессора;
  - общий объём памяти –объём памяти ОЗУ;
  - использованный объём памяти – сколько памяти ОЗУ занято;
  - свободный объём памяти – свободное количество оперативной памяти;
  - доступный объём памяти – объём памяти, который система может использовать;
  - чтение диска – количество операций вывода;
  - запись диска – количество операций ввода.

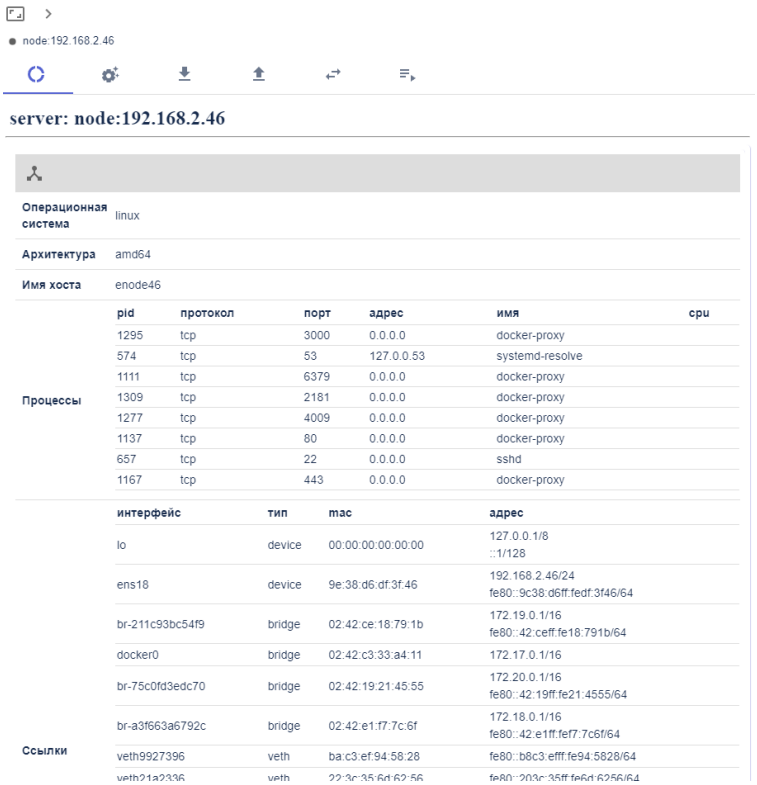


Рисунок 5.29– Информация о выбранном узле типа *server*

При нажатии на кнопку  вверху окна с информацией об узле откроется окно с настройками, в котором можно связать узел и приложение (рис 6.14) (для создания приложения необходимо пройти из главного меню в *Настройки* → *Приложения*, см раздел 11.2), а также задать узлу тип (для создания приложения необходимо пройти из главного меню в *Настройки* → *Типы узлов*, см раздел 11.3)

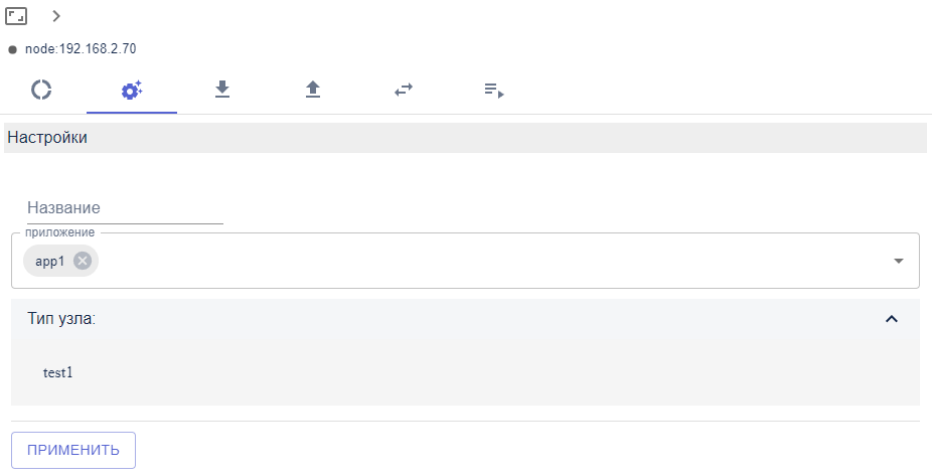


Рисунок 5.30 – Окно с настройками узла

При нажатии на кнопку  откроется окно со всеми входящими потоками (рис 6.15), где:

- время – время обнаружения потока;
- порт назначения – сетевой порт назначения;
- адрес источника – *ip* адрес сетевого устройства, который является источником потока;
- адрес назначения – ip адрес сетевого устройства, который является назначением потока;
- протокол – транспортный протокол потока;
- размер – размер в байтах данных, проходящих в потоке.

В верхней правой части окна представлены кнопки, предназначенные для изменения визуального представления таблицы и работе с ней, функционал данных кнопок был описан ранее (см. раздел 6).

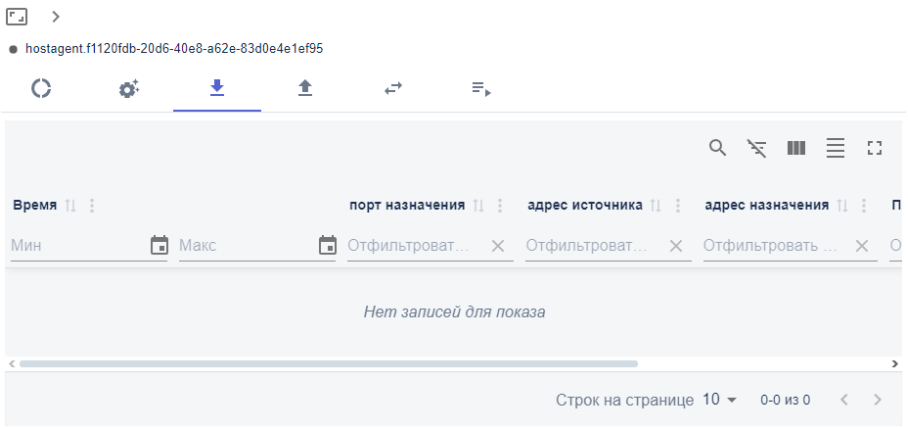


Рисунок 5.31 – Окно с входящими потоками

При нажатии на кнопку  откроется окно со всеми исходящими потоками (рис 6.16), где:

- время – время обнаружения потока;
- порт назначения - сетевой порт назначения;
- адрес источника – *ip* адрес сетевого устройства, который является источником потока;
- адрес назначения – *ip* адрес сетевого устройства, который является назначением потока;
- протокол – транспортный протокол потока;
- размер – размер в байтах данных, проходящих в потоке.

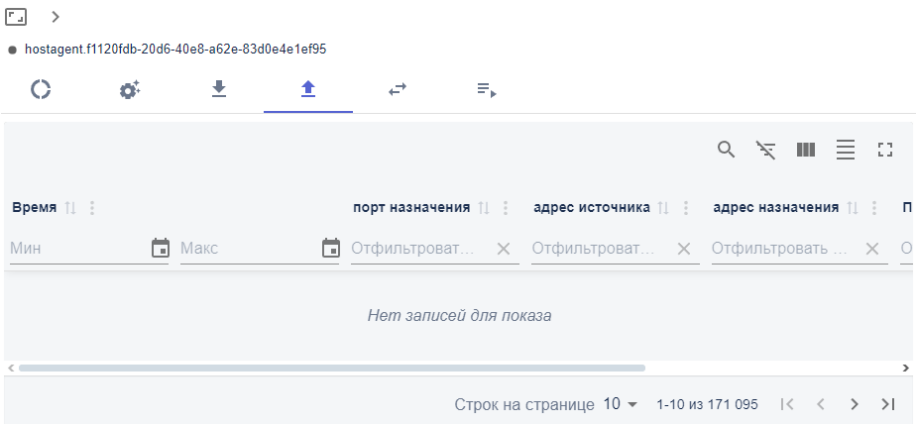


Рисунок 5.32 – Окно с исходящими потоками

При нажатии на кнопку откроется окно с информацией обо всех проходящих потоках через данный узел (рис 6.17), где:

- время – время последнего зарегистрированного пакета;
- получатель – узел назначения потока; при нажатии на кнопку можно получить информацию об узле, при нажатии на кнопку получить информацию о потоке (более подробная информация представлена в разделе 6);
- действие – создание *firewall* правило на блокировку потока; при нажатии на кнопку Block можно заблокировать выбранный поток (для просмотра и редактирования заблокированных потоков необходимо пройти из главного меню в *Firewall → Динамические правила*, см раздел 12.4);
- источник – узел источника потока.

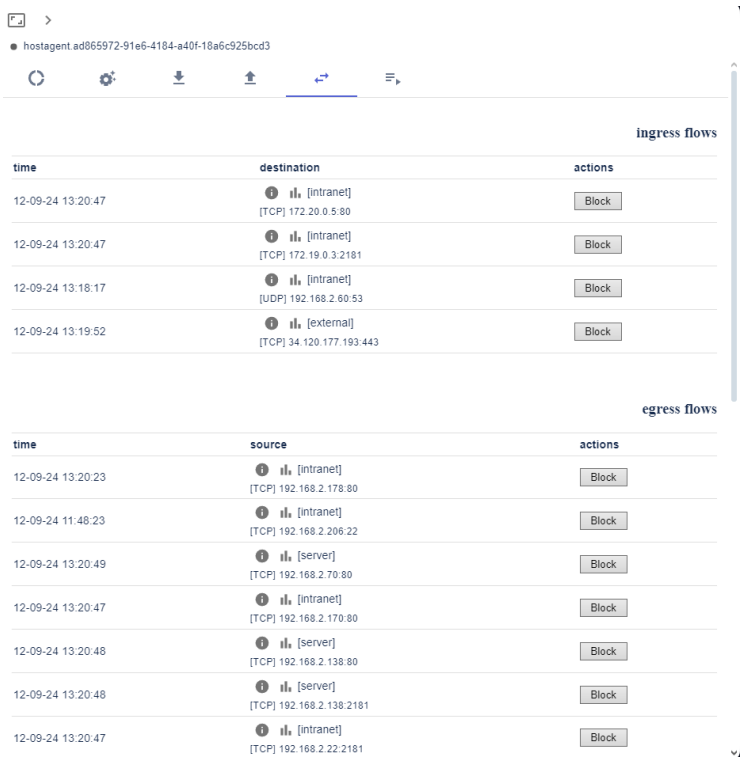


Рисунок 5.33 – Окно с информацией обо всех проходящих потоках

При нажатии на кнопку  откроется окно с информацией о выбранном узле в виде *json* (рис 7.10).

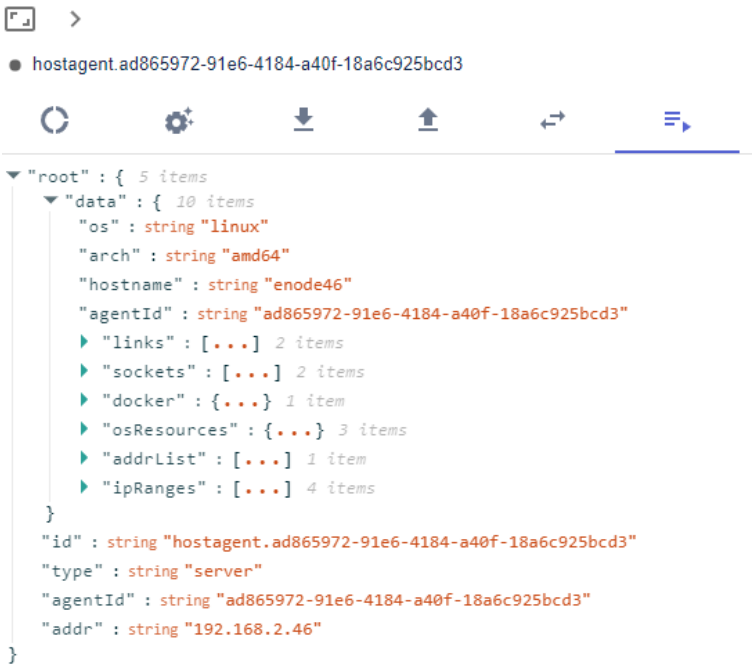


Рисунок 5.34 – Информация о выбранном узле в виде *json*

5.3. Вкладка Карты сети

Данная вкладка показывает прохождение всех потоков, зарегистрированных хост агентами. На карте непосредственно представлены хост агенты, которые установлены на операционные системы (компьютеры), они передают данные на систему управления. На 1 уровне показываются только потоки между серверами, где установлены хост агенты.

В верхней левой части экрана представлены основные кнопки, предназначенные для взаимодействия с данной вкладкой (рис. 7.1).

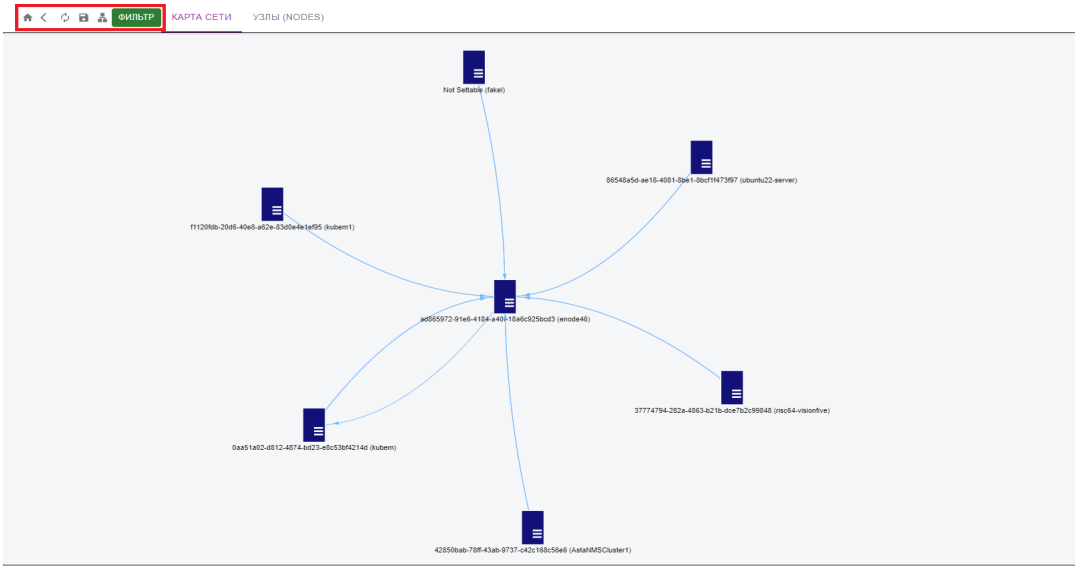


Рисунок 7.1 – Основные кнопки для взаимодействия со вкладкой "Карты сети"

Кнопка предназначена для того, вернуться на начальную страницу вкладки «**Карта сети**»;

Кнопка предназначена для того, чтобы вернуться на предыдущий уровень;

Кнопка предназначена для того, чтобы обновить список доступных агентов.

Кнопка  предназначена для того, чтобы сохранить текущее отображение.

Кнопка  предназначена для того, чтобы показать таблицу с отчётом по сетевой информации агентов (рис. 7.2).

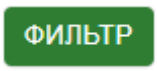
Сетевая информация хост агентов

agent id	описание	Операционная система	Интерфейс	Mac адрес	Адрес	Доменное имя
Not Settable	Not Settable	linux	lo	00:00:00:00:00:00	127.0.0.1; fe80::200:ff:fe00:0; ::1	
Not Settable	Not Settable	linux	eth0	5c:83:cd:03:ad:9a	192.168.100.146; fe80::5e83:cdff:fe03:ad9a	
Not Settable	Not Settable	linux	eth1	5c:83:cd:03:ad:9b	fe80::5e83:cdff:fe03:ad9b	
Not Settable	Not Settable	linux	eth2	5c:83:cd:03:ad:9c	fe80::5e83:cdff:fe03:ad9c	
Not Settable	Not Settable	linux	eth3	5c:83:cd:03:ad:9d	fe80::5e83:cdff:fe03:ad9d	
Not Settable	Not Settable	linux	eth4	5c:83:cd:03:ad:9e	fe80::5e83:cdff:fe03:ad9e	
Not Settable	Not Settable	linux	eth5	5c:83:cd:03:ad:9f	fe80::5e83:cdff:fe03:ad9f	
Not Settable	Not Settable	linux	eth6	5c:83:cd:03:ad:a0	fe80::5e83:cdff:fe03:ada0	
Not Settable	Not Settable	linux	eth7	5c:83:cd:03:ad:a1	fe80::5e83:cdff:fe03:ada1	
Not Settable	Not Settable	linux	pim6reg	00:00:00:00:00:00		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	lo	00:00:00:00:00:00	127.0.0.1; ::1	
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	enp5s0	22:48:4d:06:d2:b8		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	ens4f0	50:7c:6f:3b:f9:5c		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	ens4f1	50:7c:6f:3b:f9:5d		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	vmbr0	22:48:4d:06:d2:b8	192.168.2.18; fe80::2048:4dff:fe06:d2b8	
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	tap100i0	f6:67:b4:43:c9:7a		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	fwbr100i0	2e:f6:55:fe:47:65		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	fwpr100p0	ae:b2:f3:aa:38:41		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	fwln100i0	4e:3f:68:85:be:1d		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	vmbr1	50:7c:6f:3b:f9:5d	192.168.12.2; fe80::527c:6fff:fe3b:f95d	
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	tap122i0	e6:a8:ba:d2:1c:af		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	fwbr122i0	36:1c:36:36:93:fb		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	fwpr122p0	02:cb:fc:d6:9e:41		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	fwln122i0	f2:a2:64:6b:96:7e		
03000200-0400-0500-0006-000700080010	03000200-0400-0500-0006-000700080010	linux	tap122i1	5e:a2:2a:fe:88:52		

Рисунок 7.2 – Сетевая информация хост агентов

Данная таблица состоит из следующих колонок:

- *agent id* – идентификатор хост агента, который передаёт нам информацию;
- описание – имя хост агента;
- операционная система – установленная операционная система;
- интерфейс – наименование сетевого интерфейса;
- mac адрес – физический адрес интерфейса;
- адрес – *ip* адрес, установленный на сетевом интерфейсе;
- доменное имя – доменное наименование.

При нажатии на кнопку 

вызывается окно (рис. 7.3) в котором можно отфильтровать потоки конкретного приложения, находящегося на определённом хосте.

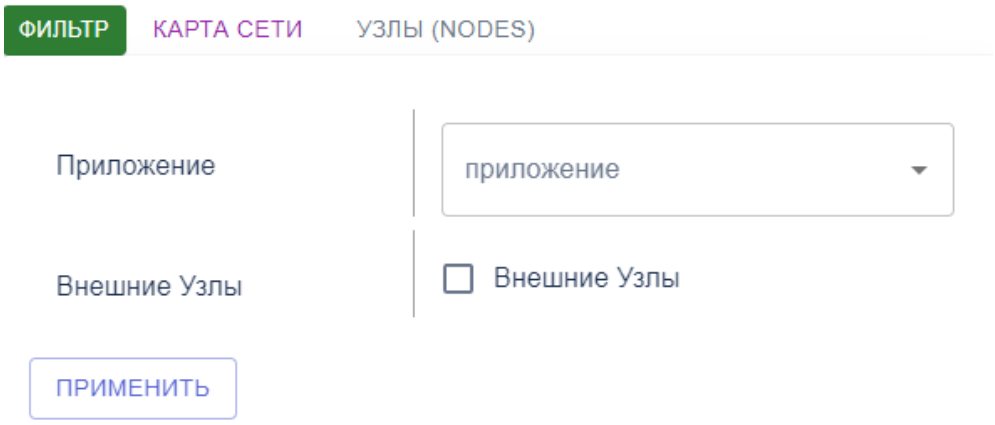


Рисунок 7.3 – Окно фильтра

При нажатии правой кнопкой мыши на любую из имеющихся иконок сервера (рис. 7.4) откроется окно с выбором следующих функций: показать подробности, показать детализацию потоков и показать информацию об узле Первые два пункта были подробно расписаны ранее (см. раздел 6). При нажатии левой кнопки мыши на любую из имеющихся иконок сервера откроется окно с подробной информацией об узле типа *server*.

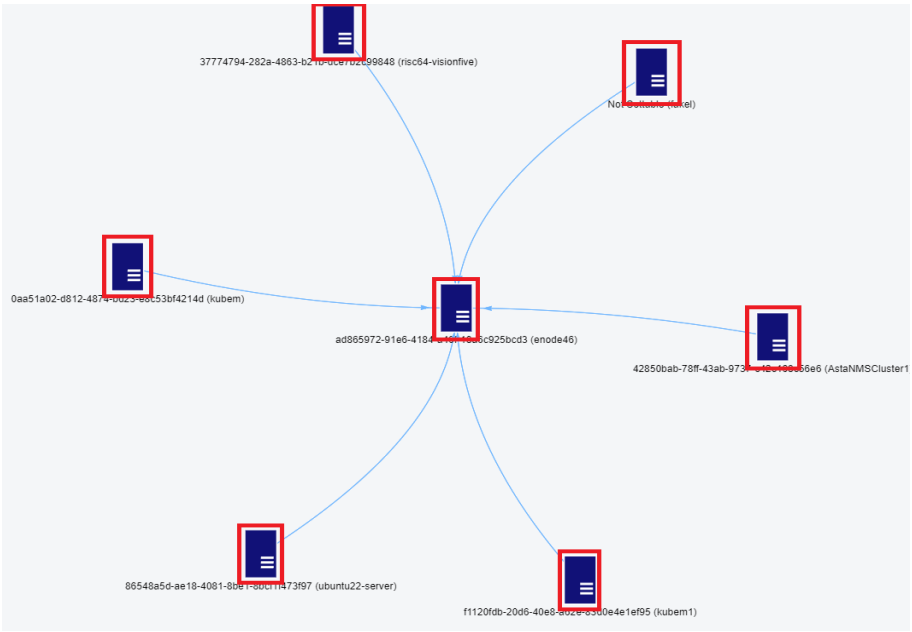


Рисунок 7.4 – Иконки серверов

При нажатии на стрелку с направление потока (рис. 7.5) откроется окно с подробной информацией о потоках (рис. 7.6). Информация о данном окне подробно расписана в разделе 6 данного руководства.

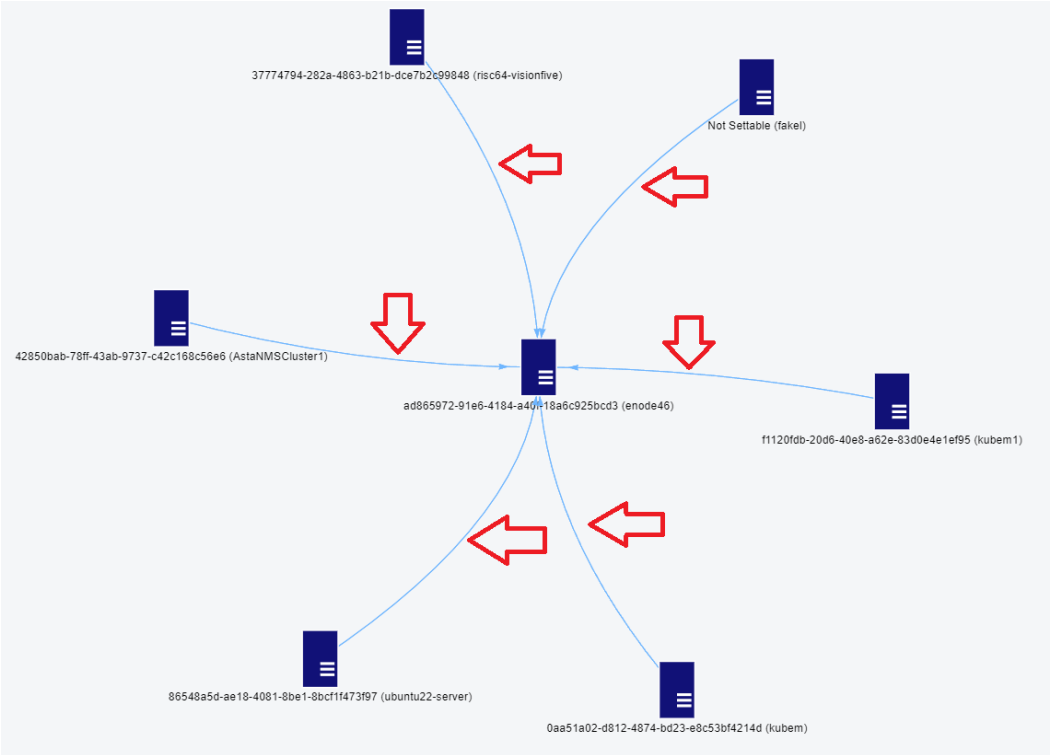


Рисунок 7.5 – Направление и движение потоков от узла к узлу

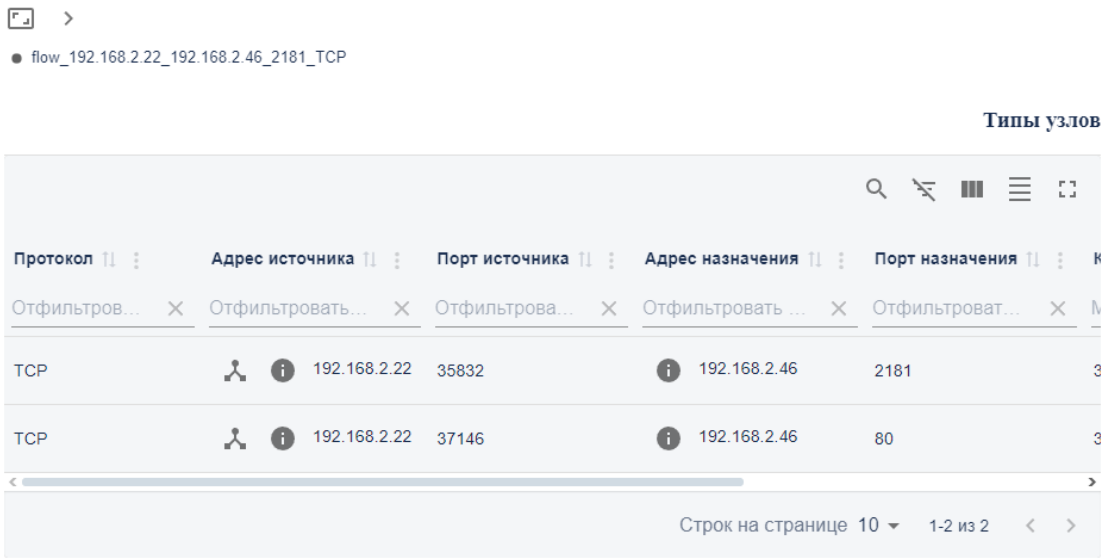


Рисунок 7.6 – Окно с информацией о типе узлов

При нажатии на вкладку «**УЗЛЫ (*NODES*)**» в табличном виде будет представлена информация об узлах с установленными агентами (рис. 7.7).

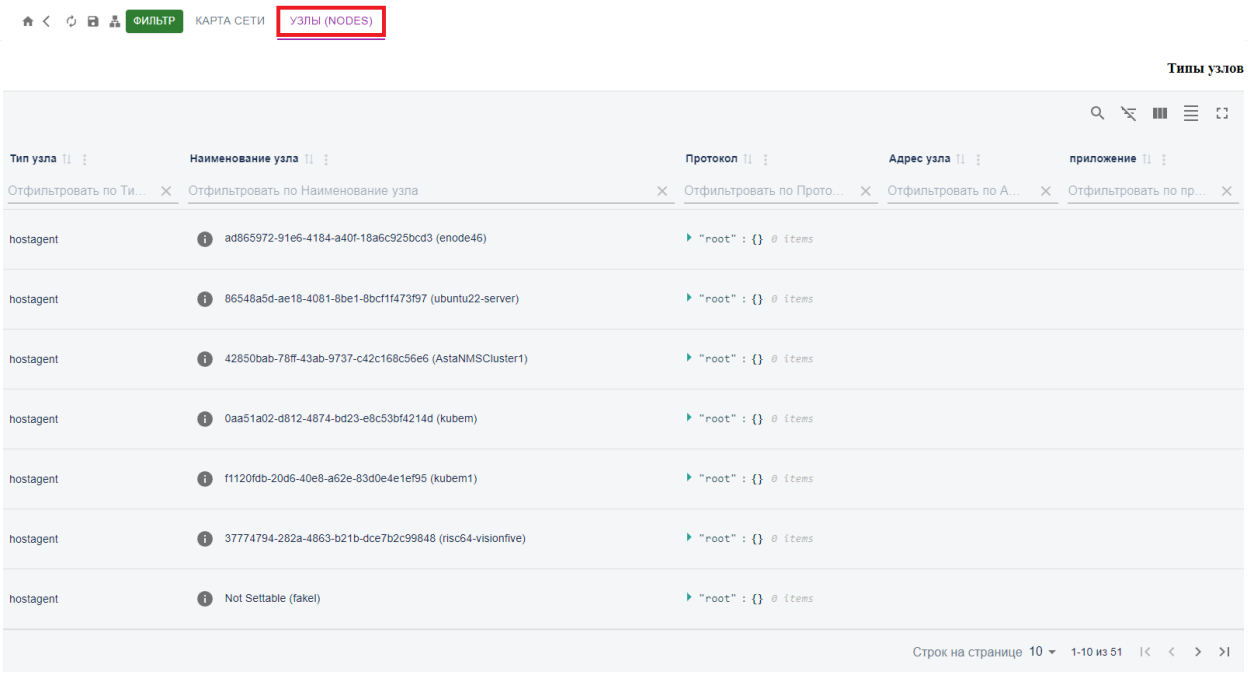


Рисунок 7.7 – Вкладка "УЗЛЫ (NODES)"

При нажатии правой кнопкой мыши на иконку сервера (рис. 7.4) и выборе пункта «**Показать подробности**», мы попадаем во внутрь устройства (на второй уровень) и видим потоки, которые находятся внутри (рис. 7.8). На данном уровне показываются потоки между следующими типами узлов: *server*, *docker* и *local*. При нажатии правой кнопкой мыши на любой из данный типов узлов откроется окно с выбором следующих функций: показать детализацию потоков, показать информацию об узле и создать узловую схему. Первые два пункта были подробно расписаны ранее (см. раздел 6). При выборе пункта «**Создать узловую схему**» будет создана схема (третий уровень), в которой показаны взаимодействия со всеми существующими типами узлов: *server, docker, local, external* и *intranet* (рис. 7.9).

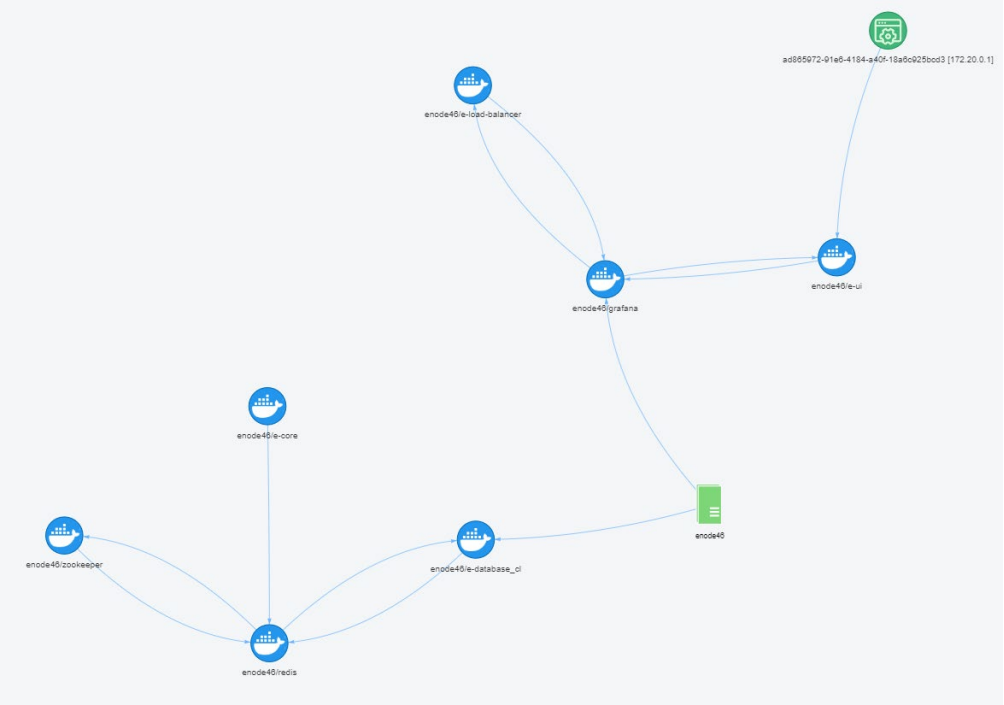


Рисунок 7.8 – Схема потоков внутри устройства (2 уровень)

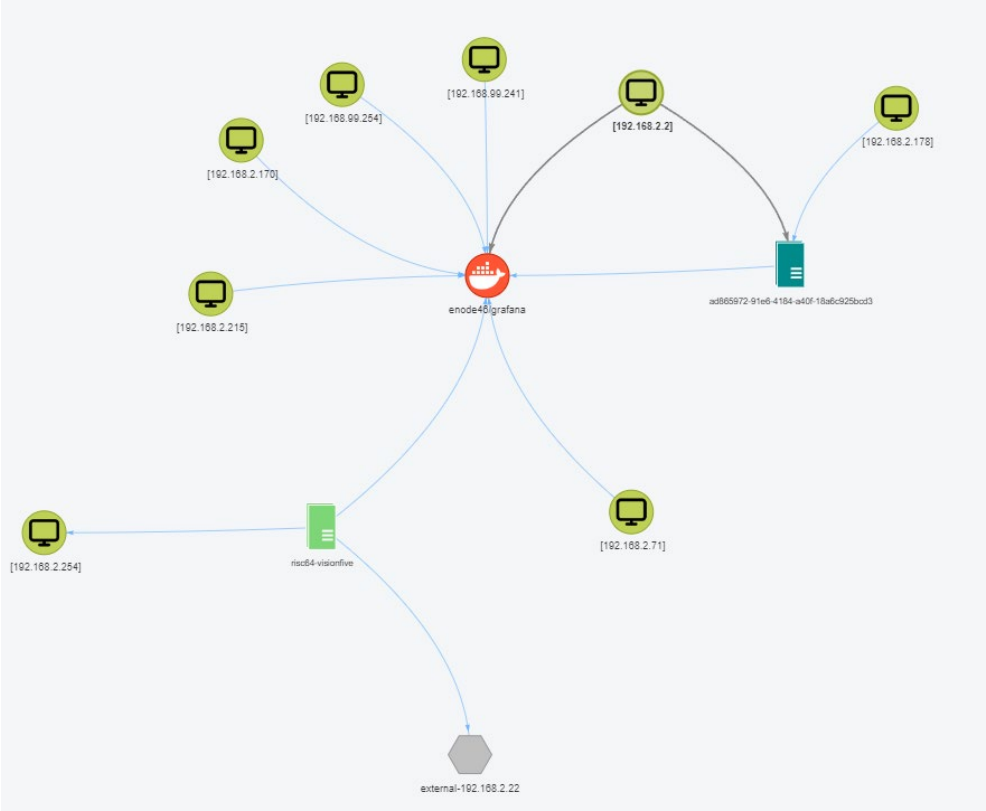


Рисунок 7.9 – Узловая схема всех потоков (3 уровень)

Для удобства отображения тёмно-зелёным выделяется сервер, при нажатии на который можно отобразить на узловой схеме его внутренние потки (рис. 7.10), красным цветом выделяется тип узла, от которого была построена узловая схема. На рисунке 7.11 представлены иконки и их значения со всех схем (1,2 и 3 уровни).

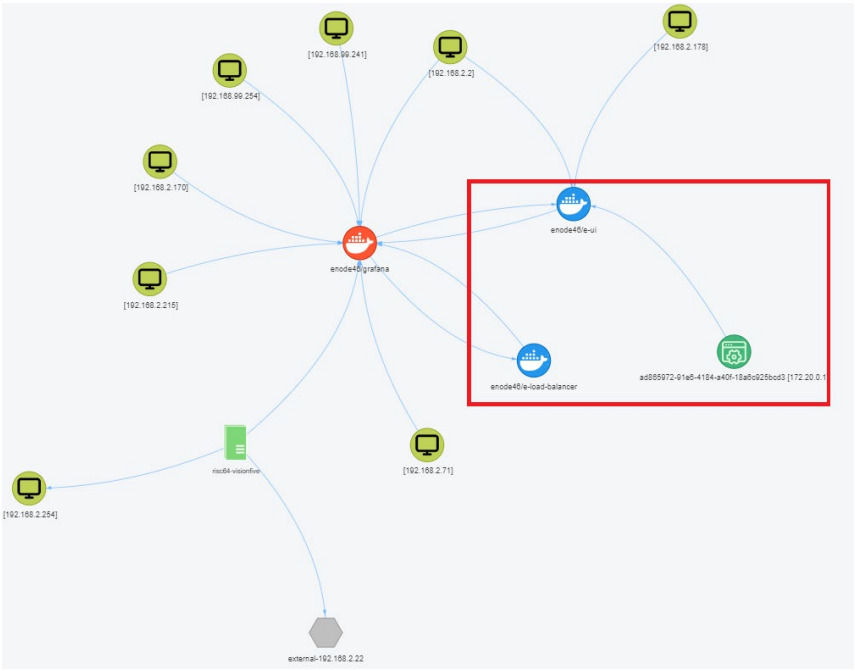


Рисунок 7.10 – Пример отображения внутренних потоков устройства на узловой схеме

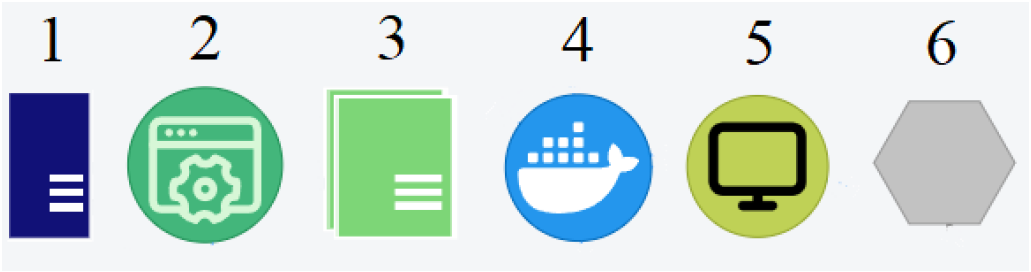


Рисунок 7.11 – Основные обозначения на схемах, где:
1 – сервер с установленным хост агентом (1 уровень);
2 – узел типа local (2 и 3 уровни);
3 – узел типа server (2 и 3 уровни);
4 – узле типа docker (2 и 3 уровни);
5 – узел типа intranet (3 уровень);
6 – узел типа external (3 уровень).

5.4. Вкладка Отчёты

Данная вкладка предназначена для формирования отчётов. При нажатии на кнопку «**Параметры отчёта**» (рис.8.1) откроется окно с фильтром настройки, где можно настроить диапазон времени (начало и конец) и выбрать тип интересующего отчёта. Доступны следующие типы:

- статистика по типам узлов;
- новые потоки;
- топ узлов источников (по количеству трафика);
- топ узлов назначения (по количеству трафика);
- топ потоков (по количеству трафика);
- топ узлов назначения (по количеству трафика по потокам).

После выбора типа отчёта и диапазона времени необходимо нажать на кнопку «**Применить**», после чего будет сформирован отчёт (рис. 8.2).

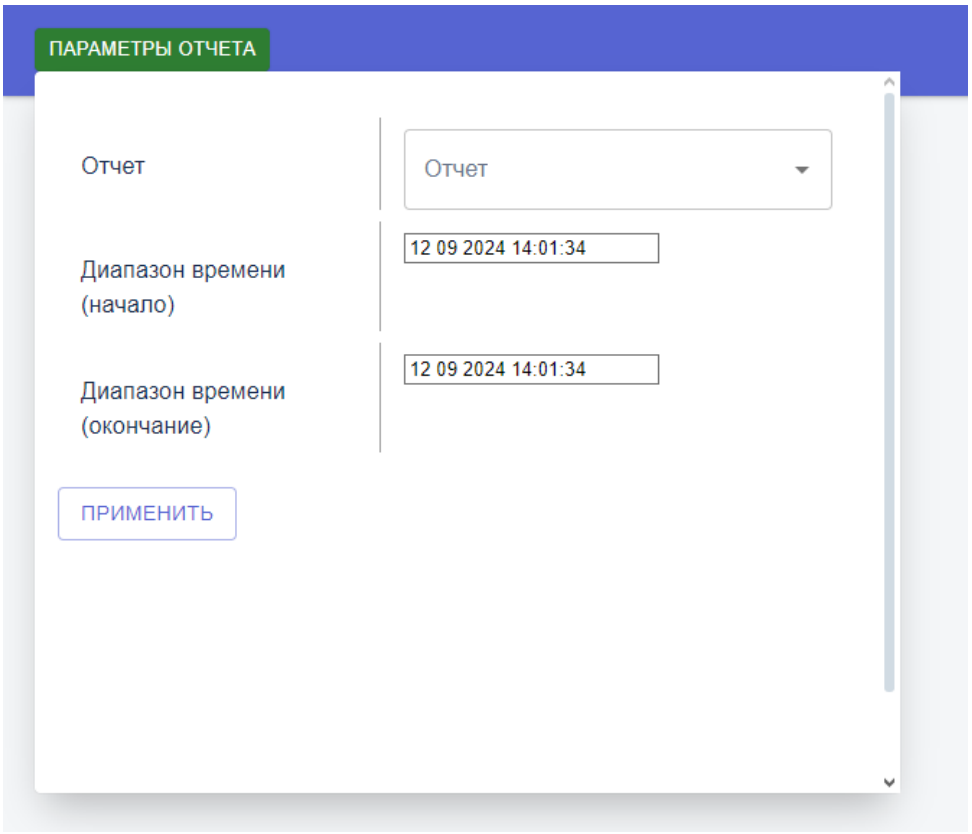


Рисунок 8.1- Параметры отчёта

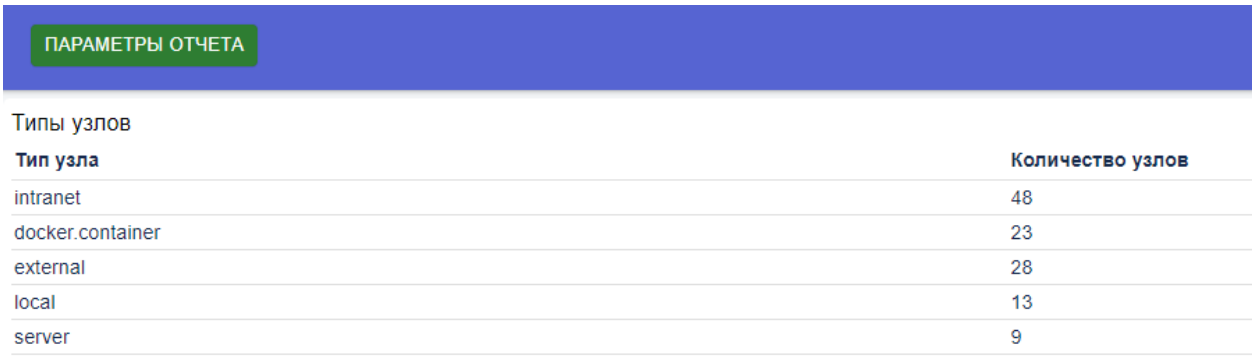


Рисунок 8.2 – Сформированный отчёт «Статистика по типам узлов»

5.5. Вкладка Пользователи

Данная вкладка предназначена для создания (рис 9.1), редактирования и удаления пользователей Системы. На главной странице показаны уже созданные пользователи (рис 9.2), а также информация о них:

- создан – дата и время создания пользователя;
- имя пользователя;
- пароль пользователя;
- роль – роль пользователя (администратор, менеджер, читатель);
- телеграмм отправка команд – отправка команд в *telegram* группу;
- почта – *email* адрес для отправки событий;
- телеграмм приём сообщений – приём сообщений из *telegram* группы;
- телеграмм *chat id* – id группы *telegram*, для рассылки событий;
- действия – кнопка для редактирования пользователя.

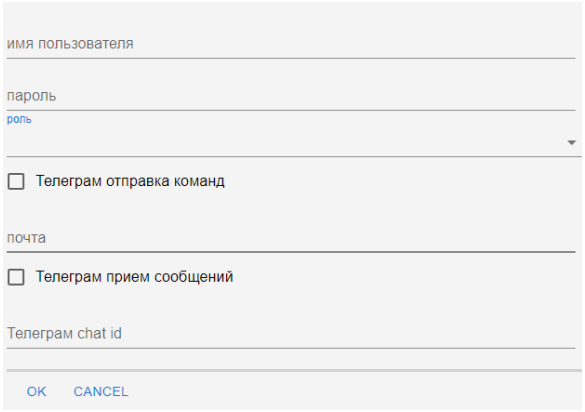


Рисунок 9.1 – Окно для создания нового пользователя

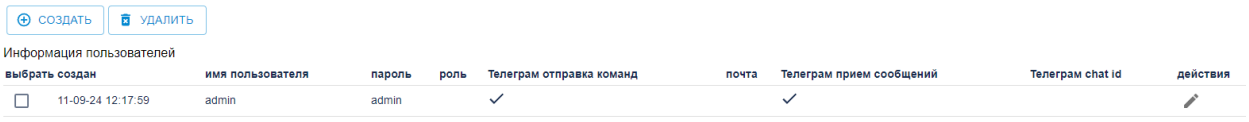


Рисунок 9.2 –Страница с информацией о созданных пользователях

5.6. Вкладка Дерево объектов

В данной вкладке представлена информация об элементах программы в виде *json*, информация берётся из базы данных. Структура вкладки представляет собой древовидную структуру. Например, есть узел *users* и есть его подузлы *user* и *admin* (рис. 10.1) . Данная вкладка необходима только для отображения информации, которая может быть полезна администратору.

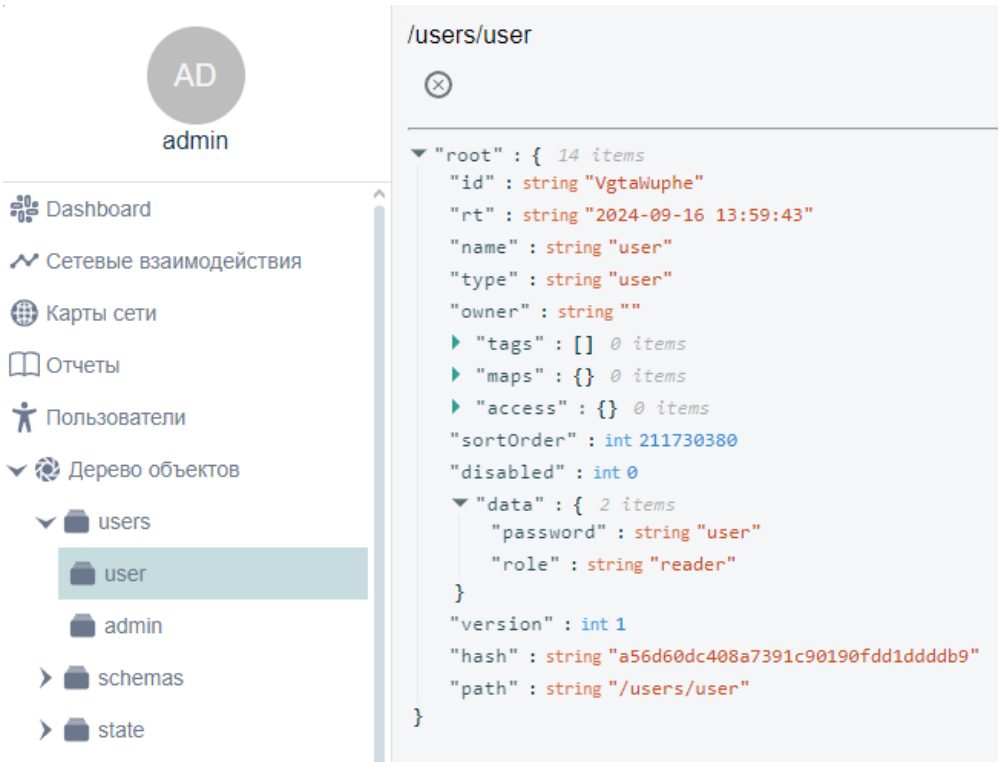


Рисунок 10.1 – Вкладка Дерево объектов

5.7. Вкладка Настройки

В данной вкладке представлены настройки агентов и системы управления просмотра и редактирования. Настройки делятся на подразделы.

5.7.1. Раздел Агенты

В данном разделе отображаются статусы всех агентов, установленных на удалённых узлах и добавленных в систему управления. Также представлены подразделы, связанные с удалённой и локальной установкой агентов на узлы.

Hostagent – микросервис, устанавливаемый на целые узлы для мониторинга. Передача конфигураций модулю производится через систему распределенных конфигураций. Все метрики и события передаются в централизованную систему управления.

Функции:

- сбор метрик о работе операционной системы (процессы, загрузка, использование ресурсов);
- сбор метрик о работе каналов связи: точка – точка, качество, количество сбоев, задержки, пропускная способность;
- сбор информации о всех сетевых пакетах на всех интерфейсах;
- применение правил межсетевого экрана;
- сбор информации о системах виртуализации;
- реализация функций *Policy Based Routing*на уровне *eBPF*;
- мониторинг состояния сетевых интерфейсов.

В центре страницы раздела «**Агенты**» находится таблица – панель управления агентами (рис 11.1), состоящая из следующих столбцов:

- выбрать – поле для группового управления;
- время создания – время добавления агента в систему управления;
- описание – наименование агента;
- активность – наличие связи между агентом и системой управления;
- конфигурация – наличие загруженной конфигурации в агент;

- правила – наличие *firewall* правил;
- ошибка – наличие ошибок;
- адрес хоста – ip адрес устройства;
- действия – кнопка редактирования.

выбрать	время создания	описание	активность	конфигурация	правила	ошибка	адрес хоста	действия
☐	13-09-24 12:03:04	03000200-0400-0500-0006-000700080010	активен	принято	не задано	-	-	✎
☐	13-09-24 12:03:04	0aa51a02-d812-4874-bd23-e8c53bf4214d	активен	принято	не задано	-	192.168.2.70	✎
☐	13-09-24 12:03:04	37774794-282a-4863-b21b-dce7b2c99848	активен	принято	не задано	-	192.168.2.22	✎
☐	13-09-24 12:03:04	42850bab-78ff-43ab-9737-c42c168c56e6	активен	не задано	не задано	-	192.168.2.138	✎
☐	13-09-24 12:03:04	86548a5d-ae18-4081-8be1-8bcf1f473f97	активен	не задано	не задано	-	192.168.2.170	✎
☐	13-09-24 12:03:04	Not Settable	активен	не задано	не задано	-	192.168.99.254	✎
☐	13-09-24 12:03:04	ad865972-91e6-4184-a40f-18a6c925bcd3	активен	принято	не задано	-	192.168.2.46	✎
☐	13-09-24 12:03:04	f1120fdb-20d6-40e8-a62e-83d0e4e1ef95	активен	не задано	не задано	-	192.168.2.71	✎

Рисунок 11.1 – Панель управления агентами

Выше данной таблицы расположены кнопки для изменения визуального представления таблицы и работе с ней (рис. 11.2).

С помощью поля «**Фильтр**» можно отфильтровать таблицу по искомому значению.

С помощью поля «**Сортировка по**» можно произвести сортировку таблицы по имени агента и времени его создания.

Кнопка «**Обновить**» необходима для обновления информации в таблице, кнопка «**Удалить**» для удаления выделенных агентов.

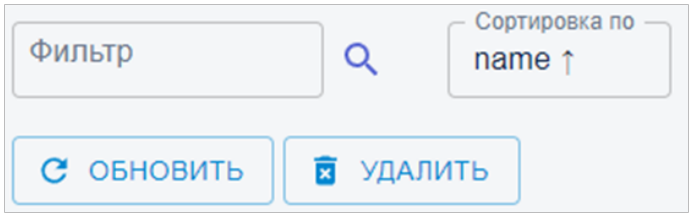


Рисунок 11.2 – Кнопки для визуального представления таблицы и работе с ней

При нажатии на кнопку  на панели управления агентами откроется окно, в котором можно редактировать выбранного агента (рис. 11.3) и посмотреть информацию о нём (рис 11.4 -11.5).

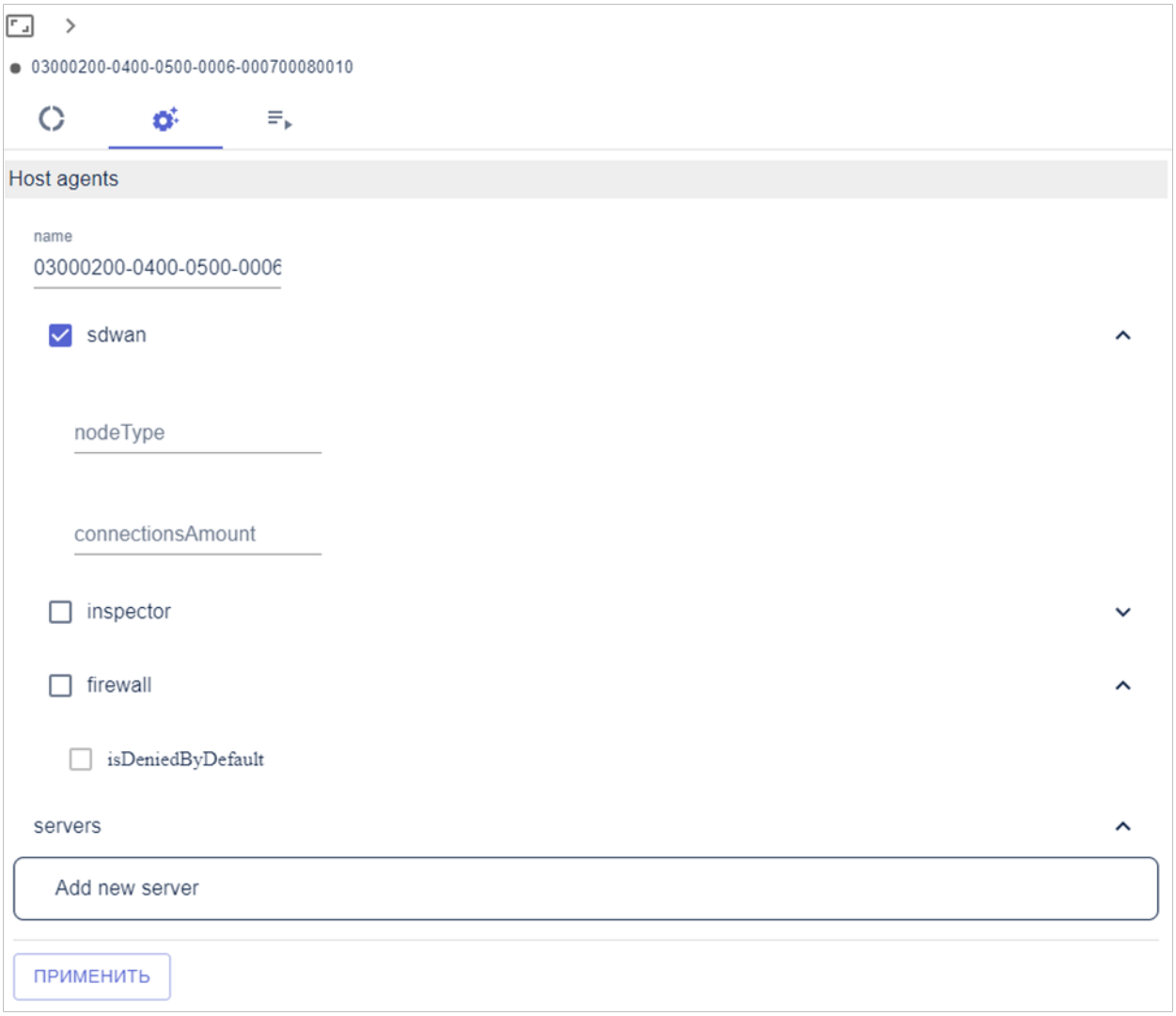


Рисунок 11.3 – Окно редактирования агента

Рисунок 11.4 – Информация об агенте

В информации об агенте представлено:

- описание - наименование агента;
- активность - наличие связи между агентом и системой управления;
- адрес хоста - *ip* адрес устройства;
- *configData* – конфигурация агента, которая настраивается во вкладке «**Настройки**».

Рисунок 11.5 - Информация об агенте в виде *json*

Ниже панели работы с агентами расположены кнопки для удалённой установки агента (рис. 11. 6) и ручной загрузки агента (рис. 11.7).

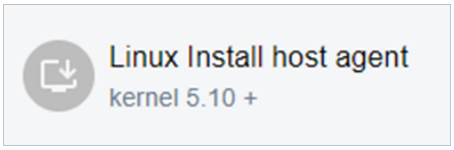


Рисунок 11.6 – Кнопка для удалённой установки агента

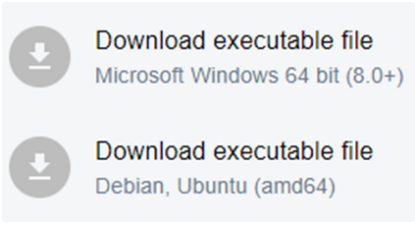


Рисунок 11.7 – Кнопки для ручной загрузки агента

Для подключения к удалённому узлу потребуется ввести следующие параметры (рис. 11.8):

- *address (ip) for ssh* – адрес узла, на котором необходимо произвести установку агента. На этом узле должен быть запущен *SSH*-сервер для подключения;
- *ssh user* – пользователь для подключения к узлу (используется протокол *SSH*);
- *ssh* password – пароль для подключения к узлу (используется протокол *SSH*).

Рисунок 11.8 – Подключение к удалённому узлу

Установка агента вручную производится путём скачивания файла и отдельно конфигурации для узла. Необходимо учитывать, что при совпадении конфигураций на разных узлах будет опрашиваться только первый узел. Даже при отключении первого агента – второй может принимать информацию только после удаления пользователем первого агента с аналогичной конфигурацией (аналогичным *ID* агента).

5.7.2. Раздел Приложения

В данном разделе производится просмотр, редактирование, создание и удаление приложений (рис. 11.10), где:

- выбрать – поле для группового управления;
- создано – дата и время создания приложения;
- наименование – наименование приложения;
- описание – описание приложения;
- действия – кнопка редактирования.

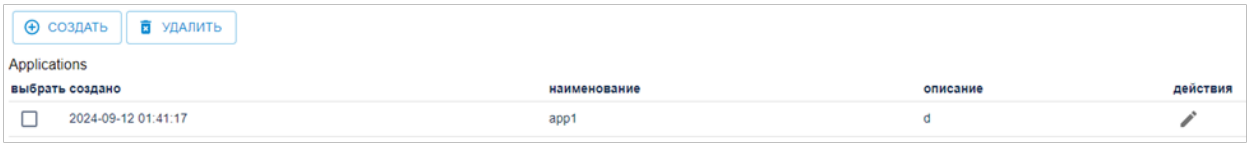


Рисунок 11.10 – Панель управления приложениями

При нажатии на кнопку появляется окно редактирования приложения (рис.11.11).

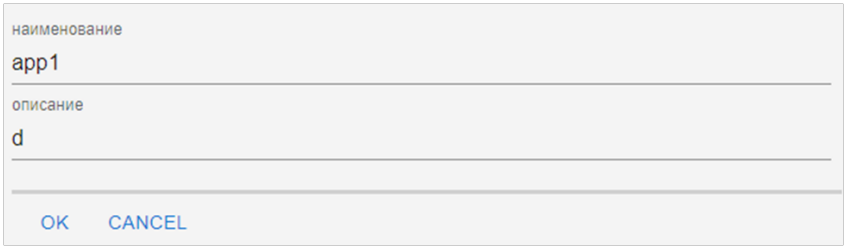


Рисунок 11.11 – Окно редактирования приложения

5.8. Раздел Типы узлов

В данном разделе можно создать типы узлов, которые в дальнейшем можно привязать к узлам, через информация об узле во вкладке «**Сетевые взаимодействия**» или «**Карта сети**» (рис. 11.12). Необходима данная функция для фильтрации узлов определённого типа.

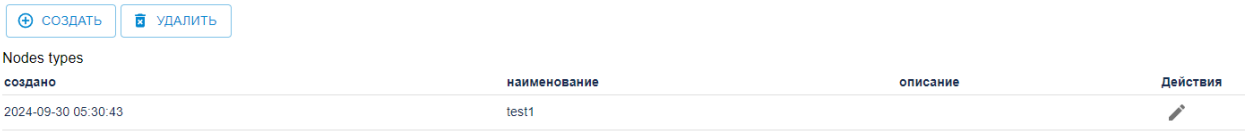


Рисунок 11.12 – Панель управления типами узлов

Раздел состоит из следующих столбцов:

- создано – дата и время создания типа узла;
- наименование – наименование типа узла;
- описание – описание типа узла;
- действия – редактирование созданного типа узла.

5.9. Раздел Игнорируемые приложения

В данном разделе находится функция, с помощью которой при построении узловой схемы, узлы, которые относятся к определённому приложению, будут скрыты на карте сети (рис. 11.13). Узлы скрываются только на узловой схеме всех потоков (3 уровень).

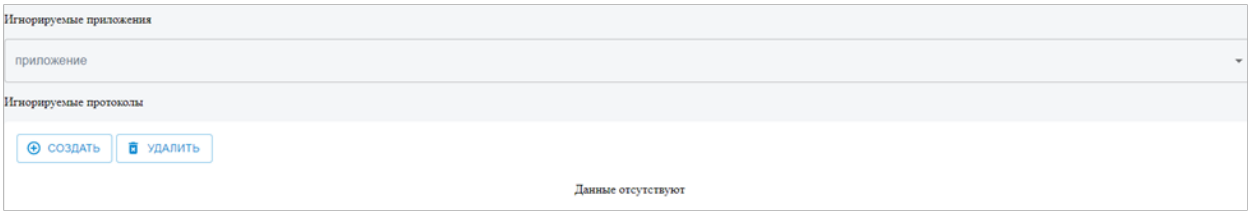


Рисунок 11.13 – Вкладка Игнорируемые приложения

5.10. Раздел Конфигурация сервера

В данном разделе производится просмотр и редактирование настроек сервера системы управления (рис. 11.14), таких как:

- наименование – имя сервера (после изменения не требует перезапуска сервера);
- внешний адрес сервера – внешний адрес сервера используется для доступа хост агентов. Именно этот адрес будет публиковаться в конфигурации хост агента для доступа к серверу (после изменения не требует перезапуска сервера);
- внутренние сети – внутренние сети компании, написанные через запятую. Как правило, используется 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16. Используются для разделения потоков информации на внешние и внутренние;
- перезапуск сервера.

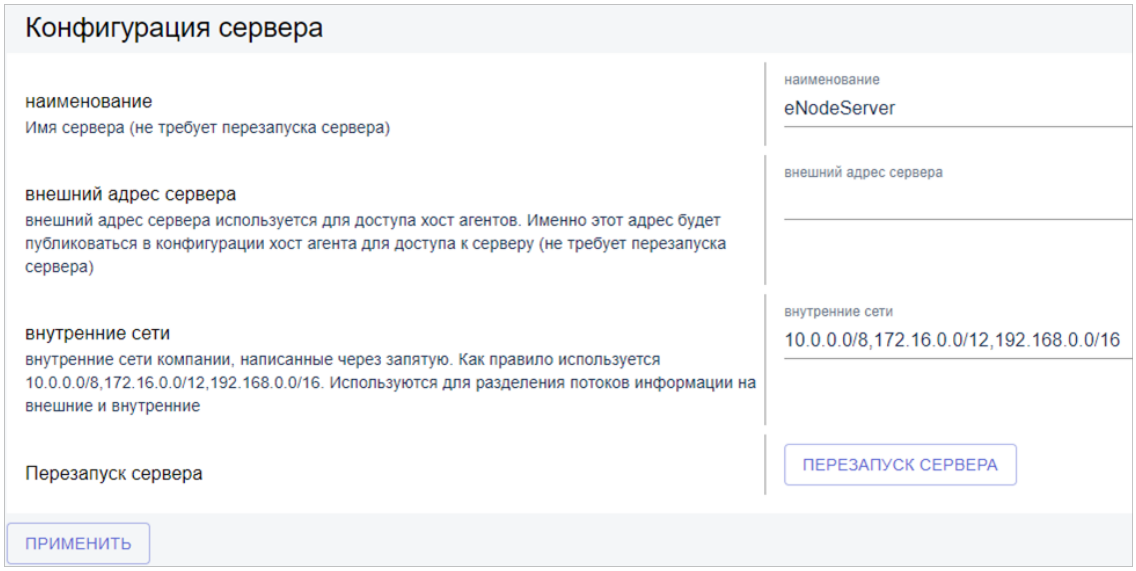


Рисунок 11.14 – Раздел Конфигурация сервера

5.11. Раздел Отправка уведомлений

В данном разделе производится просмотр и редактирование настроек отправки уведомлений (рис. 11.15), где:

- *telegram* – рассылка с использованием телеграмм бота;
- *api key* – ключ, регистрируемый на сайте *Telegram*;

- электронная почта – рассылка уведомлений с использованием электронной почты;
- *imap server* – адрес *imap* сервера получения сообщений. В системе возможность управления через сообщения;
- *smtp server* – адрес сервера отправки сообщений;
- *smtp* пароль – пароль пользователя для авторизации на почтовом сервере;
- *test* – тестовая отправка почтового сообщения.

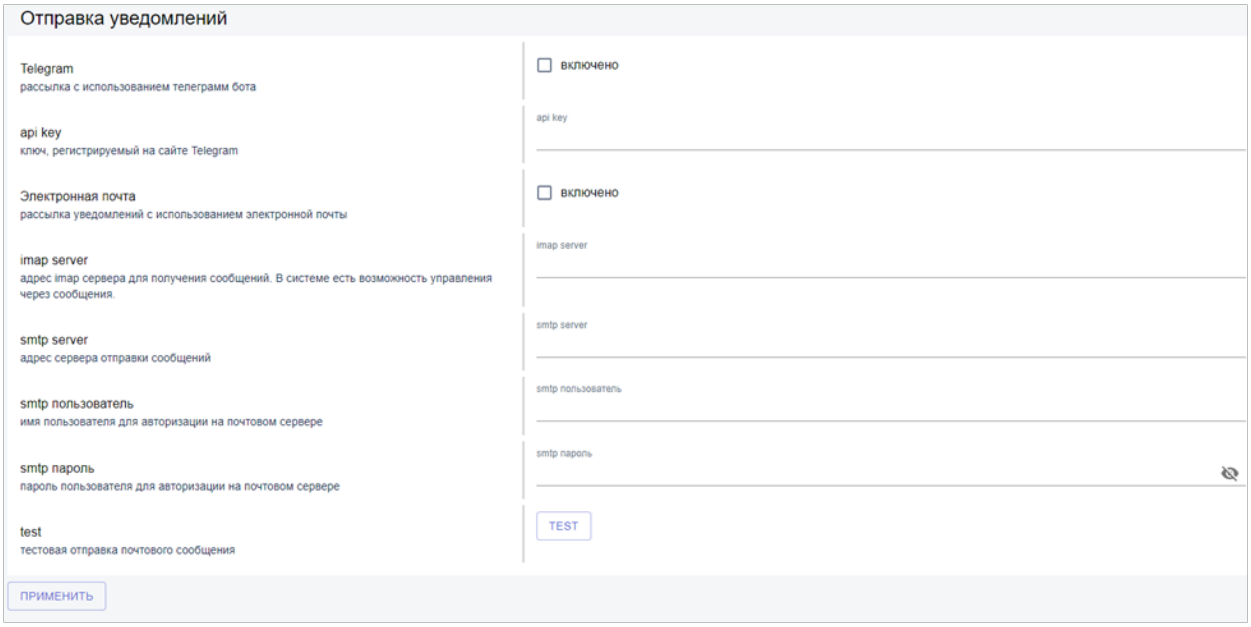


Рисунок 11.15 – Раздел Отправка уведомлений

5.12. Раздел Фильтр событий

В данном разделе находится функция, с помощью которой можно отсортировать события, находящиеся внизу экрана, при нажатии на кнопку ☰ (см. раздел 5) (рис. 11.16).

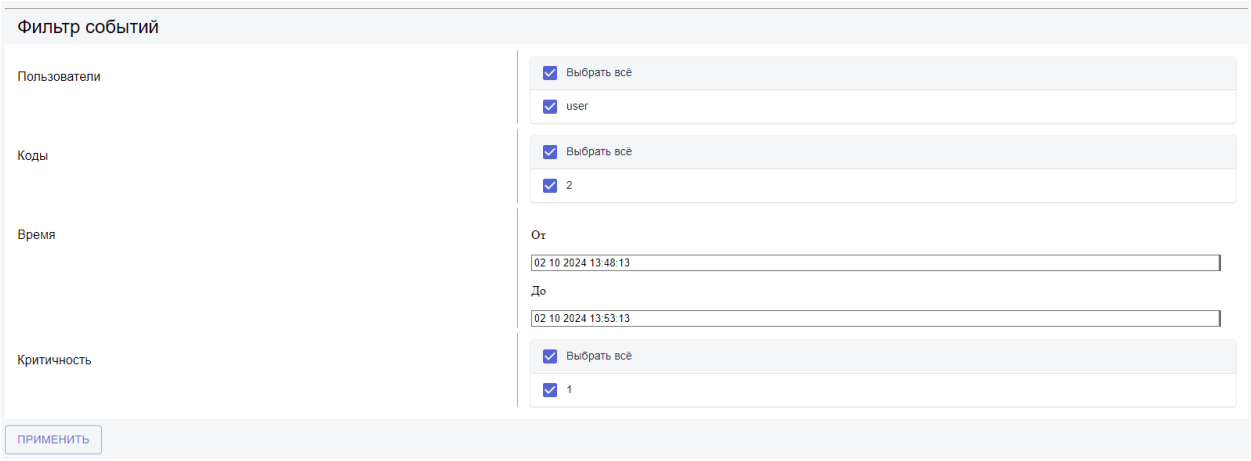


Рисунок 11.16 – Раздел Фильтр событий

5.13. Раздел Настройка хранилищ

В данном разделе производится просмотр и редактирование настроек хранилища логов, метрик, потоков и системных логов. Окно для редактирования настроек представлено на рисунке 11.17, где:

- интервал очистки – настройка интервала полной очистки хранилища (необходимо вписать число и выбрать размерность – час, день, месяц, год);
- интервал очистки с сохранением среднего – настройка очистки интервала хранилища с сохранением среднего значения (необходимо вписать число и выбрать размерность – час, день, месяц, год).

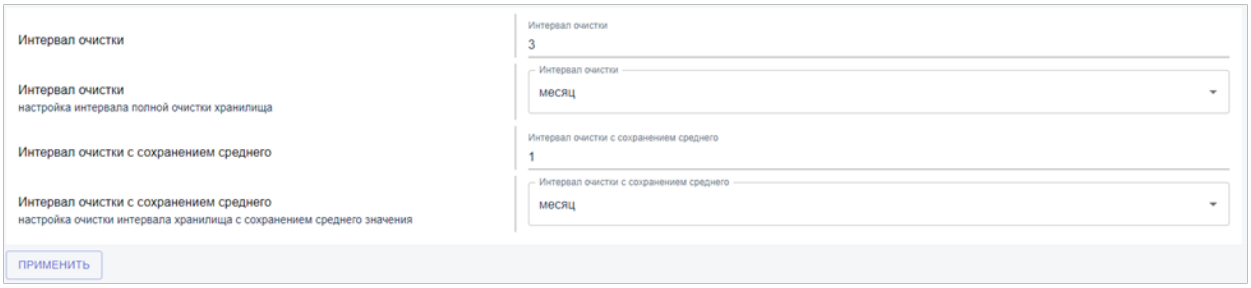


Рисунок 11.17 – Раздел Настройка хранилищ

5.14. Раздел Системные логи

В данном разделе производится просмотр и редактирование настроек сервера системных логов (рис. 11.18) и клиента системных логов (рис. 11.19).

Подраздел сервер системных логов стоит из:

- *IP* адрес – *ip* адрес системы управления;
- порт – входящий сетевой порт для получения системных логов.

Рисунок 11.18 – Подраздел Сервер системных логов

Подраздел клиент системных логов стоит из:

- *IP* адрес – *ip* адрес узла, куда следует отправлять системные логии;
- порт – входящий сетевой порт для получения системных логов;
- сохранять в базу данных – сохранять получаемые системные логи в базу данных.

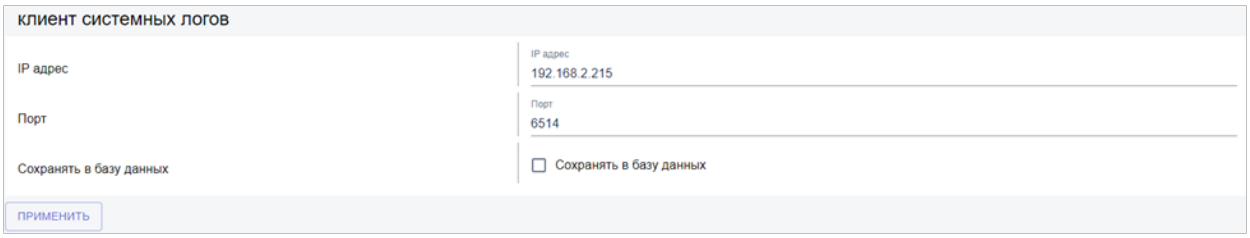


Рисунок 11.19 – Подраздел Клиент системных логов

5.15. Вкладка Firewall

В данной вкладке представлены инструменты для просмотра и редактирования правил блокировки *firewall*.

5.15.1. Раздел Статус

В данном разделе в виде графиков, диаграмм и таблиц отображены данные по статистике работы *firewall* (рис 12.1).

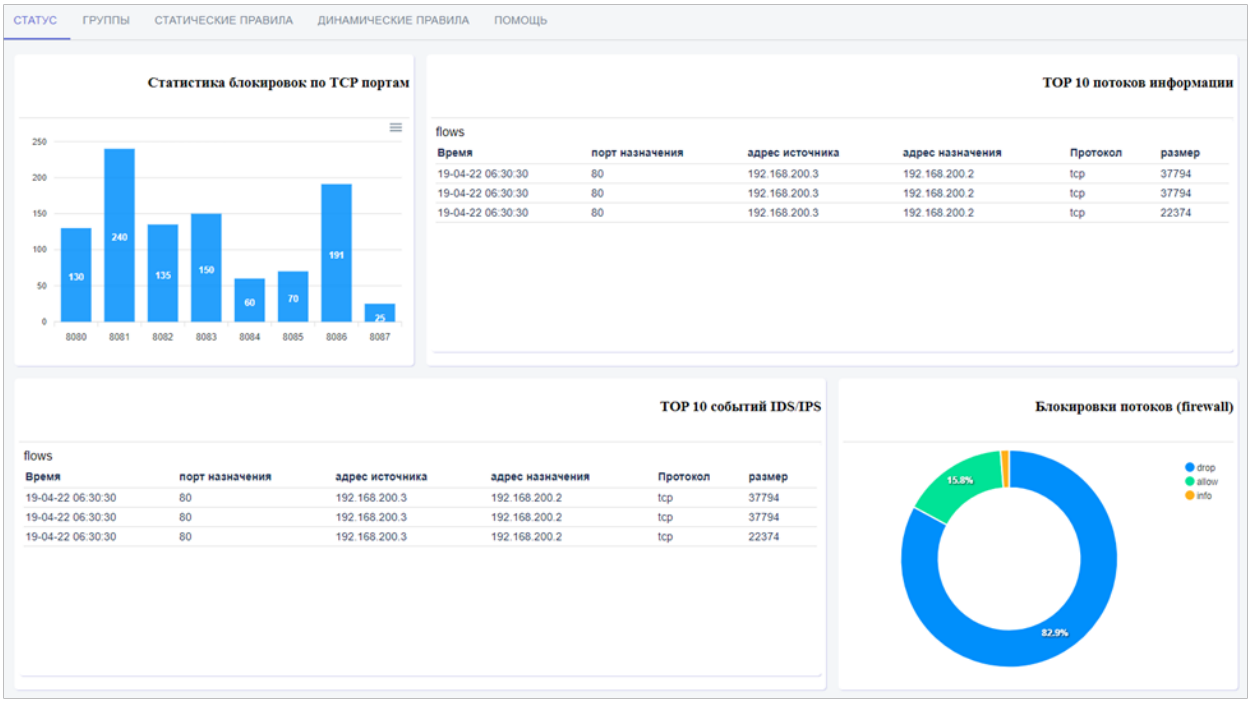


Рисунок 12.1 – Раздел Статус

В виде столбчатой диаграммы (рис 12.2) отображена статистика блокировок по портам. На оси абсцисс расположен номер сетевого порта, на оси ординат – количество блокировок. При нажатии на кнопку можно скачать данную диаграмму в формате *.SVG*, *.PNG* и *.CSV*.

Рисунок 12.2 – Столбчатая диаграмма статистики блокировок

В таблице «**Топ 10 потоков информации**» отображены 10 потоков с наибольшим размером, которые смогли отследить хост агенты (рис. 12.3), где:

- время – время фиксации потока;
- порт назначения – сетевой порт назначения;
- адрес источника – *ip* адрес сетевого устройства, который является источником потока;
- адрес назначения – *ip* адрес сетевого устройства, который является получателем потока;
- протокол - транспортный протокол потока;
- размер – размер потока.

TOP 10 потоков информации

flows

Время	порт назначения	адрес источника	адрес назначения	Протокол	размер
19-04-22 06:30:30	80	192.168.200.3	192.168.200.2	tcp	37794
19-04-22 06:30:30	80	192.168.200.3	192.168.200.2	tcp	37794
19-04-22 06:30:30	80	192.168.200.3	192.168.200.2	tcp	22374

Рисунок 12.3 – Таблица «Топ 10 потоков информации»

В виде таблицы «**Топ 10 событий IDS/IPS**» отображены случаи обнаружения вторжений и их предотвращения системой (рис 12.4), где:

- время – время фиксации потока;
- порт назначения – сетевой порт назначения;
- адрес источника – *ip* адрес сетевого устройства, который является источником потока;
- адрес назначения – *ip* адрес сетевого устройства, который является получателем потока;
- протокол - транспортный протокол потока;
- размер – размер потока.

TOP 10 событий IDS/IPS

flows

Время	порт назначения	адрес источника	адрес назначения	Протокол	размер
19-04-22 06:30:30	80	192.168.200.3	192.168.200.2	tcp	37794
19-04-22 06:30:30	80	192.168.200.3	192.168.200.2	tcp	37794
19-04-22 06:30:30	80	192.168.200.3	192.168.200.2	tcp	22374

Рисунок 12.4 – Таблица «Топ 10 событий IDS/IPS»

В виде круговой диаграммы в процентном соотношении отображены потоки, которые: *drop* – были отброшены; allow – были пропущены, info – были переназначены. (рис. 12.5).

Рисунок 12.5 – Круговая диаграмма «Блокировки потоков»

5.15.2. Раздел Группы

В данном разделе производится просмотр и редактирование *firewall* групп (рис. 12.6).

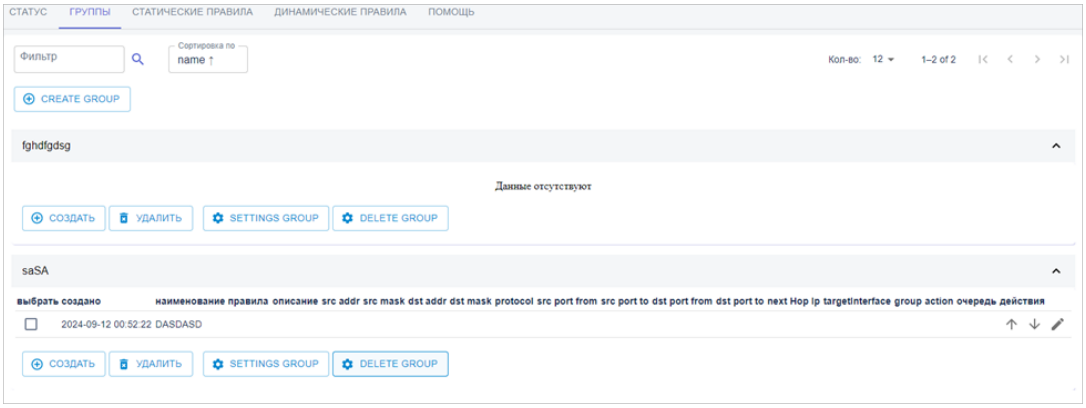


Рисунок 12.6 – Раздел «Группы»

При нажатии на кнопку «**Создать группу**» появится окно создания группы (рис.12.7), где необходимо указать:

- наименования группы;
- подробное описание группы.

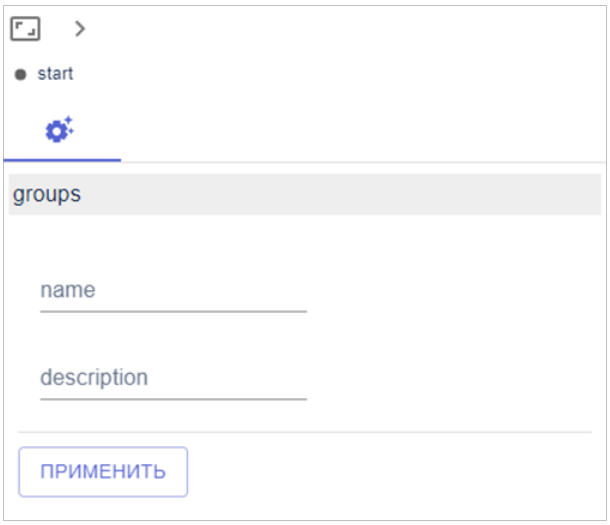


Рисунок 12.7 – Окно создания группы

При нажатии на созданную группу откроется панель с кнопками для работы с группой (рис. 12.8), где:

- создать – создать *firewall* правило;
- удалить – удалить существующее *firewall* правило;
- настройки группы – изменить наименование и описание группы;
- удалить группу – удалить созданную группу.

Рисунок 12.8 – Кнопки для работы с группой

При нажатии на кнопку «**Создать**» откроется окно (рис. 12.9), в котором необходимо прописать:

- наименование правила;
- описание – подробное описание правила;
- *IP* адрес источника – *ip* адрес узла источника потока;
- маска источника – маска подсети узла источника потока;
- *IP* адрес назначения – *ip* адрес узла назначения потока;
- маска назначения – маска подсети узла назначения потока;
- протокол – протокол обмена (необходимо выбрать из перечня);
- порт источника – исходящий сетевой порт узла источника потока;
- порт назначения – входящий сетевой порт узла источника потока;
- *IP* адрес следующего хопа – *ip* адрес узла, на который будет отправлен пакет;
- интерфейс – сетевой интерфейс на устройстве, где установлен хост агент;
- действия – действия с пакетами: отбросить пакет, перенаправить пакет (он перенаправится на адрес указанный в следующий хоп) и пропустить пакет (пакет проходит дальше к адресу назначения).

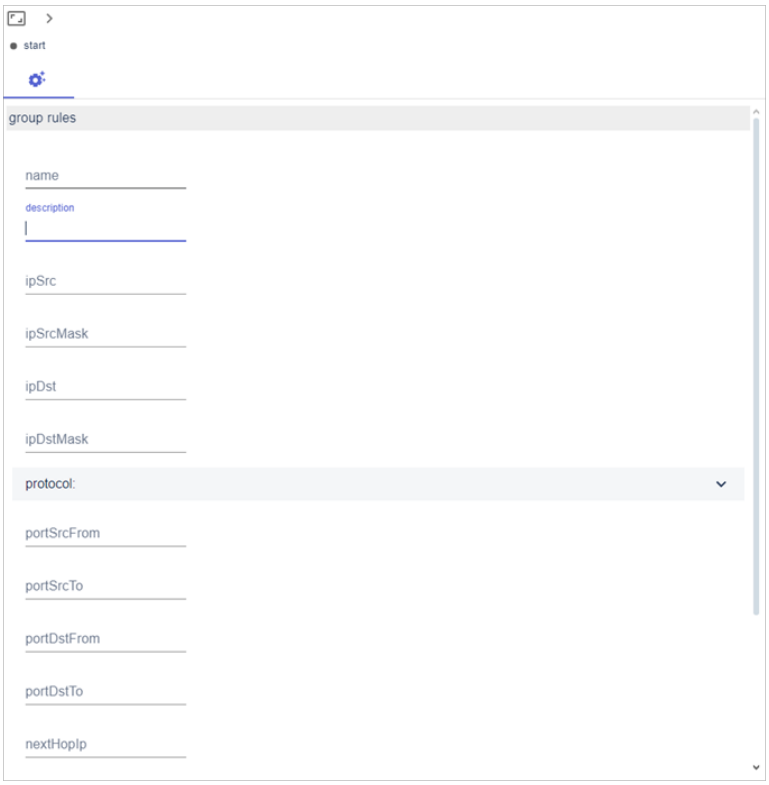


Рисунок 12.9 – Окно создания правила *firewall*

5.15.3. Раздел Статические правила

В данном разделе отображаются все хост агенты, на которые мы можем накладывать правила, созданные в предыдущем разделе, при выборе правила «**Группа**» (рис. 12.10) или задать собственное правило при выборе «**Правило**» (рис. 12.11). Для этого необходимо нажать на кнопку «**Создать**». Форма заполнения правила совпадает с формой из предыдущего раздела.

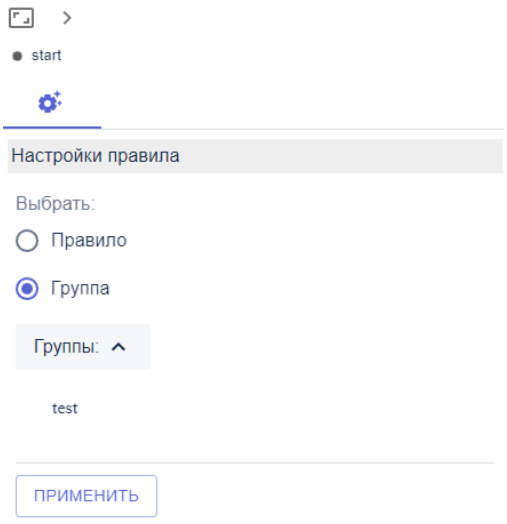


Рисунок 12.10 – Привязка созданной группы к хост агенту

Рисунок 12.11 – Создание правила для хост агента

При нажатии на кнопку «**Конфигурация**» мы можем назначит функционал, который должен выполнять данный хост агент (рис. 12.12). А также добавить новый сервер, к которому будет подключаться хост агент (для этого на сервере должен стоять **enode**).

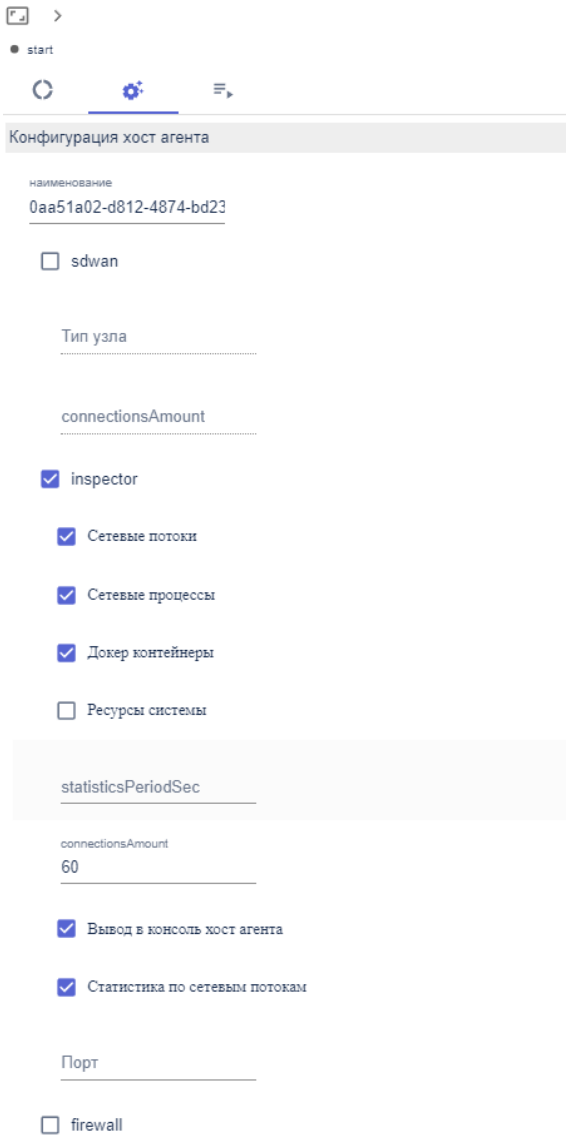


Рисунок 12.12 – Назначение конфигурации для выбранного хост агента

Роль *sdwan* – для маршрутизации (добавляются правила для перенаправления потоков), где:

- тип узла – задаётся цифрой, 1 – маршрутизирующий и 2 – не маршрутизирующий;
- *connectionsAmount* – количество соединений.

Роль inspector – для получения данных о системе и потоках (сбор информации), где:

- сетевые потоки – хост агент будет передавать информацию о сетевых потоках;

- сетевые процессы – хост агент будет передавать информацию о сетевых процессах;
- докер контейнеры – хост агент будет передовать информацию о докер контейнерах;
- ресурсы системы – хост агент будет передовать информацию о ресурсах системы, где установлен;
- вывод в консольхост агента – функция, позволяющая выводить логи хост агента в консоль (для этого хост агент должен быть установлен как сервис в операционной системе);
- статистика по сетевым потокам – хост агент будет передавать информацию по статистике потоков *firewall*.

Роль *firewall* – для фильтрации трафика (добавляются правила с действиями отбросить и пропустить), где:

- блокировать все потоки – хост агент будет блокировать абсолютно все сетевые потоки.

5.15.4. Раздел Динамические правила

В данном разделе отображаются все потоки, которые были заблокированы вручную в окне с информацией обо всех проходящих потоках через выбранный узел (рис. 12.13) (см. раздел 6).

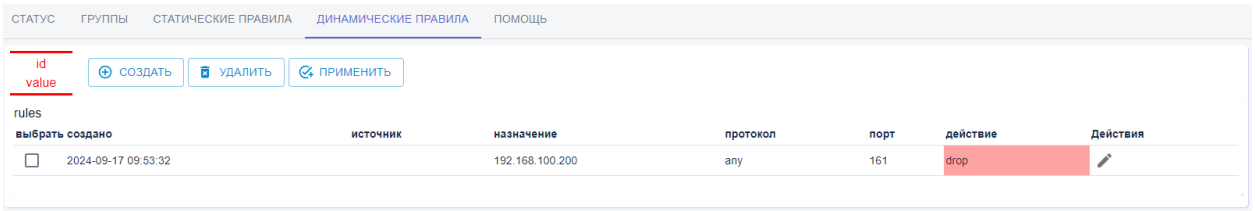


Рисунок 12.13 – Раздел динамические правила

5.15.5. Раздел Помощь

В данном разделе представлена информация, необходимая для корректного создания записи *firewall*.

5.16. Вкладка «Панель приборов»

Вкладка «Панель приборов» предназначена для отображения сводных панелей (dashboard) с консолидированной информацией о состоянии объектов мониторинга. На ней представлены ключевые показатели в виде графиков, диаграмм и счётчиков, что позволяет пользователю оперативно оценивать текущую ситуацию.

5.16.1. Счётчики событий и диаграмма

В верхней части вкладки расположена блок со счётчиками событий (Рисунок 5.2), который показывает количество событий в каждом статусе, обнаруженных Системой в процессе мониторинга. Справа от счётчиков находится круговая диаграмма (Рисунок 5.3) со статусами событий и её легенда.

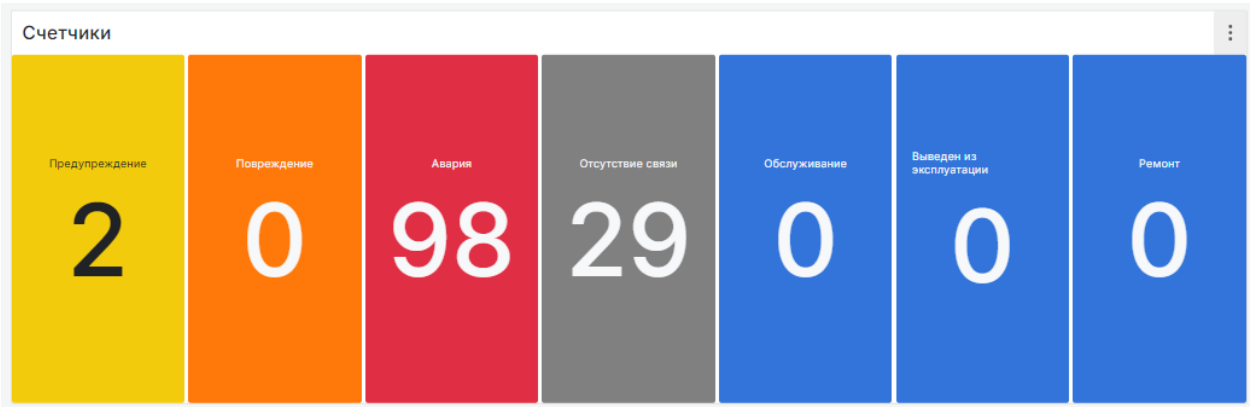


Рисунок 5.2– Счётчик событий

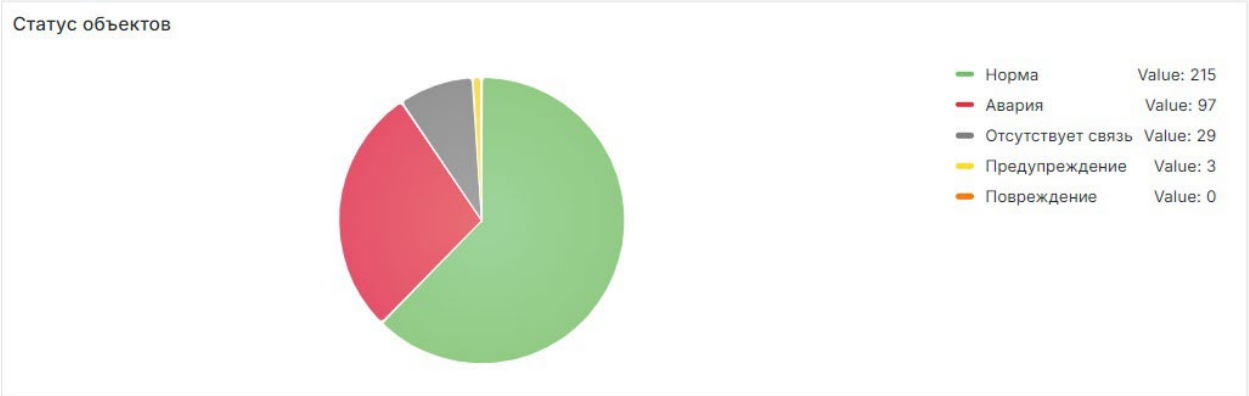


Рисунок 5.3 – Диаграмма событий

Легенда дублирует информацию счётчиков событий и позволяет выбирать, какие статусы событий учитывать при построении диаграммы. Для этого нажмите на соответствующий статус события: активный выделится ярким цветом, неактивный – приглушённым. Изменения мгновенно отобразятся на диаграмме.

Кроме того, счётчики событий дублируются внизу на панели событий справа (Рисунок 5.4) и отображаются во всех остальных вкладках Системы.

Рисунок 5.4– Дублирование счётчика событий

Счётчики событий делятся на следующие статусы:

- **Предупреждение** (желтый цвет) – события со статусом «предупреждение»;
- **Повреждение** (оранжевый цвет) события со статусом «повреждение»;
- **Авария** (красный цвет) – события со статусом «авария»;
- **Отсутствие связи** (серый цвет) – устройство стало недоступно;
- **Обслуживание** (синий цвет) – устройство находится на обслуживании;
- **Выведен из эксплуатации** (синий цвет) – устройство снято с эксплуатации;
- **Ремонт** (синий цвет) – устройство находится в ремонте.

5.16.2. Графики показателей

Ниже счётчиков событий и диаграммы располагаются графики, отражающие изменение показателей объекта мониторинга во времени. При наведении курсора мыши на график появится всплывающая подсказка со значением показателя в выбранный момент времени.

Для детального анализа данных за меньший промежуток времени можно выделить интересующий интервал на графике. Для этого необходимо нажать на график в точке начала интересующего интервала и, не отпуская кнопку мыши, переместить курсор до конечной точки интервала. Как только отпустите кнопку мыши все графики автоматически масштабируются, и данные отобразятся более детально в выбранном промежутке времени.

5.16.3. Панель настройки выбора временного диапазона

В верхней правой части интерфейса расположена панель управления (Рисунок 5.5), содержащая ключевые элементы для настройки отображения данных:

- **Элемент выбора временного интервала** (Рисунок 5.6). Позволяет выбрать период, за который будут отображаться данные на счётчиках событий, диаграммах и графиках. По умолчанию установлен диапазон «Last 30 minutes» (Последние 30 минут). При нажатии на этот элемент откроется список доступных интервалов времени: Последние 5, 15, 30 минут, 1, 3, 6, 12, 24 часов, 2, 7, 30 дней и т. д.
- **Элемент обновления данных (Refresh)** (Рисунок 5.7). Позволяет вручную обновить данные, либо настроить частоту автоматического обновления, По умолчанию время автоматического обновления 5 секунд. Возможные настройки периодичности автоматического обновления: Отключить, Авто, 5, 10, 30 с, 1, 5, 15, 30, минут, 1, 2 часа, 1 день.

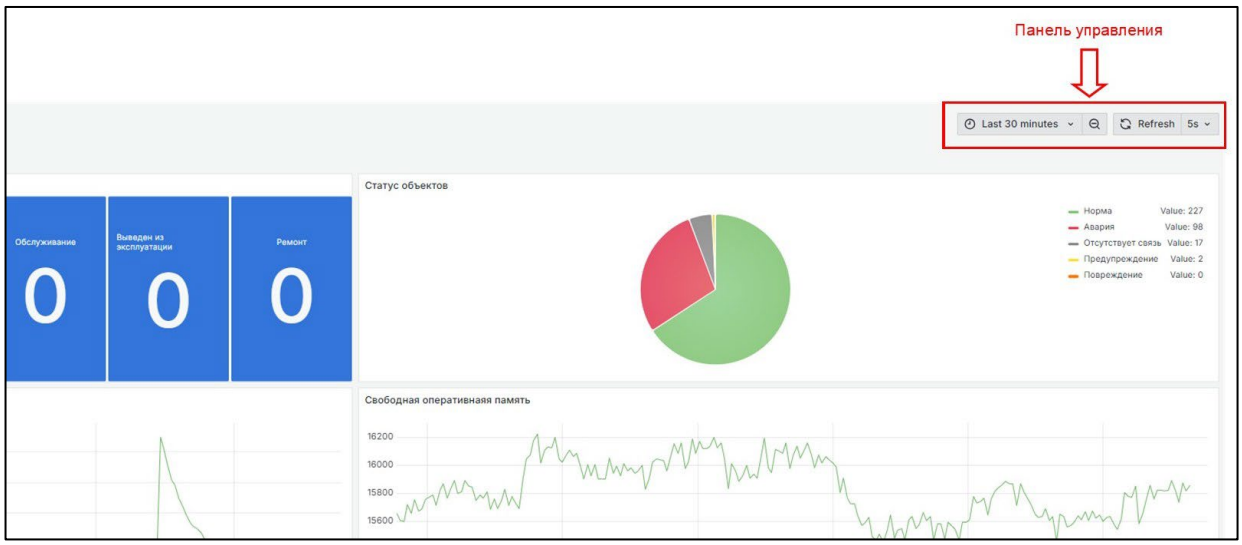


Рисунок 5.5 – Панель управления

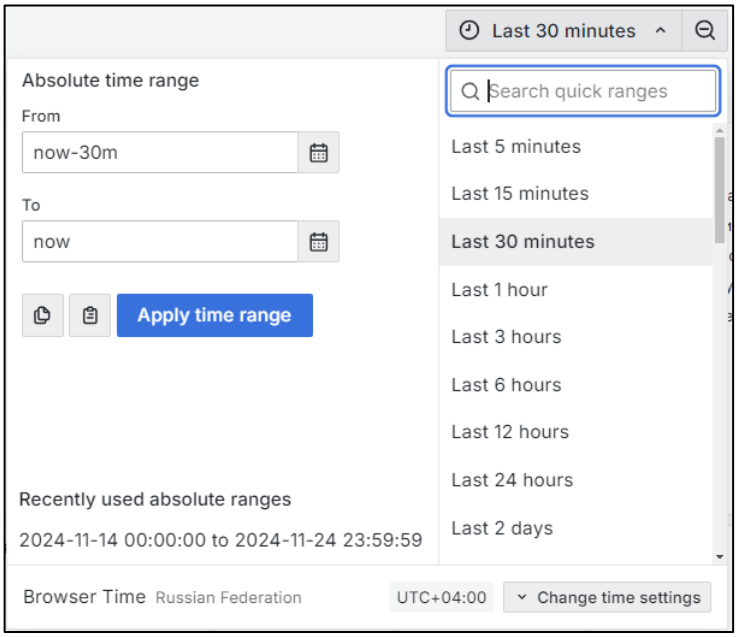


Рисунок 5.6 – Элемент выбора временного интервала

Рисунок 5.7 – Элемент обновления данных (Refresh)

Эти элементы обеспечивают гибкость при анализе данных, позволяя пользователю настраивать диапазон отображаемой информации и частоту её обновления.

5.17. Вкладка «Топология»

При переходе на вкладку «Топология» раскроется дерево объектов мониторинга, созданное пользователем со своей иерархией (Рисунок 5.8). При этом в рабочей области отобразится цифровая географическая карта, на которой точками представлено физическое расположение зданий и объектов мониторинга, которые имеют координатную привязку.

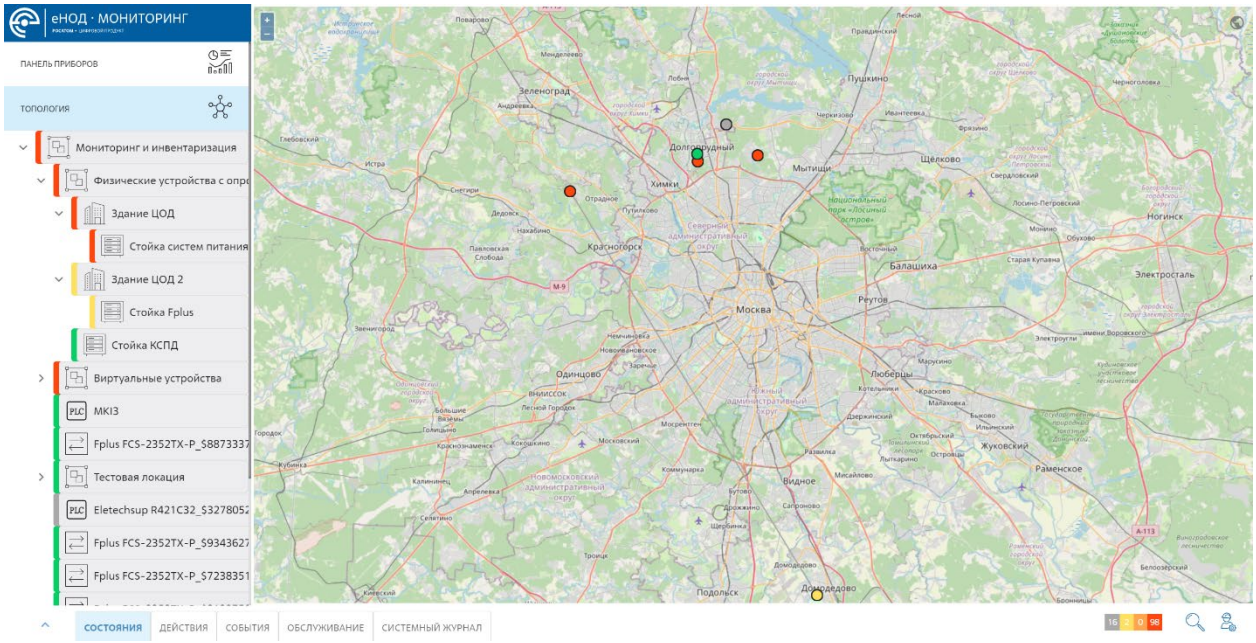


Рисунок 5.8 – Вкладка «Топология»

5.17.1. Работа с картой

Карта представляет из себя динамическую карту, которую можно масштабировать и перетаскивать ее область отображения. Для увеличения масштаба прокрутите колесо мыши вверх, для уменьшения – вниз. Либо для изменения масштаба воспользуйтесь кнопка «+» или «–», расположенные в левом верхнем углу карты. Для перемещения отображаемого участка карты нажмите кнопку мыши и перетащите в нужное направление.

При возникновении того или иного события объекты на карте окрашиваются в соответствующий цвет статуса.

При нажатии на любую точку на карте откроется окно с перечнем устройств, располагающихся внутри выбранного объекта (Рисунок 5.9).

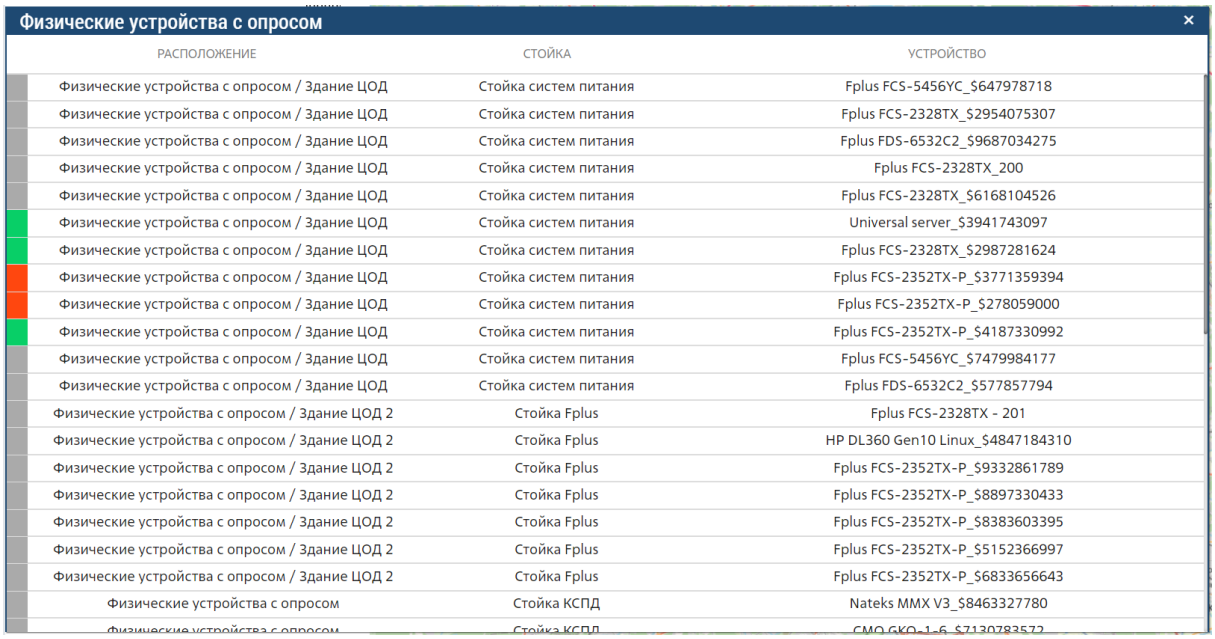


Рисунок 5.9 – Окно с перечнем устройств в выбранном объекте

В данном окне представлены следующие колонки:

- цветовая индикация – отражает наиболее важный статус, возникших при мониторинге объектов входящих в данное устройство;
- расположение – название здания или объекта, где расположено устройство;
- стойка – название стойки, где расположено устройство;
- устройство – название устройства.

При нажатии на логическое соединение, появится окно (Рисунок 5.10) со следующей информацией.

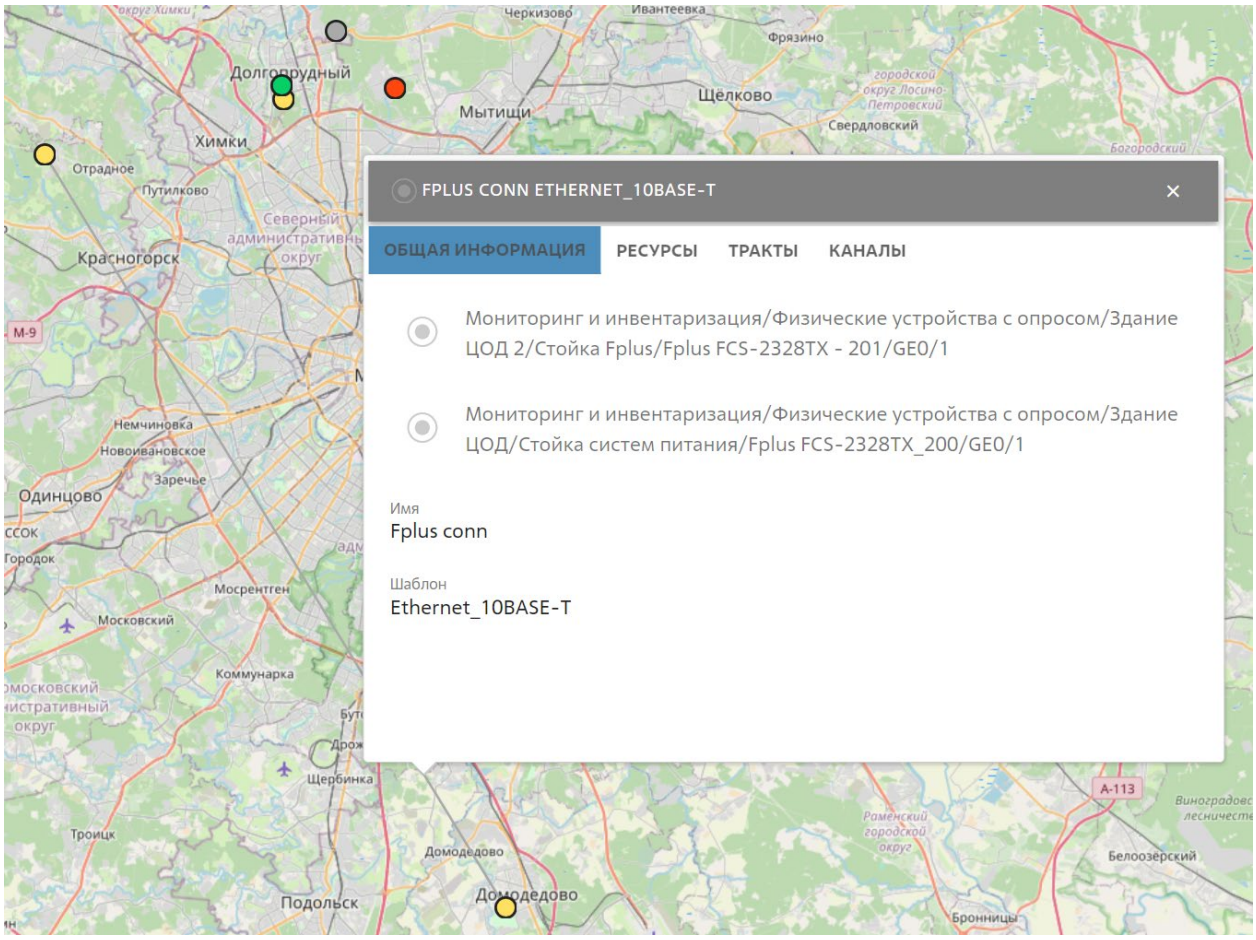


Рисунок 5.10 – Информация о связи между объектами

5.17.2. Работа с деревом объектов

Дерево объектов предназначено для отображения иерархической структуры объектов мониторинга, и может включать следующие классы объекта учёта:

- **локация** (здания, этажи, комнаты);
- **стойка** (телекоммуникационная стойка);
- **устройство** (физические и виртуальные);
- **модуль** (модули, которые устанавливаются в специальные слоты устройства).

При этом иерархическая структура строится по следующему принципу:

- в локацию могут входить:
  - другие локации (Например: Здание => этаж => комната);
  - стойки;

    - устройства;
    - модули;
- в стойку могут входить:
    - устройства;
    - модули;
- в устройство могут входить только модули.

Дерево объектов позволяет быстро переходить между различными уровнями инфраструктуры и выбирать конкретные устройства для детального анализа. С его помощью пользователь может визуализировать и анализировать инфраструктуру, что упрощает управление и контроль за состоянием объектов.

При нажатии на элемент дерева, обозначающий локацию, откроется окно с активной вкладкой **«Состав»** (Рисунок 5.11). Данная вкладка содержит перечень устройств, располагающихся внутри выбранной локации, и состоит из колонок:

- **Устройство** – приведено название устройства;
- **Шаблон** – приведен тип устройства;
- **Ip адрес** – приведен ip адрес устройства;
- **Серийный номер** – приведен серийный номер устройства;
- **Расположение** – приведено территориальное местонахождение устройства.

Отображение состава можно сортировать по одной из колонок.

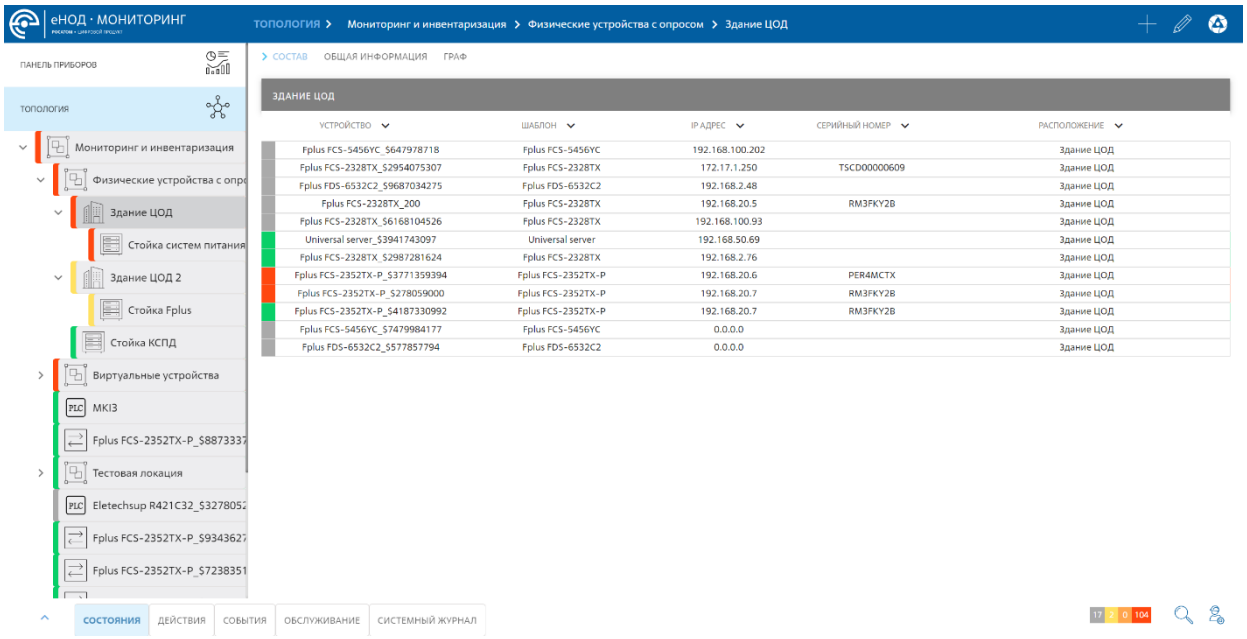


Рисунок 5.11 – «Состав»

При переходе на вкладку «Общая информация» откроется окно (Рисунок 5.12), содержащее общие сведения о выбранной локации:

- **Имя** – название объекта дерева;
- **Состояние** – в каком состоянии в текущем моменте (Введен в эксплуатацию/планируемый/строящийся);
- **Владелец** – название организации, являющейся владелец объекта;
- **Проект/титул** – в рамках какого проекта установлен данный объект;
- **Приложенные файлы** (Рисунок 5.13) – файлы, приложенные к данному объекту;
- **Статистика** (Рисунок 5.14) – статистические данные по составу устройств в данном объекте дерева.

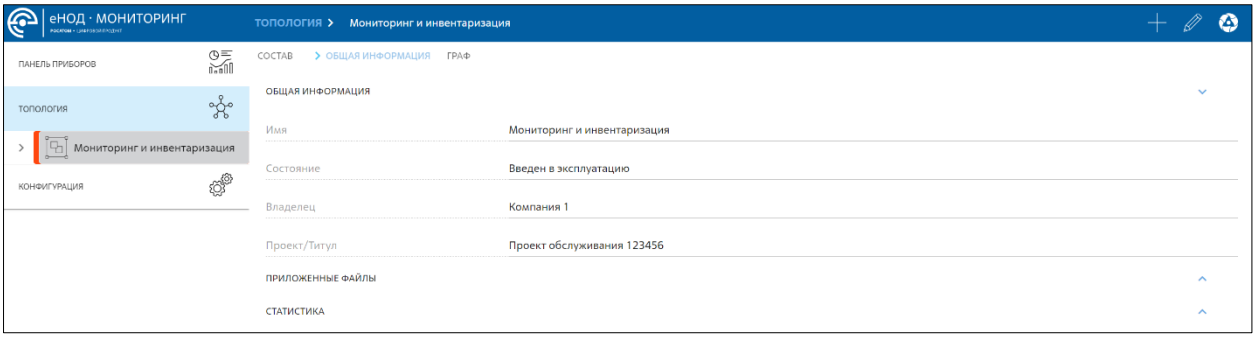


Рисунок 5.12 – «Общая информация»

Рисунок 5.13

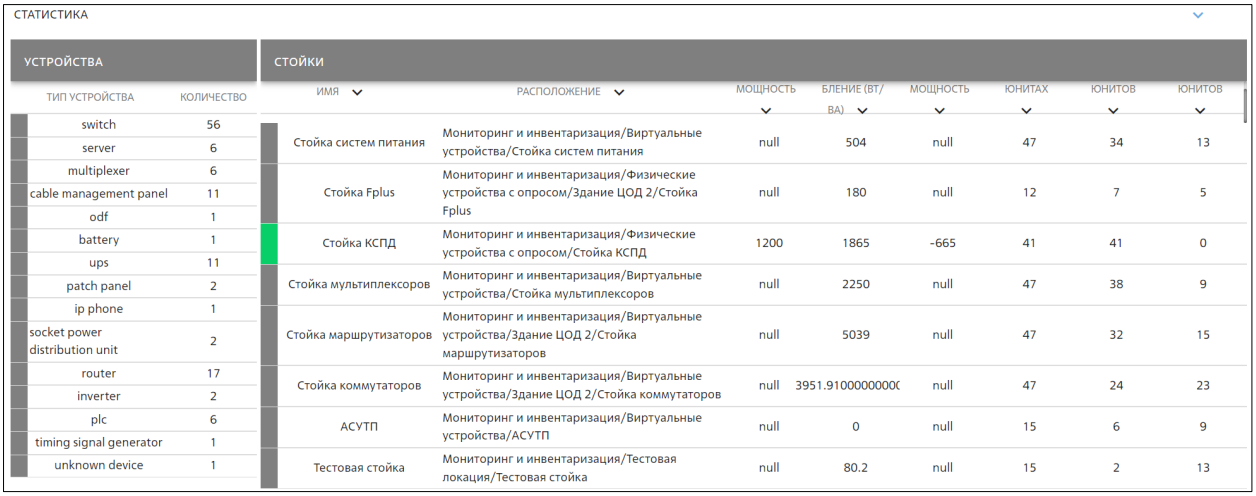


Рисунок 5.14

При переходе на вкладку **«Граф»** откроется окно (Рисунок 5.15), с графическим условным отображением устройств входящих в состав данного объекта дерева:

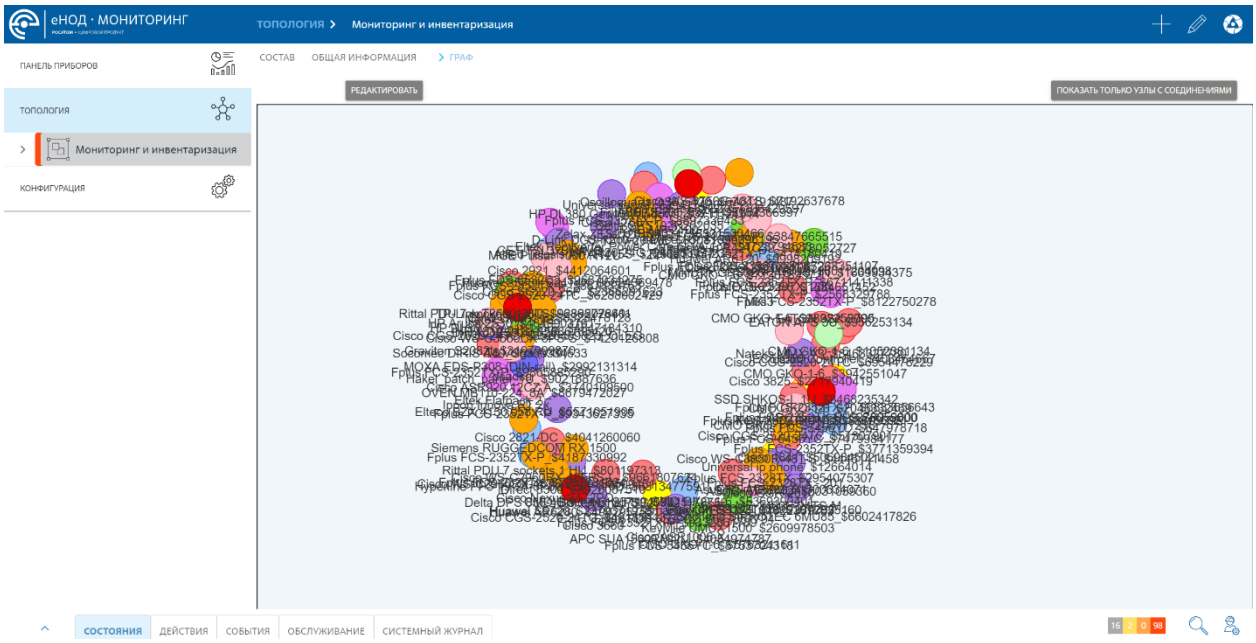


Рисунок 5.15

Если во вкладке **«Состав»** выбрать одно из устройств, то откроется окно, содержащее сведения о нем (Рисунок 5.16):

- изображение его внешнего вида;
- имя – его название;
- расположение в шкафу – расположение на лицевой стороне или тыльной;
- вкладка **«Общая информация»** – аналитическая панель с графиками по показателям мониторинга устройства;
- вкладка **«Порт GEO/1»** (Рисунок 5.17) – аналитическая панель со статистическими данными;
- вкладка **«Конфигурация»** (Рисунок 5.18) – содержит информацию о настройках конфигурации данного устройства;
- вкладка **«Консоль»** (Рисунок 5.19) – позволяет выполнить симуляцию консольного терминала для входа в устройство;
- вкладка **«Управление»** (Рисунок 5.20) – предназначена для управления устройством.

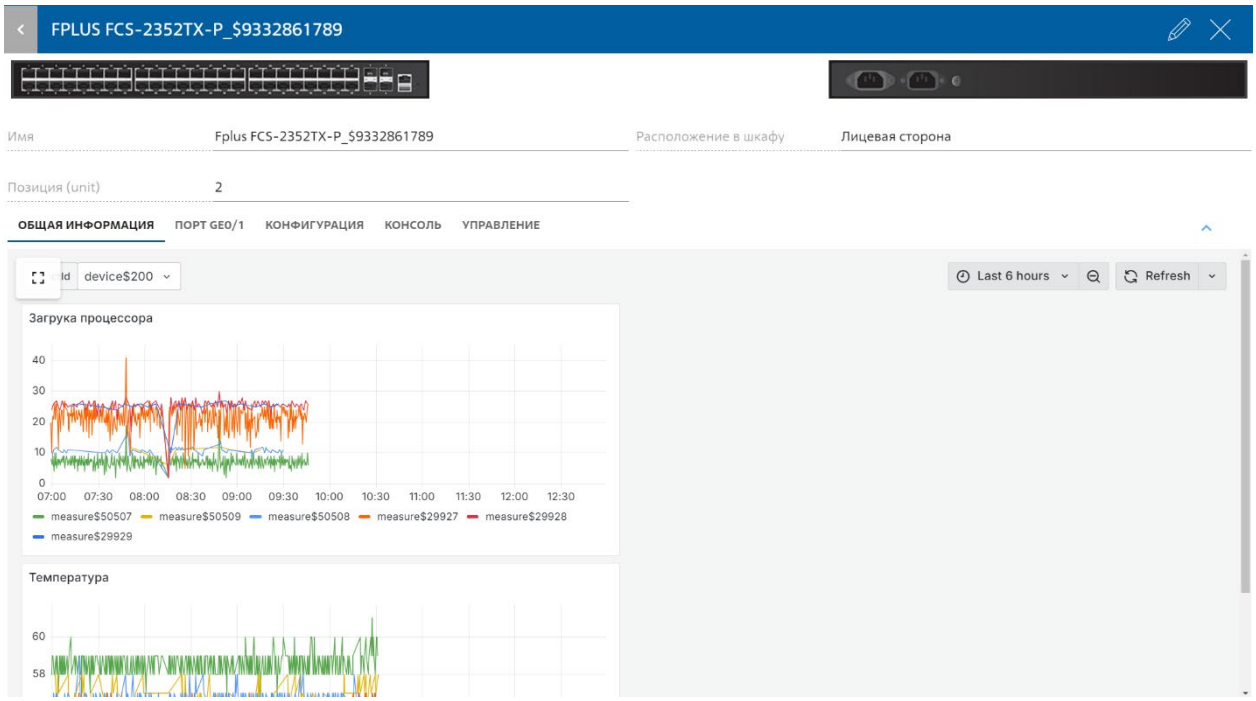


Рисунок 5.16 – Сведения об устройстве (вкладка «Общая информация»)

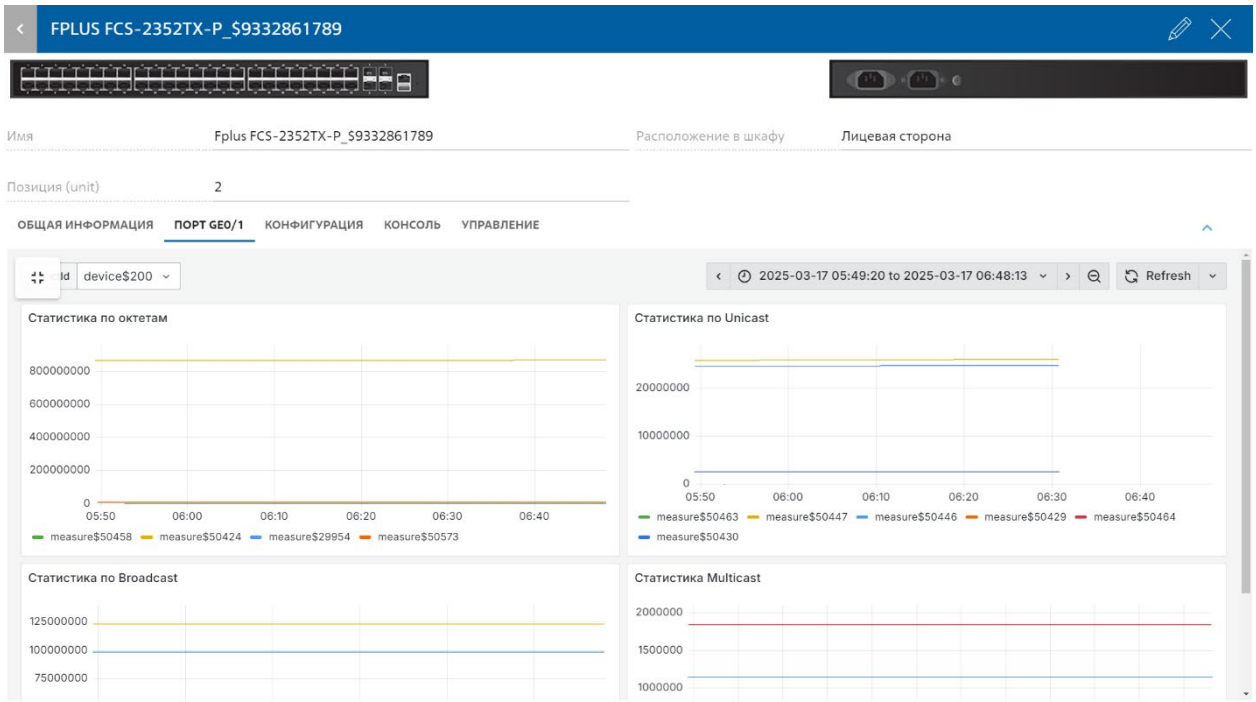


Рисунок 5.17 – Сведения об устройстве (вкладка «Порт GEO/1»)

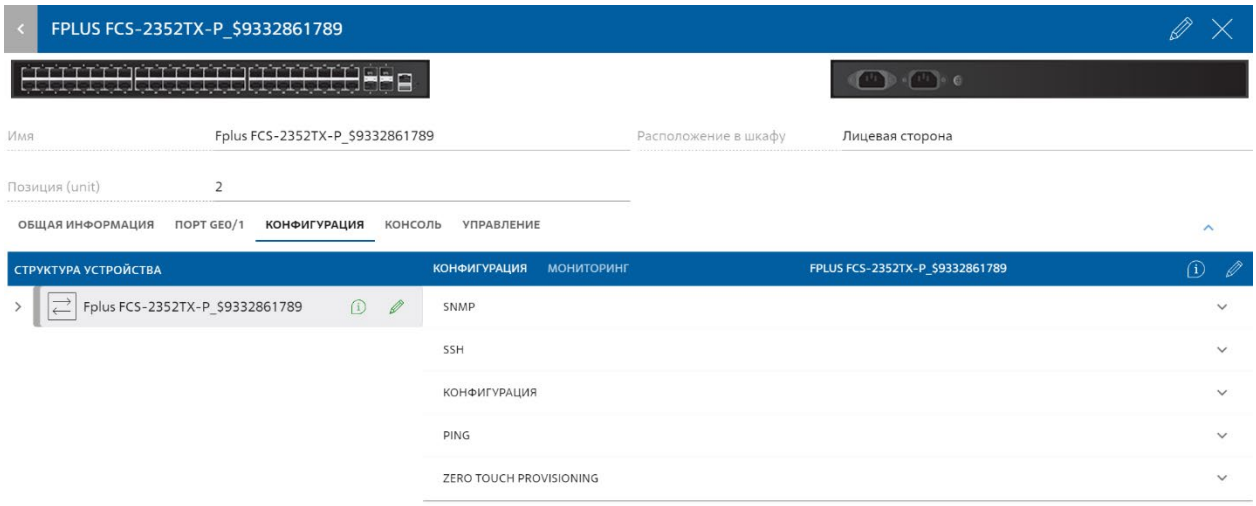


Рисунок 5.18 – Сведения об устройстве (вкладка «Конфигурация»)

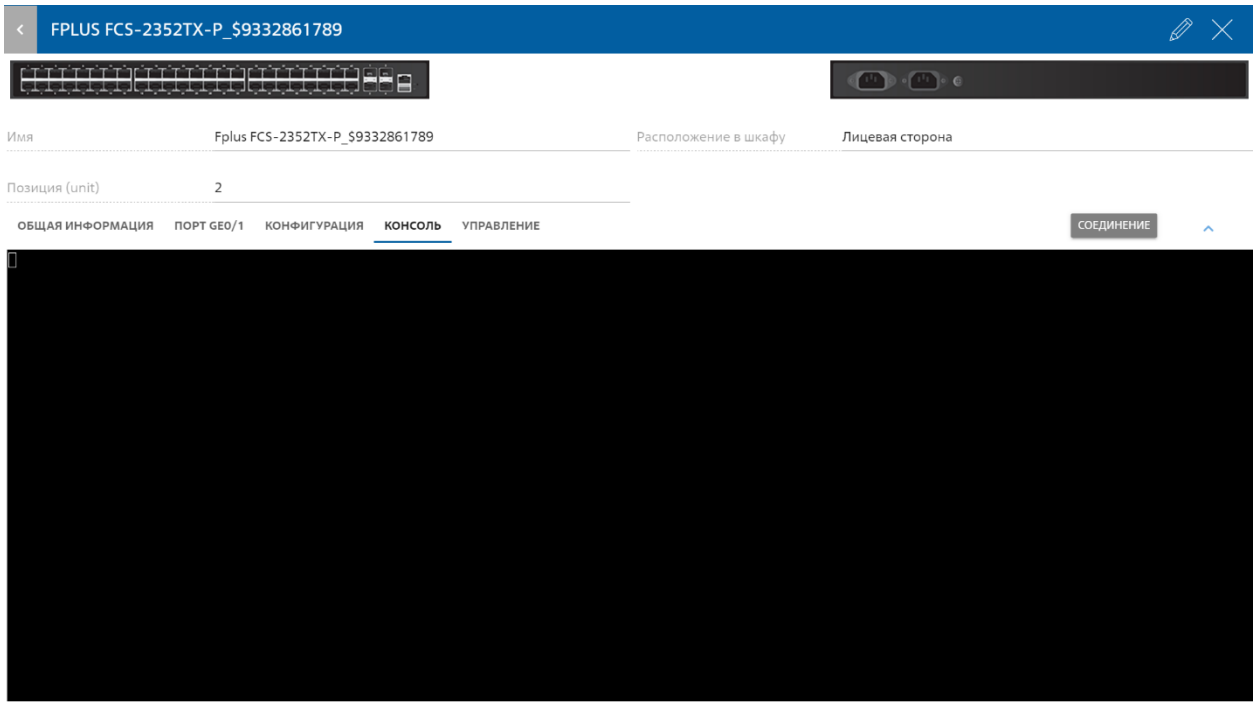


Рисунок 5.19 – Сведения об устройстве (вкладка «Консоль»)

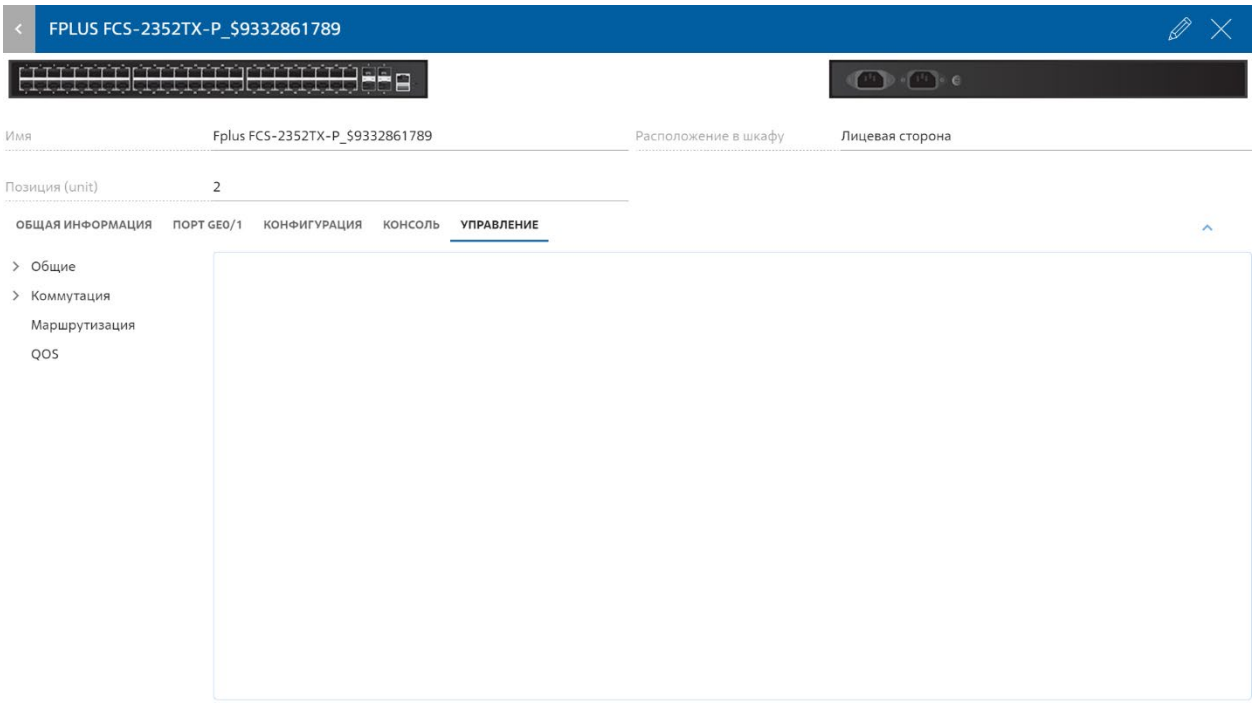


Рисунок 5.20 – Сведения об устройстве (вкладка «Управление»)

Состав вкладки «Управление» зависит от шаблона устройства.

При нажатии на элемент дерева, обозначающий стойку, откроется окно с изображением стойки с установленными в нее устройствами и активной вкладкой **«Общая информация»** (Рисунок 5.21). Вкладка «Общая информация содержит следующие сведения о стойке:

- **Имя** – название стойки;
- **Комментарий**;
- **Серийный номер** – серийный номер производителя стойки;
- **Инвентарный номер** – номер, присвоенный пользователем;
- **Дата гарантии** – срок окончания гарантийного обслуживания;
- **Ввод кабеля** – указано направление ввода кабеля;
- **Состояние** – (Введен в эксплуатацию/планируемый/строящийся);
- **Глубина** – указана максимальная посадочная глубина монтируемого устройства;
- **Высота в юнитах**;
- **Владелец** – указана организация-владелец данной стойки;

- **Обслуживающая организация** – указана организация, обслуживающая данную стойку;
- **Проект/Титул** – в рамках какого проекта установлена данная стойка.

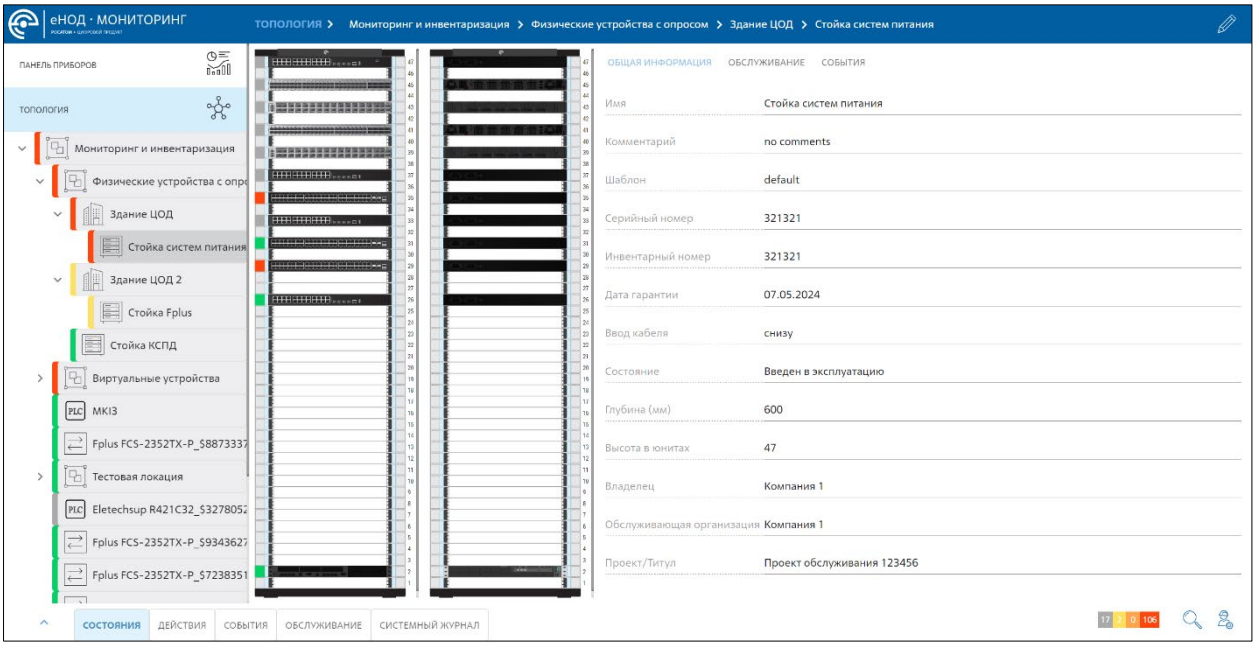


Рисунок 5.21 – Стойка. Общая информация

Во вкладке **«Обслуживание»** (Рисунок 5.22) приводится таблица с перечнем устройств, установленных в данную стойку со следующими колонками:

- **Цветовая индикация** – отражает статус события, возникшего при мониторинге устройства;
- **Позиция** – номер позиции местоположения устройства в стойке;
- **Организация** – название организации производителя устройства;
- **Устройство** – наименование модели устройства;
- **Серийный номер** – серийный номер устройства;
- **Тип устройства** – категория устройства;
- **Гарантия истекает** – указан срок окончания гарантии устройства;

- **Дата очередного ТО** – указана дата очередного технического обслуживания устройства;
- **Окончание жизненного цикла** – указана дата окончания жизненного цикла устройства.

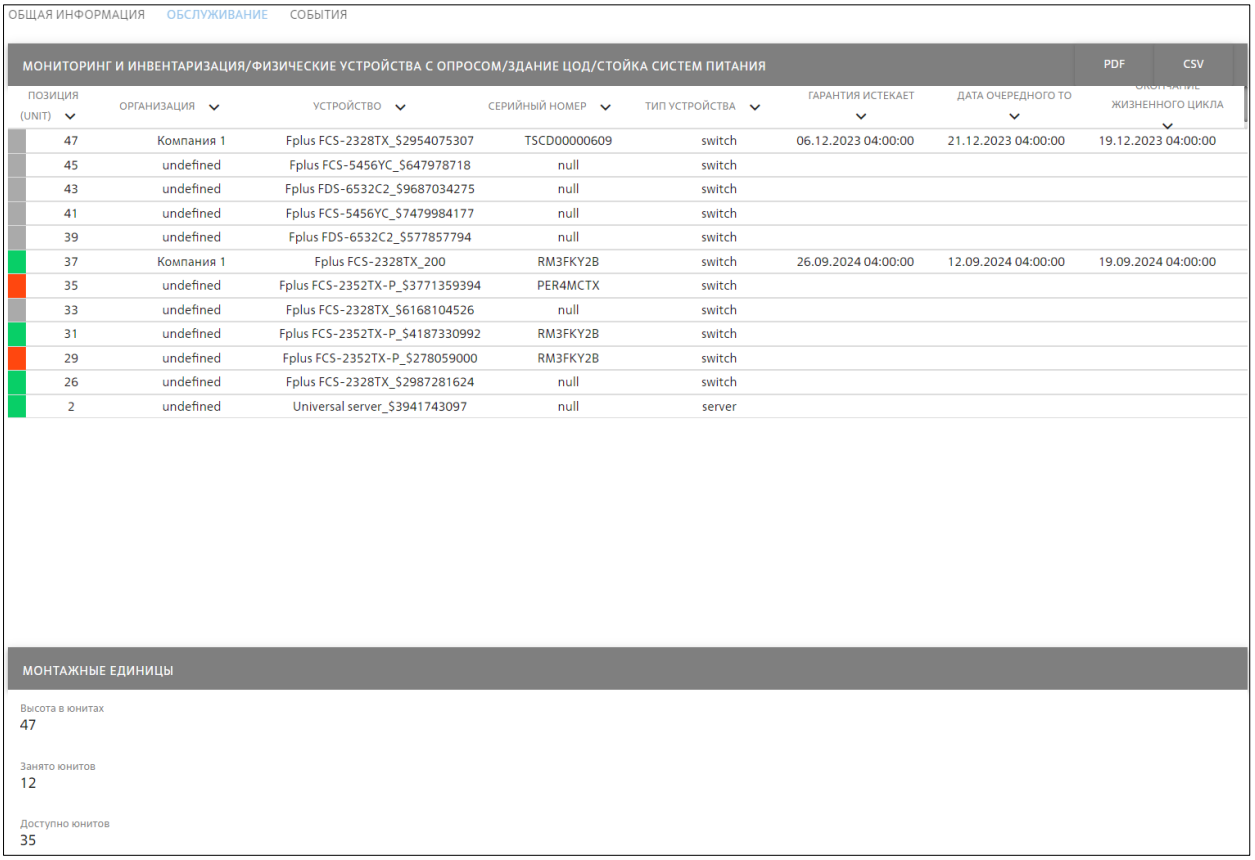


Рисунок 5.22 – Стойка. Вкладка «Обслуживание»

Ниже таблицы содержится информация, необходимая для планирования размещения устройств в стойке:

- **Высота в юнитах** – высота стойки в юнитах;
- **Занято юнитов** – количество юнитов в стойке, занятых устройствами;
- **Доступно юнитов** – количество свободных юнитов в стойке.

При выборе в дереве элемент, обозначающий **«Устройство»**, откроется окно со сведениями о нем (Рисунок 5.16).

В дереве объектов используется цветовая индикация для быстрой визуальной оценки состояния устройств и элементов инфраструктуры. Значения используемых цветов было описано ранее в подразделе 5.1 данного руководства, за исключением некоторых особенностей, свойственных вкладке «Топология»:

- Устройство может быть выделено серым цветом в случае:
  - если мониторинг на устройстве был включён, но устройство перестало отвечать (в данном случае будет сформировано и отправлено сообщение в счётчик событий, находящийся во вкладке «Панель приборов»);
  - если у устройства не предусмотрено шаблоном подключение мониторинга.
- В случае, если устройство перестало отвечать со включенным мониторингом, раздел, к которому относится устройство, будет выделен жёлтым цветом (Рисунок 5.23).

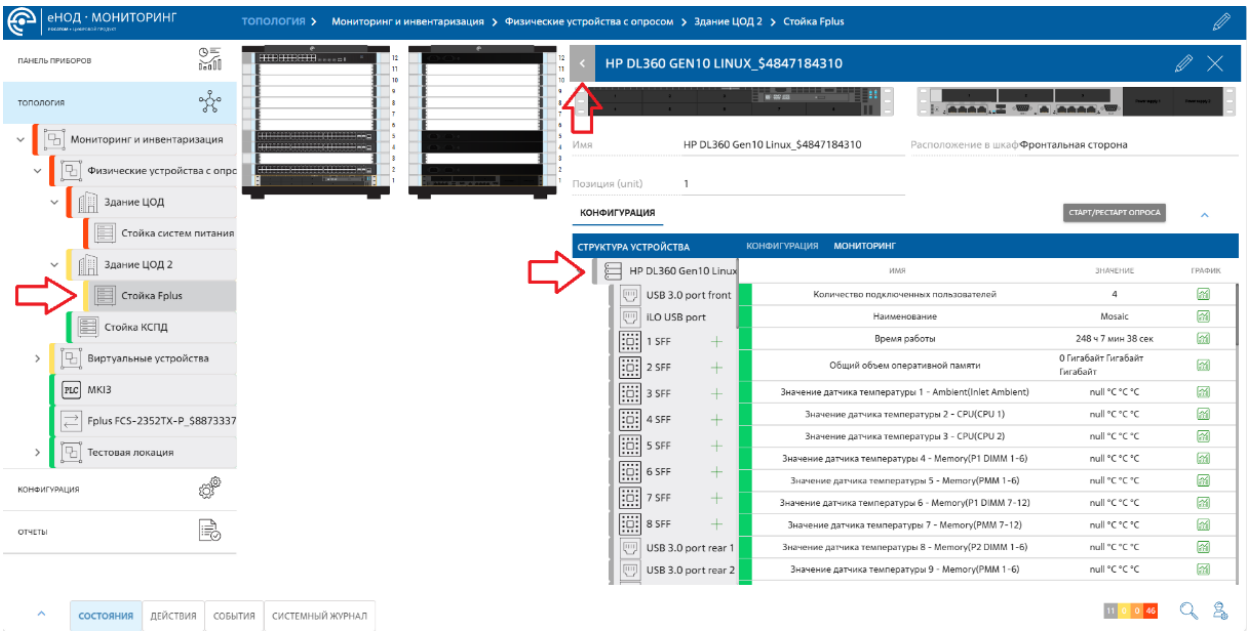


Рисунок 5.23 – Случай, когда устройство перестало отвечать со включенным мониторингом

В дереве устройств, расположенном в левой части экрана, предусмотрено наследование статуса (цветов) от вложенного объекта к корневому.

Например: если, хотя бы одно устройство поменяет статус на красный (авария), то все объекты, в состав которого входит это устройство, также перекрасятся в красный цвет (устройство => здание => локация => корневой объект) (Рисунок 5.24).

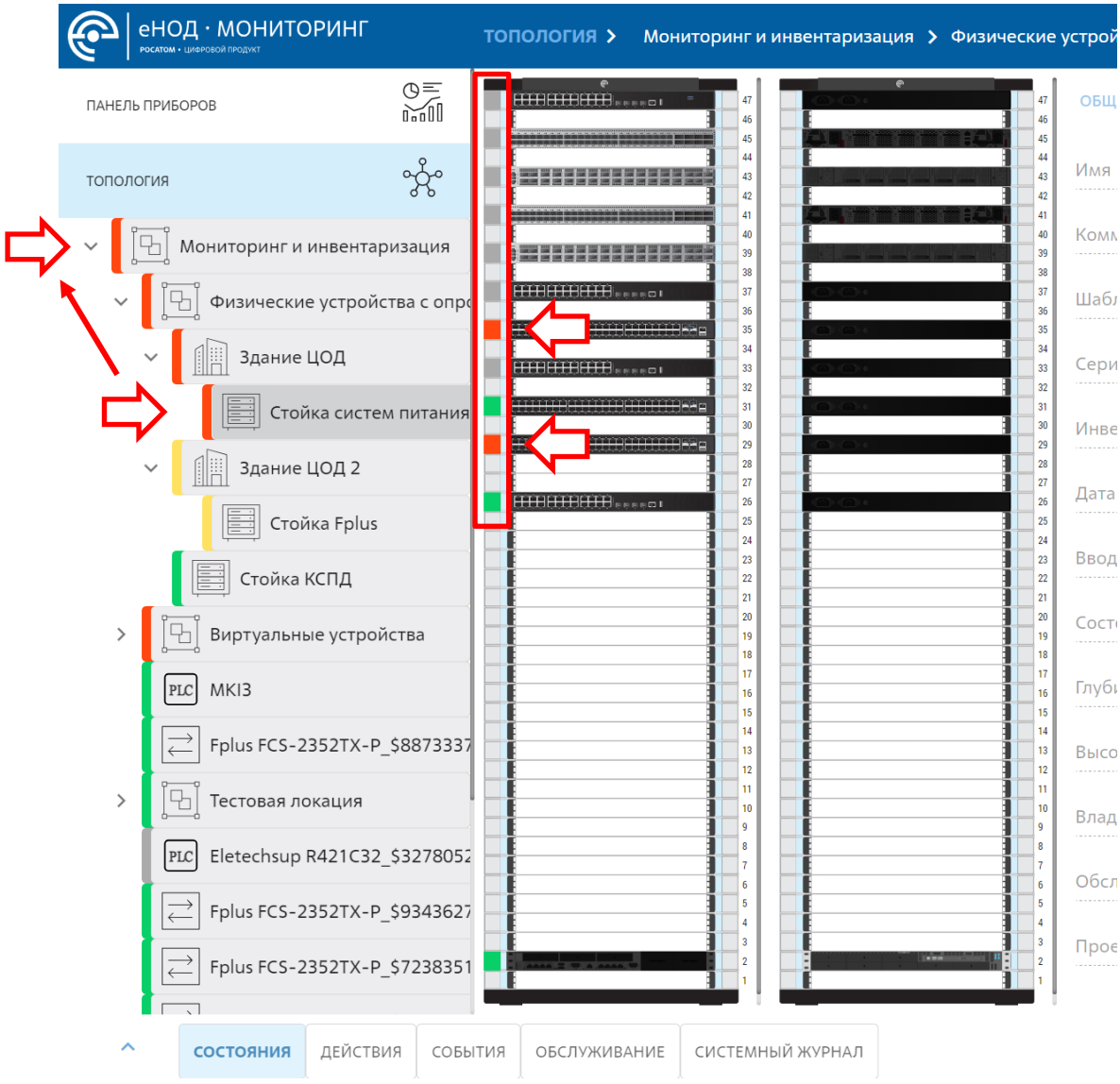


Рисунок 5.24 – Наследование статуса от вложенного объекта к корневому

5.17.3. Создание объектов

Для создания объекта во вкладке «Топология» необходимо, нажать на кнопку «Создать» (рис.6.7).

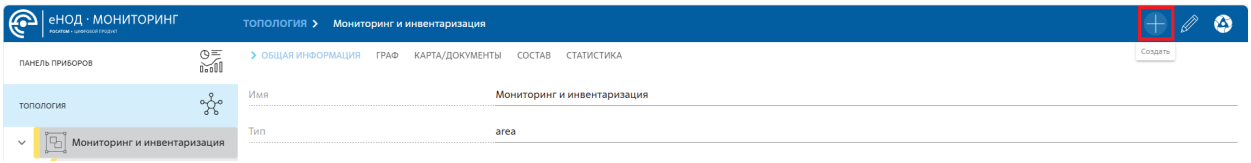


Рисунок 6.7 – Создание новых объектов

К созданию доступно 4 класса объекта учёта: локация, стойка, устройство и модуль. Из имеющихся классов можно создать следующую иерархию: модуль входит в состав устройства, устройство может находиться в стойке, стойка может располагаться на выбранной локации. Имеется возможность создать отдельно модуль без привязки к устройству и отдельно устройство без привязки к стойке. Внутри локации можно создать ещё одну локацию (например, создать этаж внутри здания или кабинет на этаже).

5.17.3.1. Создание модуля

Для создания модуля из выпадающего списка «Класс объекта учёта» необходимо выбрать класс «Модуль». Далее из обширного перечня необходимо выбрать создаваемый модуль.

5.18. Вкладка «Конфигурация»

Вкладка «Конфигурация» предназначена для управления настройками системы, включая создание, редактирование и выбор ролей пользователей и другие административные функции.

Вкладка состоит из следующих элементов:

- Пользователи;
- Уведомление;
- Техническое обслуживание;
- Zero Touch Provisioning.

5.18.1. Пользователи

Окно элемента «Пользователи» (Рисунок 5.25) предназначено для управления учётными записями пользователей и выбирать их роль. Каждая роль имеет следующие права доступа в Системе:

- Администратор – имеет все права доступа по настройке Системы и управлению учётными записями пользователей;
- Оператор – имеет права доступа только на просмотр информации о мониторинге Системы;
- Менеджер – имеет права доступ ко всем действиям, кроме доступа к вкладке «Пользователи»;
- Специалист информационной безопасности – имеет права доступа по внесению изменений в учётные записи пользователей, а также просмотр информации о мониторинге Системы.

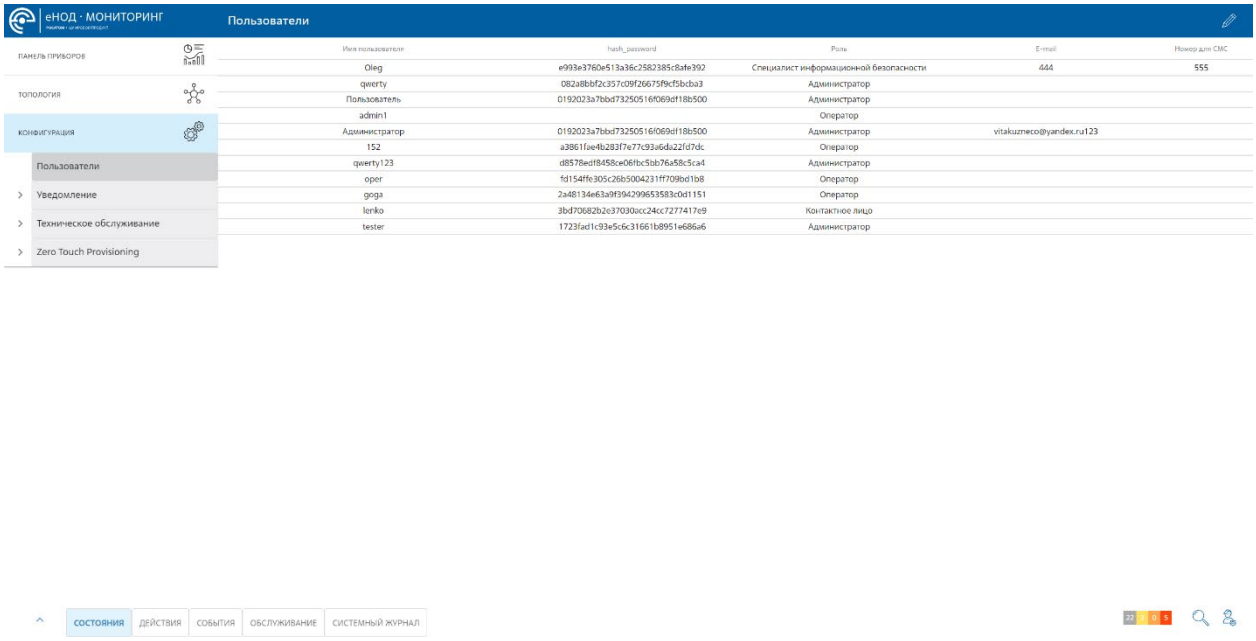


Рисунок 5.25 – Пользователи

В окне «Пользователи» отображается список всех зарегистрированных пользователей со следующими колонками:

- Имя пользователя – имя учётной записи;
- Hash password;

- Роль – Роль пользователя в системе (администратор, оператор, менеджер, специалист информационной безопасности);
- E-mail – адрес электронной почты пользователя для отправки уведомлений о возникших событиях в Системе;
- Номер для СМС – номер мобильной связи для оповещения пользователя о возникших событиях в Системе.

5.18.1.1. Создание и редактирование пользователя (доступно администратору и специалисту информационной безопасности)

Для создания нового пользователя нажмите в правом верхнем углу окна на изображение карандаша (). Затем на появившуюся кнопку «+» (). Откроется окно «Добавить нового пользователя» (Рисунок 5.26). Внесите необходимые данные пользователя. Роль пользователя выбирается выпадающим списком нажатием на соответствующее поле.

Для оповещения пользователя о возникших событиях в Системе в виде push-уведомлений в браузере необходимо активировать галочкой функцию «Подписка на Push-уведомление».

После внесения всех данных нажмите на кнопку «Добавить».

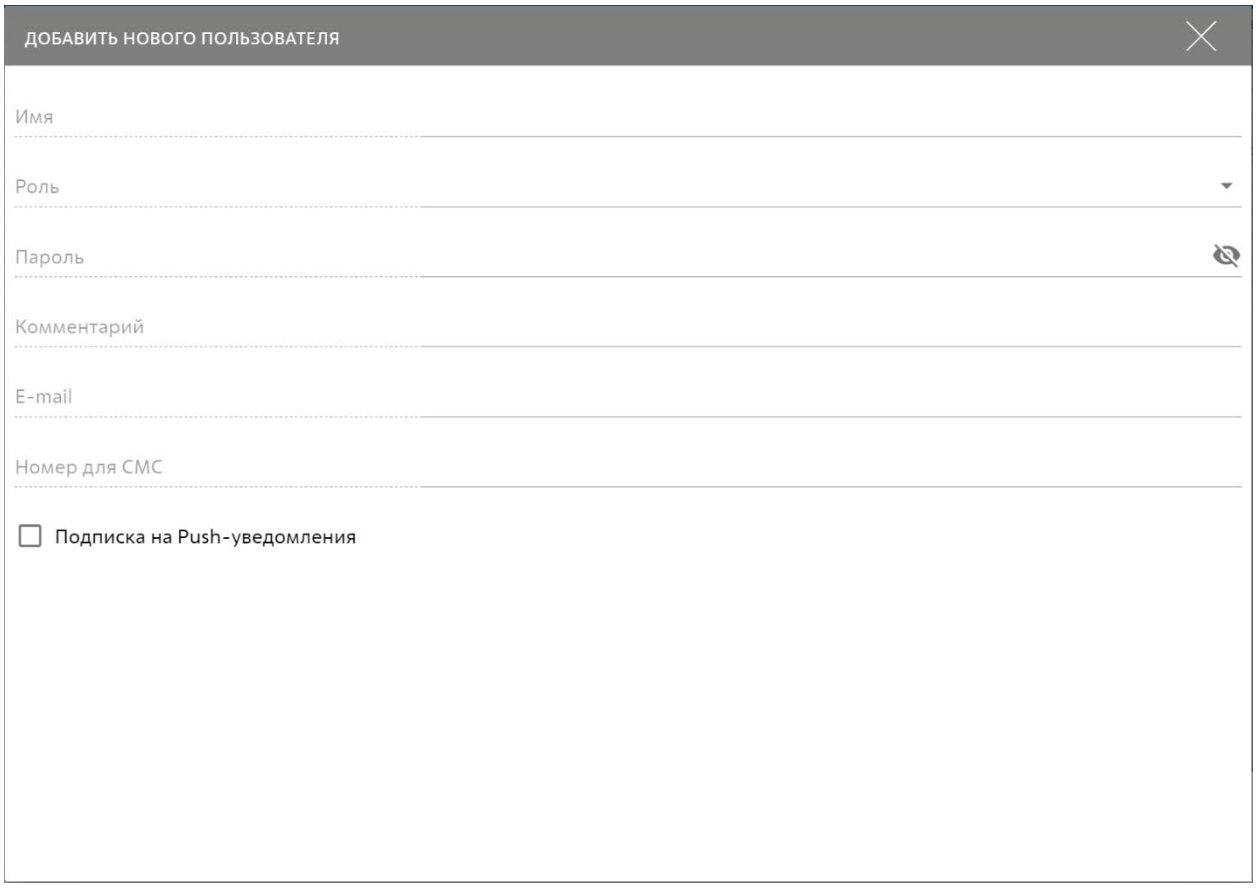


Рисунок 5.26 – Окно «Добавить нового пользователя»

Для редактирования уже имеющегося пользователя нажмите на «Карандаш» и на строку нужного пользователя, откроется окно с отображением его имени в шапке окна (Рисунок 5.27). Затем измените необходимые данные пользователя и нажмите кнопку «Добавить».

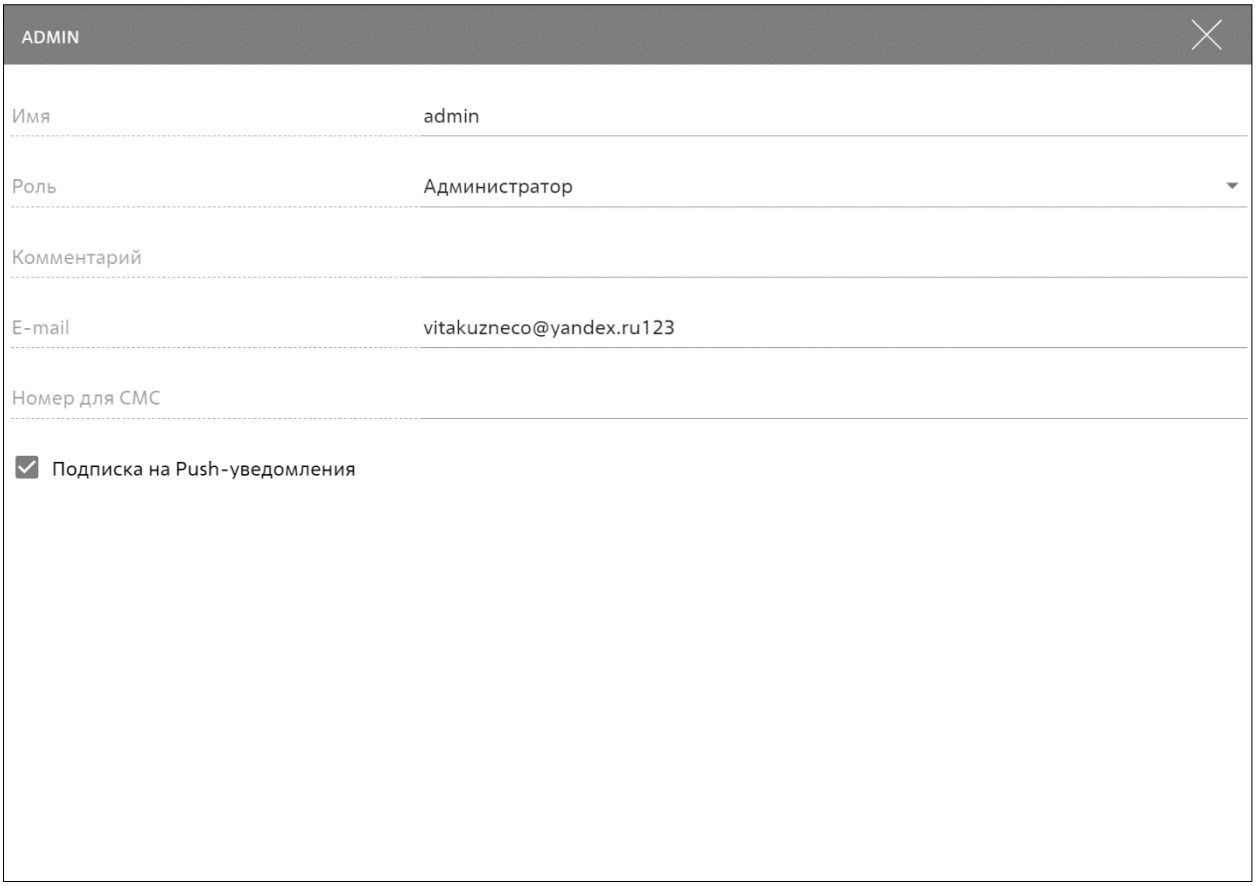


Рисунок 5.27 – Редактирование пользователя

5.18.2. Уведомление.

Вкладка «Уведомление» в системе e-node предназначена для настройки параметров уведомления о возникших событиях в Системе при помощи:

- E-mail рассылки на адреса электронной почты пользователей.

5.18.2.1. E-mail

Вкладка «E-mail» в системе e-node предназначена для настройки параметров электронной почты, используемой для отправки уведомлений и оповещений. Здесь можно настроить SMTP-сервер, аутентификацию и дополнительные параметры безопасности. При на нажатии на вкладку «E-mail» откроется окно (Рисунок 5.28) с данными по настройке её работы.

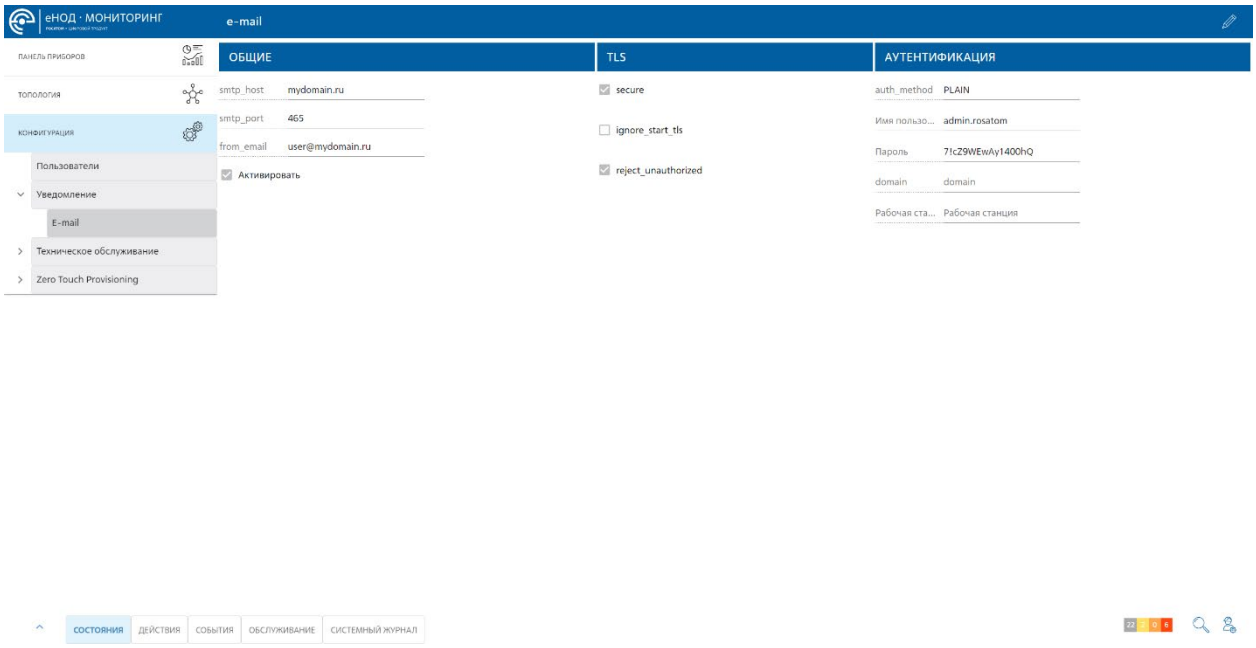


Рисунок 5.28 – Настройка E-mail оповещения

Для внесения и изменения данных необходимо в правом верхнем углу нажать на кнопку «карандаш» ( ) и внести данные в необходимые поля. Для принятия внесенных данных нажмите на «галочку» ( ), для отмены – на «крестик» ( ).

Для настройки параметров «Общие» необходимо заполнить следующие поля:

- smtp_host – если используется шифрованный канал, то возможно важно указывать доменное имя, а не IP-адрес. Зависит от того, что прописано в сертификате;
- smtp_port – порт шифрования;
- from_email – адрес отправителя. Часто совпадает с логином.

Параметры «TLS» активируются установкой флажка:

- secure – активировать, если необходим TLS-туннель, перед установкой smtp-сессии;

- ignore_start_tls – если «secure» не активирован, сервер может запросить TLS-туннель посредством команды «STARTTLS». Установите флажок, чтобы не исполнять «STARTTLS»;
- reject_ unauthorized – активируйте чтобы принимать самоподписанные сертификаты без проверки.

  ВНИМАНИЕ! Данная настройка создает уязвимость в шифровании! Предполагается, что администратор доверяет всем сертификатам! Некоторые почтовые сервера используют самоподписанные сертификаты.

Для настройки параметров «Аутентификация» необходимо заполнить следующие поля:

- auth_method – метод аутентификации. Возможно 2 способа – аутентификация по логину/ паролю (в данном случае прописать «PLAIN» или «null») или NTLM-аутентификация (в данном случае прописать «NTLM»).
- Имя пользователя – часто совпадает с адресом отправителя «from_email»;
- Пароль – пароль для аутентификации;
- domain – домен;
- Work group – название рабочей группы к которой принадлежит пользователь.

5.18.3. Техническое обслуживание

Элемент «Техническое обслуживание» в системе e-node предназначен для просмотра и управления настройками по обслуживанию системы управления.

Элемент «Техническое обслуживание» состоит из следующих элементов:

- Сессия;
- Статус обслуживания;
- Лицензирование.

5.18.3.1. Сессия

Элемент «Сессия» (Рисунок 5.29) предназначен для отображения перечня пользователей, подключенных к Системе в текущее время, и содержит следующие данные:

- ID сессии;
- ID пользователя – логин пользователя;
- Время жизни – время завершения сессии пользователя (фиксируется только у сессии Администратора, т.к. только у данного пользователя сессия автоматически закрывается при его бездействии в течении одного часа;
- Роль – роль подключенного пользователя;
- Адрес – IP-адрес подключенного пользователя.

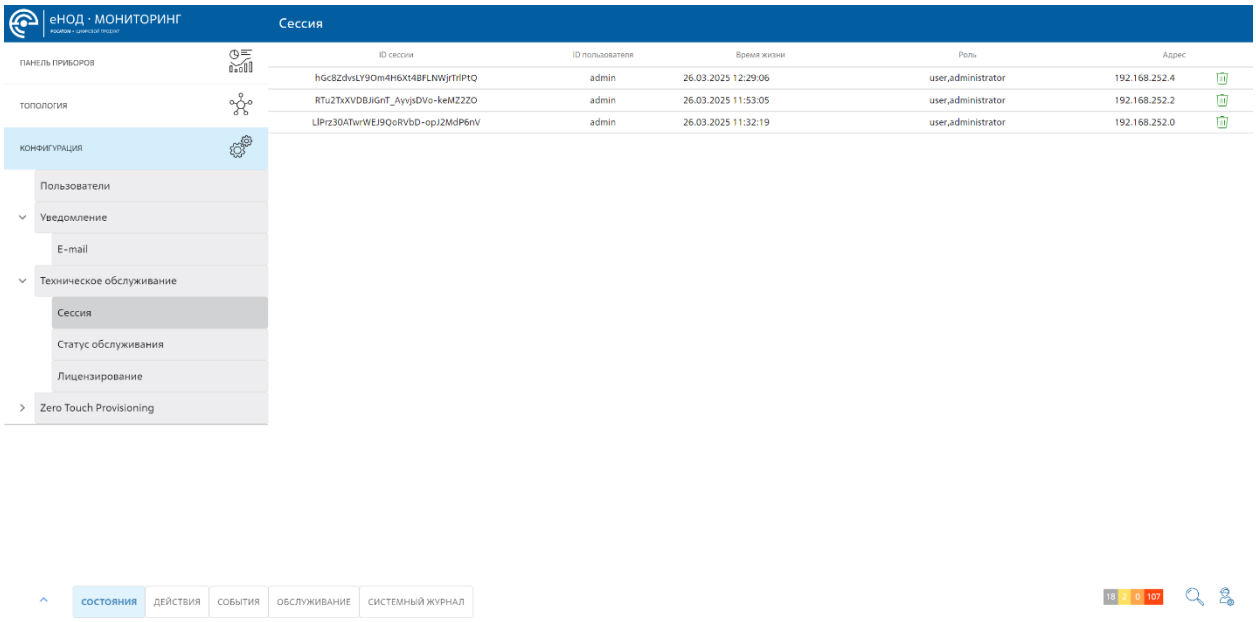


Рисунок 5.29 – Окно «Сессия»

Для принудительного завершения сессии нажмите на «Корзину» справа напротив нужного пользователя (функция доступна администратору и специалисту информационной безопасности).

5.18.3.2. Статус обслуживания

Элемент «Статус обслуживания» (Рисунок 5.30) предназначен для отображения перечня Docker-контейнеров, запущенных в Системе и содержит следующие данные:

- Контейнер – название контейнера;
- Время создания – когда он был создан;
- Статус – состояние, в котором он сейчас находится (running – работающий);
- uptime – сколько времени уже работает;
- image ID – наименование image контейнера;
- image ТЭГ – наименование ТЭГ контейнера.

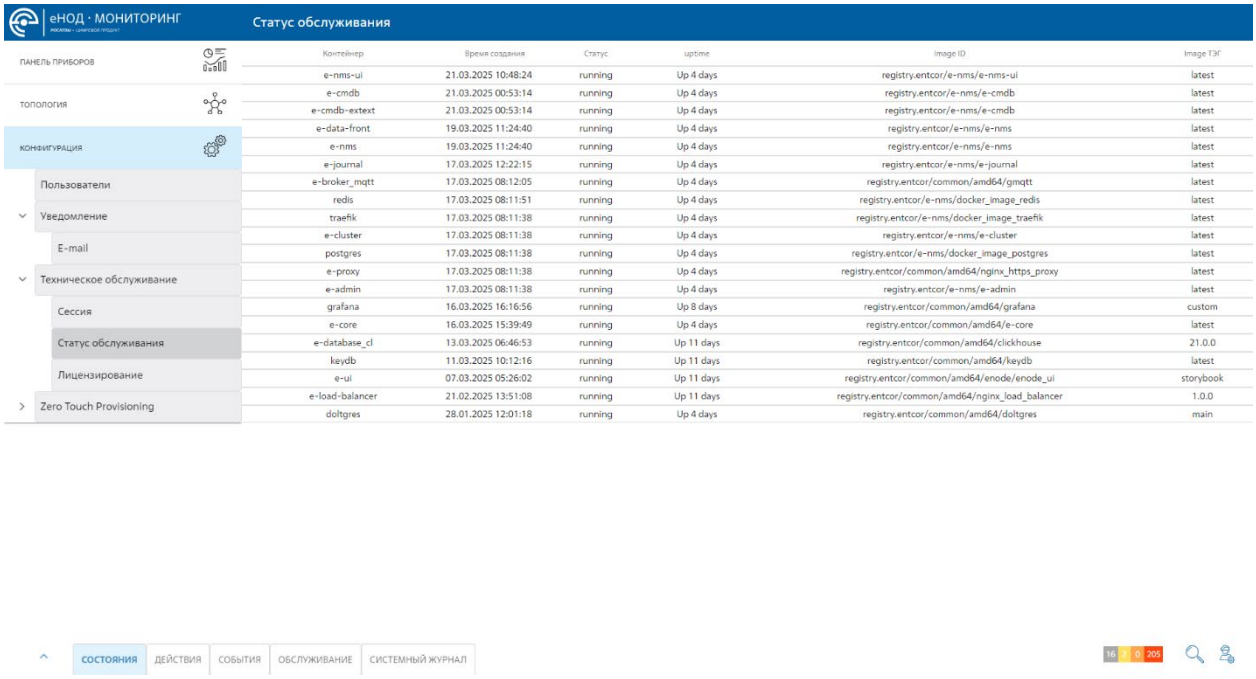


Рисунок 5.30 – Окно «Статус обслуживания»

5.18.3.1. Лицензирование

Вкладка «Лицензирование» (Рисунок 5.31) предназначена для просмотра текущих лицензионных параметров Системы на данном клиенте в формате JSON, а также для обновления самой лицензии. Для обновления лицензии на данном клиенте введите номер лицензионного ключа в поле под идентификатором лицензии и нажмите на кнопку «Обновить лицензию» (функция доступна только администратору).

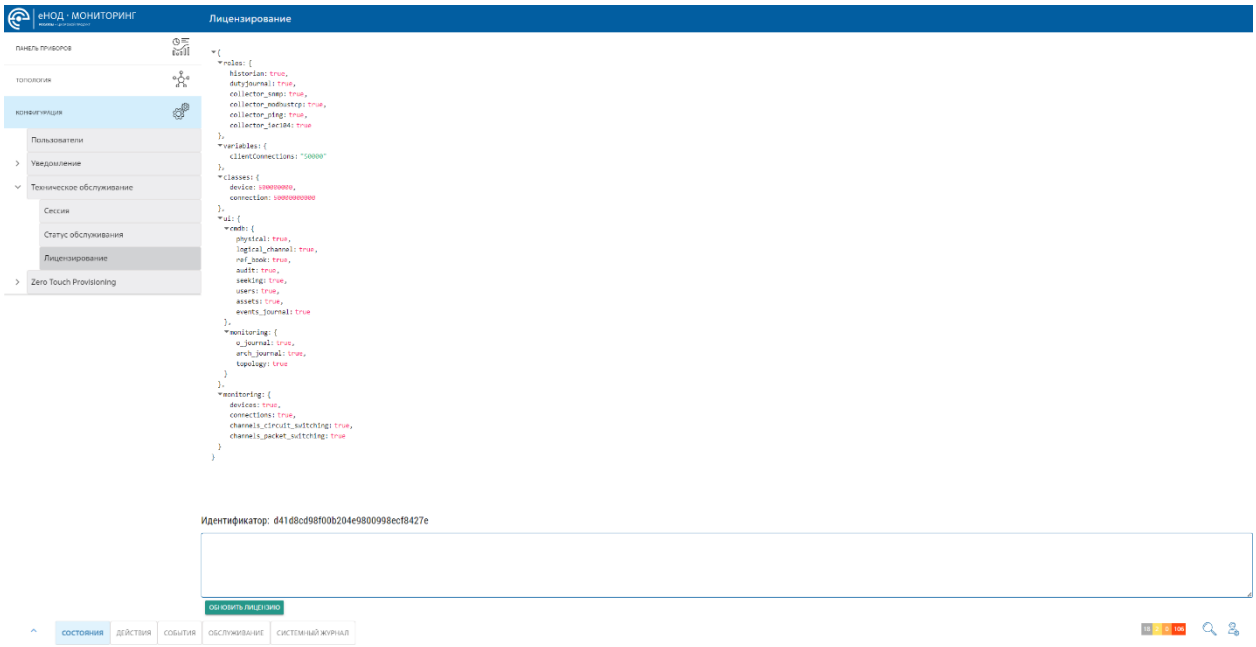


Рисунок 5.31 – Окно «Лицензирование»

5.18.4. Zero Touch Provisioning

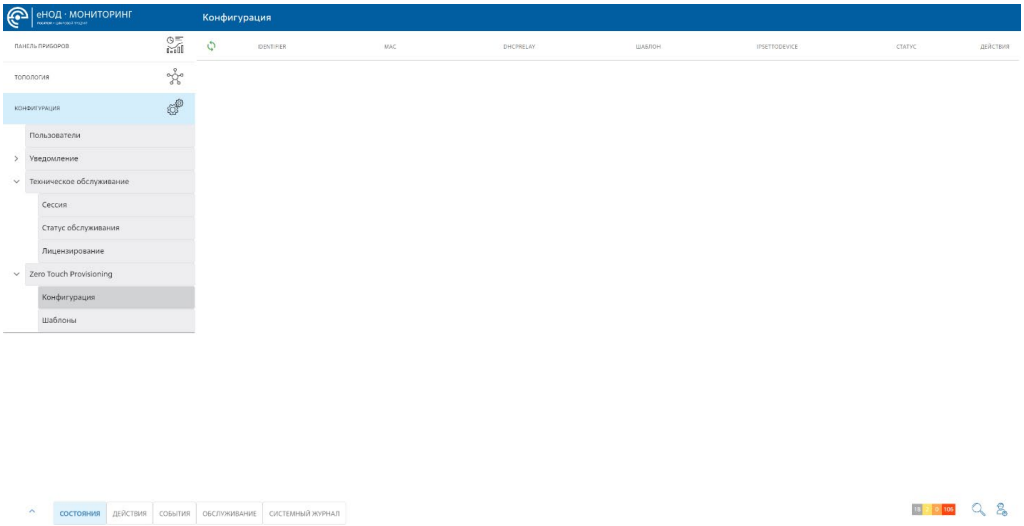


Рисунок 5.32 – Zero Touch Provisioning. Окно «Конфигурация»

5.18.4.1. Шаблоны

В данной вкладке (Рисунок 5.33) представлен перечень шаблон устройств для Zero Touch Provisioning.

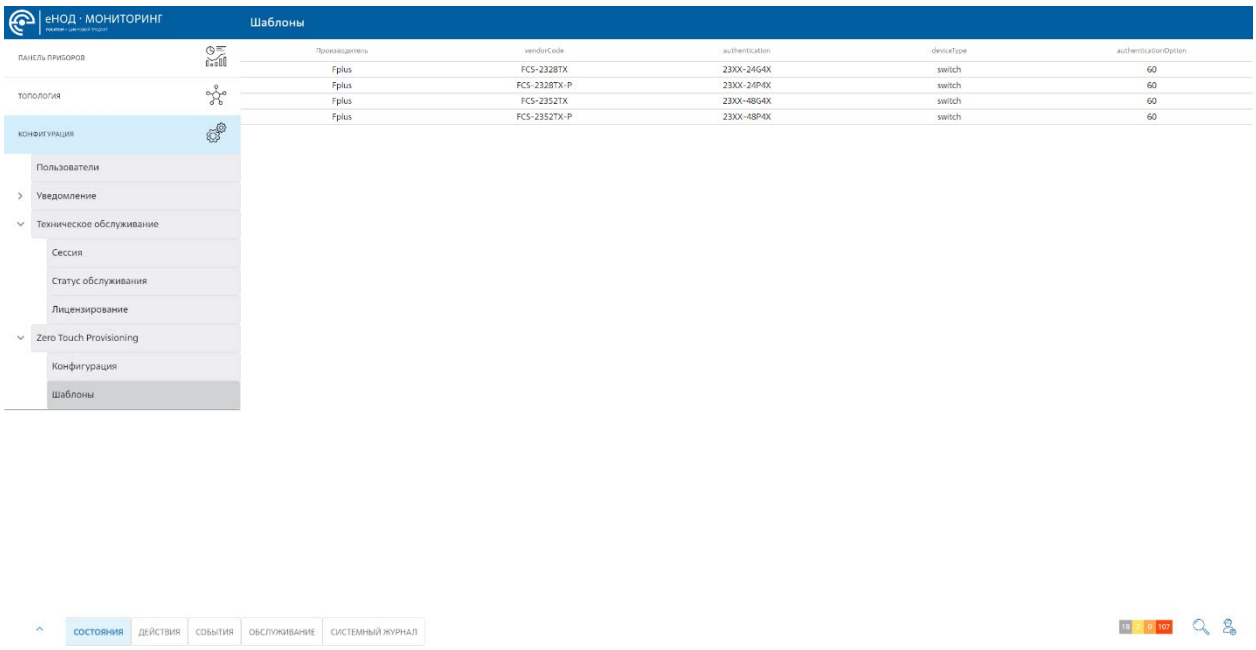
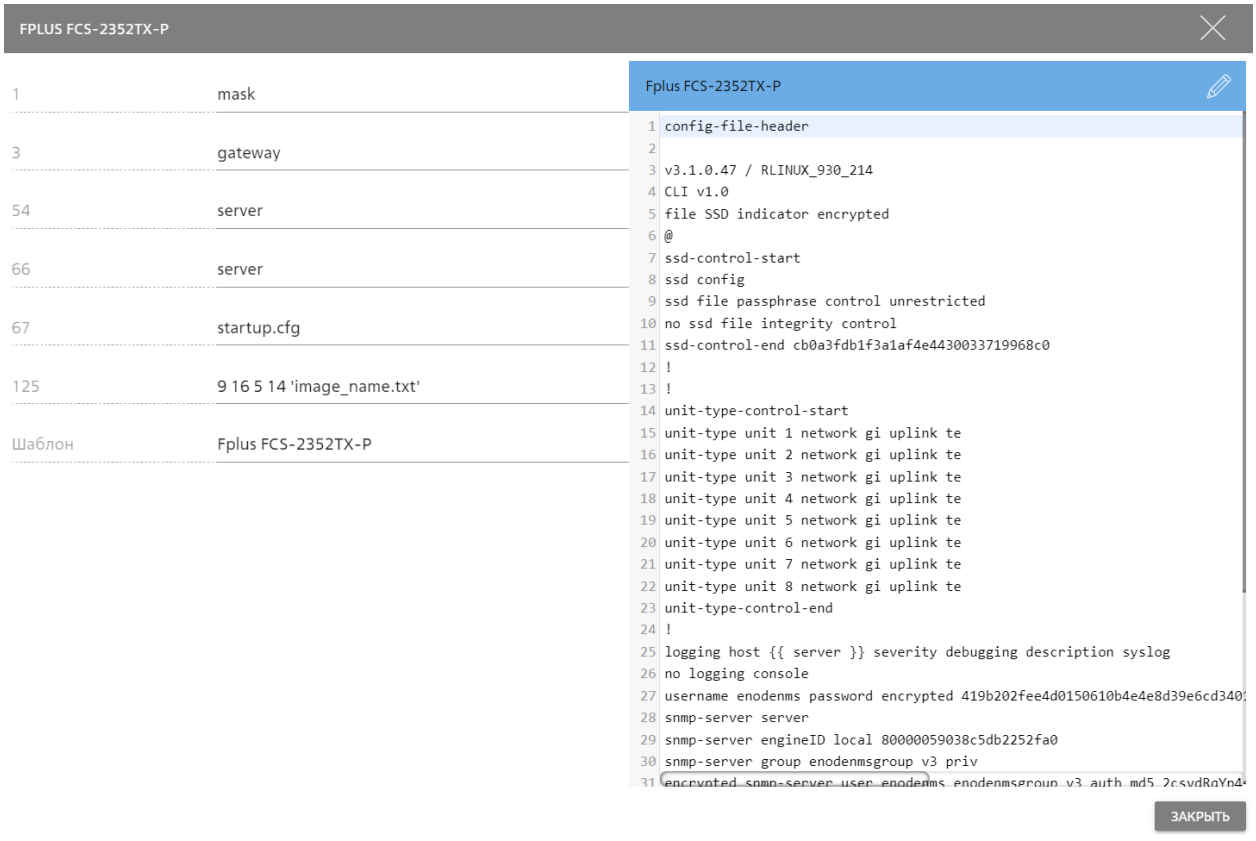


Рисунок 5.33 – Zero Touch Provisioning. Окно «Шаблоны»



5.19. Панель событий

«Панель событий» предназначена для отображения и фильтрации системных событий, уведомлений и журналов действий. Она состоит из следующих вкладок:

- Состояния;
- Действия;
- События;
- Обслуживание;
- Системный журнал.

В каждой вкладке все события отображаются с цветовой индикацией, соответствующей своему статусу, описанному в подразделе 5.1.

Внизу каждой вкладки «Панели событий» отображается номер текущей страницы и для перехода на страницу вперед нажмите стрелочку вправо, назад – стрелочку влево.

Содержимое каждой вкладки можно выгрузить в файлы в форматах **«.pdf»**, или **«.csv»** Для этого нажмите на соответствующий значок в правом углу строки заголовка выбранной вкладки.

5.19.1. Состояния

Вкладка «Состояние» (Рисунок 5.34) предназначена для отображения в хронологическом порядке перечня возникших событий объектов мониторинга на всех устройствах. Она содержит следующие данные:

- Время возникновения;
- Время квитирования;
- ID;
- Объект мониторинга;
- Класс – класс объекта мониторинга;
- Расположение – путь местоположения объекта мониторинга;
- Статус – какой характер возникшего события;
- Описание – описание возникшего события;

- Зона ответственности – ;
- Комментарий;
- Пользователь – логин пользователя, под действием которого вызвано данное событие.

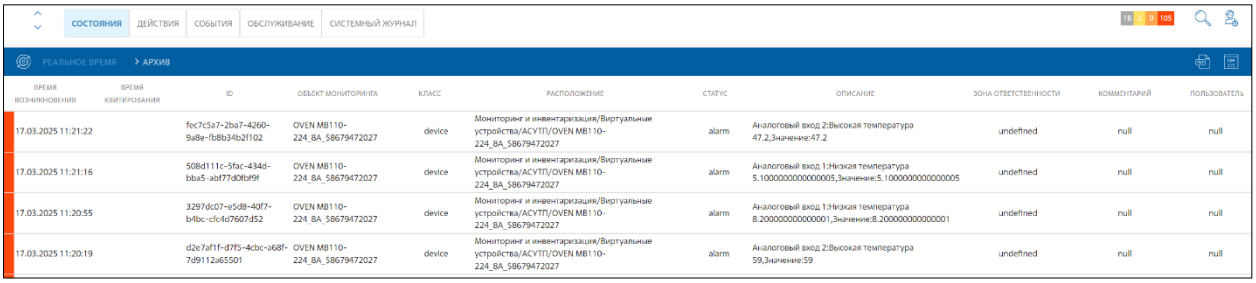


Рисунок 5.34 – Панель событий. Состояния

Отображение вкладки «Состояние» можно настроить при помощи фильтра. Для этого нажмите на символ  и во всплывающем окне (Рисунок 5.35) настройте фильтр по следующим параметрам:

- Дата начала и Дата окончания;
- Статус – статус события (Норма, Авария, Неизвестно, Предупреждение);
- Объект мониторинга – название объекта мониторинга;
- Класс – Устройство или не определено;
- Производитель – название фирмы производителя устройства;
- Тип устройства – Коммутатор, Не определено, Сервер, Программируемый логический контроллер;
- Шаблон – выбор ранее сохранённого шаблона фильтра.

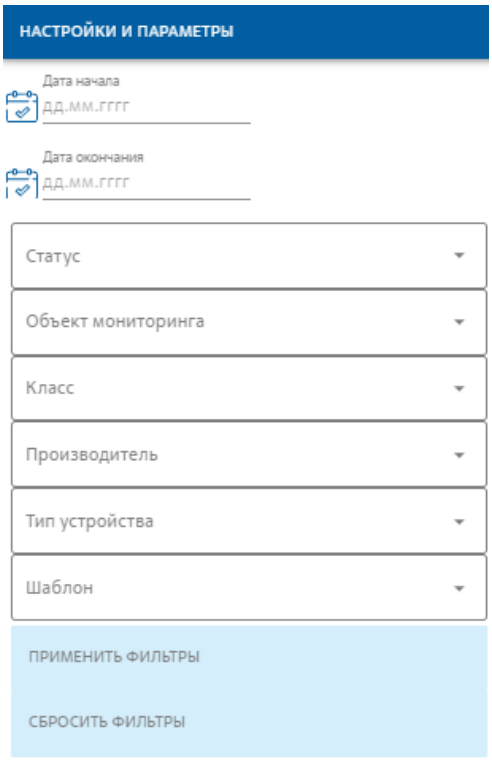


Рисунок 5.35 – Настройка фильтра вкладки «Состояния»

Фильтр позволяет сортировать список событий хотя бы по одному выбранному параметру.

После выбора всех нужных настроек нажмите на кнопку **«Применить фильтр»**. Для того чтобы сбросить настройки нажмите **«Сбросить фильтр»**.

При выборе объекта из перечня данной вкладки откроется окно с активной вкладкой «Мониторинг» (Рисунок 5.36), в которой представлена структура устройства с перечнем слотов и метрики по каждому из них. Метрики отображают:

- Имя – название слота;
- Последнее обновление – дата и время последнего обновления данных мониторинга;
- Значение – значение данных мониторинга модуля в данном слоте;
- График – ссылка на график (Рисунок 5.37).

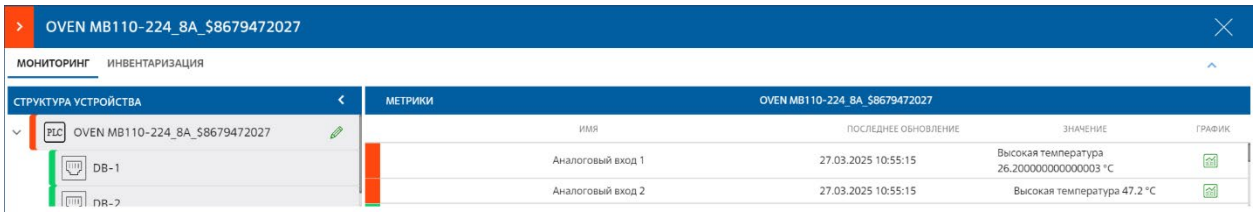


Рисунок 5.36 – Панель устройств. Окно устройства

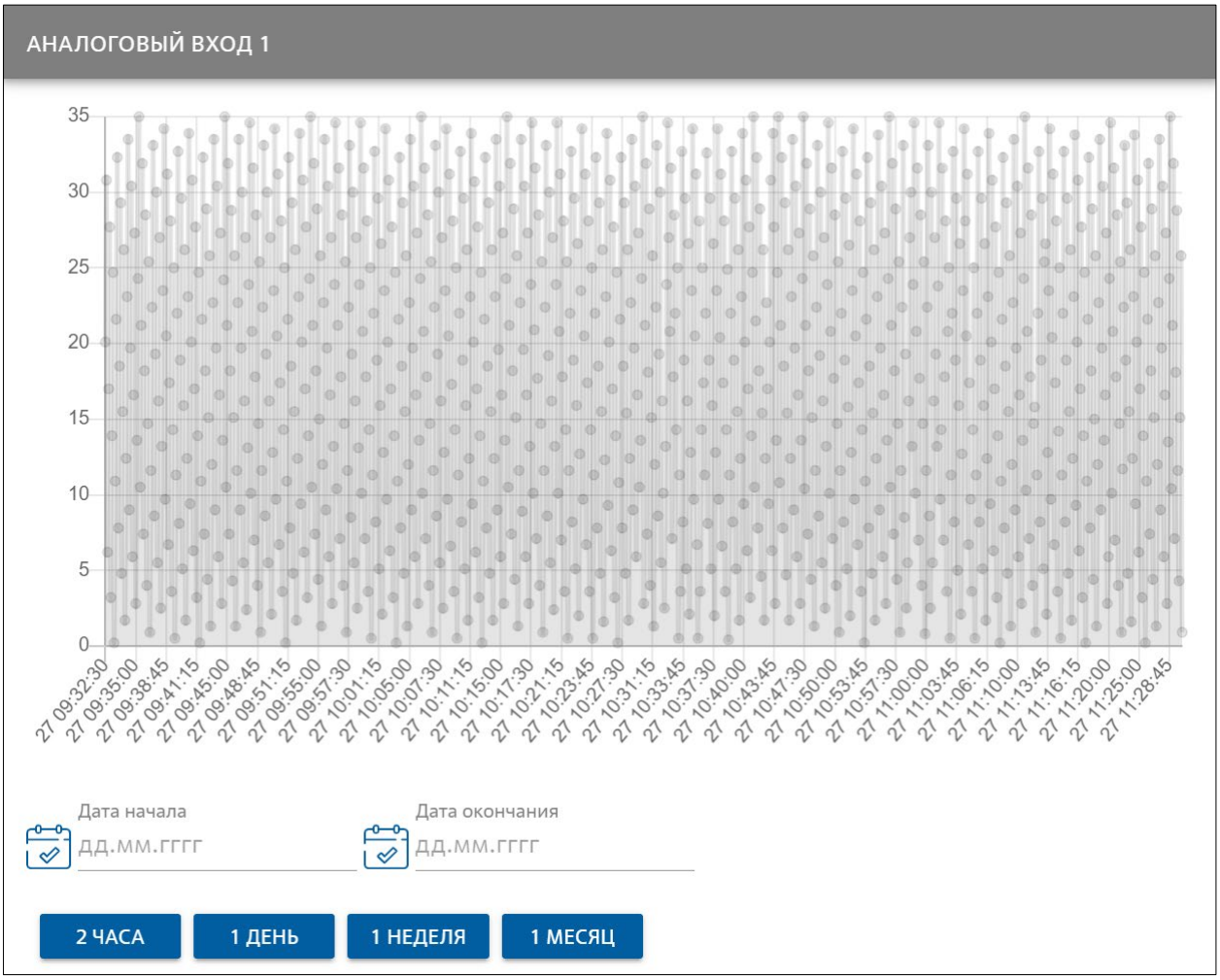


Рисунок 5.37 – Окно устройства. График

На графике отображаются значения измеряемых показателей в различный момент времени. Для указания интервала времени введите в поля «Дата начала» и «Дата окончания» нужные даты, либо воспользуйтесь предлагаемыми временными промежутками кнопками «2 часа», «1 день», «1 неделя», «1 месяц».

5.19.2. Действия

Вкладка «Действия» (Рисунок 5.38) предназначена для отображения событий, отражающие действия, совершенные по всем объектам управления. Данная вкладка имеет представление в режиме «Реальное время» и «Архив». В режиме «Реальное время» представлены все действия, которые возникли с момента запуска системы управления. Она содержит следующие данные:

- Время начала – время начала совершённого действия;
- Время завершения – время окончания совершённого действия;
- Статус – с каким статусом действие выполнено;
- Наименование задачи;
- Устройство – наименование устройства, в отношении которого действие совершено;
- Пользователь – кто автор совершённого действия;
- Описание – поле с комментариями о возникших ошибках совершенного действия.

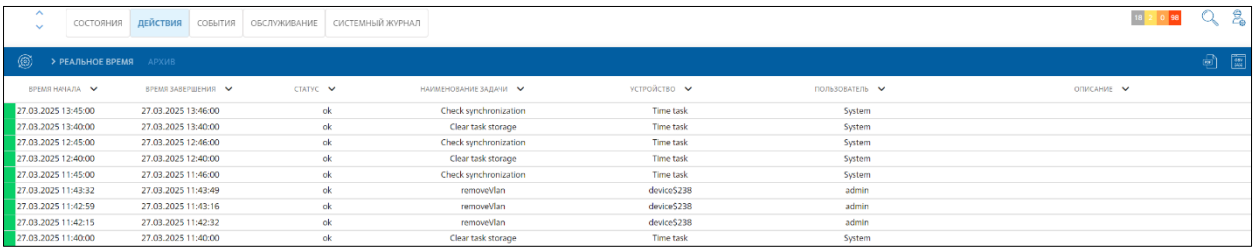


Рисунок 5.38 – Панель событий. Действия

В режиме «Архив» представлены действия, совершенные в течении всего времени работы Системы. Она имеет ту же форму представления данных, что и в режиме «Реальное время» за исключением того, что в части времени отображается время завершения действия.

Отображение вкладки «Действия» можно настроить при помощи сортировки по одной из колонок данных, а также применить фильтр.

Чтобы отсортировать список по одной из колонок данных нажмите на стрелочку рядом с именем выбранной колонки. Для сортировки сверху вниз и в алфавитном порядке стрелка должна быть направлена вниз, для сортировки снизу вверх и в обратном алфавитном порядке – вверх.

Чтобы применить фильтр нажмите на символ  и во всплывающем окне настройте фильтр по следующим параметрам:

- Дата начала и Дата окончания;
- Статус;
- Наименование задачи;
- Устройство;
- Пользователь.

Фильтр позволяет сортировать список событий хотя бы по одному выбранному параметру.

Если во вкладке «Действия» нажать на выбранное событие откроется окно (Рисунок 5.39) со списком сообщений Системы, сформированных во время выполнения данного действия, которое отражает:

- Идентификатор выбранного действия;
- Сообщение – выводится текст самого сообщения;
- Статус – насколько успешно событие данного действия выполнено;
- Описание – краткое описание по данному событию.

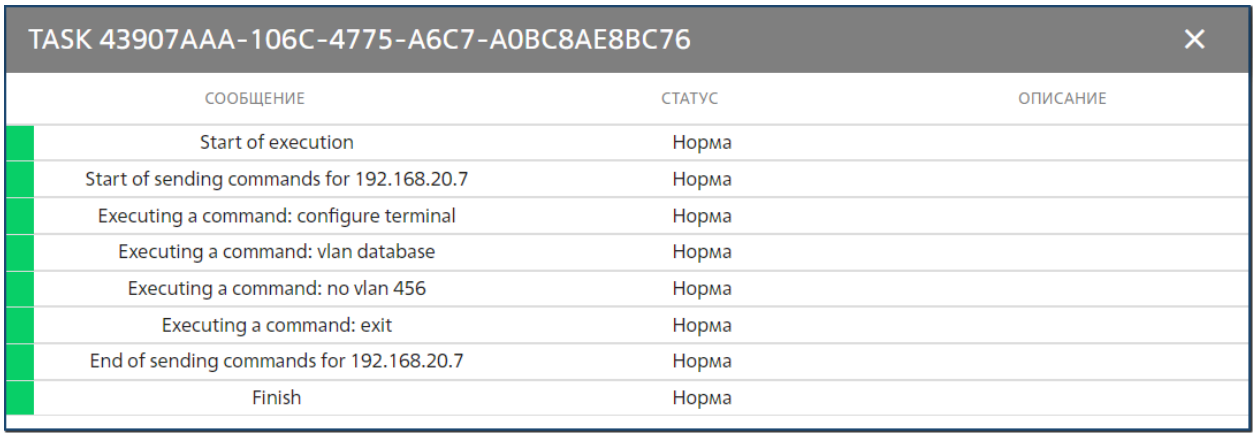


Рисунок 5.39 – Действия. Окно сообщений

5.19.3. События

Вкладка «События» предназначена (Рисунок 5.40) для отображения перечня событий, поступивших от устройства по протоколу SYSLOG, и содержит следующие данные:

- Тип;
- Время;
- Строгость;
- Хост;
- Описание.

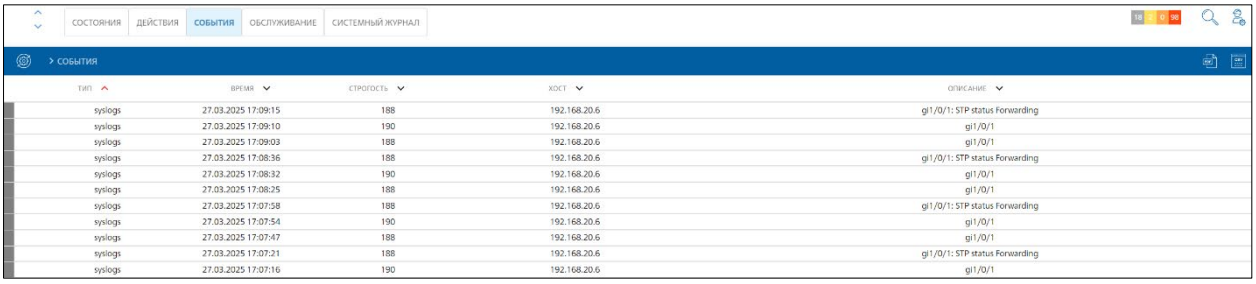


Рисунок 5.40 – Панель событий. События

Отображение вкладки «События» можно настроить при помощи сортировки по одной из колонок данных, а также применить фильтр.

Чтобы отсортировать список по одной из колонок данных нажмите на стрелочку рядом с именем выбранной колонки. Для сортировки сверху вниз и в алфавитном порядке стрелка должна быть направлена вниз, для сортировки снизу вверх и в обратном алфавитном порядке – вверх.

Чтобы применить фильтр нажмите на символ  и во всплывающем окне настройте фильтр по следующим параметрам:

- Дата начала и Дата окончания;
- Тип;
- Строгость;
- Хост.

Фильтр позволяет сортировать список событий хотя бы по одному выбранному параметру.

5.19.4. Обслуживание

Вкладка «Обслуживание» (Рисунок 5.41) предназначена для отображения всех событий технического обслуживания устройств, и содержит следующие данные:

- Состояние – текущий статус события;
- Event name – Название события;
- Дата – дата и время завершения события;
- Тип – тип события обслуживания;
- Имя – название объекта обслуживания;
- Автор – автор события обслуживания;
- Расположение – путь местоположения объекта обслуживания.

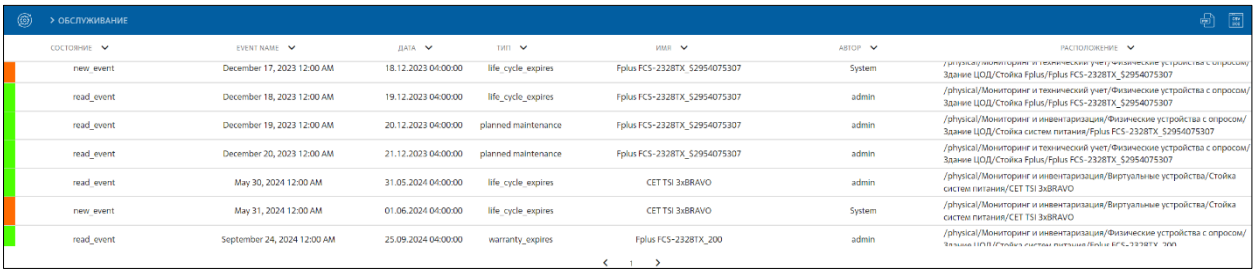


Рисунок 5.41 – Панель событий. Обслуживание

Отображение вкладки «Обслуживание» можно настроить при помощи сортировки по одной из колонок данных, а также применить фильтр.

Чтобы отсортировать список по одной из колонок данных нажмите на стрелочку рядом с именем выбранной колонки. Для сортировки сверху вниз и в алфавитном порядке стрелка должна быть направлена вниз, для сортировки снизу вверх и в обратном алфавитном порядке – вверх.

Чтобы применить фильтр нажмите на символ  и во всплывающем окне настройте фильтр по следующим параметрам:

- Дата начала и Дата окончания;
- Состояние;
- Event name;
- Дата;
- Тип;
- Имя;
- Автор;
- Расположение.

Фильтр позволяет сортировать список событий хотя бы по одному выбранному параметру.

Если во вкладке «Обслуживание» нажать на выбранное событие откроется окно (Рисунок 5.42) с дополнительными сведениями о нём.

Чтобы откорректировать сведения или указать комментарии нажмите на «Карандаш» и внесите изменения.

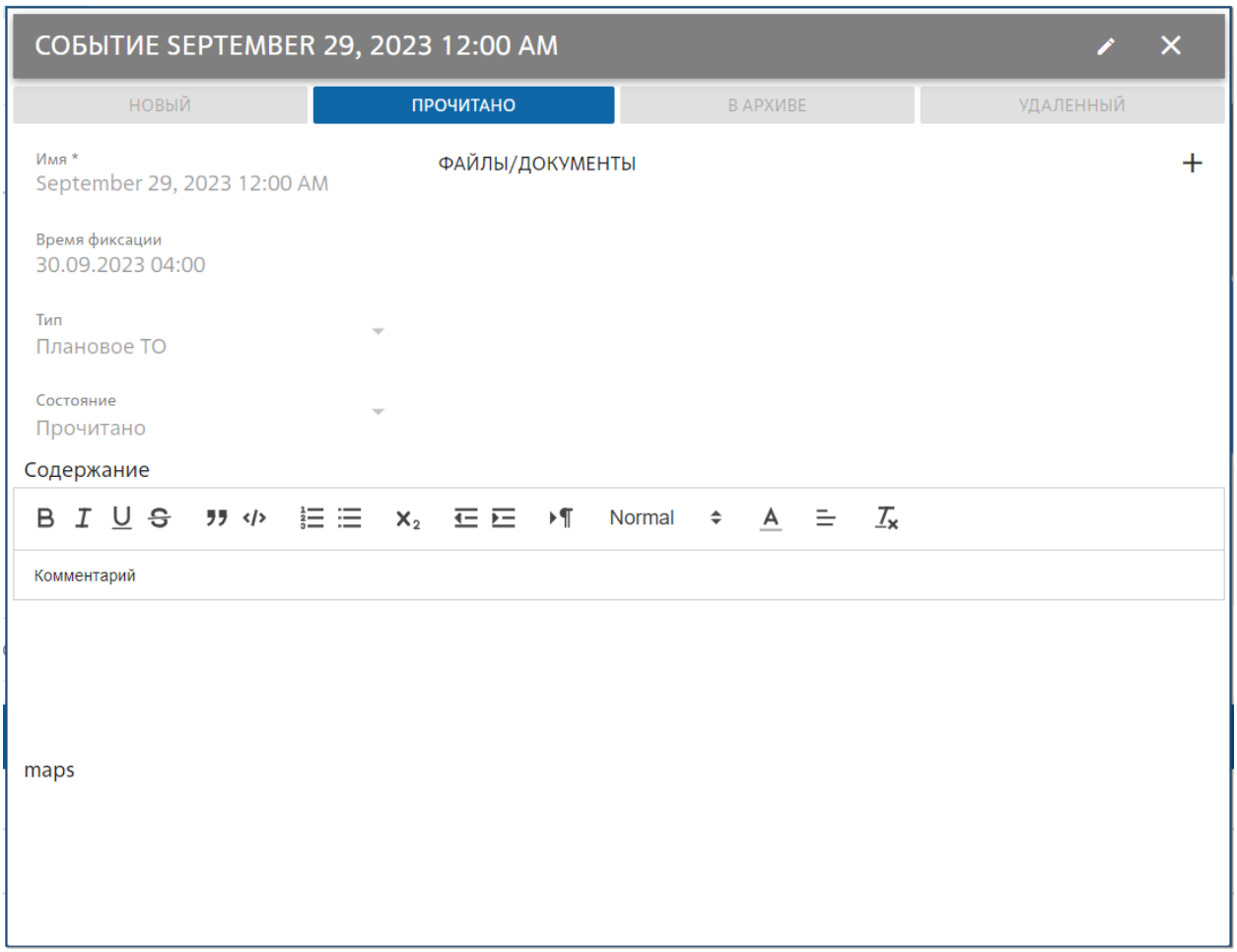


Рисунок 5.42 – Окно события вкладки «Обслуживание»

5.19.5. Системный журнал

Вкладка «Системный журнал» (Рисунок 5.43) предназначена для отображения перечня событий, внесенных в системный журнал системы управления e-node, и содержит следующие данные:

- Тип – источник сервиса;
- Время;
- Строгость;
- Хост;
- Описание.

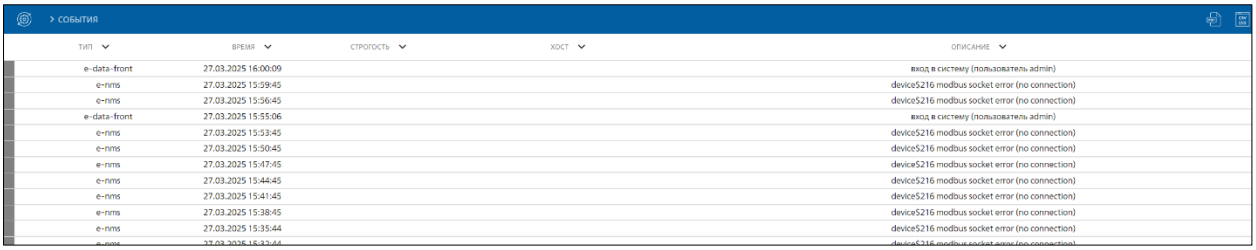


Рисунок 5.43 – Панель событий. Системный журнал

Отображение вкладки «Системный журнал» можно настроить при помощи сортировки по одной из колонок данных, а также применить фильтр.

Чтобы отсортировать список по одной из колонок данных нажмите на стрелочку рядом с именем выбранной колонки. Для сортировки сверху вниз и в алфавитном порядке стрелка должна быть направлена вниз, для сортировки снизу вверх и в обратном алфавитном порядке – вверх.

Чтобы применить фильтр нажмите на символ  и во всплывающем окне настройте фильтр по следующим параметрам:

- Дата начала и Дата окончания;
- Тип;
- Строгость;
- Хост.

Фильтр позволяет сортировать список событий хотя бы по одному выбранному параметру.