Платформа Радар

Руководство администратора

Версия 4.1.0

ООО «Пангео Радар»

Оглавление

1. Общие сведения о «Платформе Радар»

Специализированное программное обеспечение «**Платформа Радар**» (далее – **СПО РАДАР**, **Платформа Радар**, платформа) является программным средством общего назначения со встроенными средствами защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, и предназначено для автоматизации процессов сбора, обработки и корреляции событий информационной безопасности (далее – ИБ) с целью выявления инцидентов и организации реагирования на них.

Платформа обеспечивает решение следующих задач:

- сбор информации об активах, их учет и управление записями об активах;
- сбор событий ИБ от активов и/или от установленного на активах ПО;
- автоматическая обработка поступивших событий (нормализация, обогащение);
- загрузка и анализ результатов работы сканеров уязвимостей;
- корреляция событий, создание записей об инцидентах и управление ими;
- автоматизированный контроль реагирования на инциденты, контроль устранения;
- получение, обновление и использование информации об угрозах;
- ручной анализ событий ИБ при расследовании инцидентов;
- формирование отчетов, в том числе в графическом виде (рабочие столы).

СПО РАДАР имеет сертификат соответствия ФСТЭК России № 4210 от 05 февраля 2020 г. (переоформлен 22 марта 2022 г.), срок действия: пять лет.

2. Требования

Для работы с сервисом пользователю необходимы:

- Современный компьютер с операционной системой. Работа с сервисом возможна на следующих ОС:
  - Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;
  - Apple Mac OS X: 10.6 (Snow Leopard) и выше;
  - Linux: AltLinux 7 (x86/x64), Debian 7 (x86/x64), Mint 13 (x86/x64), SUSE Linux Enterprise Desktop 12 (x64), openSUSE 13 (x86/x64), Ubuntu 12.04 (x86/x64) и более современные версии указанных дистрибутивов
- Монитор с разрешением не менее 1920x1080.

Для работы с графическим интерфейсом **СПО Радар** на АРМ пользователя должен быть установлен один из следующих браузеров:

- **Microsoft Edge;**
- **Google Chrome;**
- **Mozilla Firefox;**
- **Яндекс.Браузер.**

3. Вход в платформу

Вход пользователей в **Платформу Радар** осуществляется через Web-браузер.

Для входа в платформу в браузере перейдите по адресу https://host:port//

Где:

- host – IP-адрес или доменное имя устройства, на котором расположен сервер платформы;
- port – порт, который задан для точки подключения.

Откроется окно «Вход» (см. «Рис. 1»).

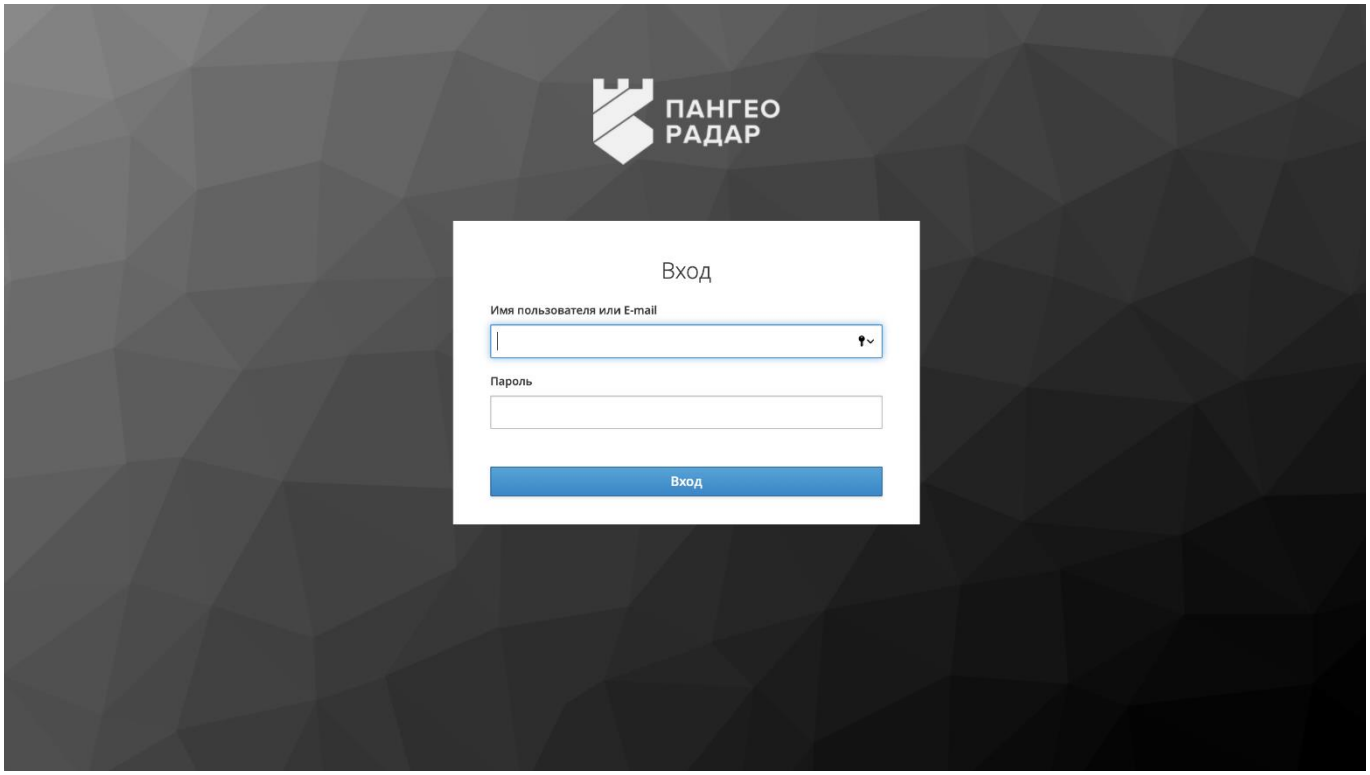


Рис. 1 – Окно входа в платформу

Укажите имя пользователя и пароль в соответствующих полях и нажмите кнопку **Войти**.

При первой аутентификации **Платформа Радар** может потребовать от пользователя сменить пароль.

После входа в платформу откроется раздел «Рабочие столы», в котором отображаются интерактивные информационные панели с информацией о текущем состоянии безопасности. Подробнее см. раздел «Рабочие столы».

4. Интерфейс платформы

Интерфейс платформы состоит из шапки сайта, панели разделов, боковой панели, рабочей области и элементов управления

Рабочая область раздела имеет два варианта представления:

- через универсальные таблицы;
- через боковую панель и формы работы с объектами (просмотр, создание, редактирование).

По умолчанию все разделы открываются в табличном представлении (см. Рис. 2).

Рис. 2 – Интерфейс Платформы Радар. Табличное представление

Для переключения с табличного представления раздела на боковую панель необходимо открыть объект на просмотр (кнопка  или по ссылке в колонке **Название**). Откроется представление раздела через боковую панель и форма просмотра выбранного объекта (см. «Рис. 3»).

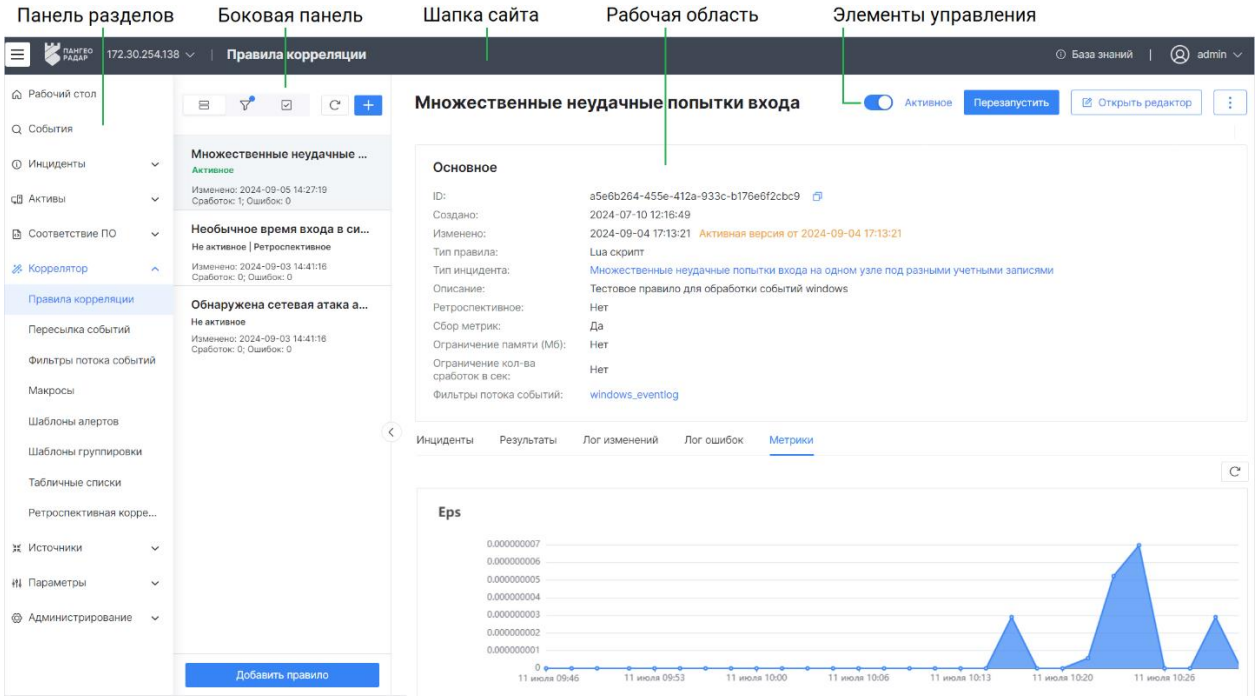
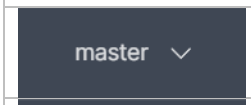
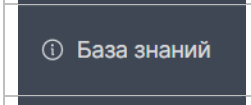
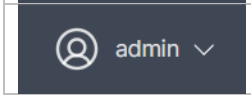


Рис. 3 – Интерфейс Платформы Радар. Представление через боковую панель и формы объектов

4.1 Шапка сайта

Шапка сайта является единой для всех разделов платформы и содержит следующие элементы управления:

Кнопка	Действие
	показать/скрыть панель разделов
	выбор инстанса
	доступ к базе знаний платформы
	наименование текущей учетной записи и доступ к выходу из учетной записи

4.2 Панель разделов

Для каждого пользователя список разделов формируется индивидуально в соответствии с возможностями, выданными данному пользователю.

Список разделов, доступных в секции **Администрирование** панели разделов **Платформы Радар**:

- Рабочие столы. Раздел предназначен управления интерактивными информационными панелями.
- Отчеты. Раздел предназначен для формирования отчетов о состоянии информационной безопасности.

- Мониторинг. Раздел предназначен для отслеживания метрик мониторинга платформы.
- Пользователи и права. Раздел предназначен для управления доступом к платформе и содержит следующие настройки:
    - Пользователи – управление пользователями платформы;
    - Группы – управление группами пользователей;
    - Роли – управление возможностями, которые доступны пользователям в платформе;
    - Аудит действий – просмотр действий, совершаемых пользователями в платформе;
    - События входа –просмотр событий входа в платформу;
    - LDAP – настройка интеграции с сервером LDAP;
    - Доступ к данным – управление доступом пользователей к данным (активам, событиям и т.д.).
- Кластер. Раздел предназначен для управления кластером платформы и содержит следующие настройки:
    - Узлы системы – управление узлами кластера;
    - Управление конфигурацией – управление параметрами сервисов;
    - API ключи – управление доверенными ключами API, которые используются для межсервисного взаимодействия и для обращения в **Платформу Радар** из сторонних решений посредством публичного API;
    - Учетные записи для сбора данных – управление учетными записями для сбора данных с хостов и активов;
    - Планировщик задач – управление и организация периодических задач кластера;
    - Скрипты – управление скриптами, которые можно удаленно запустить на узле кластера для выполнения необходимых действий;
    - Управление мультиарендностью – настройка **Платформы Радар** для работы в инфраструктуре мультитенант или мультиарендность.
- Репутационные списки. Раздел предназначен для управления репутационными списками, которые могут использоваться в процедуре обогащения событий;
- Источники IOC. Раздел предназначен для настройки поставщиков индикаторов компрометации, которые используются при работе репутационных списков.
- Лицензия. Раздел предназначен для просмотра параметров лицензии и повторной активации лицензии.

4.3 Универсальные таблицы

Универсальные таблицы в платформе – это список объектов, представленных в табличном виде и имеющие единые элементы управления (см. «Рис. 4»).

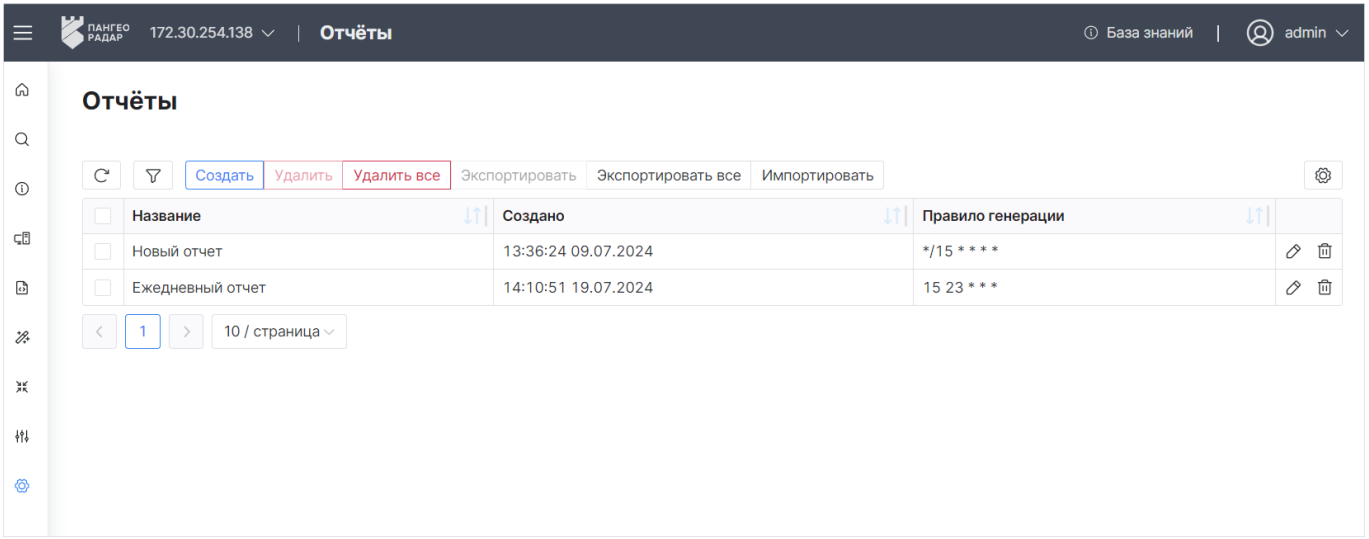


Рис. 4 -- Рабочая область. Таблицы

Элементы управления располагаются над таблицей и в общем случае состоят из следующих кнопок:

Кнопка	Действие
	обновление данных
	настройка сортировки и фильтрации записей таблицы
	если у кнопки есть специальный значок, то это означает что к таблице применяется фильтр
Создать	создание записи/объекта в таблице
Удалить	удаление выбранной записи/объекта из таблицы
Удалить все	удаление всех показанных записей/объектов. Будут удалены все записи/объекты, попавшие под параметры сортировки и фильтрации
Экспортировать	экспорт выбранной записи/объекта
Экспортировать все	экспорт всех показанных записей/объектов. Будут выгружены в архив все записи/объекты, попавшие под параметры сортировки и фильтрации
Экспортировать выбранные в csv	массовый экспорт выбранных записей/объектов в формат CSV
Экспортировать в csv	экспорт всех показанных записей/объектов в формат CSV. Будут выгружены в файлы формата CSV все записи/объекты, попавшие под параметры сортировки и фильтрации
Импортировать	импорт записей/объектов в таблицу
Переместить в папку	переместить выбранные объекты в папку

Кнопка	Действие
	настройка столбцов таблицы

В колонках таблицы могут располагаться следующие кнопки:

Кнопка	Действие
	выбор направления сортировки выбранной колонки
	просмотр подробных сведений об объекте
	изменение информации об объекте
	удаление объекта

4.3.1 Настройка сортировки и фильтрации записей таблицы

Для поиска необходимого объекта по значениям полей и формирования списка может быть использован фильтр. Для настройки фильтра выполните следующие действия:

1. Нажмите на кнопку  . Откроется блок для настройки сортировки и фильтрации (см. «Рис. 5»).

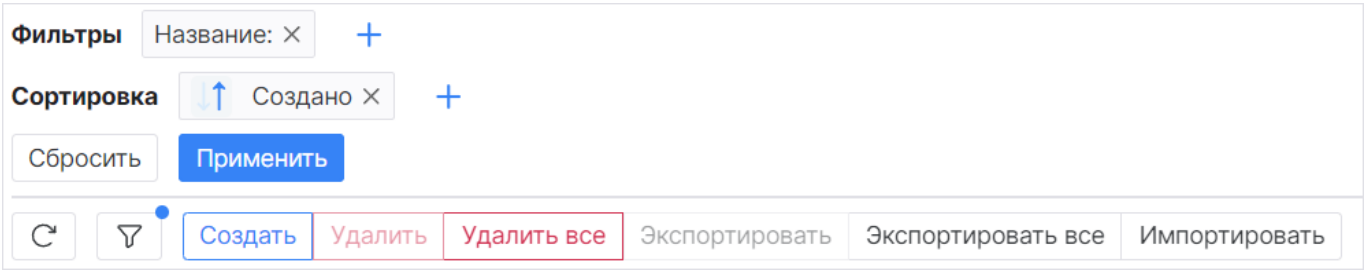


Рис. 5 – Таблица. Блоки для настройки фильтров и сортировки

2. В блоке **Фильтры** нажмите кнопку «+» для добавления столбца, по которому будет выполняться фильтрация. Можно выполнить фильтрацию по значения нескольких столбцов.
3. В блоке **Сортировка** нажмите кнопку «+» для выбора столбца, по значениям которого будет задано направление сортировки (**↓, ↑**). Можно выполнить сортировку по значениям нескольких столбцов.
4. Нажмите кнопку **Применить**. При просмотре таблицы к ней будет автоматически применяться настроенный фильтр.
5. Если необходимо очистить параметры фильтра, то нажмите кнопку **Сбросить**.

4.3.2 Настройки отображения полей

Для изменения состава отображаемых полей (колонок таблицы) используйте кнопку  . При нажатии на кнопку откроется список, в котором можно выбрать поля для отображения (см. «Рис. 6»).

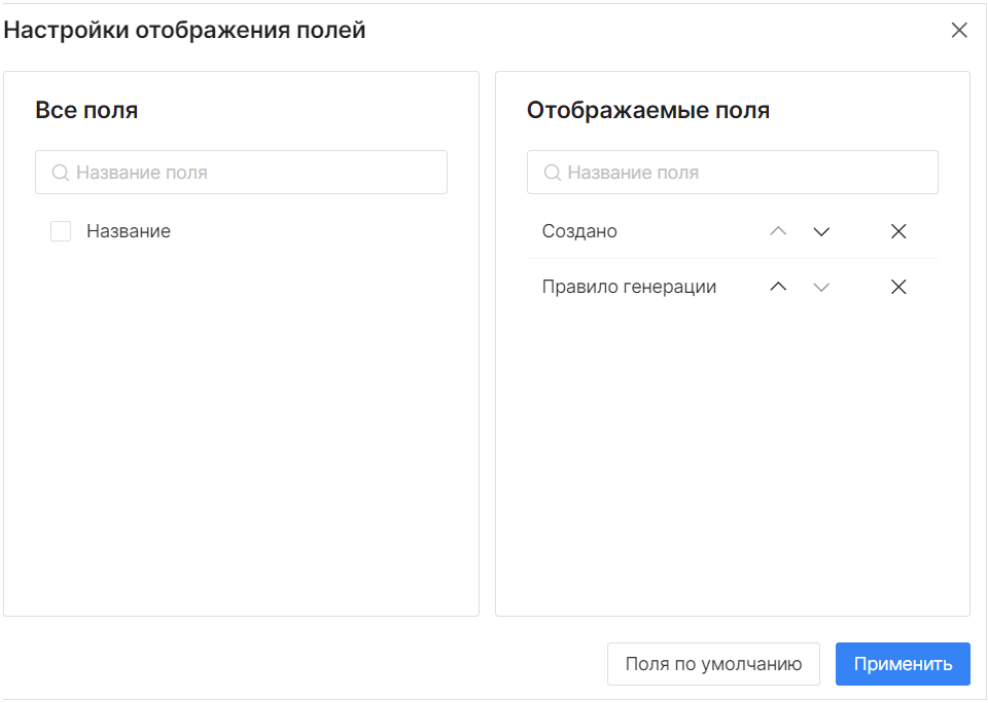


Рис. 6 – Настройки отображения полей

4.4 Боковая панель

В общем случае боковая панель предназначена для поиска, сортировки, фильтрации и выбора объекта, для вывода информации о нем в рабочей области (см. «Рис. 7»).

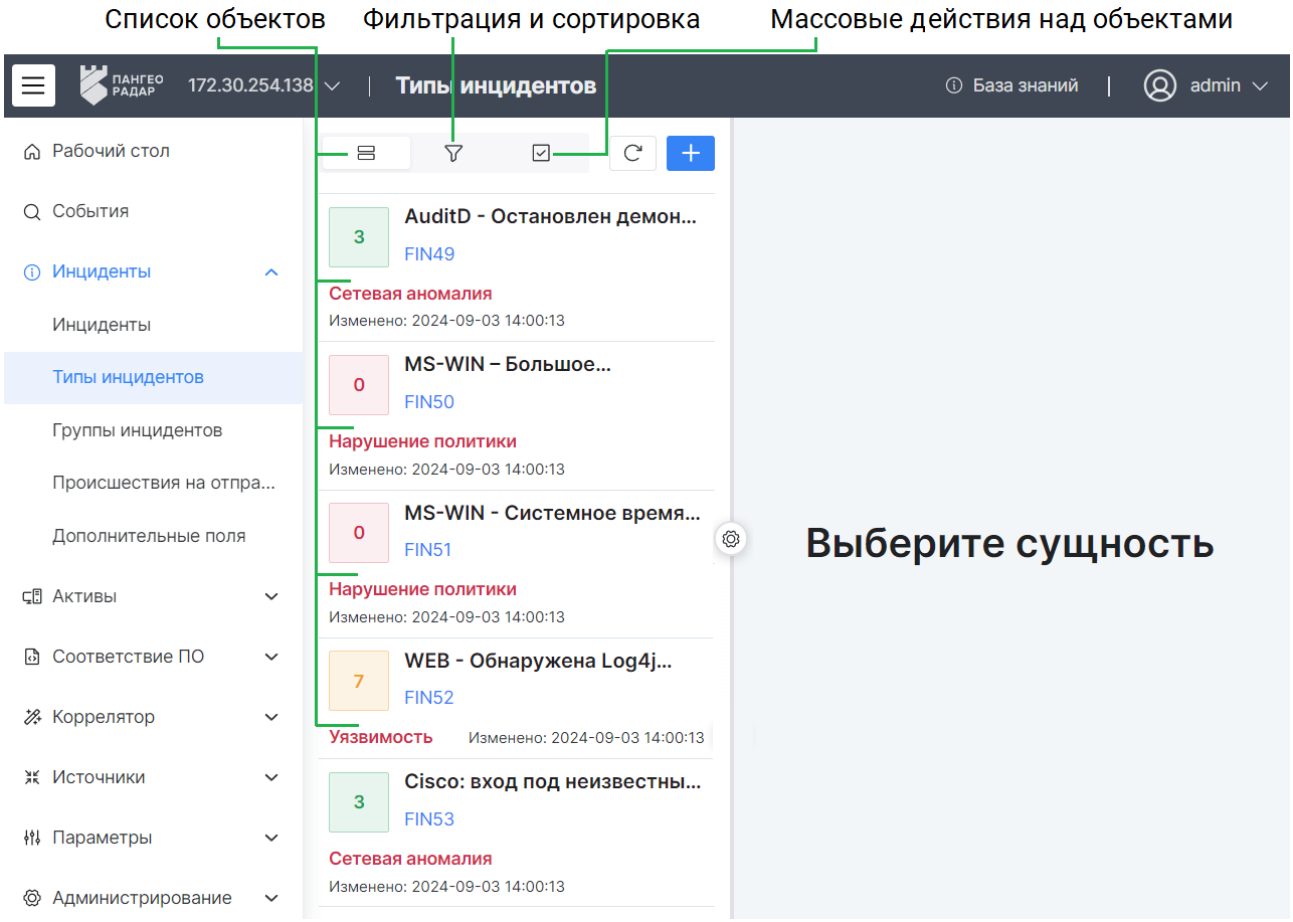


Рис. 7 – Боковая панель. Список объектов

На боковой панели доступны следующие элементы управления:

Кнопка	**Действие**
+	показать/скрыть панель разделов
	настройка сортировки и фильтров для поиска
	включение возможности выбора объектов для выполнения над ними массовых операций и доступ к следующим действиям над объектами: - импорт объектов; - экспорт выбранных объектов; - экспорт всех объектов - удаление выбранных объектов; - удаление всех объектов.
Нажатие ЛКМ по объекту	выбор объекта и вывод информации об объекте в рабочую область
	настройка отображения боковой панели

4.4.1 Поиск объектов в списке

Для поиска объекта нажмите кнопку  , укажите значение или часть значения в поле **Текстовый поиск** и нажмите кнопку **Применить**. Будут выданы подходящие данные.

4.4.2 Сортировка и фильтрация объектов в списке

1. Нажмите кнопку  . Откроется блок для настройки сортировки и фильтрации объектов в списке (см. «Рис. 8»).

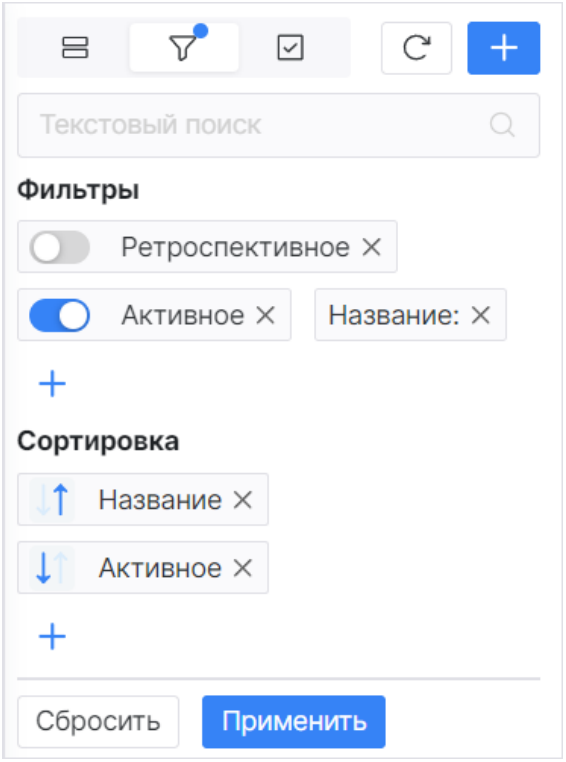


Рис. 8 – Боковая панель. Сортировка и фильтрация

2. Если для объекта доступна фильтрация по конкретным полям (для некоторых объектов фильтрация недоступна), то в блоке **Фильтрация** укажите необходимые значения полей.
3. В блоке **Сортировка** выполните следующие действия:
   - Добавьте поля, по которым должна выполняться сортировка
   - Выберите направление сортировки:
     - ↓ - от последнего к первому;
     - ↑ - от первого к последнему.
4. Нажмите кнопку **Применить**.

   Если необходимо очистить параметры сортировки и фильтрации, то нажмите кнопку **Сбросить**.

4.4.3 Массовые действия

Количество массовых операций, доступных над объектами в разделах платформы, может отличаться.

В общем случае над объектами доступны следующие массовые действия:

- **Импортировать** - импорт объектов в платформу;

- **Экспортировать** - экспорт выбранных объектов;
- **Экспортировать все** - экспорт всех отфильтрованных объектов. Будут экспортированы все объекты, попавшие под параметры сортировки и фильтрации;
- **Удалить** - удаление выбранных объектов;
- **Удалить все** - удаление всех отфильтрованных объектов. Будут удалены все объекты, попавшие под параметры сортировки и фильтрации.

Для выполнения массового действия выполните следующие шаги:

1. Нажмите на кнопку ⋮ и из выпадающего списка выберите пункт **Массовые действия**. Появятся флаги для выбора табличных списков (см. «Рис. 9»).

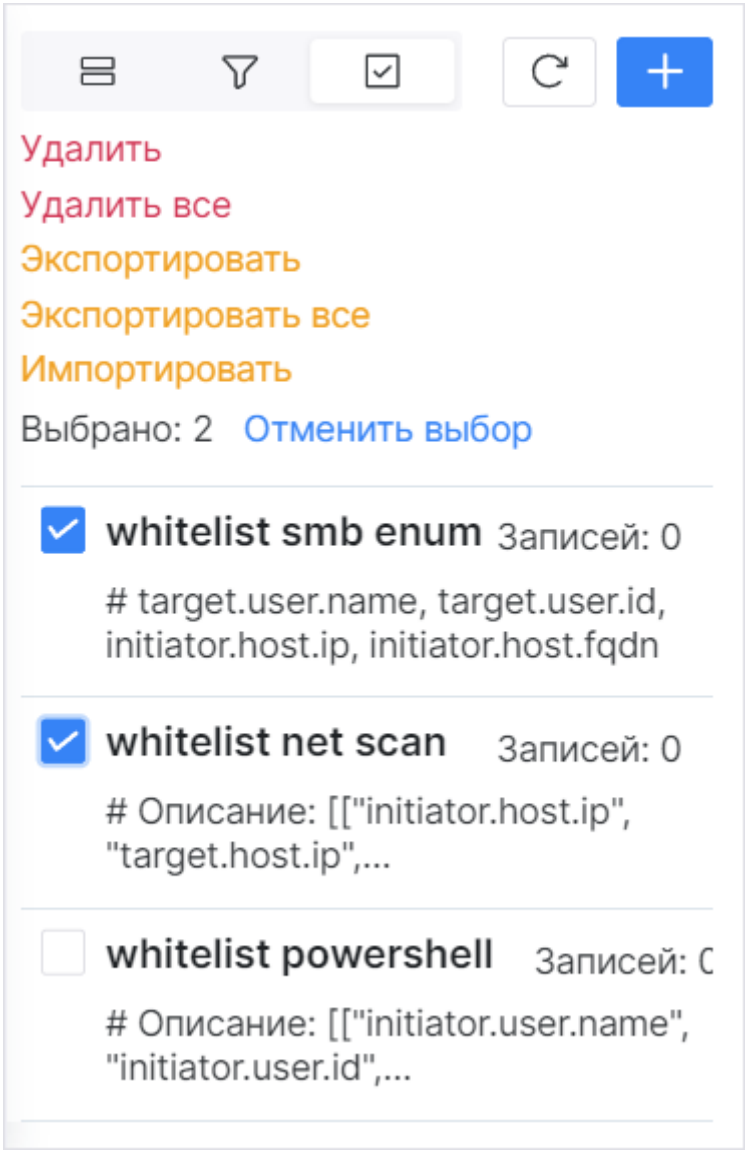


Рис. 9 – Массовые действия над табличными списками

2. Выберите объекты, установив соответствующие флаги.
3. Нажмите на соответствующую кнопку действия.
4. Завершите действие в открывшемся окне.

4.5 Папки контента

Для упрощения работы и структурирования пользовательского контента в платформе используется механизм **папок**.

Управление папками контента выполняется в разделе **Параметры → Папки контента**.

Просмотр содержимого папок выполняется через боковую панель соответствующего раздела
(см. «Рис. 10»).

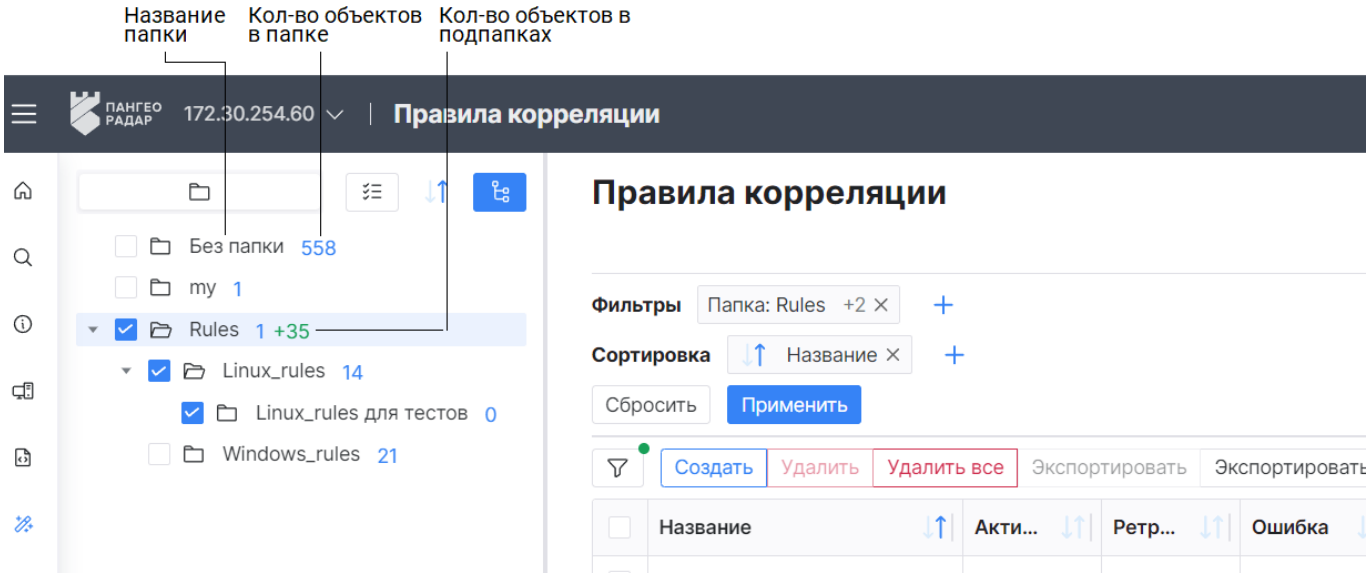


Рис. 10 – *Боковая панель. Папки контента*

При просмотре содержимого папок доступны следующие элементы управления:

Кнопка	Действие
/	выбрать элементы/отменить выбор элементов
	настройка сортировки и фильтров для поиска
/	включение/выключение режима каскадного выбора. Режим позволяет по клику на папку автоматически выбрать папки на всю глубину вложения. Режим по умолчанию включен

Отображение содержимого папок работает по следующему принципу:

- при клике на папку, в универсальной таблице отобразится содержимое выбранной папки;
- если папка является родительской, то при клике на папку раскрывается дерево дочерних папок;
- если установлены флаги для нескольких папок, в универсальной таблице отобразятся все объекты, содержащиеся в выбранных папках;
- если включен каскадный режим, то при клике на родительскую папку автоматически устанавливаются флаги на дочерние папки.

Для создания пользовательского контента в папке выполните следующие действия:

1. Перейдите в нужный раздел.
2. Начните процесс создания.
3. В поле **Папка** из выпадающего списка выберите нужную папку.

Для переноса пользовательского контента в папку выполните следующие действия:

1. Перейдите в нужный раздел.
2. Выберите нужные объекты, установив соответствующие флаги.
3. Нажмите кнопку **Переместить в папку**.
4. В открывшемся окне выберите папку и нажмите кнопку **Переместить**.

В версии 4.1.0 данный механизм доступен для следующего контента:

- Правила корреляции.

4.6 Формы работы с объектами

Основная работа пользователя с объектами осуществляется на странице **Форма работы с объектами**. Формы объектов могут быть следующих типов:

- Создание;
- Просмотр;
- Редактирование.

Форма работы с объектами имеет различный вид в зависимости от объекта и выполняемого действия (см. «Рис. 11»).

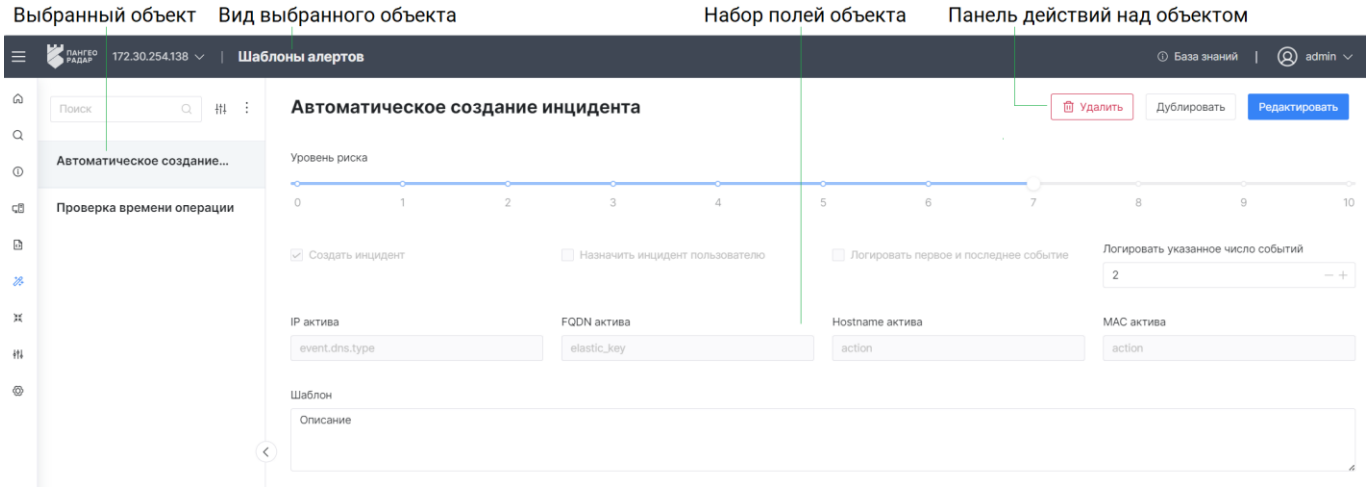


Рис. 11 – Рабочая область. Форма объекта

В общем случает страница состоит из следующих элементов:

- **Поля формы** – содержит поля для указания сведений и выполнения настроек объекта;

- **Панель действий** – содержит кнопки для работы с объектами. Кнопки, которые не помещаются на панели действий, будут помещены в выпадающее меню, доступное по кнопке  .

Панель действий может содержать следующие элементы управления:

Кнопка	Тип формы объекта	Действие
Редактировать /	Просмотр	Изменение информации об объекте
Дублировать	Просмотр	Создание нового объекта на основе существующего
Назначить пользователю /	Просмотр	Выдача прав на работу с объектом выбранному пользователю
Назначить группе пользователей /	Просмотр	Выдача прав на работу с объектом выбранной группе пользователей
Написать ответственному	Просмотр	Написать сообщение ответственному пользователю. История сообщений доступна в профиле пользователя
Добавить в группу	Просмотр	Добавление объекта в выбранную группу
Опубликовать	Просмотр	Публикация изменений на всех подчиненных инстансах
Сохранить	Создание / Редактирование	Сохранение сведений об объекте
Сбросить	Создание / Редактирование	Сброс введенных сведений об объекте
Создать	Создание	Создание объекта
←	Все	Возврат на предыдущую страницу

4.6.1 Шаблоны объектов

Для упрощения создания/редактирования объектов в платформе используется механизм **шаблонов**.

Шаблон будет определять структуру данных, внешний вид и поведение форм создания/редактирования объектов.

Для создания шаблона выполните следующие действия:

1. Откройте необходимый объект на создание или редактирование.
2. Настройте поля формы.
3. Нажмите кнопку **Сохранить как шаблон** (располагается внизу формы).
4. Укажите название шаблона в открывшемся окне и нажмите кнопку **Сохранить**.
5. Шаблон будет сохранен в платформе. Информацию о шаблоне можно посмотреть в разделе **Параметры → Шаблоны**.

Для использования шаблона выполните следующие действия:

1. Откройте форму необходимого объекта на создание или редактирование.
2. В поле **Использовать существующий шаблон** из выпадающего списка выберите заранее созданный шаблон.
3. Поля формы будут автоматически заполнены данными из шаблона.

В версии 4.1.0 данный механизм доступен для следующих объектов:

- Профили сбора.

4.6.2 Визуализации

Визуализации – это графики, виджеты, метрики и т.д. (см. «Рис. 12»).

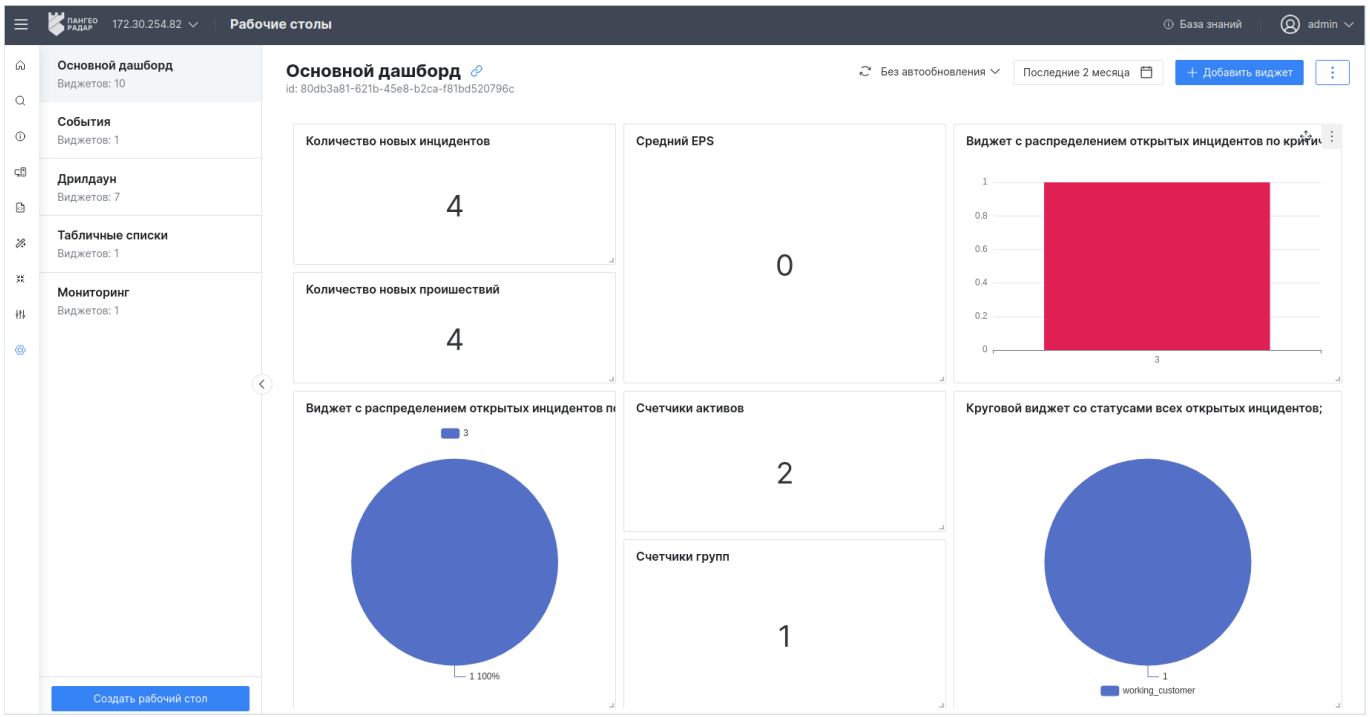


Рис. 12 – Рабочая область. Визуализации

Визуализации имеют различные элементы управления, которые подробно расписаны в соответствующих разделах.

5. Рабочие столы

5.1 Общие данные

Рабочие столы – это интерактивные информационные панели, которые отображают данные о состоянии информационной безопасности.

Отображение информации выполняется с помощью следующих типов виджетов:

- временной ряд;
- круговая диаграмма;
- таблица;
- текст;
- гистограмма;
- метрика;
- изображение.

Подробнее о каждом типе виджета вы можете ознакомиться в разделе «Конструктор виджетов». Работа с рабочими столами включают в себя следующие процессы:

1. Создание рабочего стола.
2. Редактирование рабочего стола.
3. Управление виджетами.
4. Копирование рабочего стола.
5. Создание отчета.
6. Удаление рабочего стола.

Для работы с рабочими столами перейдите в новый интерфейс, откройте раздел **Администрирование** → **Рабочие столы** и выберите рабочий стол из списка.

Внешний вид рабочего стола формируется в зависимости от выставленной пользователем конфигурации виджетов.

Пример интерфейса раздела представлен на «Рис. 13».

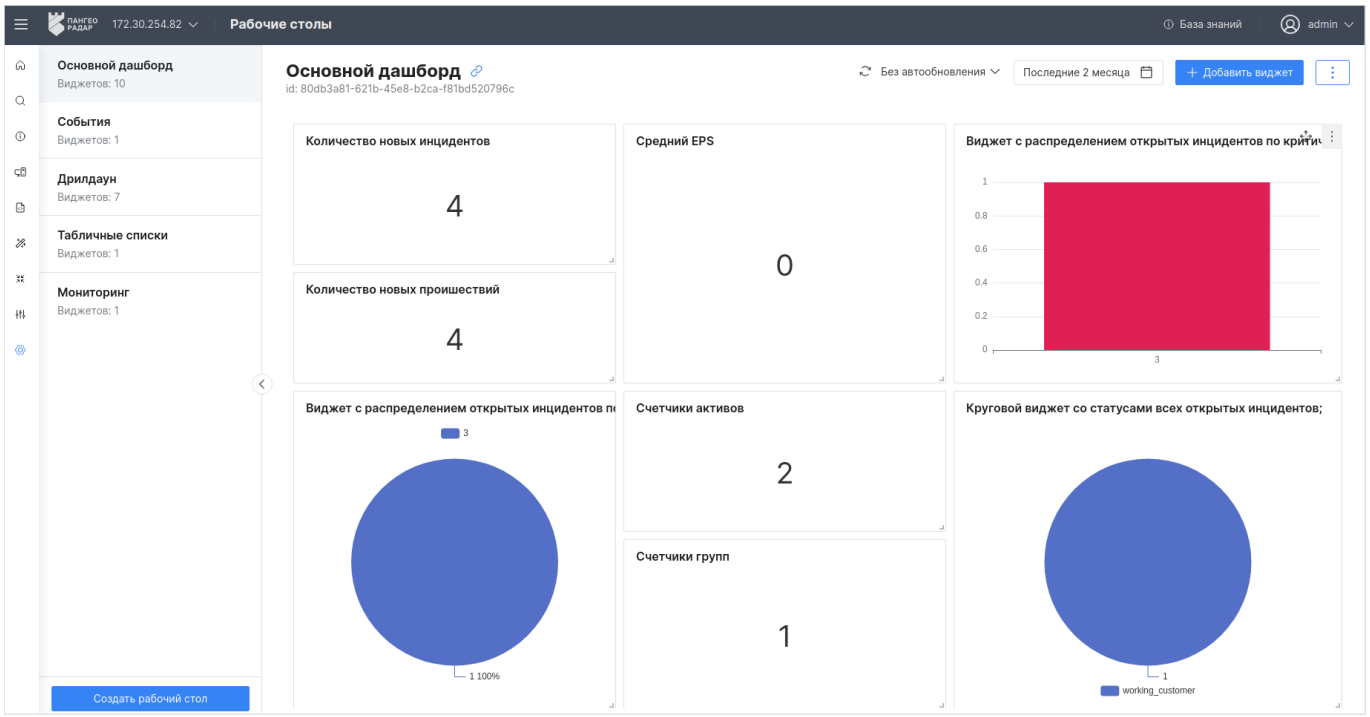


Рис. 13 – Интерфейс раздела "Рабочие столы"

Раздел состоит из следующих блоков:

- **Список рабочих столов**, в котором отображается информация о доступных рабочих столах:
  - название рабочего стола;
  - количество виджетов, добавленных на рабочий стол.
- **Рабочая область**, в которой отображается информация о выбранном рабочем столе:
  - название рабочего стола;
  - идентификатор рабочего стола;
  - информация о виджетах, добавленных на рабочий стол: заголовок, описание и содержимое виджета (см. «Рис. 14»);
  - режим автообновления рабочего стола;
  - период времени, за который формируется информация для рабочего стола.

Пример отображения информации о виджете приведен на «Рис. 14».

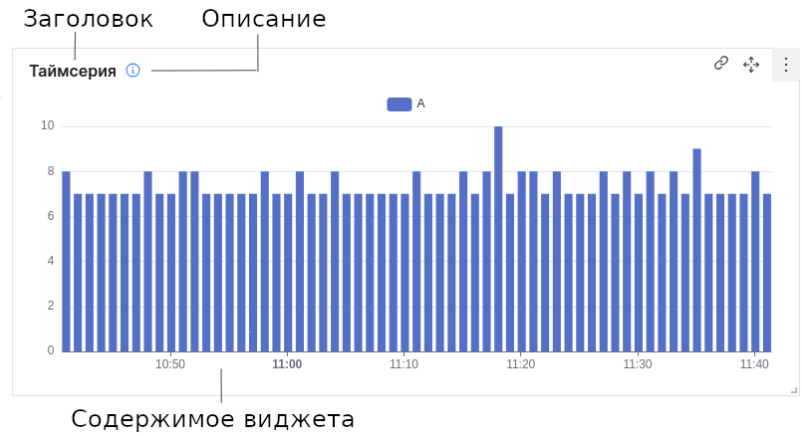


Рис. 14 – Пример виджета

На странице доступны следующие элементы управления рабочим столом:

Кнопка	**Действие**
Создать рабочий стол	создание нового рабочего стола
	копирование ссылки на рабочий стол
	обновление отображаемой информации
	выбор временного диапазона для формирования данных
+ Добавить виджет	создание виджета в конструкторе
	доступ к следующим действиям над рабочим столом: – редактирование; – создание копии; – создание отчета; – удаление.

При наведении мыши на виджет, становятся доступны следующие элементы управления виджетом:

Кнопка	**Действие**
	переход в соответствующий раздел платформы к табличному представлению данных
	перемещение виджета по рабочему столу
	доступ к следующим действиям над виджетом: – редактирование; – удаление; – копирование настроек.

5.2 Создание рабочего стола

Перейдите в раздел **Администрирование → Рабочие столы** и нажмите кнопку Создать рабочий стол. Откроется окно "Создание рабочего стола" (см. «Рис. 15»).

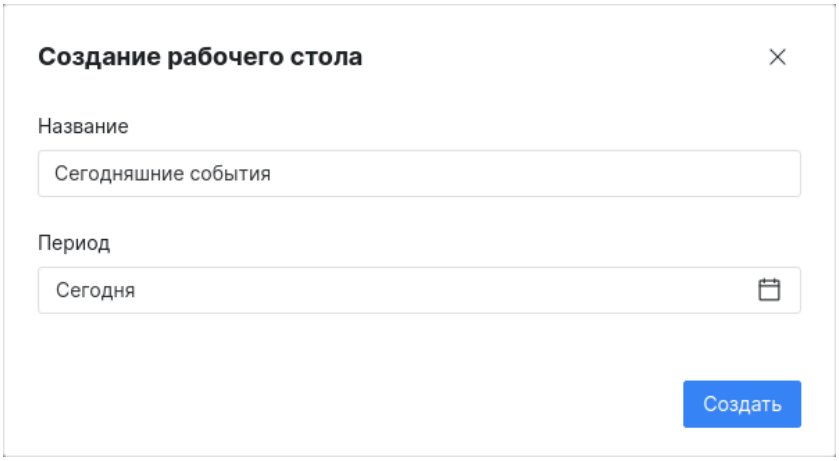


Рис. 15 – Окно "Создание рабочего стола"

Выполните следующие действия:

1. В поле "Название" укажите название рабочего стола.
2. В поле "Период" из выпадающего списка выберите период, по которому будут выводиться данные на рабочий стол.
3. Нажмите кнопку **Создать**.

После создания рабочего стола рекомендуется выполнить следующие действия:

- настроить права доступа пользователей к рабочему столу (подробнее см. раздел «Редактирование рабочего стола»);
- настроить вывод данных, добавив необходимое количество виджетов (подробнее см. раздел «Управление виджетами»).

5.3 Редактирование рабочего стола

Выберите нужный рабочий стол. Нажмите кнопку  и из выпадающего списка выберите пункт **Редактировать**.

Откроется страница редактирования рабочего стола (см. «Рис. 16»).

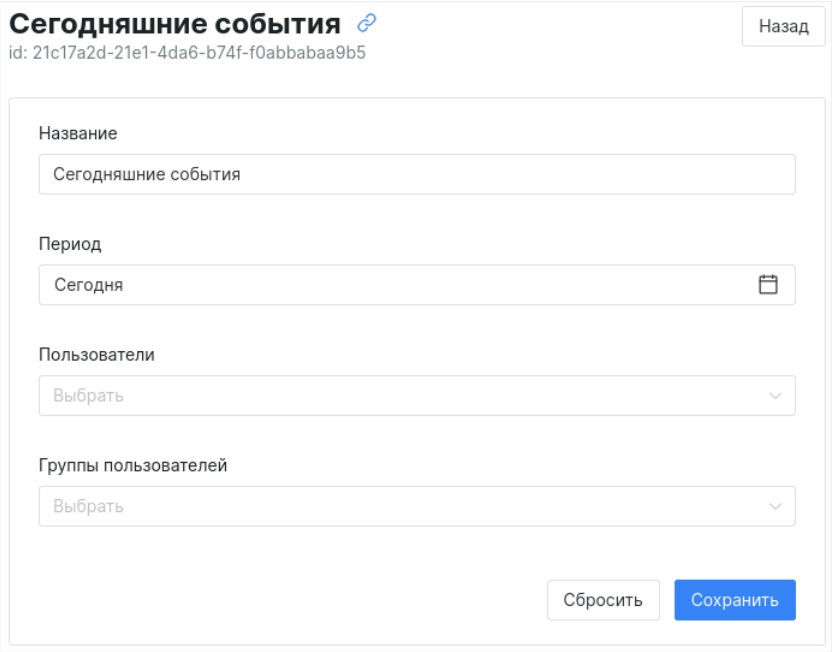


Рис. 16 – Страница редактирования рабочего стола

При необходимости измените данные о рабочем столе и нажмите кнопку **Сохранить**.

Настроить права доступа пользователей к рабочему можно следующими способами:

- в поле "Пользователи" из выпадающего списка выберите пользователей, которым будет доступен рабочий стол;
- в поле "Группы пользователей" из выпадающего списка выберите группы пользователей, которым будет доступен рабочий стол.

5.4 Управление виджетами

При открытии рабочего стола, данные выводятся в соответствии с заданными параметрами. Все данные визуализируются на рабочем столе с помощью виджетов. Настройка виджетов выполняется в специальном конструкторе (см. раздел «Конструктор виджетов»).

При работе с виджетами выполняются следующие процессы:

1. Установка периода и обновление данных виджета.
2. Добавление виджета на рабочий стол.
3. Переход к табличному представлению данных.
4. Редактирование виджета.
5. Копирование виджета.
6. Изменение расположения виджета.
7. Изменение размера виджета.
8. Удаление виджета.

5.4.1 Установка периода и обновление данных виджетов

При необходимости вы можете временно изменить период формирования данных, выставленный по умолчанию для рабочего стола.

Для этого выполните следующие действия:

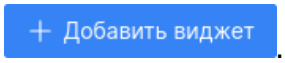
1. Нажмите кнопку  . Откроется окно выбора временного диапазона.
2. Выберите период. Доступные значения:
    - за все время;
    - текущие: минута, час, день, месяц, год;
    - последние: минуты, часы, месяца, года;
    - период можно указать вручную в соответствующих полях. Поддерживается формат дат из «Grafana. Единицы измерения и временной диапазон».
3. Нажмите кнопку **Применить**.

Для обновления отображаемых данных нажмите кнопку  .

Для того, чтобы информация по новым данным автоматически обновлялась, необходимо из выпадающего списка выбрать режим автообновления. Доступны следующие режимы: без автообновления, 1 сек, 30 сек, 1 мин, 5 мин.

5.4.2 Добавление виджета на рабочий стол

Для добавления виджета на рабочий стол выполните следующие действия:

1. Выберите нужный рабочий стол и нажмите кнопку 

.
2. Выполните настройку виджета в конструкторе (подробнее см. раздел «Конструктор виджетов»).
3. Добавьте необходимое количество виджетов на рабочий стол.

5.4.3 Переход к табличному представлению данных

Платформа позволяет перейти к табличному представлению данных выбранного виджета.

Переход выполняется на соответствующую страницу в зависимости от настроек поля **Датасет** в конструкторе (подробнее см. раздел «Конструктор виджетов»). Например, если используется датасет "Инциденты", то переход будет в раздел **Инциденты** с уже сформированной таблицей по параметрам фильтра из виджета.

Для перехода к табличному представлению данных выберите нужный виджет и нажмите кнопку  .

5.4.4 Редактирование виджета

Для редактирования виджета выполните следующие действия:

1. Перейдите на рабочий стол и выберите виджет.

2. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Редактировать**.
3. Выполните настройку виджета в конструкторе (подробнее см. раздел «Конструктор виджетов»).

5.4.5 Копирование настроек виджета

Для копирования настроек виджета выполните следующие действия:

1. Перейдите на рабочий стол и выберите виджет.
2. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Копировать настройки**.
3. Затем вы можете передать настройки другому пользователю, или создать новый виджет на основе скопированного.

Чтобы применить скопированные настройки необходимо начать процесс создания или редактирования виджета. Для применения скопированных настроек нажмите кнопку 📋 в конструкторе виджетов (подробнее см. раздел «Конструктор виджетов»).

5.4.6 Изменение расположения виджета

Для изменения расположения виджета выполните следующие действия:

1. Перейдите на рабочий стол и выберите виджет.
2. Нажмите и удерживайте кнопку ✥ .
3. Перемещайте мышку в нужном направлении.
4. Отпустите кнопку после перемещения.

5.4.7 Изменение размера виджета

Для изменения размера виджета выполните следующие действия:

1. Перейдите на рабочий стол и выберите виджет.
2. Нажмите и удерживайте правый нижний угол виджета (см. «Рис. 17»).

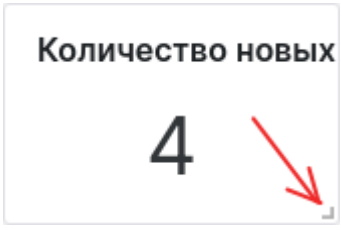


Рис. 17 – Кнопка изменения размера виджета

3. Перемещайте мышку в нужном направлении.
4. Отпустите правый нижний угол после перемещения.

5.4.8 Удаление виджета

Для удаления виджета с рабочего стола выполните следующие действия:

1. Перейдите на рабочий стол и выберите виджет.
2. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Удалить**.
3. Подтвердите удаление в открывшемся окне. Виджет будет удален с рабочего стола.

5.5 Копирование рабочего стола

Платформа Радар позволяет создавать рабочие столы на основе существующих. Для этого выберите нужный рабочий стол. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Создать копию**. Будет создан рабочий стол с аналогичными параметрами.

5.6 Создание отчета

Платформа Радар позволяет формировать отчеты, которые предоставляют наглядные данные, чтобы помочь вам оценить эффективность и производительность платформы.

Отчет можно сформировать в том числе и на основе данных, выведенных на рабочий стол.

Для этого выберите нужный рабочий стол и выполните следующие действия:

1. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Создать отчет**. Откроется окно "Создание отчета" (см. «Рис. 18»).

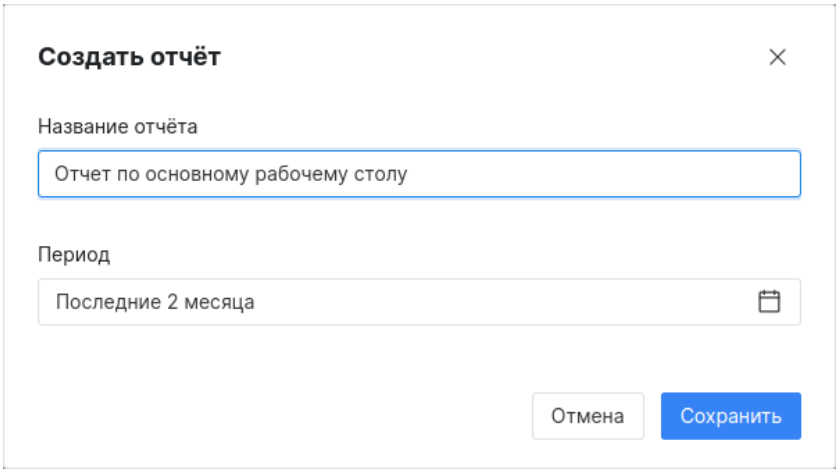


Рис. 18 – Окно "Создать отчет"

2. Укажите следующие данные:
   - в поле "Название отчета" укажите название отчета;
   - в поле "Период" из выпадающего списка выберите период формирования отчета.
3. Нажмите кнопку **Сохранить**. Откроется страница с отчетом (см. «Рис. 19»).

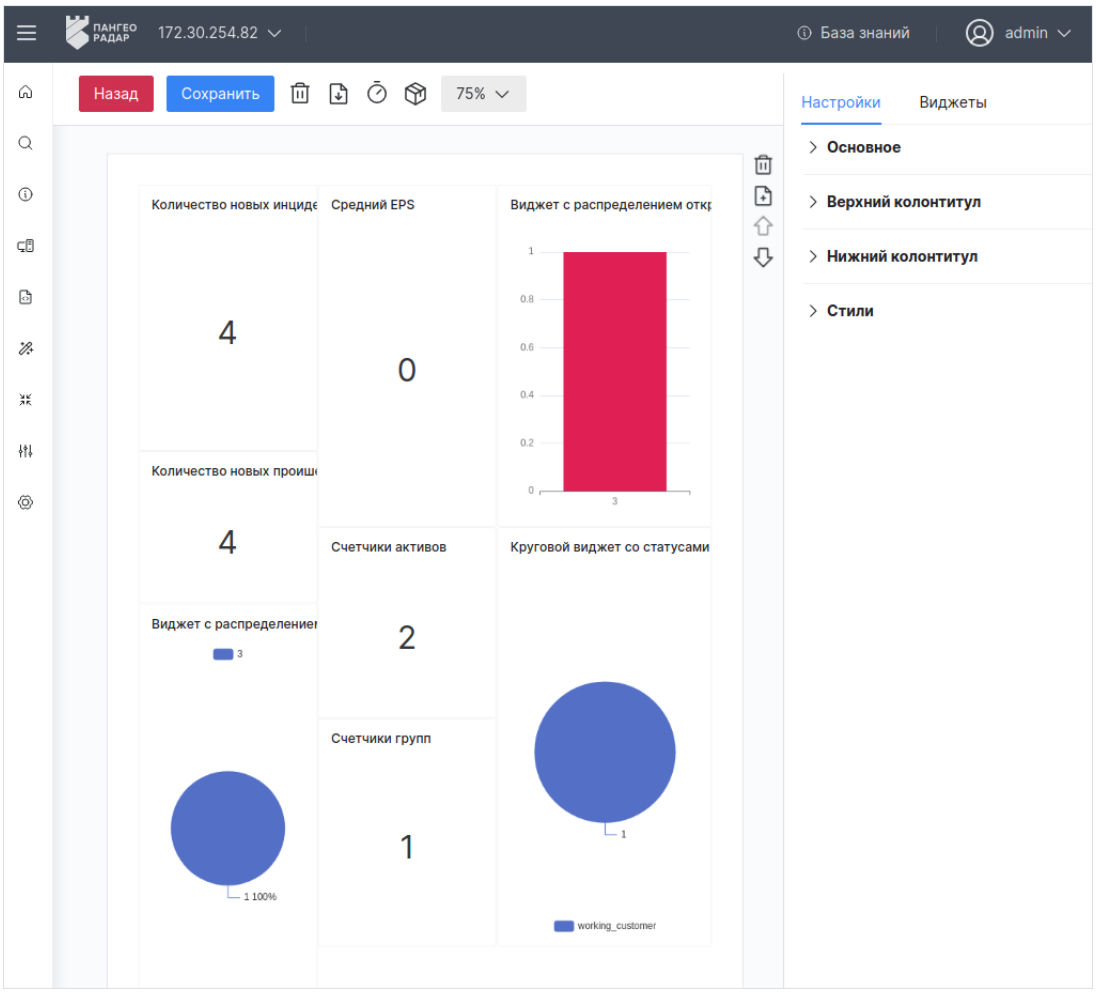


Рис. 19 – Страница с отчетом

Дальнейшие действия над отчетом выполняются в разделе «Отчеты».

5.7 Удаление рабочего стола

Выберите нужный рабочий стол, нажмите кнопку  и из выпадающего списка выберите пункт **Удалить**. Подтвердите удаление в открывшемся окне.

5.8 Grafana. Единицы измерения и временной диапазон

Grafana поддерживает следующие единицы измерения временного диапазона:

- s (секунды);
- m (минуты);
- h (часы);
- d (дни);
- w (недели);
- M (месяцы);
- y (годы).

Оператор минус позволяет сделать шаг назад во времени относительно выбранного значения текущей даты и времени, или значения **now**. Если необходимо отобразить полный период единицы измерения (день, неделю, месяц и т.д.), необходимо добавить «/<единица измерения времени>» в конце.

В таблице приведены примеры временных диапазонов:

Пример относительного диапазона	**От**	**До**
Последние 5 минут	now-5m	now
Прошедший день	now/d	now
На этой недели	now/w	now/w
Пока что на этой недели	now/w	now
В этом месяце	now/M	now/M
Пока что в этом месяце	now/M	now
Предыдущий месяц	now-1M/M	now-1M/M
Пока что в этом году	now/y	now

6. Конструктор виджетов

Платформа Радар позволяет визуализировать данные с помощью виджетов. Виджеты применяются при работе с данными в разделах **Рабочие столы** и **Отчеты**.

Перейти в конструктор виджетов можно несколькими способами:

- **Способ 1**. Из раздела **Рабочие столы** начать процесс добавления или редактирования виджета;
- **Способ 2**. Из раздела **Отчеты** начать процесс редактирования виджета.

Внешний вид конструктора виджетов приведен на «Рис. 20».

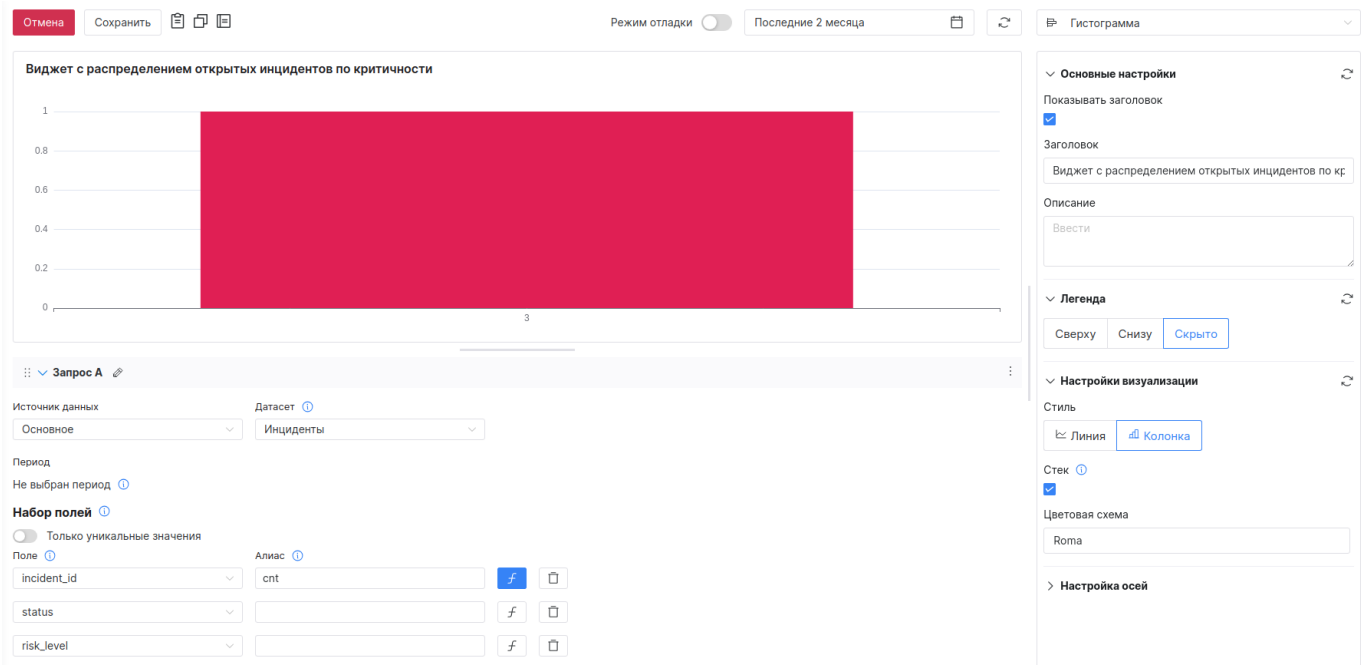


Рис. 20 – Страница "Конструктор виджетов"

Конструктор состоит из следующих блоков:

- панель действий;
- режим визуализации/Режим отладки;
- конструктор запросов;
- настройка визуализации виджета, которая включает:
    - выбор типа виджета;
    - основные настройки;
    - настройку внешнего вида виджета.

Панель действий

Блок располагается вверху страницы конструктора виджетов (см. «Рис. 21»).

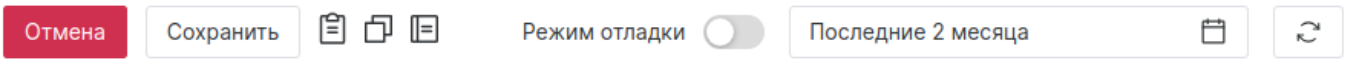


Рис. 21 – Конструктор виджетов. Блок "Панель действий"

На панели действий доступны следующие элементы управления:

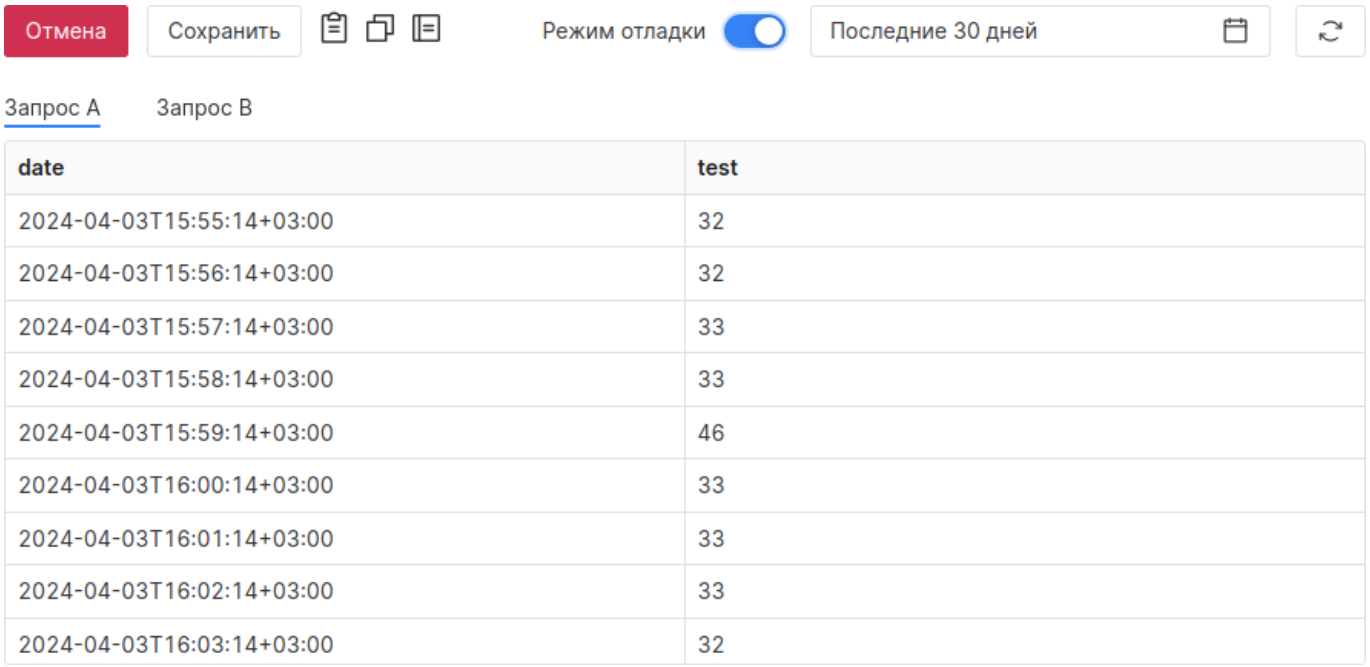
Кнопка	Действие
Отмена	отмена изменений и возврат на предыдущую страницу
Сохранить	сохранение информации о виджете
	вставить скопированные настройки виджета
	скопировать настройки
	переход к управлению предустановками настроек виджета
Режим отладки	включение/выключение режима отладки. При включенном режиме будут показаны данные, возвращаемые из источника
	выбор периода формирования данных виджета
	обновление отображаемой информации

Режим визуализации/Режим отладки

Блок располагается по центру конструктора. Переключение между режимами выполняется с помощью переключателя **Режим отладки**. В режиме визуализации можно посмотреть то, как виджет будет выглядеть на рабочем столе или странице отчета (см. «Рис. 22»).

Рис. 22 – Конструктор виджетов. Блок "Режим визуализации"

В режиме отладки можно посмотреть корректность работы написанных запросов (см. «Рис. 23»).



date	test
2024-04-03T15:55:14+03:00	32
2024-04-03T15:56:14+03:00	32
2024-04-03T15:57:14+03:00	33
2024-04-03T15:58:14+03:00	33
2024-04-03T15:59:14+03:00	46
2024-04-03T16:00:14+03:00	33
2024-04-03T16:01:14+03:00	33
2024-04-03T16:02:14+03:00	33
2024-04-03T16:03:14+03:00	32

Рис. 23 – Конструктор виджетов. Блок "Режим отладки"

Конструктор запросов

Блок располагается под режимом визуализации/отладки (см. «Рис. 24»).

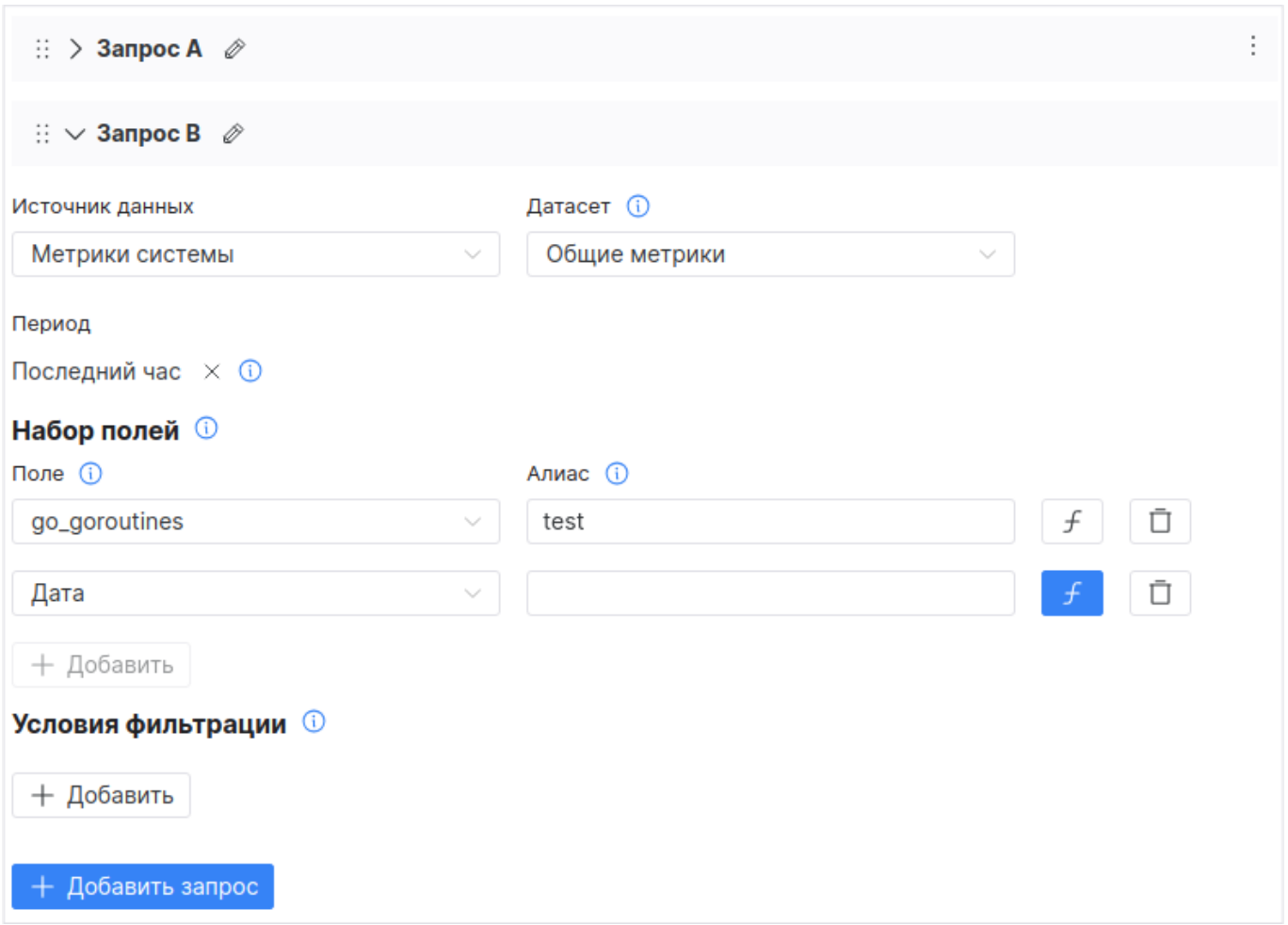


Рис. 24 – Конструктор виджетов. Блок "Конструктор запросов"

В конструкторе запросов доступны следующие элементы управления запросами:

Кнопка	Действие
+ Добавить запрос	добавление запроса
	изменение расположения запроса
	изменение наименования запроса
	доступ к следующим действиям над запросом: – скопировать настройки; – вставить настройки; – дублировать; – удалить.
+ Добавить	добавление параметра
	удаление параметра из запроса
	добавление агрегацию в запрос
	синий индикатор обозначает что к запросу добавлена агрегация. При повторном клике можно ее изменить

Настройка внешнего вида виджета

Блок располагается в правой части страницы конструктора и формируется в зависимости от выбранного виджета (см. «Рис. 25»).

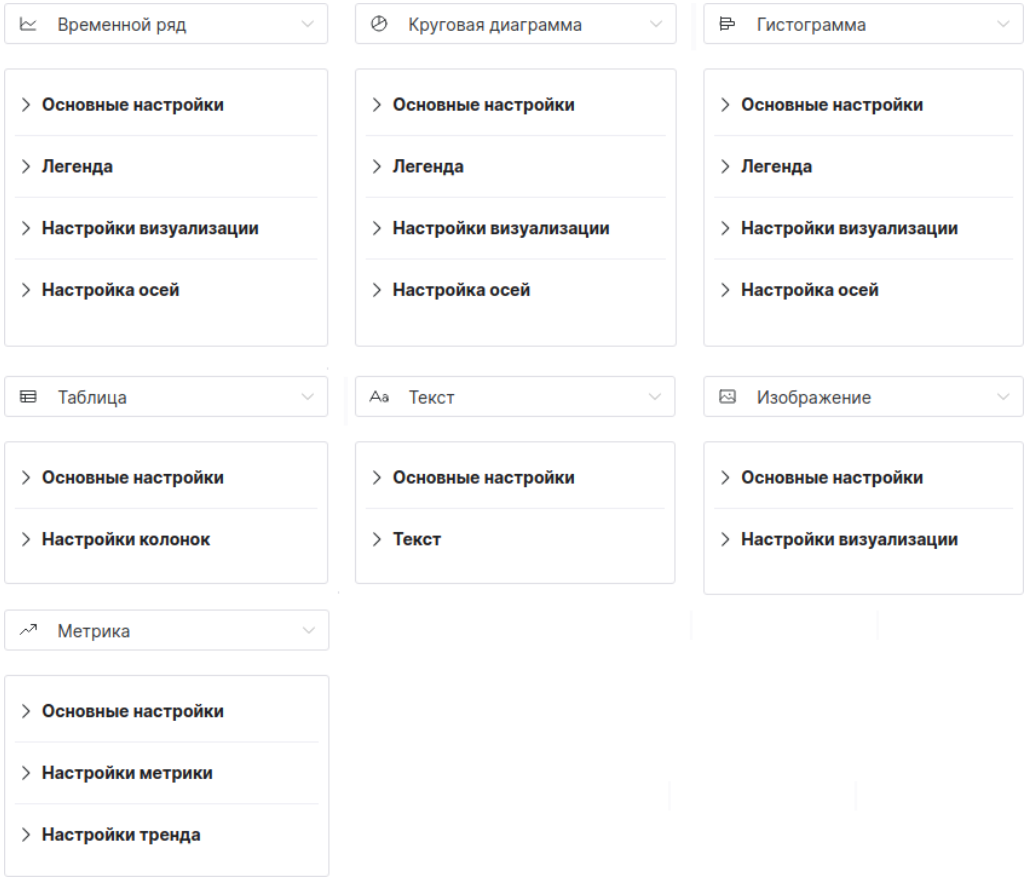


Рис. 25 – Конструктор виджетов. Блок "Настройка внешнего вида виджета"

6.1 Особенности работы в конструкторе

Каждый виджет обладает своим уникальным способом визуализации данных и имеет ряд персональных настроек.

По типу запросов виджеты делятся на виджеты с серией запросов и на виджеты без серии запросов (простые):

- Для следующих типов виджетов можно задать серию запросов:
  - временной ряд;
  - гистограмма;
  - круговая диаграмма;
  - метрика;
  - таблица.
- Для следующих типов виджетов нельзя задать серию запросов:
  - текст;
  - изображение.

Стандартный процесс настройки виджета может выглядеть следующим образом:

1. Выберите тип виджета из выпадающего списка.
2. Укажите "Основные настройки виджета".
3. Если для виджета доступна настройка серии запросов, то включите **Режим отладки**.
4. Настройте запрос или серию запросов.
5. Обновите отображаемую информацию и проверьте работу запросов в **Режиме отладки**.
6. Удостоверьтесь что все настроенные запросы работают корректно.
7. Для настройки параметров визуализации отключите **Режим отладки**.
8. Укажите настройки визуализации серии запросов.
9. Удостоверьтесь что визуализация данных в виджете работает корректно.
10. Сохраните изменения нажав соответствующую кнопку.

6.2 Конструктор запросов

Управление запросами включает в себя следующие процессы:

1. Добавление запроса.
2. Дублирование запроса.
3. Копирование параметров запроса.
4. Удаление запроса.

6.2.1 Добавление запроса

Примечание: перед началом процесса добавления запроса рекомендуется включить **Режим отладки**. После изменения запроса рекомендуется обновлять данные с помощью кнопки для проверки корректности запроса.

Для начала процесса добавления запроса нажмите кнопку + Добавить запрос.

При необходимости вы можете изменить наименование запроса нажав кнопку .

Добавление запроса можно условно разделить на несколько шагов:

- Шаг 1. Выбор источника данных и датасета.
- Шаг 2. Настройка периода формирования запроса.
- Шаг 3. Добавление набора полей, информация по которым будет обрабатываться запросом.
- Шаг 4. Настройка условий фильтрации выбранных полей.
- Шаг 5. Настройка группировки и сортировки выбранных полей.

6.2.1.1 Шаг 1. Выбор источника данных и датасета

На данном шаге необходимо выбрать источник данных, информация из которого будет обрабатываться запросом, и соответствующий набор данных - датасет (см. «Рис. 26»).

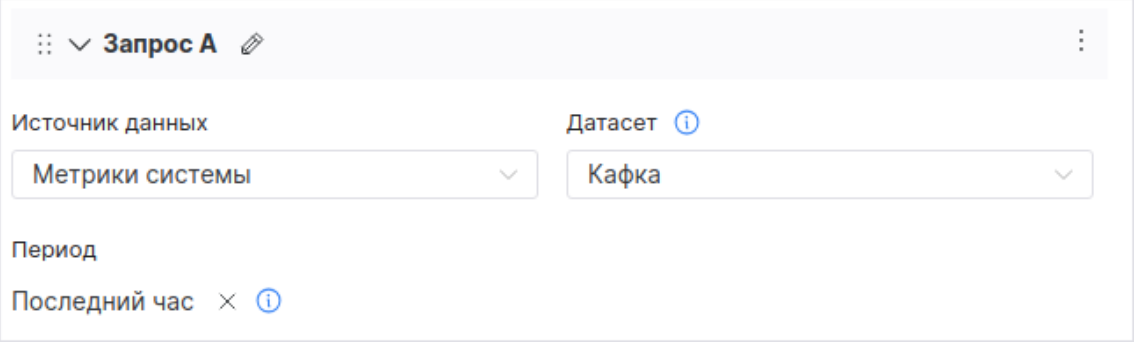


Рис. 26 – Конструктор запросов. Выбор источника данных, датасета и периода

Соответствие источников данных и датасетов приведено в таблице:

Источник данных	Датасет
Основное	Инциденты
События	– Все; – Нормализованные; – Обработанные; – Ошибки.
Метрики системы	– Менеджер кластера; – Кафка; – Коллектор логов; – Коррелятор; – Общие метрики; – Хранилище событий; – Коллектор метрик;

Источник данных	Датасет
	– Rsyslog.
Табличные списки	Датасет формируется на основе данных, созданных пользователем при работе с табличными списками

6.2.1.2 Шаг 2. Выбор периода формирования запроса

Примечание: период, указанный для запроса, всегда имеет приоритет над периодом, указанным для рабочего стола или отчета.

Для изменения периода формирования запроса (см. «Рис. 26») выполните следующие действия:

1. Нажмите на соответствующее поле. Откроется окно выбора временного диапазона.
2. Выберите период. Доступные значения:
   - за все время;
   - текущие: минута, час, день, месяц, год;
   - последние: минуты, часы, месяца, года;
   - период можно указать вручную в соответствующих полях. Поддерживается формат дат из **Grafana**.
3. Нажмите кнопку **Применить**.

6.2.1.3 Шаг 3. Настройка набора полей

На данном шаге вы добавляете в запрос конкретные поля из выбранного датасета. Для каждого поля при необходимости можно задать **Алиас** и **Агрегацию**.

Алиас - это ключ, по которому можно определить выбранное поле при настройке визуализации виджета. Если вам необходимо чтобы визуализация строилась по одинаковым полям, но из разных запросов, то задайте этим полям одинаковый Алиас.

Агрегация - возможность выбрать функцию группировки результатов, которые будут выводиться при построении визуализации. Набор параметров агрегации для каждого поля является уникальным. Например, если вам необходимо чтобы по одной из шкал временного ряда, значения указывались по минутам, то задайте для поля с типом "Дата" соответствующую агрегацию. При отсутствии группировки агрегируются все результаты выбранного поля. Агрегацию можно выполнить по следующим функциям:

- count - по любым значениям;
- min - по минимальным значениям;
- max - по максимальным значениям;
- sum - по сумме всех значений;
- avg - по среднему значению;
- interval - по интервалу (минуты, часы и.д.).

Для настройки набора полей выполните следующие действия:

1. Если вы хотите, чтобы в запросе отображались только уникальные значения полей, то включите переключатель **Только уникальные значения**.
2. Нажмите кнопку + Добавить.
3. Появятся параметры для настройки поля (см. «Рис. 27»).

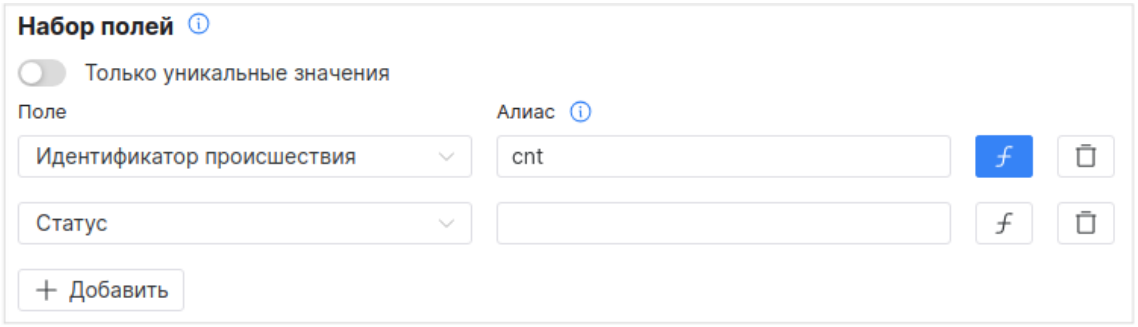


Рис. 27 – Конструктор запросов. Набор полей

4. Выберите необходимое поле датасета из выпадающего списка.
5. При необходимости укажите алиас.
6. При необходимости задайте агрегацию. Для этого нажмите на кнопку добавления агрегации. Откроется окно "Настройки поля" (см. «Рис. 28»).

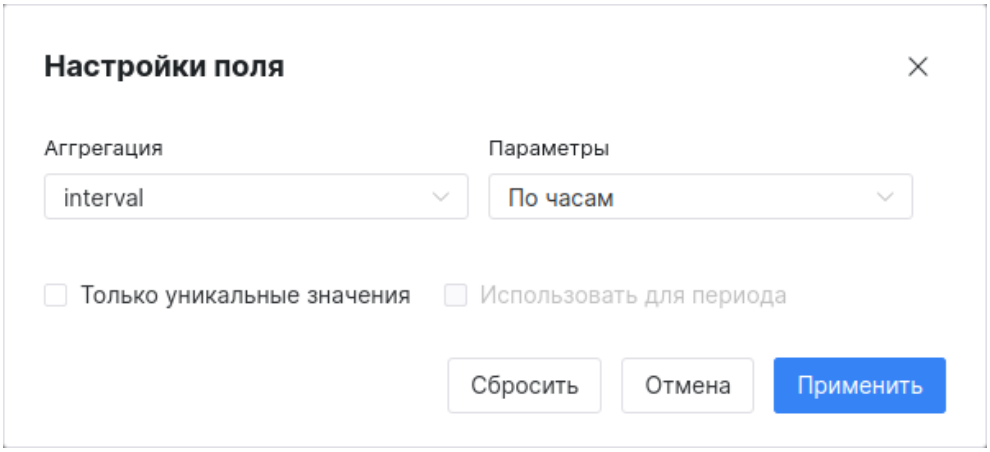


Рис. 28 – Окно "Настройки поля"

7. Укажите в окне следующие данные:
   - в поле "Агрегация" из выпадающего списка выберите функцию группировки результатов запроса;
   - в поле "Параметры" из выпадающего списка выберите параметры функции;
   - если необходимо выполнять агрегацию только по уникальным значениям, то установите соответствующий флаг;
   - если необходимо чтобы агрегация применялась только в рамках заданного периода, то установите флаг **Использовать для периода** (только для полей с типом date).
8. Добавьте необходимое количество полей.

6.2.1.4 Шаг 4. Условия фильтрации

После добавления полей в запрос при необходимости можно указать точную фильтрацию для каждого поля, участвующего в запросе. Для добавления условия фильтрации выполните следующие действия:

1. Нажмите кнопку + Добавить. Появятся параметры для настройки условия фильтрации (см. «Рис. 29»).

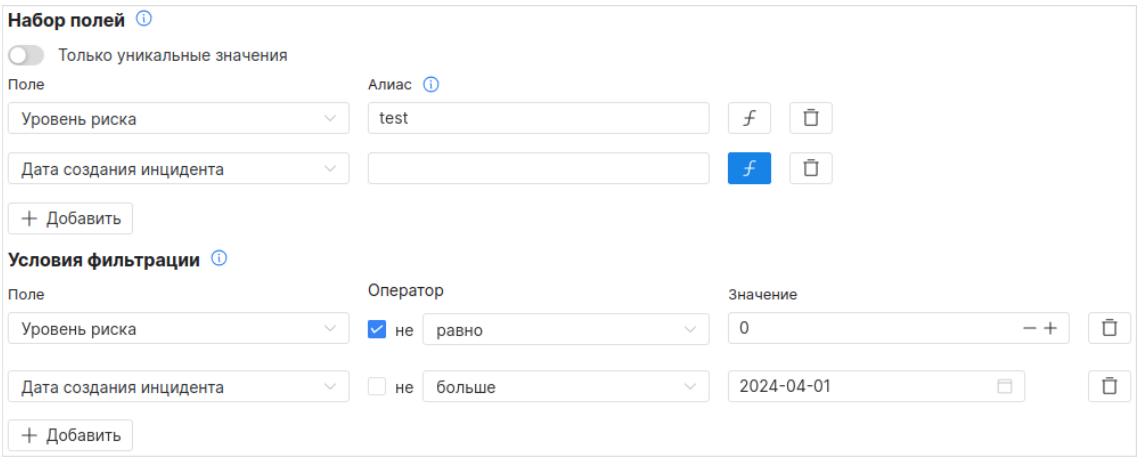


Рис. 29 – Конструктор запросов. Условия фильтрации

2. Выберите поле из выпадающего списка, по которому вы хотите настроить фильтрацию.
3. Выберите логический оператор.
4. Укажите значение оператора.
5. Добавьте фильтрацию по всем необходимым полям.

6.2.1.5 Шаг 5. Группировка и Сортировка

Примечание: данный шаг недоступен для полей из источника данных **Метрики системы**.

Группировка используется для объединения результатов по настроенным функциям агрегаций. Например, если вы хотите получить результаты по уровню риска инцидента и дате создания инцидента и при этом выставили агрегацию для поля "Уровень риска" в count, то вам необходимо будет выполнить группировку по полю "Дата создания". В результате вы получите группировку всех инцидентов с одинаковым уровнем риска по датам.

Для настройки нажмите кнопку + Добавить и выберите поле, по которому вы хотите выполнить группировку (см. «Рис. 30»).

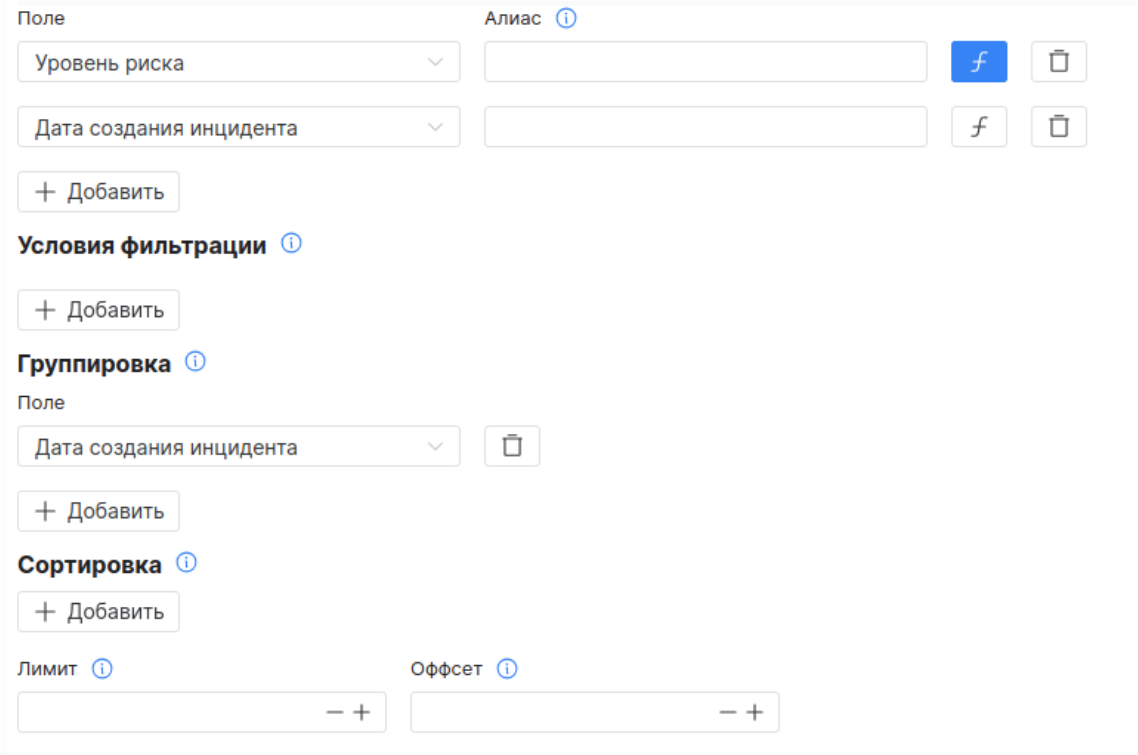


Рис. 30 – Конструктор виджетов. Группировка и сортировка

Сортировка настраивает порядок отображения результатов запроса: **asc/desc**. Для сортировки можно настроить следующие параметры:

- **Лимит** - сколько элементов возвращать в запросе;
- **Оффсет** - сколько элементов пропустить.

Для настройки сортировки выполните следующие действия:

1. Нажмите кнопку Добавить. Появятся параметры для настройки сортировки (см. «Рис. 30»).
2. Выберите поле из выпадающего списка, по которому вы хотите настроить сортировку.
3. Выберите направление сортировки: asc/desc.
4. В поле "Лимит" укажите значение лимита.
5. В поле "Оффсет" укажите значение оффсета.

6.2.2 Копирование запроса

Вы можете скопировать параметры запроса и передать их другому пользователю. Для этого выберите нужный запрос, нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Скопировать настройки**. Настройки будут скопированы в буфер обмена.

Для того чтобы применить скопированные настройки выберите нужный запрос, нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Вставить настройки**. Настройки из буфера обмена будут применены к запросу.

6.2.3 Дублирование запроса

Вы можете создать новый запрос на основе существующего. Для этого выберите нужный запрос, нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Дублировать**. В списке запросов появится дубликат запроса.

6.2.4 Удаление запроса

Для удаления запроса выберите нужный запрос, нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Удалить**.

6.3 Настройка внешнего вида виджета

Примечание: настройку внешнего вида виджета рекомендуется выполнять после настройки серии запросов и в режиме визуализации (переведите переключатель **Режим отладки** в состояние "выключен").

Настройку внешнего вида виджета условно можно разделить на следующие действия:

- выбор типа виджета из выпадающего списка;
- установка основных настроек виджета;
- персональная настройка выбранного типа виджета.

6.3.1 Основные настройки виджета

Блок "Основные настройки" является общим для всех типов виджетов (см. «Рис. 31»).

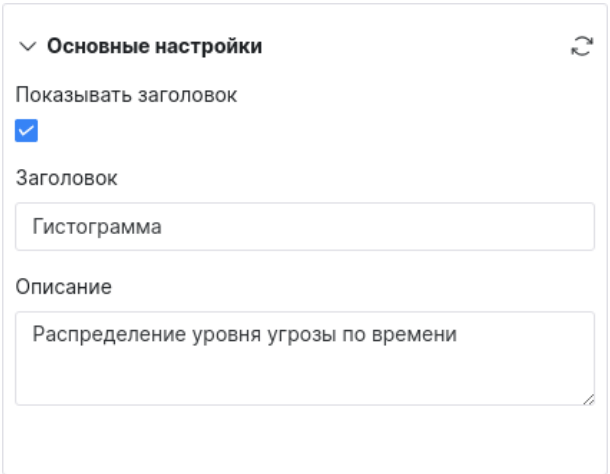


Рис. 31 – Основные настройки виджетов

В блоке доступны следующие настройки:

- Флаг "Показывать заголовок" - включение/выключение отображения наименования виджета на рабочем столе/отчете;
- Заголовок - наименование виджета;
- Описание - дополнительная информация о виджете.

Пример отображения основных настроек приведен на «Рис. 32»

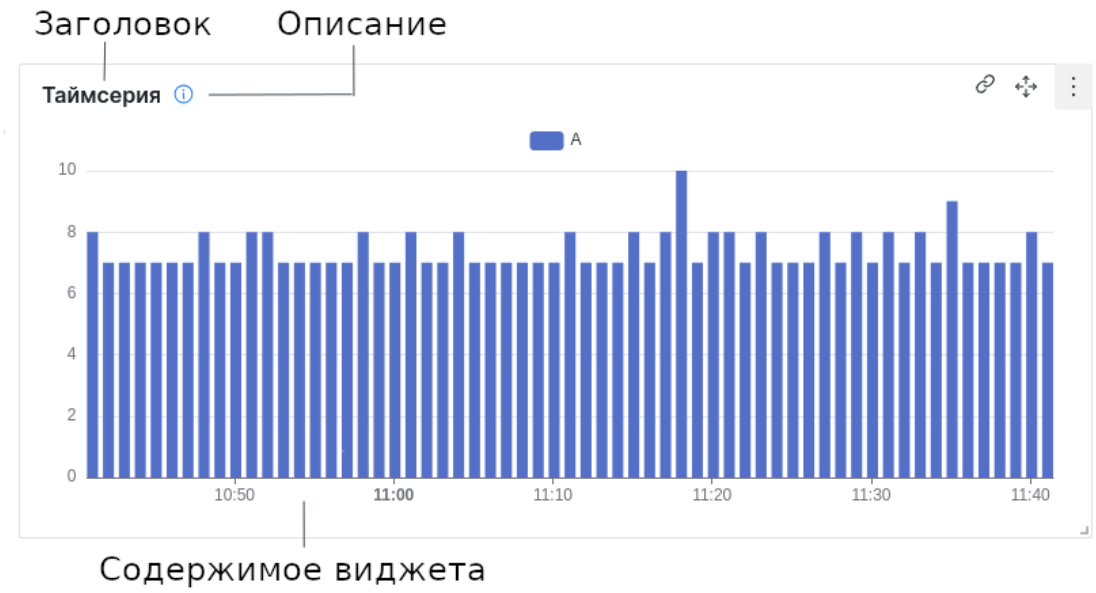


Рис. 32 – Отображение основных настроек на виджете

6.3.2 Временной ряд

Виджет отображает график с группировкой по количеству значений параметра от выбранного источника за определенный период времени. Пример внешнего вида приведен на «Рис. 33».

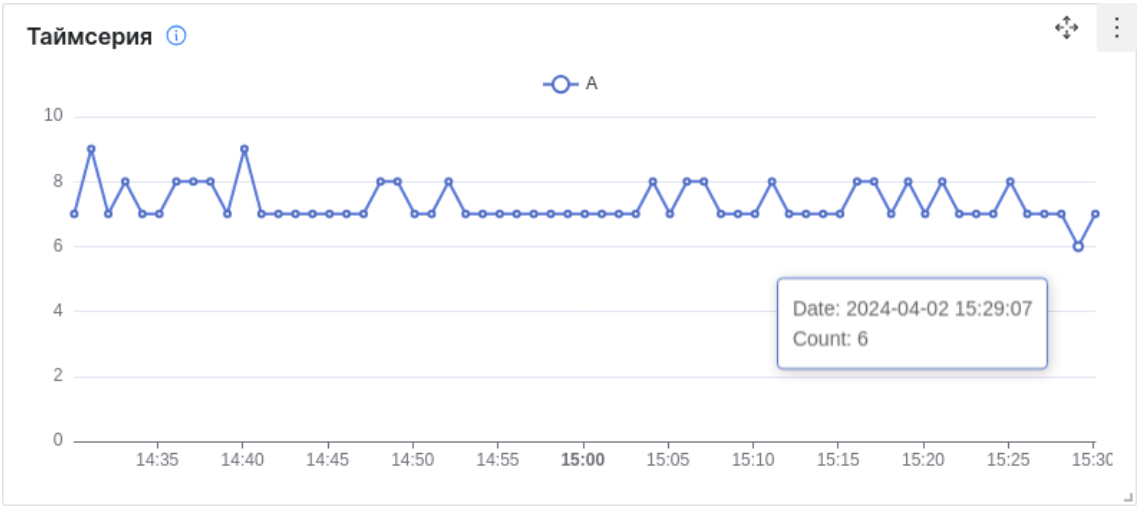


Рис. 33 – Виджет "Временной ряд"

Настройка внешнего вида виджета включает в себя следующие шаги:

- Шаг 1. Настройка осей для отображения графика.
- Шаг 2. Настройка визуализации результатов запроса.
- Шаг 3. Настройка легенды.

Пример настроек приведен на «Рис. 34».

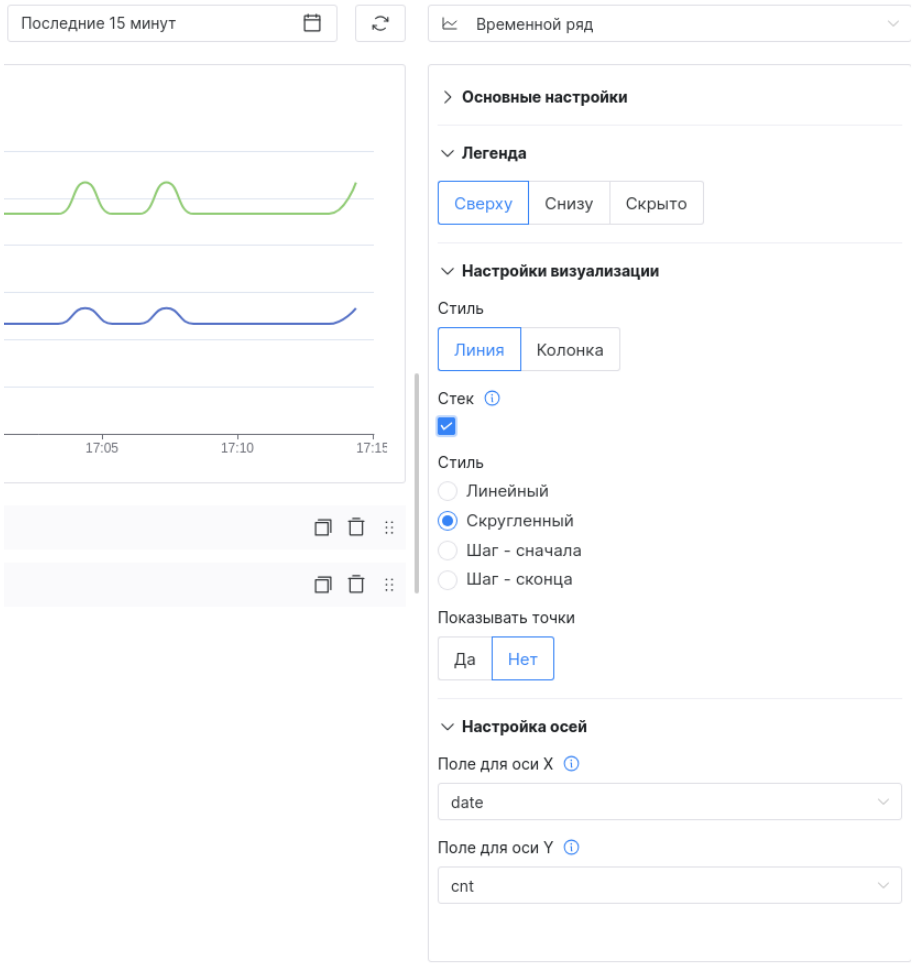


Рис. 34 – Виджет "Временной ряд". Настройки

6.3.2.1 Шаг 1. Настройка осей

Примечание: значения полей, которые доступны для выбора при настройке данного шага, формируются на основе данных, указанных в запросе (подробнее см. раздел «Добавление запроса»).

Настройка позволяет выбрать значения полей для оси X и для оси Y, по которым будет строиться график.

Для настройки осей выполните следующие действия:

1. Из выпадающего списка выберите поле для оси X.
2. Из выпадающего списка выберите поле для оси Y.
3. Проверьте отображение осей на виджете.

6.3.2.2 Шаг 2. Настройка визуализации

Настройка позволяет выбрать один из двух стилей графика:

- линия;
- колонка.

При выборе стиля "Линия" доступна возможность настроить дополнительные параметры:

- Внешний вид линий на графике:
  - линейный;
  - скругленный;
  - шаг с начала;
  - шаг с конца.
- Включение/выключение отображения точек.

Примеры визуализации графика приведены на «Рис. 35».

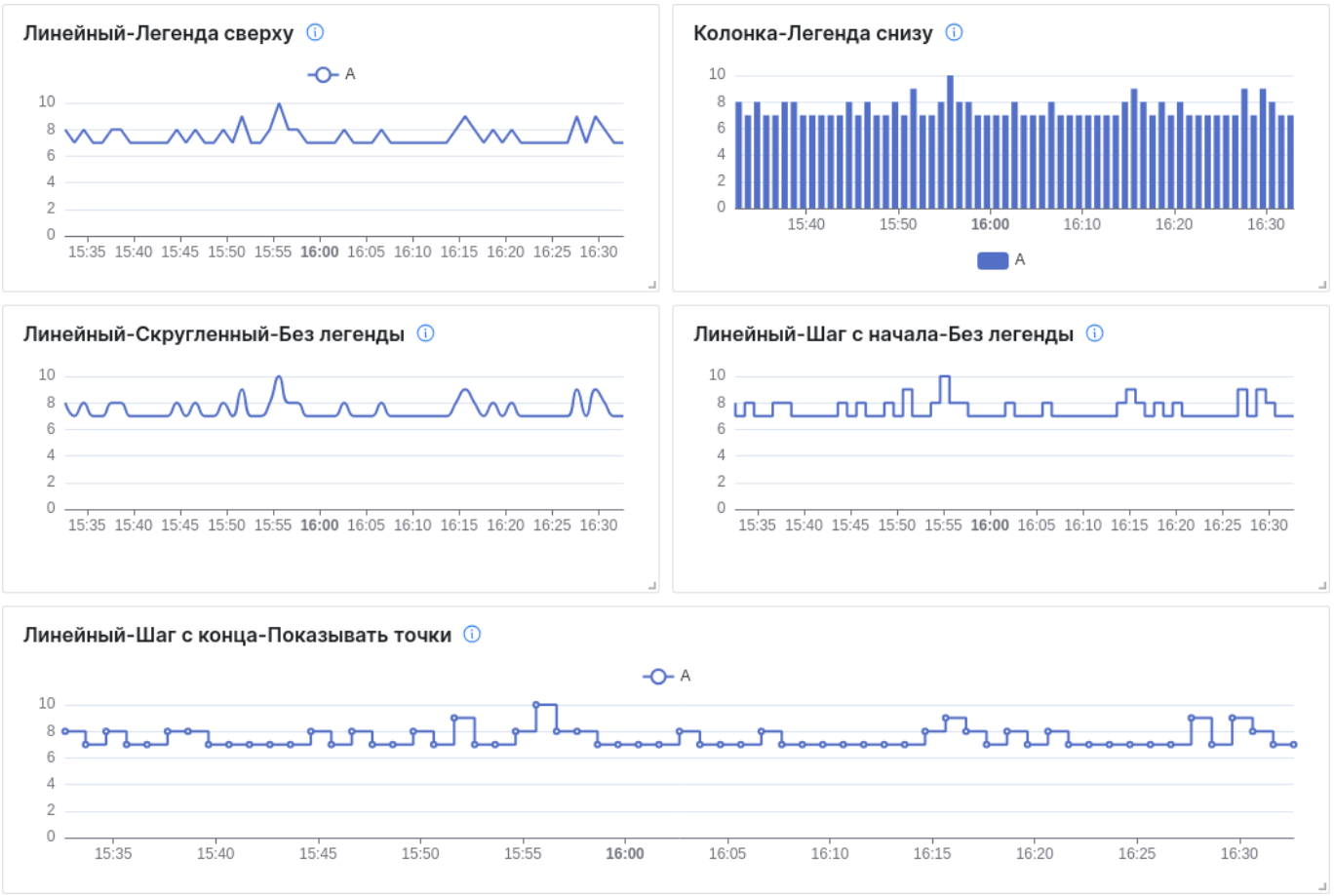


Рис. 35 – Примеры визуализации настроек виджета "Временной ряд"

Стек - настройка отвечает за группировку колонок или линий. Если вы настроили несколько запросов для виджета, то для удобства отображения мы можете установить флаг **Стек**.

Если в параметрах различных серий запросов используются разный набор полей, то чтобы объединить их необходимо ввести одинаковое название для каждого **Алиас** (подробнее см. раздел «Добавление запроса»). Для объединения полей при визуализации необходимо в параметрах блока "Настройка осей" указать **Алиас**.

Пример отображения с включенным и выключенным стеком приведен на «Рис. 36».

Рис. 36 – Пример визуализации виджета со стеком

Для настройки визуализации выполните следующие действия:

1. Выберите стиль: линия или колонка.
2. При необходимости включите стек, установив соответствующий флаг.
3. Если выбран стиль линия, то выберите ее тип: линейный, скругленный, шаг с начала, шаг
   с конца.
4. При необходимости включите отображение точек, включив соответствующий переключатель.

6.3.2.3 Шаг 3. Легенда

Настройка отвечает за выбор способа отображения легенды на графике. Выберите место отображения легенды: сверху, снизу или не отображать.

6.3.3 Круговая диаграмма

Виджет отображает группировку по выбранным параметрам с процентным распределением. Пример визуализации приведен на «Рис. 37».

Рис. 37 – Виджет "Круговая диаграмма"

Пример настроек приведен на «Рис. 38».

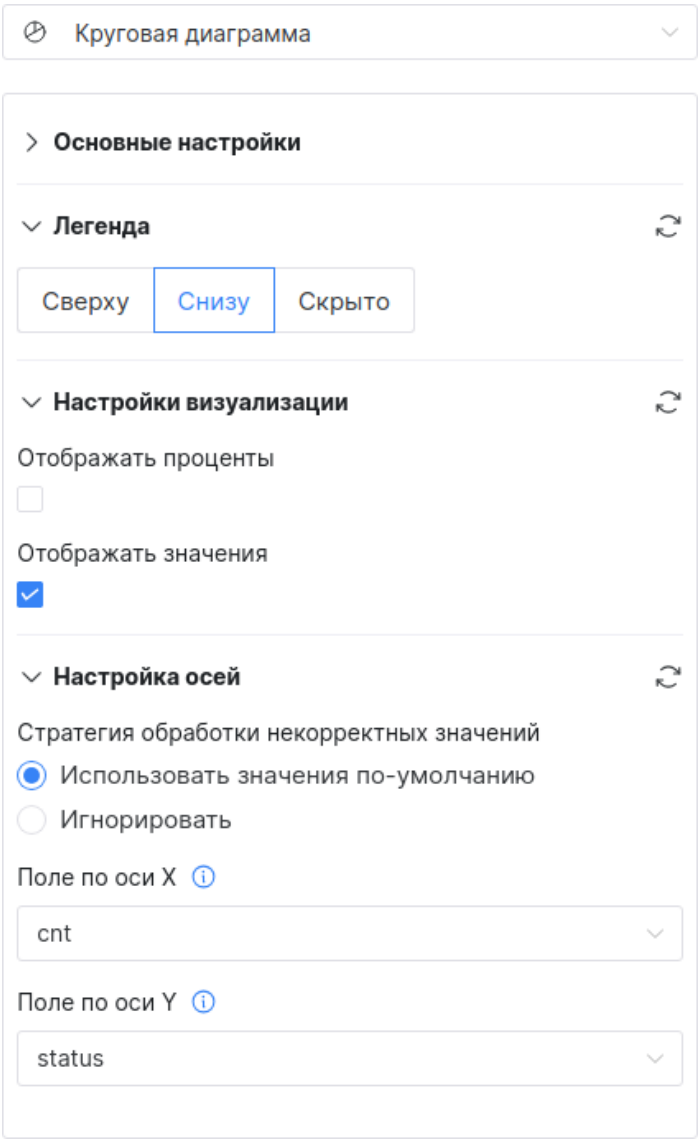


Рис. 38 – Виджет "Круговая диаграмма". Настройки

Для настройки внешнего вида виджета выполните следующие действия:

1. В блоке "Настройка осей" укажите следующие данные:

- выберите стратегию обработки некорректных значений: игнорировать или использовать по умолчанию;
- из выпадающего списка выберите поле для оси X;
- из выпадающего списка выберите поле для оси Y.

2. В блоке "Настройка визуализации" при необходимости включите отображение следующих данных:
   - проценты по выбранным полям;
   - значения по выбранным полям.
3. В блоке "Легенда" выберите место расположения легенды.

Примечание: значения полей, которые доступны для выбора при настройке в блоке "Настройка осей", формируются на основе данных, указанных в запросе (подробнее см. раздел «Добавление запроса»).

Варианты настроек визуализации приведены на «Рис. 39».

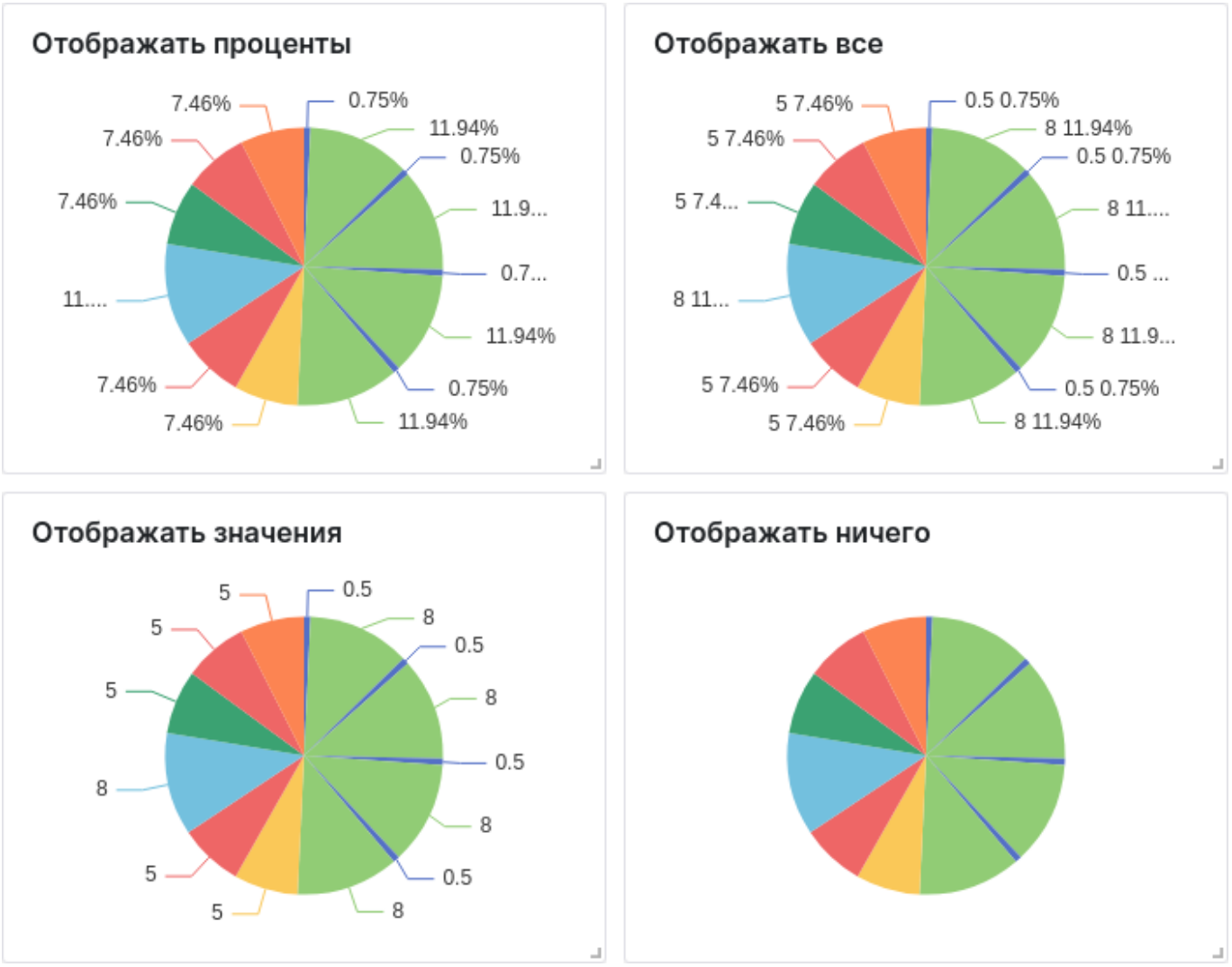


Рис. 39 – Примеры визуализации настроек виджета "Круговая диаграмма"

6.3.4 Таблица

Виджет отображает выбранные показатели в табличном варианте. Пример визуализации приведен на «Рис. 40».

Рис. 40 – Виджет "Таблица"

Пример блока "Настройки" приведен на «Рис. 41».

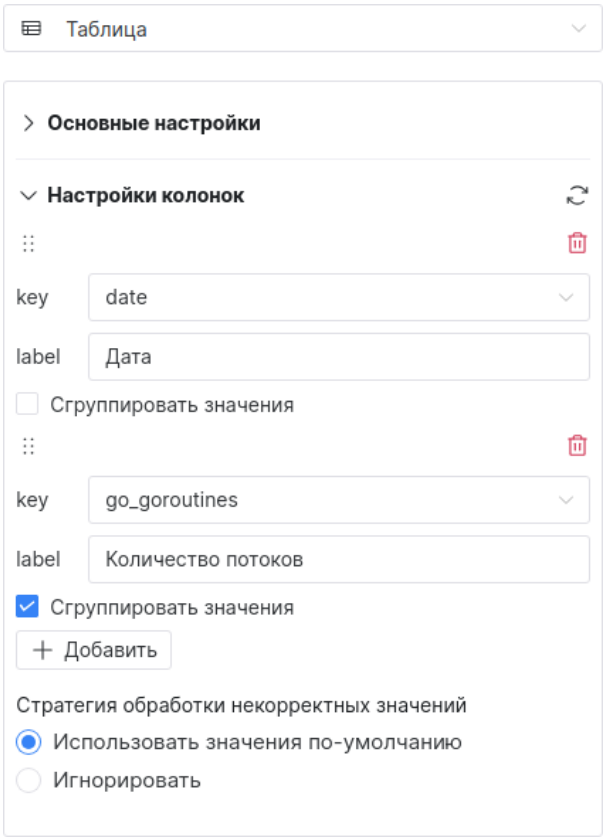


Рис. 41 – Виджет "Таблица". Настройки

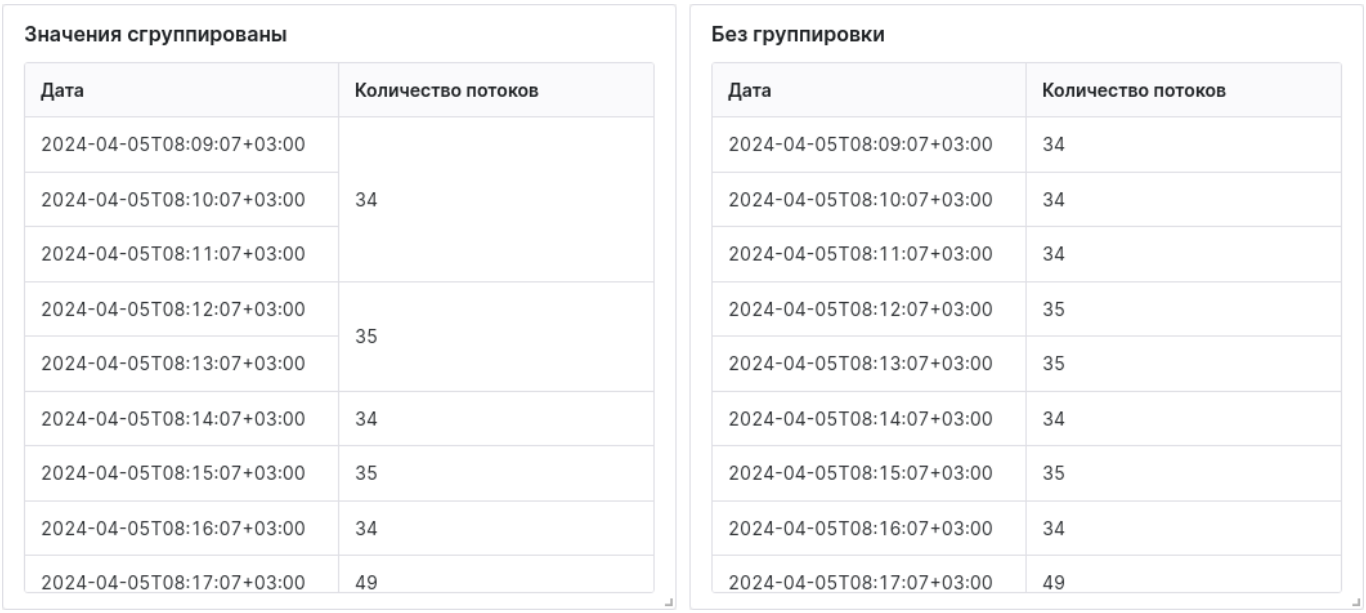
Для настройки внешнего вида виджета выполните следующие действия:

1. Для добавления колонок в таблицу нажмите кнопку Добавить. Добавьте необходимое количество колонок.
2. В поле "key" из выпадающего списка выберите поле или алиас из набора полей запроса, значения которого будут отображаться в колонке.

3. В поле "label" укажите наименование колонки, которое будет отображаться в виджете.
4. При необходимости установите флаг "Сгруппировать значения" для объединения результатов запроса по выбранному полю в одну ячейку таблицы.
5. Выберите стратегию обработки некорректных значений: игнорировать или использовать по умолчанию.

Примечание: значения полей, которые доступны для выбора при настройке колонок таблицы, формируются на основе данных, указанных в запросе (подробнее см. раздел «Добавление запроса»).

Примеры визуализации настроек приведены на «Рис. 42».



Значения сгруппированы

Дата	Количество потоков
2024-04-05T08:09:07+03:00	34
2024-04-05T08:10:07+03:00	
2024-04-05T08:11:07+03:00	
2024-04-05T08:12:07+03:00	35
2024-04-05T08:13:07+03:00	
2024-04-05T08:14:07+03:00	34
2024-04-05T08:15:07+03:00	35
2024-04-05T08:16:07+03:00	34
2024-04-05T08:17:07+03:00	49

Без группировки

Дата	Количество потоков
2024-04-05T08:09:07+03:00	34
2024-04-05T08:10:07+03:00	34
2024-04-05T08:11:07+03:00	34
2024-04-05T08:12:07+03:00	35
2024-04-05T08:13:07+03:00	35
2024-04-05T08:14:07+03:00	34
2024-04-05T08:15:07+03:00	35
2024-04-05T08:16:07+03:00	34
2024-04-05T08:17:07+03:00	49

Рис. 42 – Примеры визуализации настроек виджета "Таблица"

6.3.5 Текст

Примечание: данный тип виджета не поддерживает серию запросов.

Виджет отображает текст, указанный пользователем.

Пример визуализации приведен на «Рис. 43».

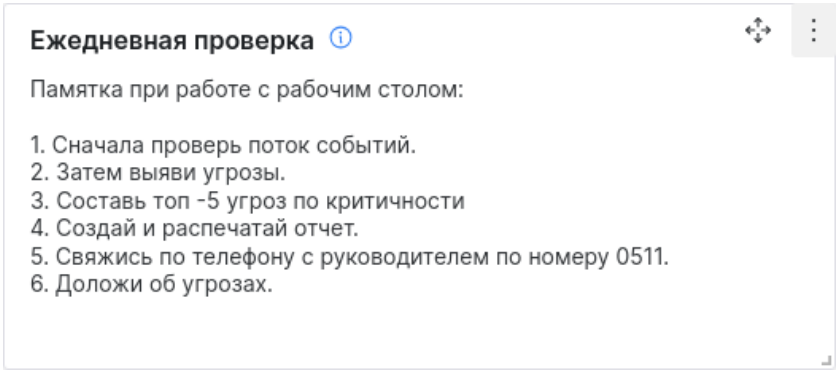


Рис. 43 – Виджет "Текст"

Пример настроек приведен на «Рис. 44».

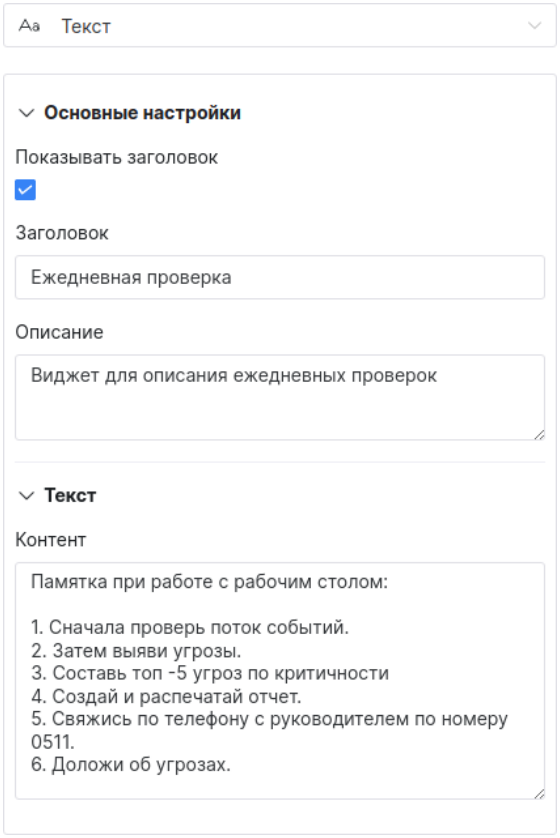


Рис. 44 – Виджет "Текст". Настройки

Для настройки виджета в блоке "Текст" укажите необходимую информацию.

6.3.6 Гистограмма

Виджет отображает столбчатую диаграмму с группировкой по количеству значений параметра от выбранного источника за определенный период времени. Пример внешнего вида приведен на «Рис. 45».

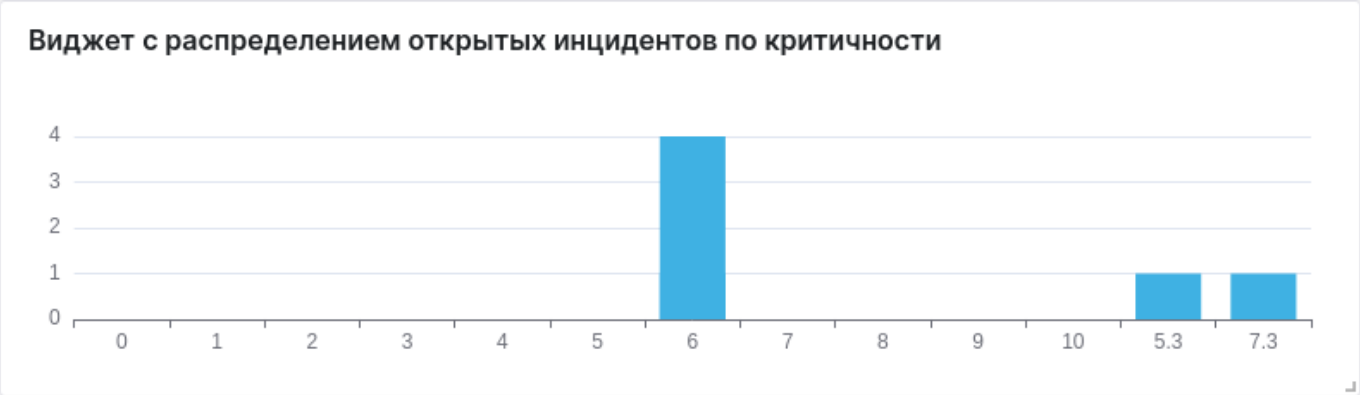


Рис. 45 – Виджет "Гистограмма"

Настройка внешнего вида виджета включает в себя следующие шаги:

- Шаг 1. Настройка осей для отображения графика.
- Шаг 2. Настройка визуализации результатов запроса.
- Шаг 3. Настройка легенды.

Пример настроек приведен на «Рис. 46».

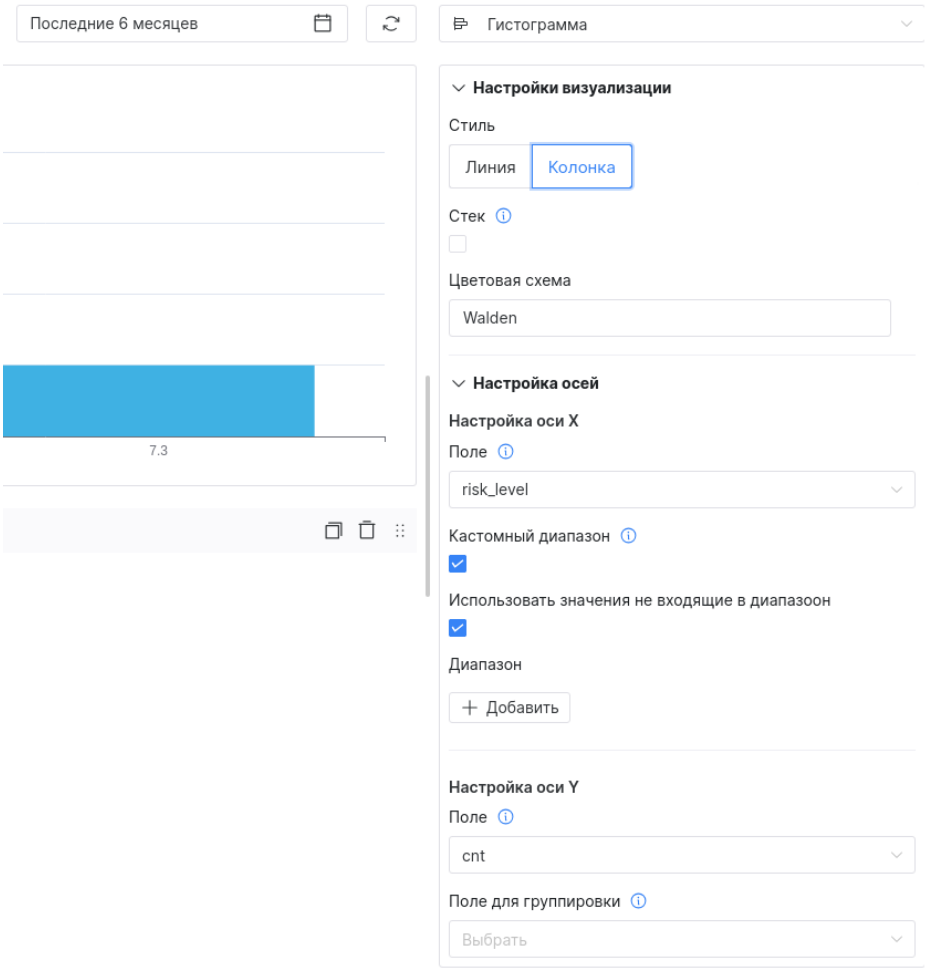


Рис. 46 – Виджет "Гистограмма". Настройки

6.3.6.1 Шаг 1. Настройка осей

Примечание: значения полей, которые доступны для выбора при настройке шага, формируются на основе данных, указанных в запросе (подробнее см. раздел «Добавление запроса»).

Настройка позволяет выбрать значения полей для оси X и для оси Y, по которым будет строиться график.

Для настройки осей выполните следующие действия:

1. Из выпадающего списка выберите поле для оси X.
2. Если вы хотите задать конкретный диапазон по оси X, по которому будут визуализироваться результаты запроса, то установите флаг "Кастомный диапазон". Появятся поля для настройки диапазона:
   - нажмите кнопку + Добавить;
   - укажите диапазон в соответствующем поле;
   - если вы хотите использовать значения, не входящие в диапазон, то установите соответствующий флаг.

3. Из выпадающего списка выберите поле для оси Y.
4. Проверьте отображение осей на виджете.

6.3.6.2 Шаг 2. Настройка визуализации

Настройка позволяет выбрать следующие параметры:

- стиль диаграммы: линия или колонка;
- включить или выключить стек;
- выбрать цветовую схему диаграммы.

При выборе стиля "Линия" доступна возможность настроить дополнительные параметры:

- Внешний вид линий на диаграмме:
  - линейный;
  - скругленный;
  - шаг с начала;
  - шаг с конца.
- Включение/выключение отображения точек.

Примеры визуализации графика приведены на «Рис. 47».

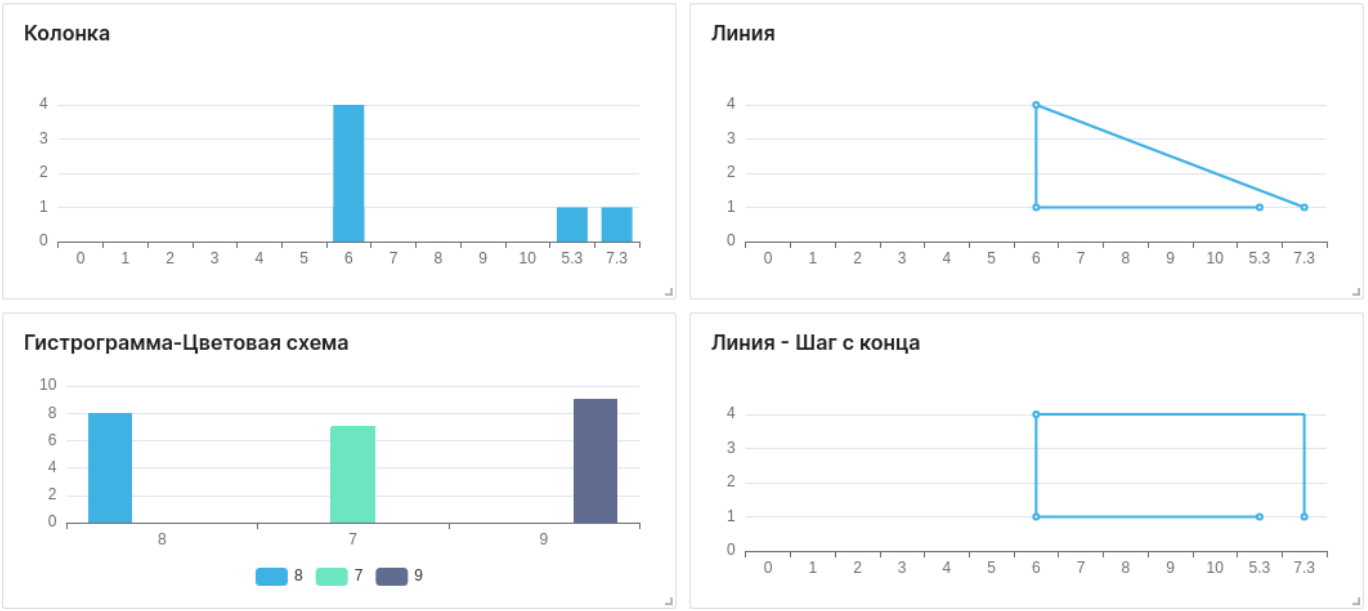


Рис. 47 – Примеры визуализации настроек виджета "Гистаграмма".

Стек - настройка отвечает за группировку колонок или линий. Если вы настроили несколько запросов для виджета, то для удобства отображения мы можете установить флаг **Стек**.

Если в параметрах различных серий запросов используются разный набор полей, то чтобы объединить их необходимо ввести одинаковое название для каждого **Алиас** (подробнее см. раздел «Добавление запроса»). Для объединения полей при визуализации необходимо в параметрах блока "Настройка осей" указать **Алиас**.

Пример отображения с включенным и выключенным стеком приведен на «Рис. 48».

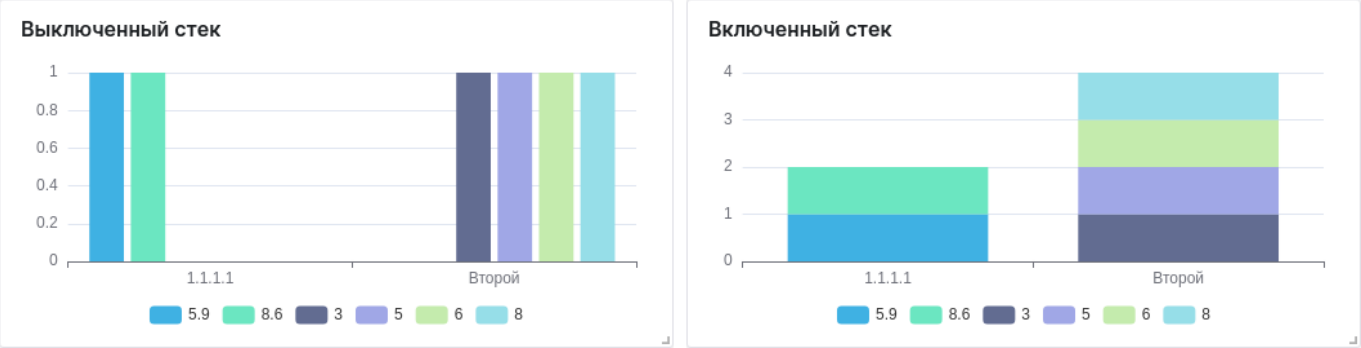


Рис. 48 – Примеры визуализации виджета со стеком

Для настройки визуализации выполните следующие действия:

1. Выберите стиль: линия или колонка.
2. При необходимости включите стек, установив соответствующий флаг.
3. Если выбран стиль линия, то выберите ее тип: линейный, скругленный, шаг с начала, шаг
   с конца.
4. Выберите цветовую схему.

6.3.6.3 Шаг 3. Легенда

Настройка отвечает за выбор способа отображения легенды на графике. Выберите место отображения легенды: сверху, снизу или не отображать.

6.3.7 Метрика

Виджет отображает тренд изменения выбранного показателя за период времени. Пример внешнего вида приведен на «Рис. 49».

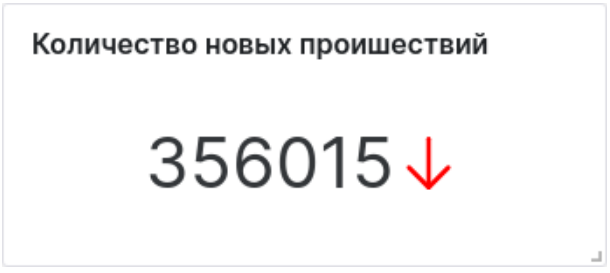


Рис. 49 – Виджет "Метрика"

Пример настроек приведен на «Рис. 50».

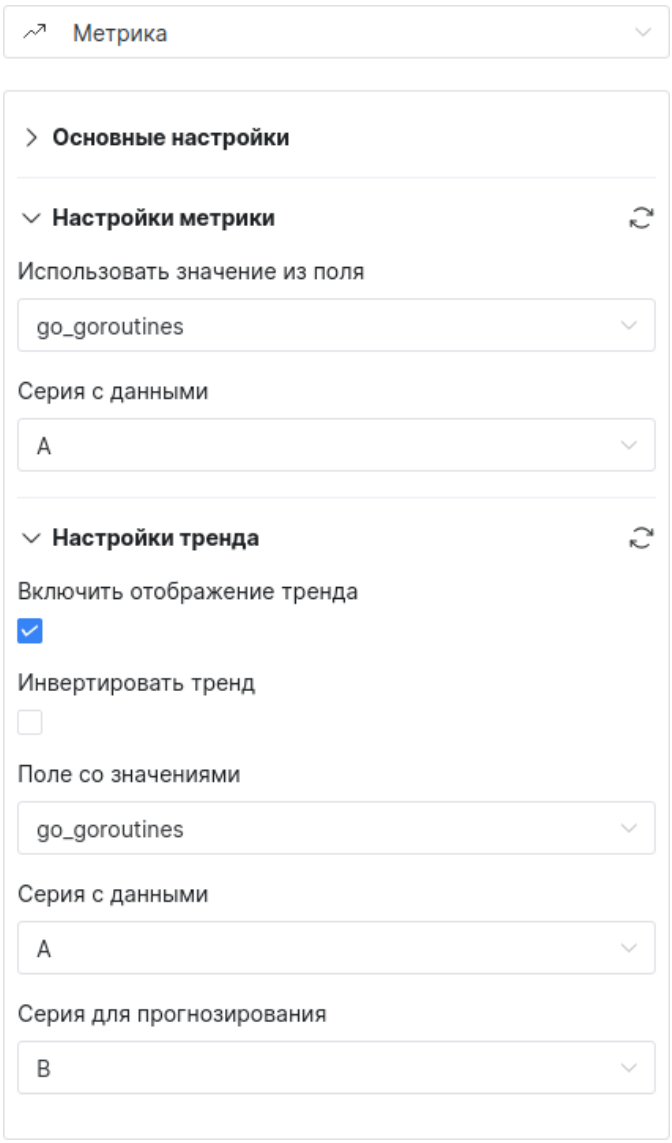


Рис. 50 – Виджет "Метрика". Настройки

Для настройки виджета выполните следующие действия:

1. В блоке "Настройки метрики" укажите следующие данные:
    - в поле "Использовать значение из поля" выберите поле, значение из которого будет использоваться при подсчете метрики;
    - в поле "Серия с данными" из выпадающего списка выберите запрос.
2. В блоке "Настройки тренда" укажите следующие данные:
    - для отображения тренда на виджете установите соответствующий флаг;
    - для изменения направления отображения тренда установите флаг "Инвертировать тренд";
    - в полях "Поле со значениями" и "Серия с данными" выберите запрос и поле, значение из которого будет использоваться для отображения численной части метрики;
    - в поле "Серия для прогнозирования" выберите запрос, по которому будет отображаться изменение тренда.

Примечание: значения полей, которые доступны для выбора при настройке в блоках "Настройки метрики" и "Настройки тренда", формируются на основе данных указанных в запросе (подробнее см. раздел «Добавление запроса»).

Примеры визуализации виджета приведены на «Рис. 51».

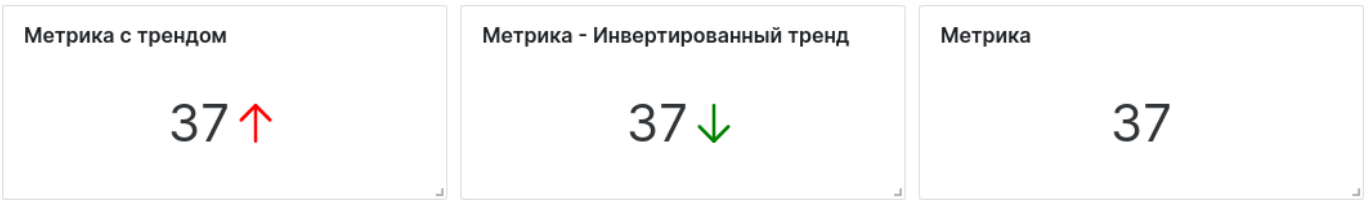


Рис. 51 – Примеры визуализации настроек виджета "Метрика"

6.3.8 Изображение

Виджет отображает изображение, загруженное пользователем.

Пример внешнего вида представлен на «Рис. 52».

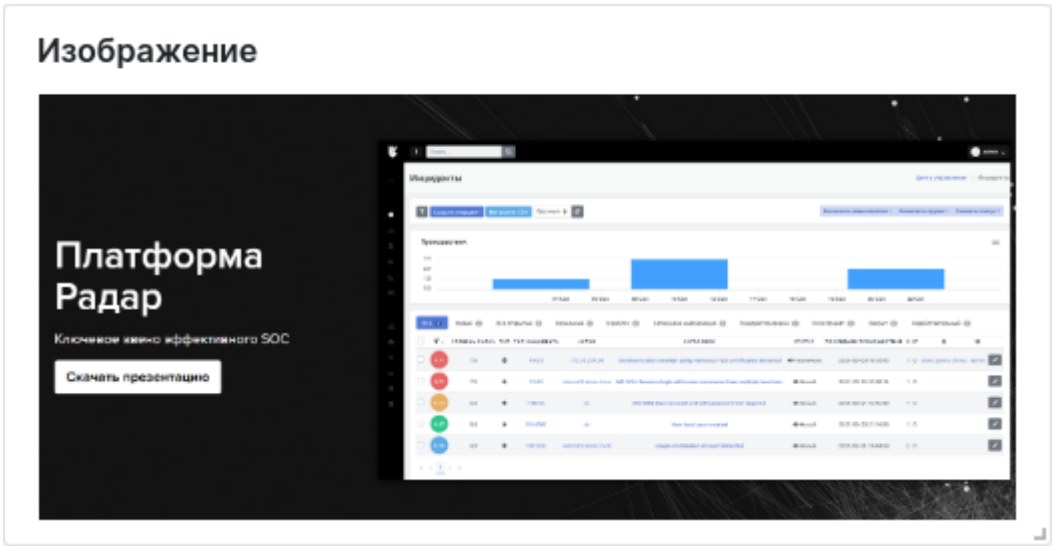


Рис. 52 – Виджет "Изображение"

Пример настроек приведен на «Рис. 53».

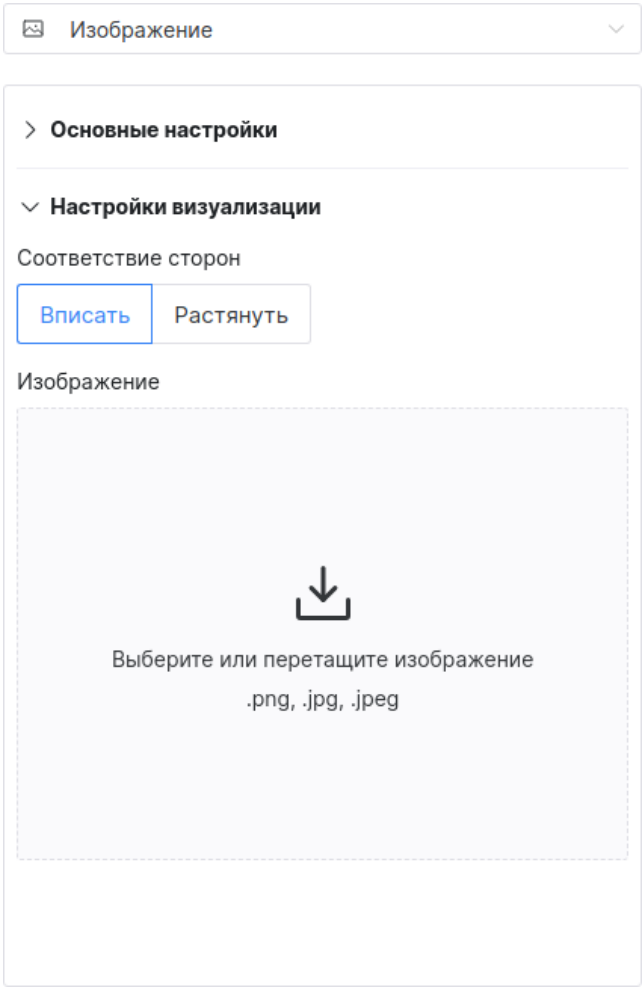


Рис. 53 – Виджет "Изображение". Настройки

Для настройки виджета выполните следующие действия:

1. Выберите соответствие сторон: вписать изображение или растянуть изображение.
2. Загрузите изображение с помощью стандартного механизма выбора и загрузки изображения на сайт.

6.4 Копирование виджета

Вы можете скопировать параметры виджета и передать их другому пользователю или создать новый виджет на основе существующего.

Есть несколько способов для копирования параметров:

- **Способ 1**. В конструкторе виджетов нажмите кнопку . Настройки виджета будут скопированы в буфер обмена.
- **Способ 2**. Перейдите в раздел **Администрирование** → **Рабочие столы**, выберите виджет, нажмите кнопку и из выпадающего списка выберите пункт **Копировать настройки**.

- **Способ 3**. Перейдите в раздел **Администрирование** → **Отчеты**, выберите виджет, нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Копировать настройки**.

Для того чтобы применить скопированные настройки откройте конструктор виджетов и нажмите кнопку .

6.5 Предустановки

Предустановки используются для быстрой настройки виджетов на основе шаблона.

Вы можете добавить собственные шаблоны настроек виджетов в список предустановок.

Для создания виджета с помощью предустановки откройте конструктор виджетов и нажмите кнопку .

В открывшемся окне "Предустановки" (см. «Рис. 54») выберите предустановку и нажмите кнопку .

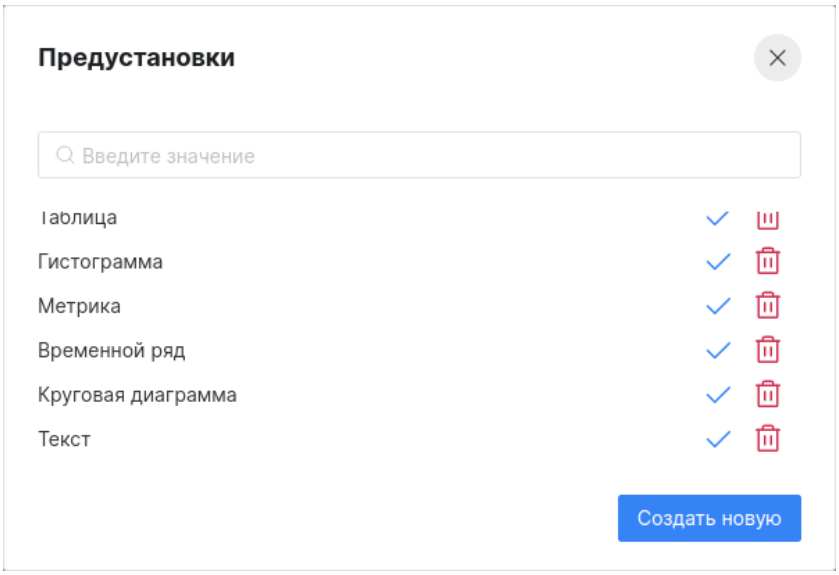


Рис. 54 – Окно "Предустановки"

Для создания предустановки выполните следующие действия:

1. Настройте запросы и визуализацию виджета.
2. Нажмите кнопку и в открывшемся окне "Предустановки" (см. «Рис. 54») нажмите кнопку **Создать новую**.
3. В открывшемся окне укажите название предустановки.
4. Нажмите кнопку **Создать**.

7. Отчеты

7.1 Общие данные

Платформа Радар позволяет формировать отчеты, которые предоставляют наглядные данные, чтобы помочь вам оценить эффективность и производительность платформы.

Отображение информации выполняется с помощью следующих типов виджетов:

- временной ряд;
- круговая диаграмма;
- таблица;
- текст;
- гистограмма;
- метрика;
- изображение.

Подробнее о каждом типе виджета вы можете ознакомиться в разделе «Конструктор виджетов».

Работа с отчетами включают в себя следующие процессы:

1. «Создание отчета».
2. «Конструктор отчета».
3. «Настройка расписания генерации отчета».
4. «Настройка прав доступа к отчету».
5. «Импорт отчетов».
6. «Экспорт отчетов».
7. «Удаление отчета».

В разделе «Архив отчетов» выполняется работа с архивом сгенерированных отчетов.

Для работы с отчетами перейдите в новый интерфейс и откройте раздел **Администрирование → Отчеты** (см. «Рис. 55»).

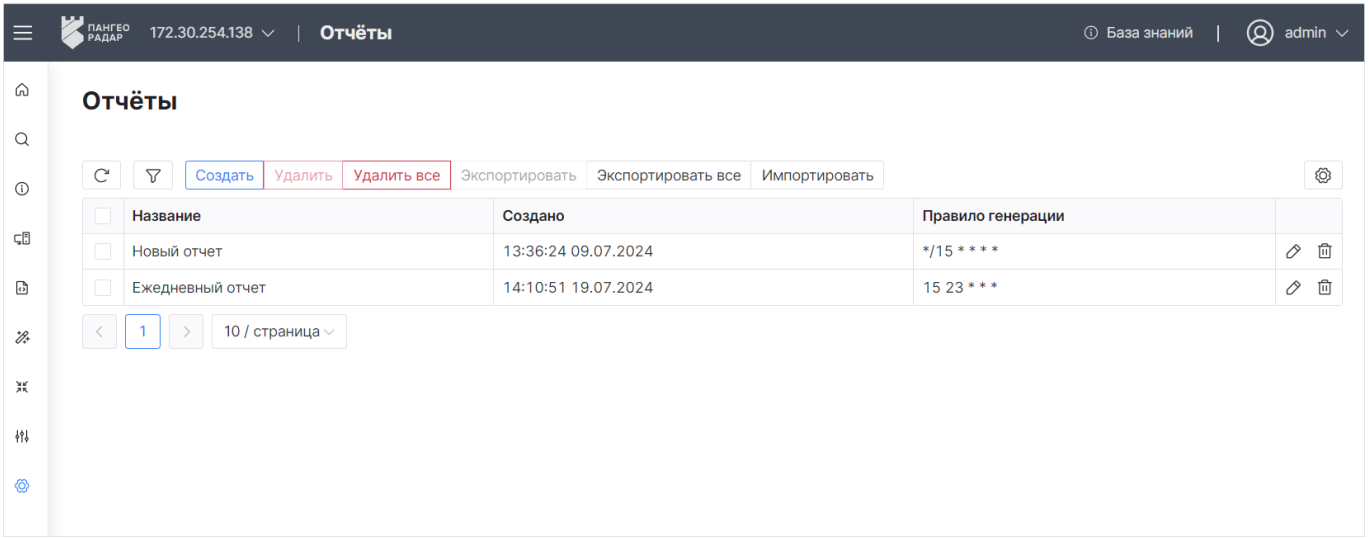


Рис. 55 – Раздел "Отчеты"

В разделе отображается следующая информация:

- Название - наименование отчета;
- Создано - дата и время создания отчета;
- Правило генерации - расписание автоматической генерации отчета.

7.2 Создание отчета

Перейдите в раздел **Администрирование** → **Отчеты** и нажмите кнопку **Создать**.

Откроется окно "Создать отчет" (см. «Рис. 56»).

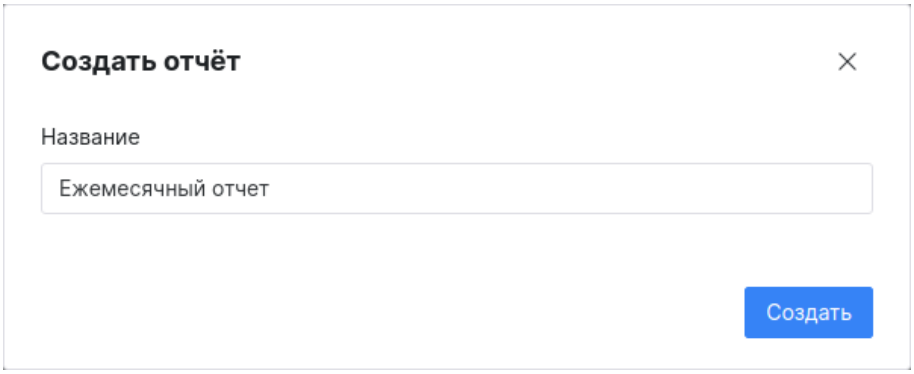


Рис. 56 – Окно "Создать отчет"

Выполните в окне следующие действия:

1. В поле "Название" укажите название отчета.
2. Нажмите кнопку **Создать**.
3. Будет создан отчет и произойдет переход в конструктор отчета (см. «Рис. 57»).

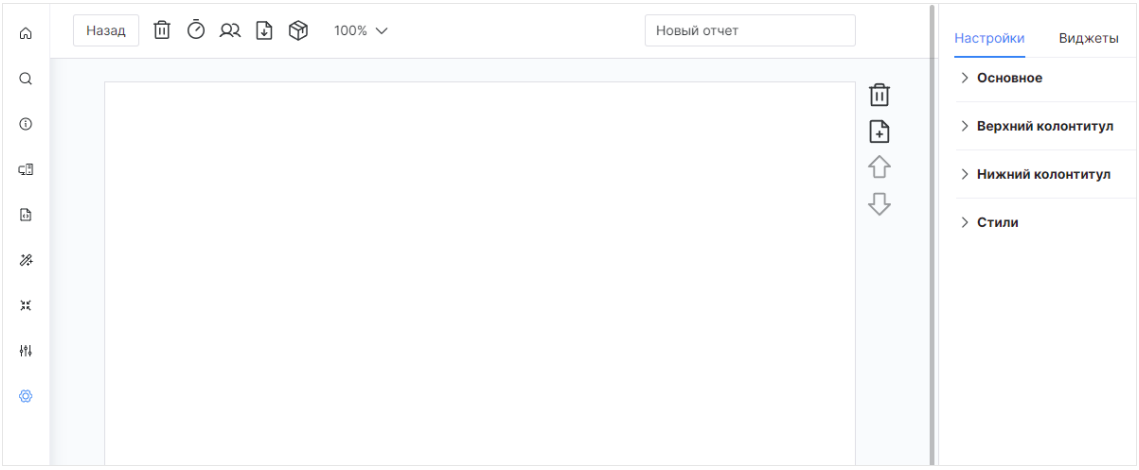


Рис. 57 – Страница "Конструктор отчета"

7.3 Конструктор отчета

Примечание: при настройке отчета все изменения автоматически сохраняются.

Настройка отчета выполняется на странице "Конструктор отчета" (см. «Рис. 58»).

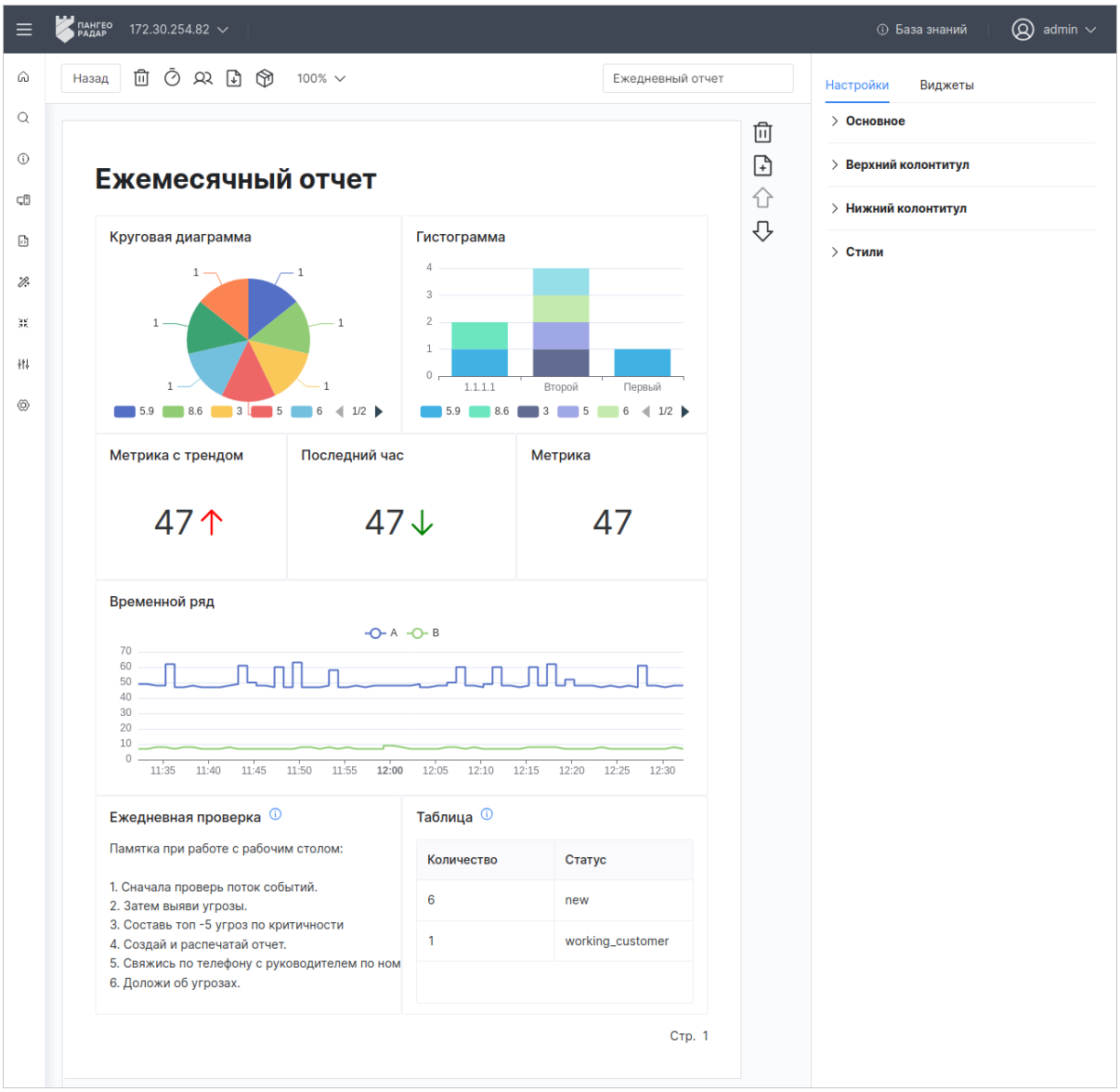


Рис. 58 – Интерфейс страницы "Конструктор отчета"

Страницу можно открыть следующими способами:

- перейти в раздел **Администрирование** → **Отчеты**, выбрать нужный отчет из списка и нажать кнопку в соответствующей строке;
- выполнить процесс создания отчета. После создания отчета страница "Конструктор отчета" откроется автоматически.

Внешний вид отчета формируется в зависимости от выставленной пользователем конфигурации настроек страниц отчета и виджетов.

Конструктор состоит из следующих блоков:

- панель действий, где располагаются элементы управления;
- рабочая область, где располагаются страницы отчета, на которых отображаются виджеты;
- настройка страниц, где выполняется настройка внешнего вида страниц отчета.

Панель действий

Блок располагается вверху конструктора (см. «Рис. 59»).

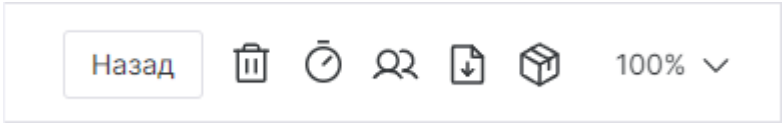


Рис. 59 – Страница "Конструктор отчета". Блок "Панель действий"

На панели действий доступны следующие элементы управления:

Кнопка	Действие
Назад	возвращение к списку отчетов
	удаление отчета
	настройка расписания генерации отчетов
	настройка прав доступа пользователей к отчету
	экспорт отчета в файл формата .pdf
	просмотр списка сгенерированных по расписанию отчетов
100%	изменение масштаба отображения страниц отчета

Рабочая область

Пример внешнего вида блока приведен на «Рис. 60».

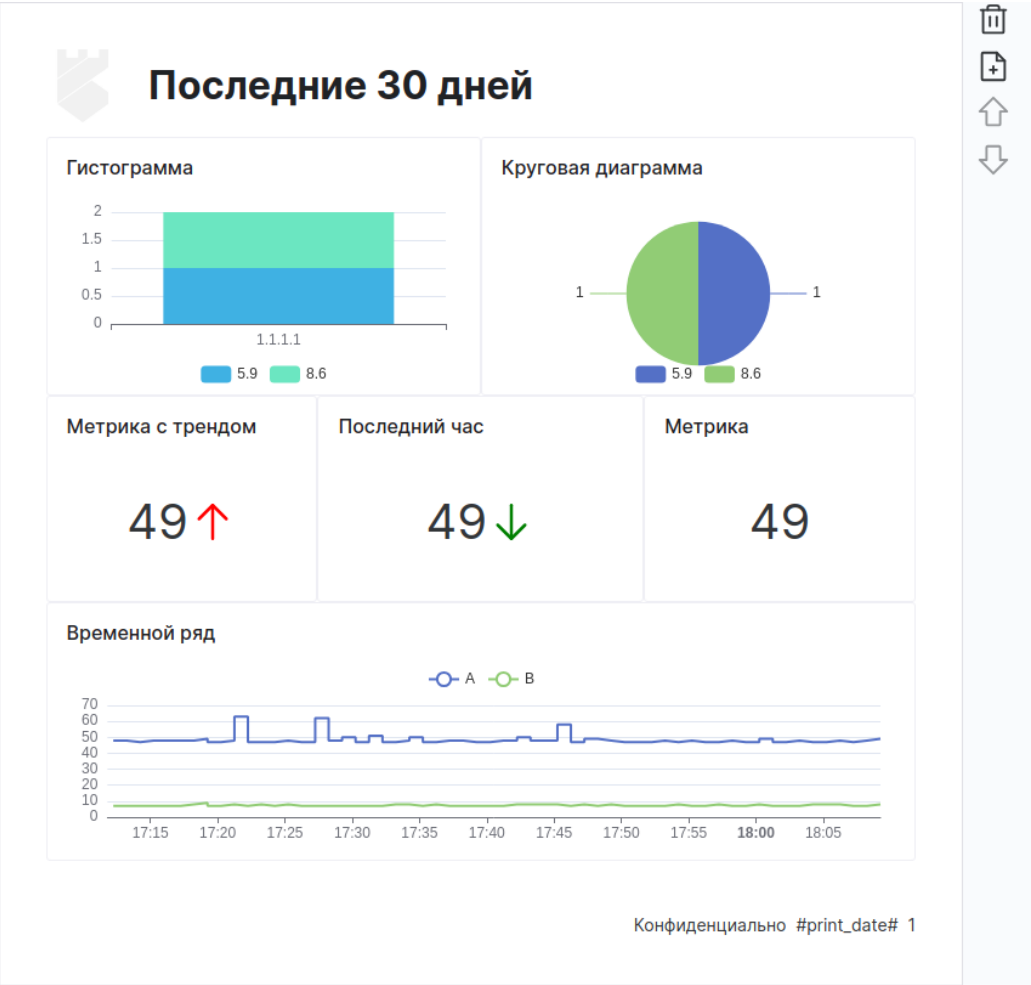


Рис. 60 – Страница "Конструктор отчета". Блок "Рабочая область"

В рабочей области доступны следующие элементы управления:

Кнопка	Действие
	удаление страницы из отчета
	добавление страницы в отчет
	перемещение страницы вниз. После действия текущая страница поменяется местами со следующей страницей
	перемещение страницы вверх. После действия текущая страница поменяется местами с предыдущей страницей

При наведении курсора на виджет становятся доступны следующие элементы управления:

Кнопка	Действие
	доступ к следующим действиям над виджетом: – редактирование; – удаление; – копирование настроек.
	изменение размера виджета

Настройка страниц

Блок состоит из двух вкладок:

- **Настройки** – настройки страниц отчета, включающие в себя:
  - Основное – настройка периода и правила генерации наименования отчета;
  - Верхний колонтитул – настройка текста и изображения на верхнем колонтитуле;
  - Нижний колонтитул – настройка текста, нумерации страниц и отображения даты на нижнем колонтитуле;
  - Стили – настройка используемых шрифтов.
- **Виджеты** – список доступных типов виджетов, которые можно добавить на страницу отчета.

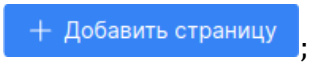
Настройка отчета состоит из следующих процессов:

1. Добавление страницы.
2. Выбор периода формирования данных виджетов.
3. Настройка наименования отчета в момент генерации.
4. Настройка страниц, которая включает в себя:
   - настройку верхнего колонтитула;
   - настройку нижнего колонтитула;
   - настройку стиля шрифтов.
5. Настройка виджетов, которая включает в себя:
   - добавление виджета на страницу отчета;
   - редактирование виджета;
   - копирование настроек виджета;
   - изменение размера виджета;
   - изменение расположения виджета;
   - удаление виджета.
6. Изменение порядка страниц.
7. Удаление страницы.

7.3.1 Добавление страницы

На страницах можно расположить виджеты для отображения данных.

Добавление страниц в отчет выполняется следующим образом:

- если в отчете нет страниц, то нажмите кнопку 

;
- если в отчете уже есть страницы, то нажмите кнопку  .

Добавьте необходимое количество страниц в отчет.

7.3.2 Выбор периода формирования данных виджетов

Выбор периода формирования данных виджетов выполняется в блоке **Настройки → Основное** (см. «Рис. 61»).

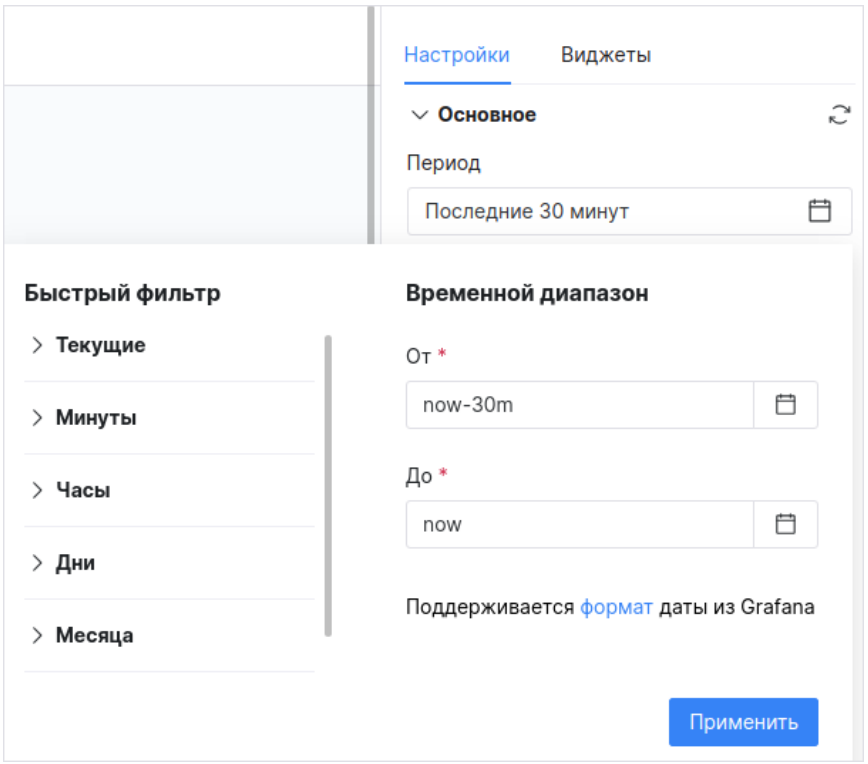


Рис. 61 – Выбор периода формирования данных виджетов

Для настройки периода выполните следующие действия:

1. В поле **Период** нажмите кнопку . Откроется окно выбора временного диапазона (см. «Рис. 61»).
2. Выберите период. Доступные значения:
   - текущие: минута, час, день, месяц, год;
   - последние: минуты, часы, месяца, года;
   - период можно указать вручную в соответствующих полях. Поддерживается формат дат из **Grafana**.
3. Нажмите кнопку **Применить**.

7.3.3 Настройка наименования отчета в момент генерации

Вы можете настроить расписание генерации отчета (подробнее см. раздел «Настройка расписания генерации отчета»).

В момент генерации, отчету присваивается наименование в соответствии с настроенным правилом.

Настройка правила выполняется в блоке **Настройки → Основное**. В поле "Маска для генерации названия" укажите необходимую маску (см. «Рис. 62»).

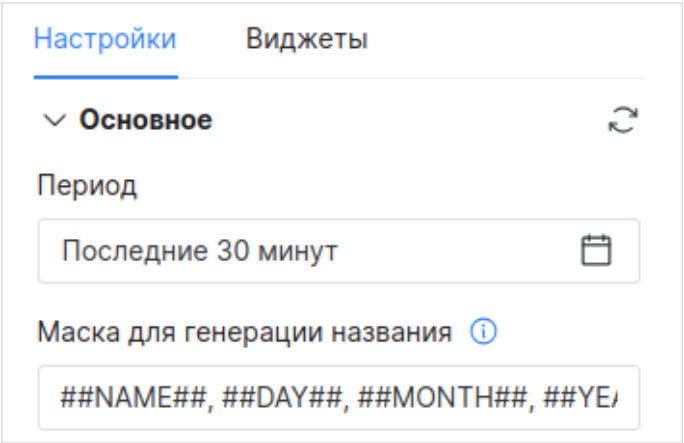


Рис. 62 – Настройка маски для генерации названия

Доступные значения:

- ##NAME## - название отчета;
- ##ID## - идентификатор отчета;
- ##MINUTE## - минута в момент генерации;
- ##HOUR## - час в момент генерации;
- ##DAY## - день в момент генерации;
- ##MONTH## - месяц в момент генерации;
- ##YEAR## - год в момент генерации.

7.3.4 Настройка страниц

7.3.4.1 Настройка верхнего колонтитула

При необходимости вы можете настроить отображение заголовка и изображение в верхнем колонтитуле.

Настройка выполняется в блоке **Настройки → Верхний колонтитул** (см. «Рис. 63»).

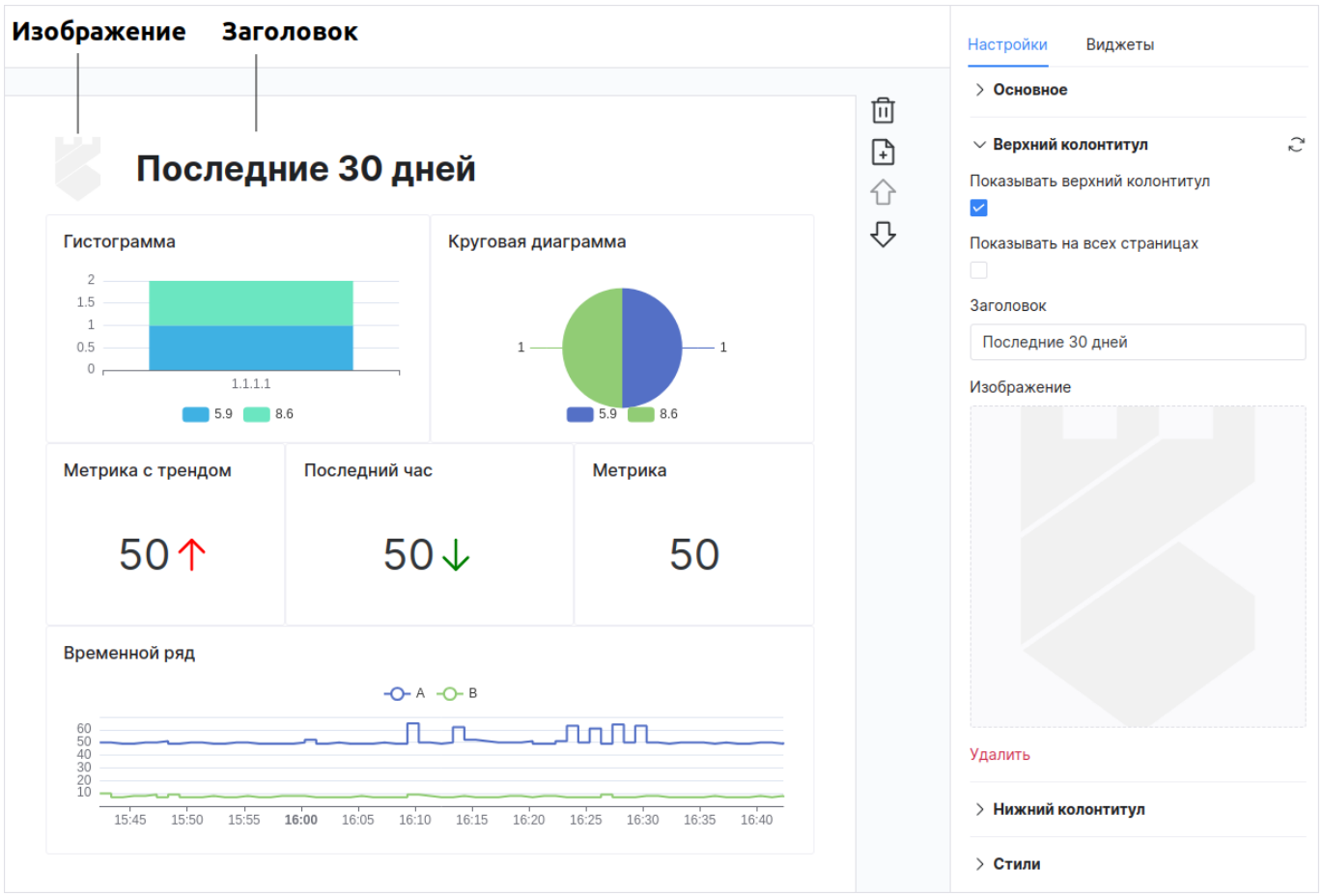


Рис. 63 – Настройка верхнего колонтитула

Для настройки верхнего колонтитула выполните следующие действия:

1. Для отображения верхнего колонтитула установите флаг "Показывать верхний колонтитул".
2. Для отображения верхнего колонтитула на всех страницах отчета установите флаг "Показывать на всех страницах".
3. В поле "Заголовок" укажите заголовок отчета.
4. В поле "Изображение" загрузите изображение с помощью стандартного механизма выбора и загрузки изображения на сайт.

7.3.4.2 Настройка нижнего колонтитула

Для многостраничных отчетов вы можете настроить отображение нумерации страниц, даты и текста в нижнем колонтитуле.

Настройка выполняется в блоке **Настройки → Нижний колонтитул** (см. «Рис. 64»).

Рис. 64 – Настройка нижнего колонтитула

Для настройки нижнего колонтитула выполните следующие действия:

1. Для отображения нижнего колонтитула установите флаг "Показывать нижний колонтитул".
2. Для отображения нижнего колонтитула на первой странице отчета установите флаг "Показывать на первой странице".
3. Для отображения нумерации страниц установите флаг "Показать номер страницы".
4. Для отображения даты генерации отчета установите флаг "Показывать дату".
5. В поле "Текст" укажите необходимый текст.

7.3.4.3 Настройка стиля шрифта

Вы можете настроить стиль шрифта, отображаемый в виджетах.

Настройка выполняется в блоке **Настройки → Стили**.

Для выбора стиля шрифта в поле "Используемый шрифт" из выпадающего списка выберите шрифт.

При необходимости вы можете загрузить собственный стиль шрифта. Для этого нажмите кнопку **Загрузить** и укажите путь к файлу со стилем шрифта.

7.3.5 Настройка виджетов

Данные, формируемые для отчета, отображаются с помощью виджетов. Настройка виджетов включат в себя следующие процессы:

1. Добавление виджета на страницу отчета.
2. Редактирование виджета.

3. Копирование настроек виджета.
4. Изменение расположения виджета.
5. Изменение размера виджета
6. Удаление виджета.

7.3.5.1 Добавление виджета

Добавление виджета на страницу отчета выполняется из вкладки **Виджеты** (см. «Рис. 65»).

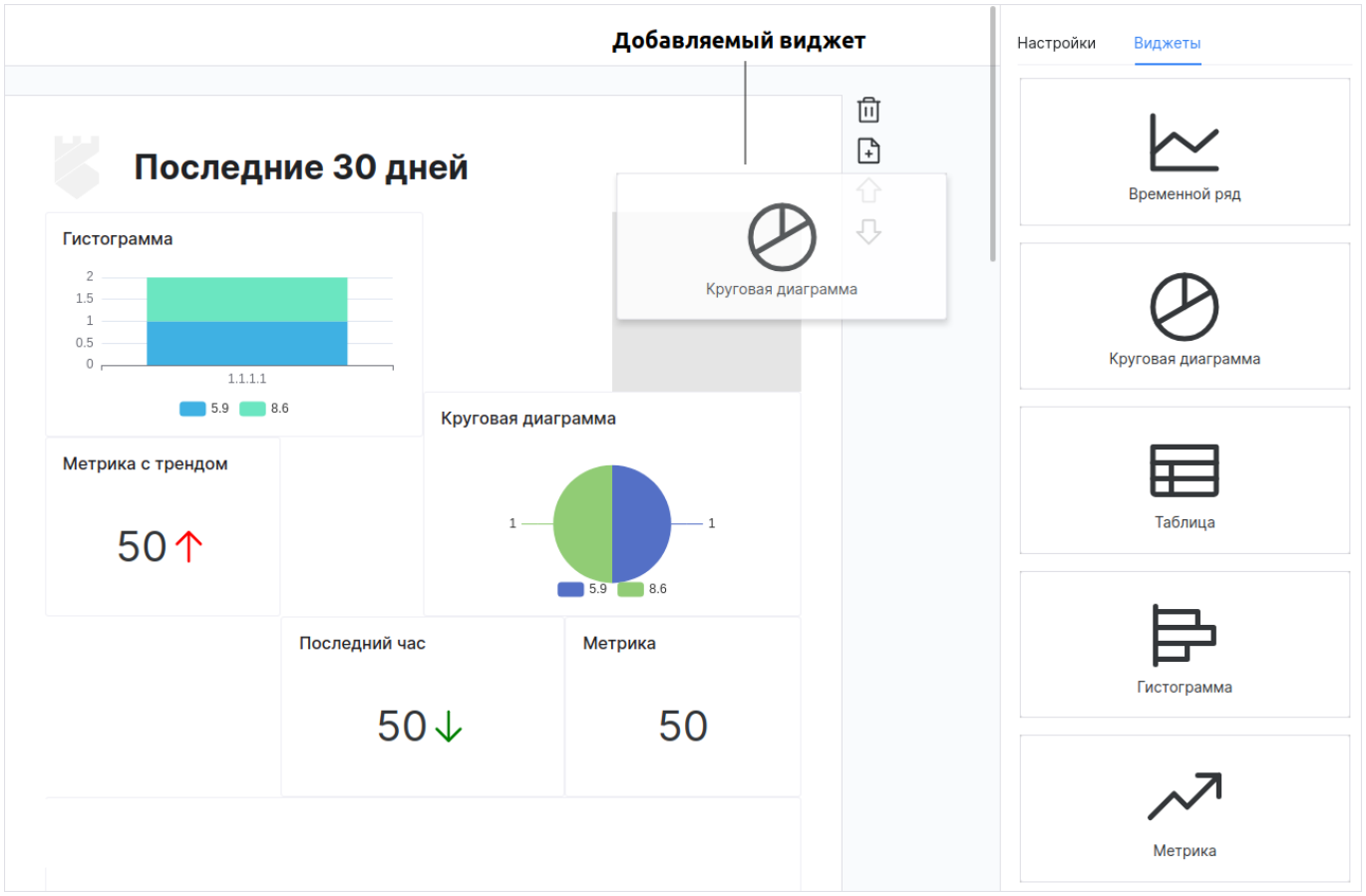


Рис. 65 – Страница "Конструктор отчета". Вкладка "Виджеты"

Для добавления виджета на страницу отчета выполните следующие действия:

1. Наведите курсор мыши на нужный виджет и зажмите ЛКМ.
2. Перетащите виджет на страницу отчета. Место, на котором можно расположить виджет, будет подсвечено.
3. Отпустите ЛКМ.
4. Добавьте необходимое количество виджетов в отчет.

7.3.5.2 Редактирование виджета

Для редактирования виджета выполните следующие действия:

1. Перейдите на страницу "Конструктор отчета" и выберите виджет.

2. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Редактировать**.
3. Выполните настройку виджета в конструкторе (подробнее см. раздел «Конструктор виджетов»).

7.3.5.3 Копирование настроек виджета

Для копирования настроек виджета выполните следующие действия:

1. Перейдите на страницу "Конструктор отчета" и выберите виджет.
2. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Копировать настройки**.
3. Затем вы можете передать настройки другому пользователю, или создать новый виджет на основе скопированного.

Чтобы применить скопированные настройки необходимо начать процесс редактирования виджета. Для применения скопированных настроек нажмите кнопку в конструкторе виджетов (подробнее см. раздел «Конструктор виджетов»).

7.3.5.4 Изменение расположения виджета

Для изменения расположения виджета выполните следующие действия:

1. Перейдите на страницу "Конструктор отчета" и наведите курсор мыши на нужный виджет. Курсор мыши примет следующий вид: .
2. Зажмите ЛКМ и перемещайте мышку в нужном направлении.
3. Отпустите ЛКМ после перемещения.

7.3.5.5 Изменение размера виджета

Для изменения размера виджета выполните следующие действия:

1. Перейдите на страницу "Конструктор отчета" и выберите виджет.
2. Нажмите и удерживайте кнопку в правом нижнем углу виджета.
3. Перемещайте мышку в нужном направлении.
4. Отпустите кнопку после перемещения.

7.3.5.6 Удаление виджета

Для удаления виджета со страницы отчета выполните следующие действия:

1. Перейдите на страницу "Конструктор отчета" и выберите виджет.
2. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Удалить**.
3. Подтвердите удаление в открывшемся окне. Виджет будет удален со страницы отчета.

7.3.6 Изменение порядка страниц

Если у вас многостраничный отчет, то при необходимости вы можете изменить порядок страниц.

Для перемещения страницы вниз, выберите нужную страницу и нажмите кнопку . Выбранная страница поменяется местами со следующей страницей.

Для перемещения страницы вверх, выберите нужную страницу и нажмите кнопку . Выбранная страница поменяется местами с предыдущей страницей.

7.3.7 Удаление страницы

Для удаления страницы из отчета, выберите нужную страницу и нажмите кнопку .

7.4 Настройка расписания генерации отчета

Работа с генерацией отчетов по расписанию проходит по следующему сценарию:

1. Настройка расписания генерации отчета пользователем.
2. Автоматическая генерация отчета по расписанию с сохранением отчетов в архив.
3. Просмотр архива пользователем и экспорт выбранных отчетов в виде файлов.

Для настройки расписания генерации отчета выполните следующие действия:

1. Настройте отчет и нажмите кнопку . Откроется окно "Планировщик" (см. «Рис. 66»).

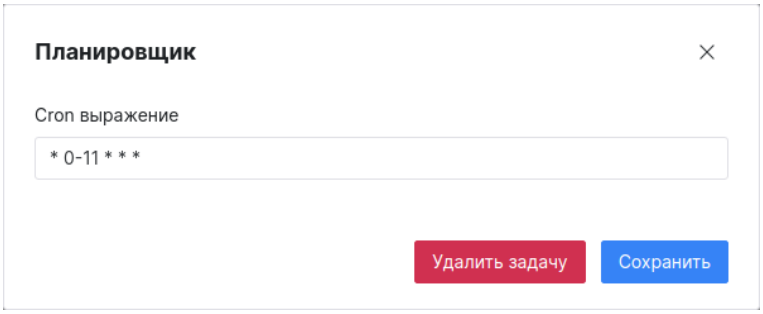


Рис. 66 – Окно "Планировщик"

2. Укажите в окне **Cron выражение**.
3. Нажмите кнопку **Сохранить**. Будет создана задача планировщика.

Для удаления задачи планировщика необходимо выбрать отчет, для которого настроено расписание, нажать кнопку и в открывшемся окне нажать кнопку **Удалить задачу**.

7.4.1 Просмотр истории генерации отчета

Для просмотра архива по отчету перейдите на страницу "Конструктор отчета" и нажмите кнопку . Откроется окно "Список отчетов" (см. «Рис. 67»).

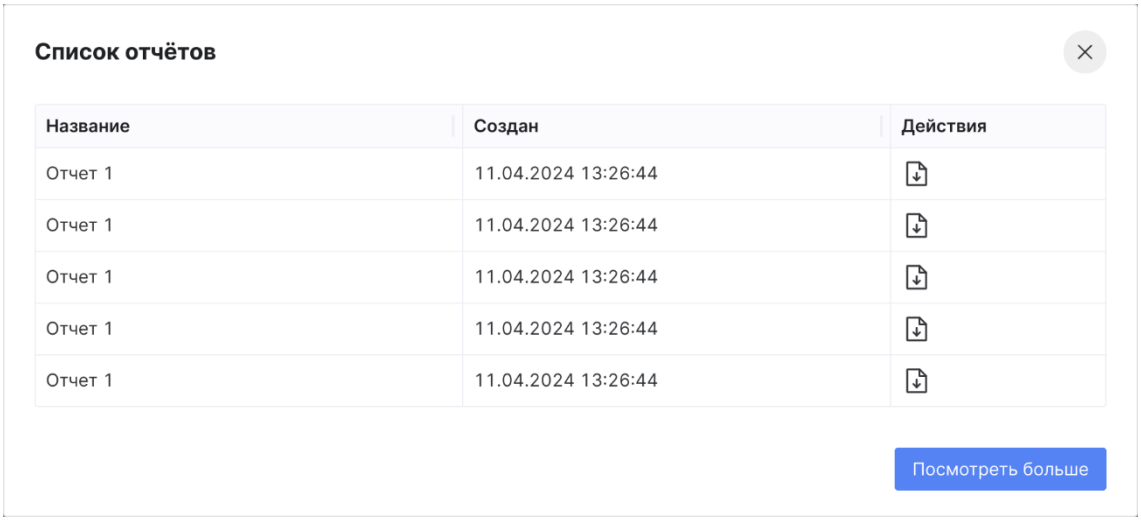


Рис. 67 – Окно "Список отчетов"

В окне отображается следующая информация:

- Название - название отчета;
- Создан - дата и время генерации отчета.

Для экспорта отчета нажмите кнопку .

Для просмотра истории генерации по всем отчетам нажмите кнопку **Посмотреть больше** (подробнее см. раздел «Архив отчетов»).

7.5 Настройка прав доступа к отчету

Перейдите на страницу "Конструктор отчета" и нажмите кнопку . Откроется окно "Редактирование прав" (см. «Рис. 68»).

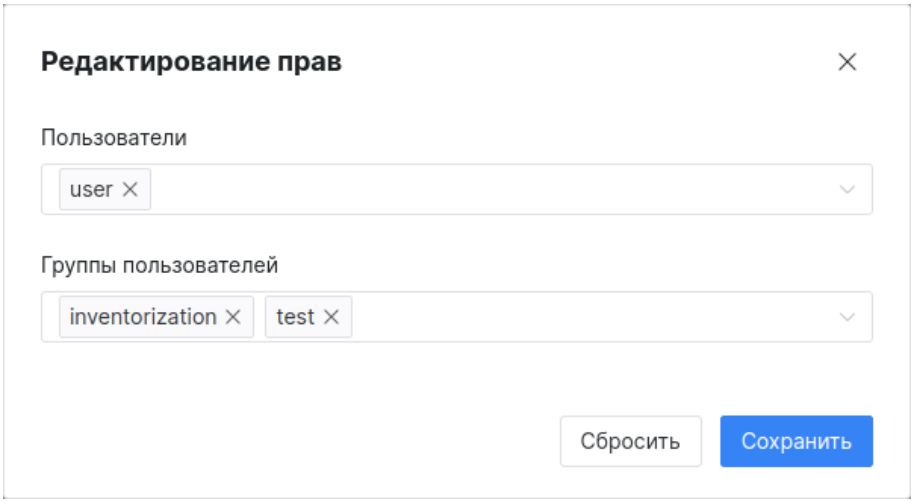


Рис. 68 – Окно "Редактирование прав"

Настройте права доступа одним из следующих способов:

- в поле "Пользователи" из выпадающего списка выберите пользователей, которым будет доступен отчет;
- в поле "Группы пользователей" из выпадающего списка выберите группы пользователей, которым будет доступен отчет.

7.6 Импорт отчетов

Для импорта отчетов выполните следующие действия:

1. Перейдите в раздел **Администрирование → Отчеты**.
2. Нажмите кнопку **Импортировать**.
3. В открывшемся окне укажите путь к архиву с отчетами.
4. Нажмите кнопку **Открыть**.

7.7 Экспорт отчетов

Выполнить экспорт отчетов можно двумя способами:

- экспорт в файл формата .pdf;
- экспорт в архив.

Способ 1. Экспорт в файл формата .pdf

1. Перейдите на страницу "Конструктор отчета".
2. Настройте отчет и нажмите кнопку  .
3. В открывшемся окне укажите путь для сохранения отчета.
4. Отчет будет сохранен в файл формата .pdf.

Способ 2. Экспорт в архив

Для экспорта одного или нескольких отчетов в архив формата .zip выполните следующие действия:

1. Перейдите в раздел **Администрирование → Отчеты**.
2. Установите флаги напротив нужных отчетов.
3. Нажмите кнопку **Экспортировать**.
4. Будет сформирован архив с отчетами в формате .zip.
5. Нажмите кнопку **Скачать** и укажите путь для сохранения архива.

Для экспорта всех отчетов, отображаемых в таблице, нажмите кнопку **Экспортировать все**.

7.8 Удаление отчета

Удаление отчета можно выполнить следующими способами:

- Из конструктора отчетов. Перейдите на страницу "Конструктор отчета" и нажмите кнопку  . Подтвердите удаление в открывшемся окне.
- Из таблицы "Отчеты". Перейдите в раздел **Администрирование → Отчеты**, выберите нужный отчет из списка и нажмите кнопку  в соответствующей строке;
- Массовое удаление отчетов:

- перейдите в раздел **Администрирование → Отчеты**, установите флаги напротив нужных отчетов и нажмите кнопку **Удалить**.
- для удаления всех отчетов, отображаемых в таблице, нажмите кнопку **Удалить все**.

7.9 Архив отчетов

Отчеты, сгенерированные по расписанию, помещаются в архив (подробнее см. раздел «Настройка расписания генерации отчета»). Для просмотра истории генерации по всем отчетам перейдите в раздел **Администрирование → Архив отчетов** (см. «Рис. 69»).

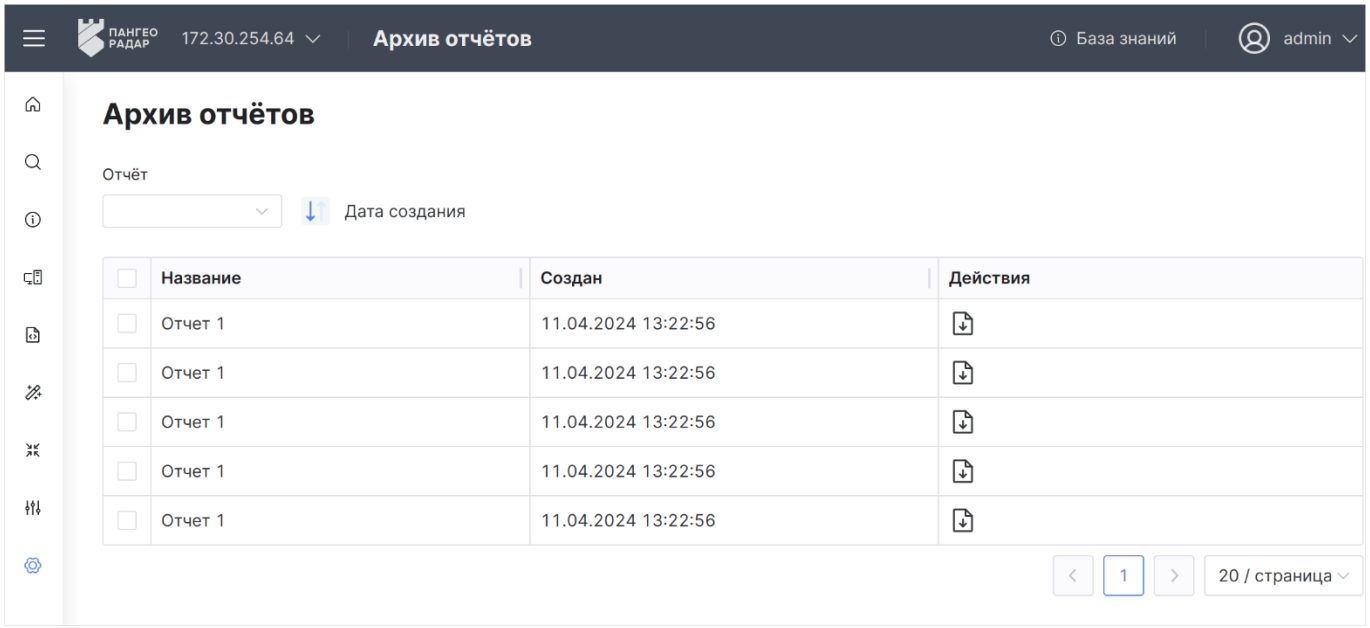


Рис. 69 – Раздел "Архив отчетов"

В разделе отображается следующая информация:

- Название - название отчета;
- Создан - дата и время генерации отчета.

Для формирования списка отчетов выполните следующие действия:

1. В поле "Отчет" из выпадающего списка выберите отчет.
2. Выберите направление сортировки:
   - ↓ - от последнего к первому;
   - ↑ - от первого к последнему.

Для экспорта отчетов выполните следующие действия:

1. Отметьте отчеты, которые необходимо экспортировать, установив флаг в соответствующей строке.
2. Нажмите кнопку .
3. В открывшемся окне укажите путь для сохранения отчетов.

8. Мониторинг

Внимание! *В настоящем разделе описаны общие данные о мониторинге и приемы работы с элементами интерфейса. Подробная информация о собираемых метриках приведена в документе «Перечень метрик мониторинга»*.

8.1 Общие данные

В качестве системы мониторинга используются сервисы **Prometheus** и **Grafana**.

Prometheus собирает сведения о работе платформы и ресурсах.

Grafana выводит данные сведения на следующие приборные панели:

- **Общий мониторинг**– мониторинг основных параметров **Платформы Радар**;
- **Поток событий** – мониторинг параметров потока событий;
- **Kafka** – мониторинг параметров системы обмена сообщениями «Kafka»;
- **Статистика потока** – мониторинг показателей обработки потока событий;
- **OpenSearch** – мониторинг параметров поисковой системы «OpenSearch»;
- **Лог коллектор** – мониторинг показателей работы агентов сбора лог-коллектора.

Сервисы **Node-exporter**, **Kafka-exporter**, **Opensearch-exporter** отвечают за сбор метрик с узлов платформы, службы **Kafka** и хранилища обработанных событий, соответственно.

Рекомендации по установке сервисов для обеспечения сбора метрик и мониторинга платформы:

- **Prometheus** – устанавливается на сервер с ролью "Monitoring" и собирает метрики с использованием различных экспортеров:
- **Node_exporter** – устанавливается на каждый узел платформы и позволяет собирать метрики операционной системы;
- **Kafka_exporter** – устанавливается на сервер с ролью "Balancer" и позволяет собирать метрики **Kafka**;
- **Opensearch-exporter** – устанавливается на сервер с ролью "Data" и позволяет собирать метрики OpenSearch.

Примечание: *В Платформе Радар предусмотрена возможность передачи метрик производительности во внешние системы мониторинга*.

Платформа Радар обеспечивает многострочный вывод метрик производительности в формате строки «Prometheus» (ключ, значение), что позволяет экспортировать метрики в систему «Zabbix».

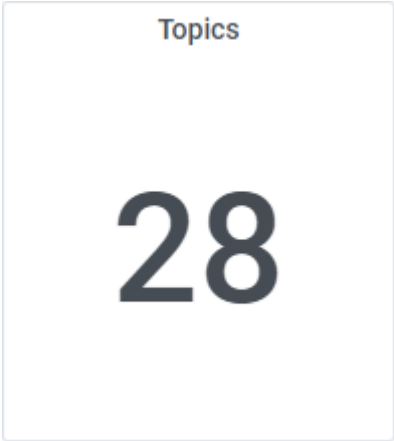
8.2 Элементы управления мониторингом

Для просмотра приборных панелей перейдите в раздел **Мониторинг** и из выпадающего списка выберите необходимый пункт: **Общий мониторинг**, **Поток событий**, **Kafka**, **Статистика поток** или **OpenSearch**. Откроется выбранная приборная панель.

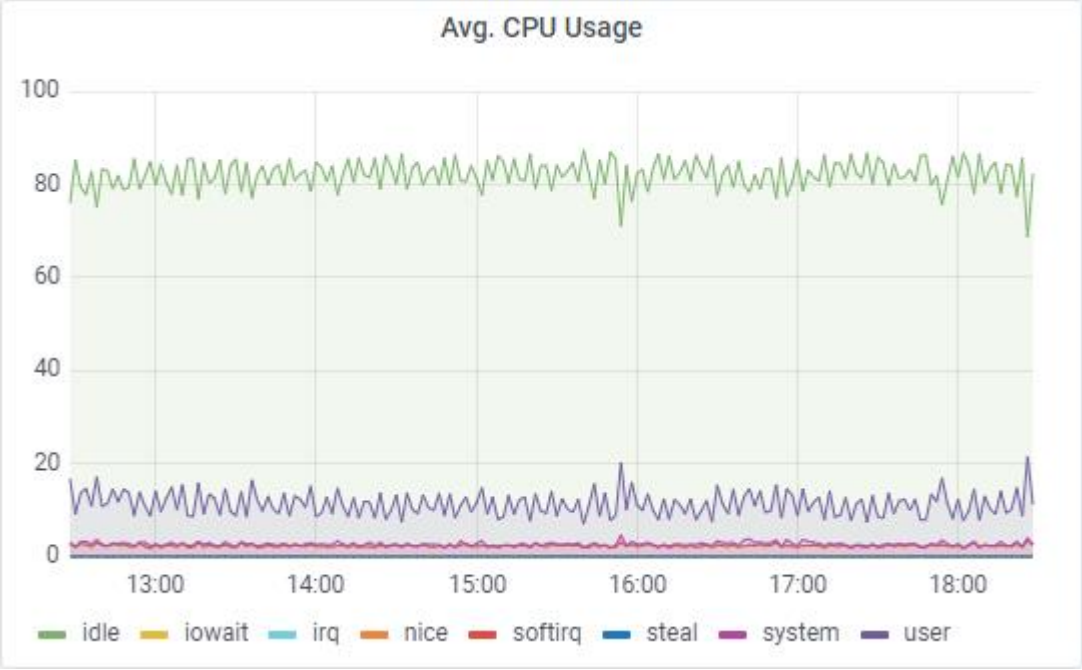
Для отображения информации в приборных панелях используются виджеты.

В общем случае используются следующие типы виджетов:

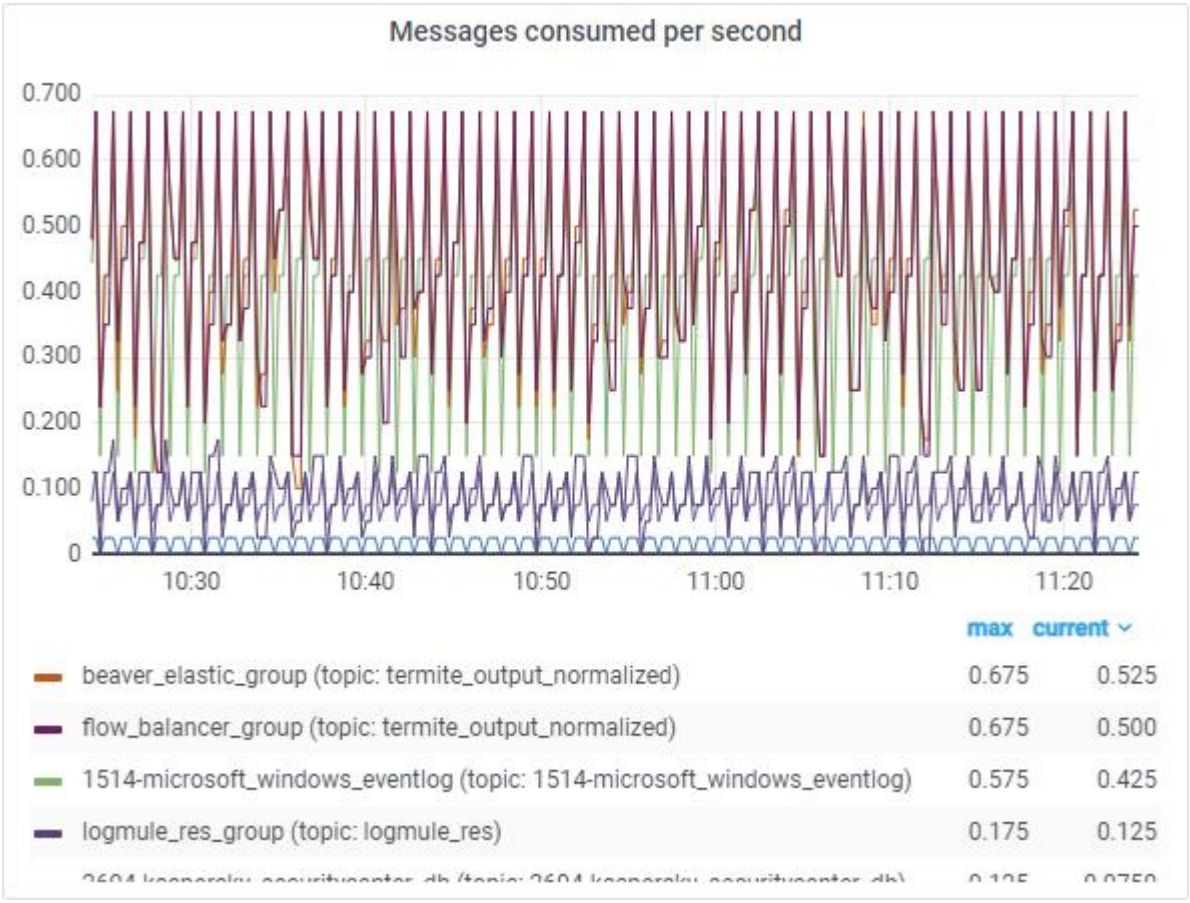
- **Первый тип** – виджет, отображающий конкретное значение метрики:



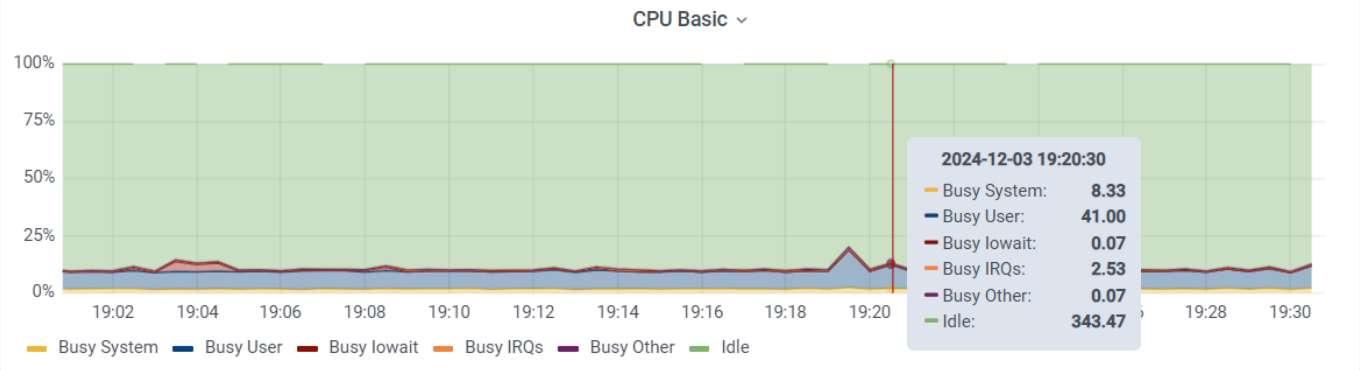
- **Второй тип** – виджет, отображающий тенденцию изменения показателя за период времени в виде графика:



- **Третий тип** – виджет, отображающий тенденцию изменения показателя за период времени в виде графика с таблицей:



При наведении курсора мыши на виджет с графиком будет выведена дополнительная информация:



При клике на наименование виджета, откроется выпадающий список со следующими действиями:

- **View** – открыть виджет на весь экран;
- **Share** – поделиться виджетом. Будет предоставлен механизм по извлечению ссылки на виджет, созданию снимка (snapshot) или копированию виджета в буфер обмена;
- **Inspect** – просмотр подробного журнала виджета, который при необходимости можно скачать в формате .csv;
- **More...** – доступ к дополнительным действиям над виджетом, например скрыть/показать легенду.

По клавише **Esc** открывается панель инструментов сервиса **Grafana**, которая предоставляет следующие дополнительные функции:

- выбрать источник данных для отображения метрик;
- выбрать конкретный хост;
- задать период формирования информации на виджетах;
- задать период автоматического обновления информации на виджетах.

Чтобы скрыть панель инструментов сервиса **Grafana** нажмите кнопку  .

9. Управление доступом к платформе

9.1 Пользователи

Работа с пользователями включает в себя следующие процессы:

1. «Добавление пользователя».
2. «Добавление атрибутов пользователю».
3. «Редактирование информации о пользователе».
4. «Смена пароля пользователя».
5. «Активация и блокировка пользователя».
6. «Назначение роли пользователю».
7. «Удаление роли у пользователя».
8. «Добавление пользователя в группу».
9. «Исключение пользователя из группы».
10. «Удаление пользователя».

Для работы с пользователями перейдите **Администрирование** → **Пользователи и роли** → вкладка **Пользователи** (см. «Рис. 70»).

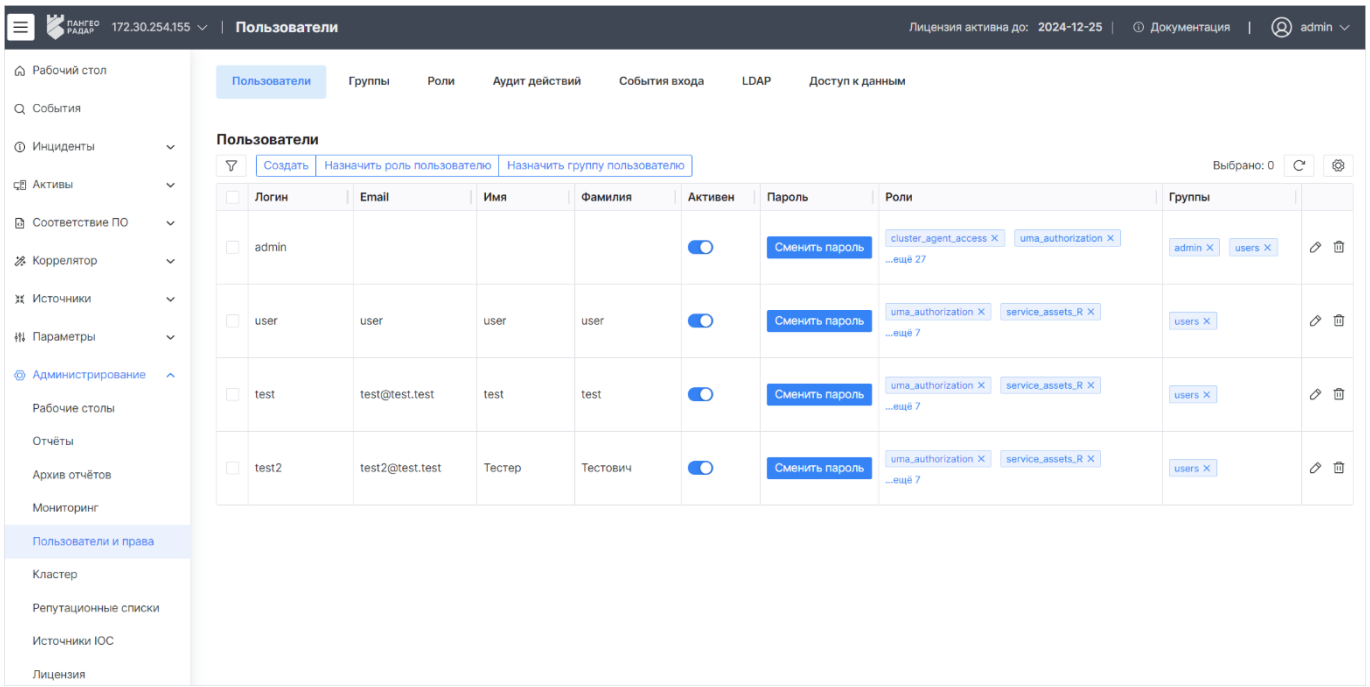


Рис. 70 – Раздел "Пользователи и роли". Вкладка "Пользователи"

На вкладке отображается информация о пользователях:

- **Логин** – уникальное имя пользователя в платформе;
- **Email** – адрес электронный почты;
- **Имя** – имя пользователя платформы;

- **Фамилия** – фамилия пользователя платформы;
- **Активен** – состояние учетной записи пользователя. Пользователь может находиться в следующих состояниях:
  - Активен – пользователь может работать в системе;
  - Не активен – работа пользователя в системе приостановлена.
- **Роли** – список ролей, назначенных пользователю. Список ролей пользователя состоит из двух частей:
  - роли, непосредственно назначенные пользователю;
  - роли, выданные пользователю от групп, в которых он состоит.
- **Группы** – список групп, в которые добавлен пользователь.

9.1.1 Добавление пользователя

1. Нажмите кнопку **Создать**. Откроется окно "Добавить пользователя" (см. «Рис. 71»).

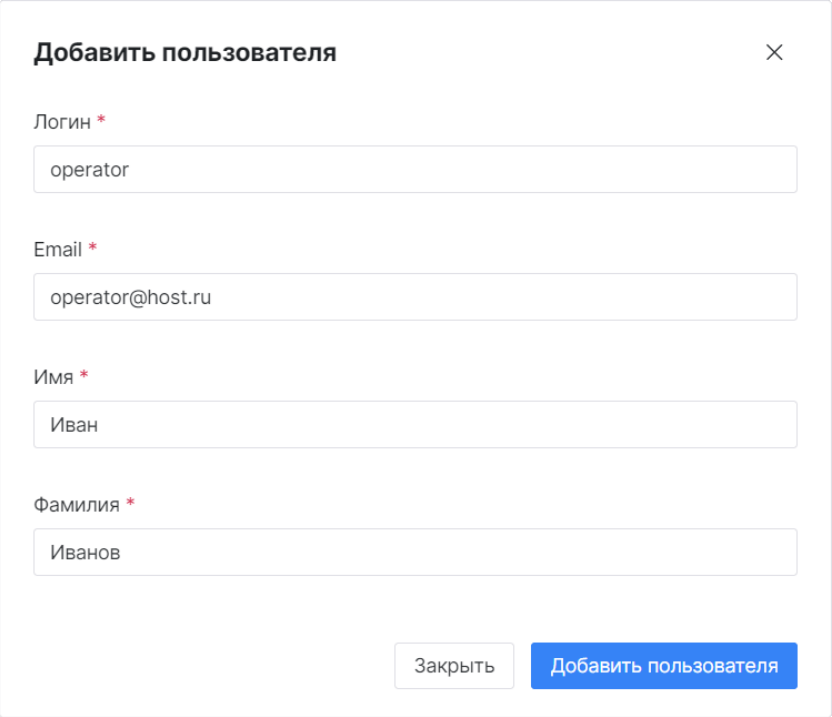


Рис. 71 – Окно "Добавить пользователя"

2. Укажите в окне информацию о пользователе:
   - в поле **Логин** укажите уникальное имя пользователя в платформе;
   - в поле **Email** укажите адрес электронной почты, который будет использоваться для получений уведомлений;
   - в полях **Имя** и **Фамилия** укажите имя и фамилию пользователя.
3. Нажмите кнопку **Добавить пользователя**.

9.1.2 Добавление атрибутов пользователю

Пользователю могут быть назначены атрибуты, влияющие на поведение **Платформы Радар** или содержащие информационный характер. Список системных атрибутов приведен в таблице 1.

Таблица 1 – Список системных атрибутов

Название	Описание
tz	Конвертация временных меток в интерфейсе в нужную для пользователя таймзону. По умолчанию – Europe/Moscow.
is_system_notification	Доставка системных уведомлений от Платформы Радар пользователю на E-mail. Параметр будет включен при указании любого значения.
locale	Регион пользователя. По умолчанию – ru.

Примечание: список атрибутов не ограничивается системными, вы можете добавить произвольное количество собственных атрибутов. Они будут нести исключительно информационный характер.

Для добавления атрибутов пользователю выполните следующие действия:

1. В строке нужного пользователя нажмите кнопку . Откроется окно "Редактировать пользователя" (см. «Рис. 72»).

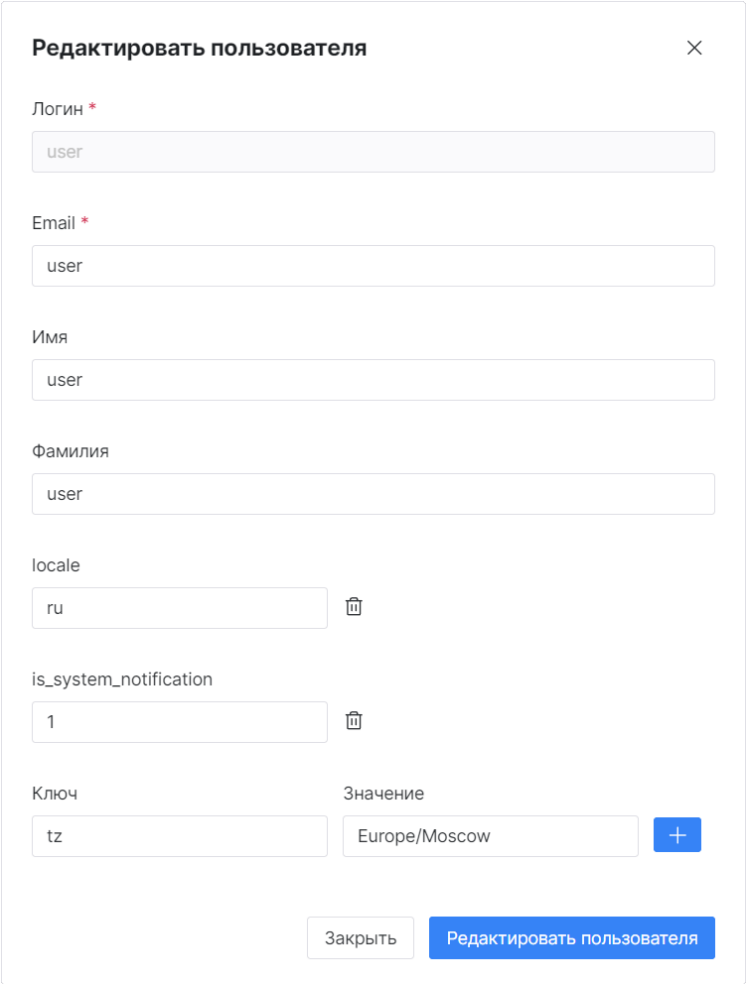


Рис. 72 – Окно "Редактировать пользователя"

2. Укажите информацию об атрибутах:
    - в поле **Ключ** укажите название атрибута;
    - в поле **Значение** укажите значение атрибута;
    - нажмите кнопку  для добавления атрибута;
    - повторите действия для добавления необходимых атрибутов.
3. Нажмите кнопку **Редактировать пользователя** для сохранения изменений.

9.1.3 Редактирование информации о пользователе

1. Выберите нужного пользователя из списка на вкладке "Пользователи" и нажмите кнопку  .
2. Измените основную информацию о пользователе.
3. Измените атрибуты пользователя.
4. Нажмите кнопку **Редактировать пользователя** для сохранения изменений.

9.1.4 Смена пароля пользователя

1. Выберите нужного пользователя из списка на вкладке "Пользователи" и нажмите кнопку **Сменить пароль**. Откроется окно "Сменить пароль" (см. «Рис. 73»)

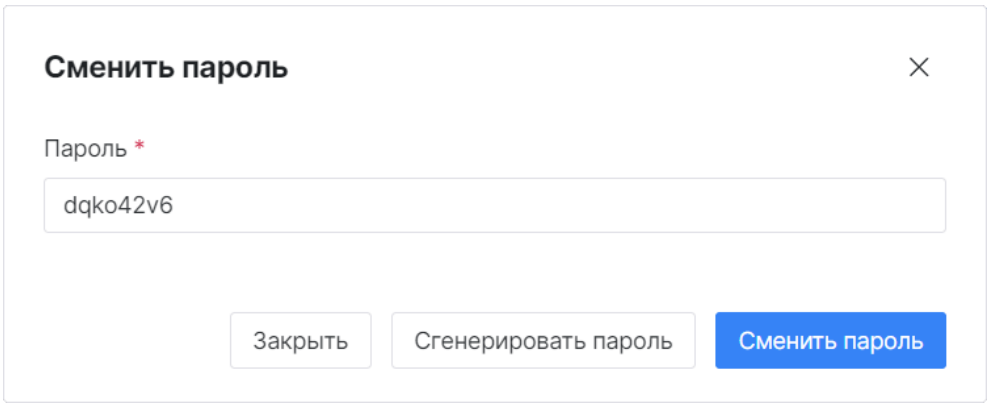


Рис. 73 – Окно "Сменить пароль"

2. В поле **Пароль** укажите новый пароль пользователя.
3. При необходимости вы можете сгенерировать случайный пароль, для этого нажмите кнопку **Сгенерировать пароль**.
4. Нажмите кнопку **Сменить пароль** для сохранения изменений.

9.1.5 Активация и блокировка пользователя

Для изменения состояния учетной записи пользователя используйте переключатель в графе **Активен** (см. «Рис. 70»).

9.1.6 Назначение роли пользователю

1. Нажмите кнопку **Назначить роль пользователю**. Откроется окно "Назначить роль пользователю" (см. «Рис. 74»).

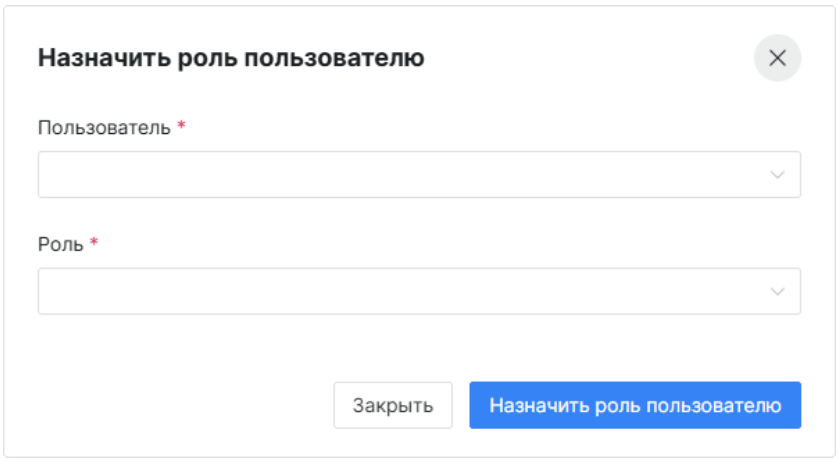


Рис. 74 – Окно "Назначить роль пользователю"

2. Укажите в окне следующую информацию:
   - в поле **Пользователь** из выпадающего списка выберите пользователя, которому будет назначена роль;

- в поле **Роль** из выпадающего списка выберите роль. Список ролей приведен в разделе «Роли».

3. Нажмите кнопку **Назначить роль пользователю**.

9.1.7 Удаление роли у пользователя

Примечание: *нельзя удалить роли, выданные пользователю от групп, в которых он состоит. Чтобы лишить пользователя подобной роли, исключите его из соответствующей группы.*

1. Найдите нужного пользователя из списка на вкладке "Пользователи".
2. В графе **Роли** нажмите на кнопку × рядом с наименованием нужной роли (см. «Рис. 75»).

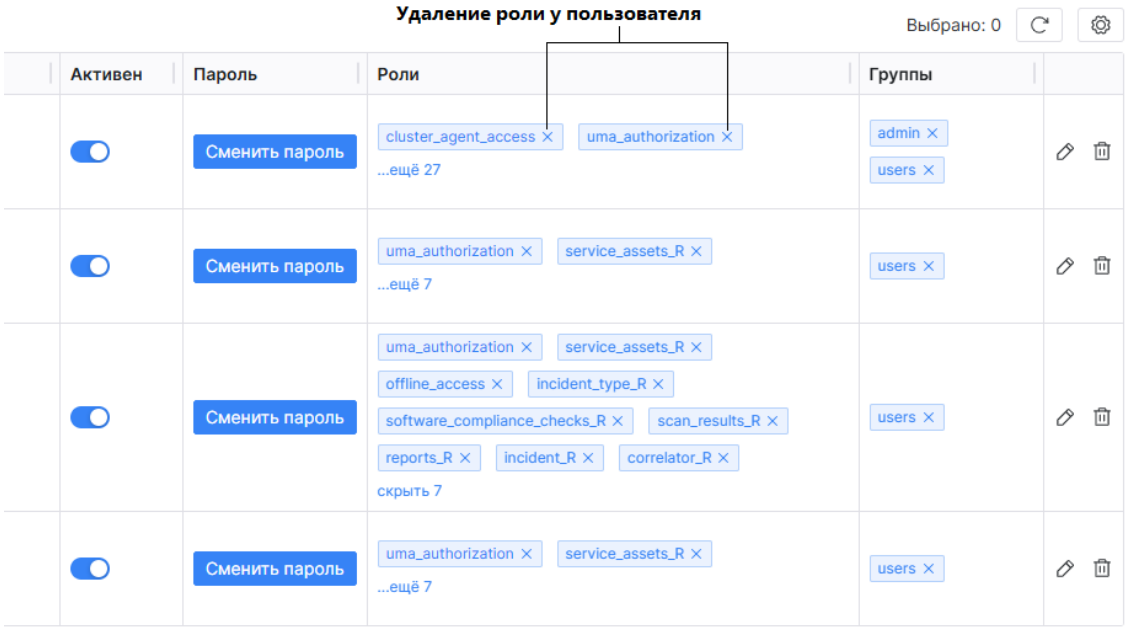


Рис. 75 – *Удаление роли у пользователя"*

3. Подтвердите удаление в открывшемся окне.

9.1.8 Добавление пользователя в группу

1. Нажмите кнопку **Назначить группу пользователю**. Откроется окно "Назначить группу пользователю" (см. «Рис. 76»).

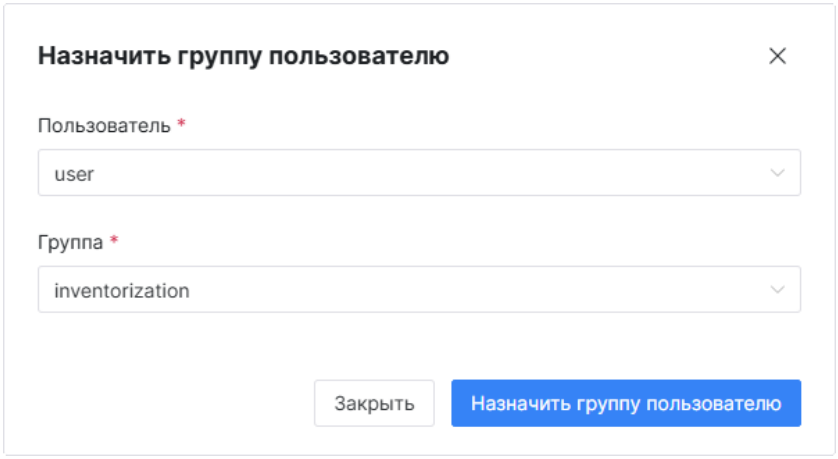


Рис. 76 – Окно "Назначить группу пользователю"

2. Укажите в окне следующую информацию:
   - в поле **Пользователь** из выпадающего списка выберите пользователя, который будет добавлен в группу;
   - в поле **Группа** из выпадающего списка выберите группу (подробнее о группах см. раздел «Группы пользователей»).
3. Нажмите кнопку **Назначить группу пользователю**.

9.1.9 Исключение пользователя из группы

1. Найдите нужного пользователя в списке на вкладке "Пользователи".
2. В графе **Группы** нажмите на кнопку ✕ рядом с наименованием нужной группы (см. «Рис. 77»).

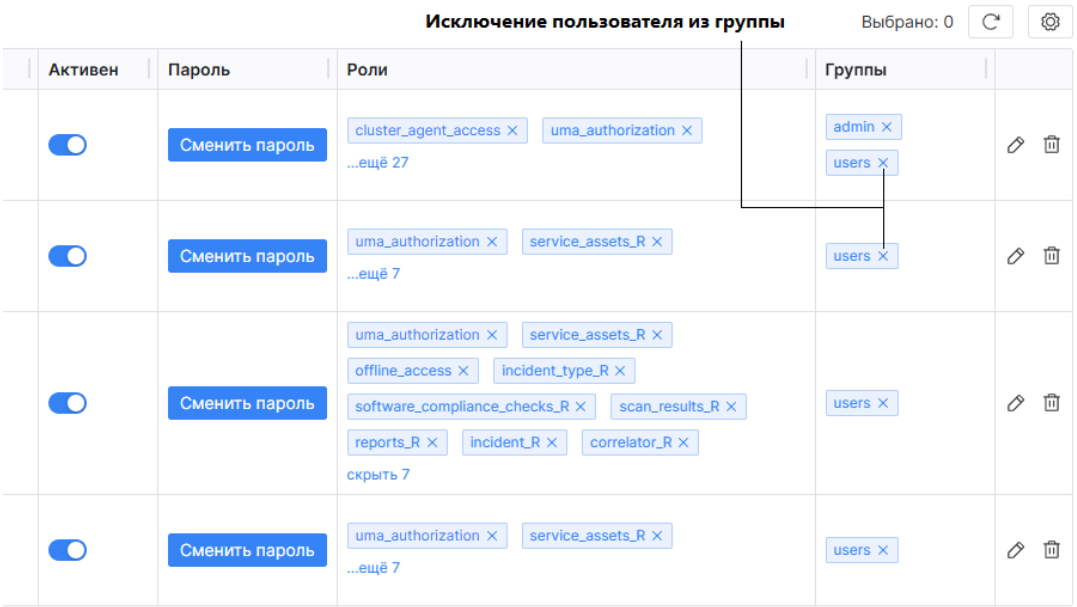


Рис. 77 – Исключение пользователя из группы"

3. Подтвердите удаление в открывшемся окне.

9.1.10 Удаление пользователя

1. В строке нужного пользователя нажмите кнопку .
2. Подтвердите удаление в открывшемся окне.

9.2 Группы пользователей

Группы пользователей предназначены для упрощения администрирования пользователей платформы.

Работа с группами пользователей включает в себя следующие процессы:

1. «Создание группы пользователей».
2. «Редактирование группы пользователей».
3. «Назначение роли группе пользователей».
4. «Удаление роли у группы пользователей».
5. «Удаление группы пользователей».

Для работы с группами пользователей перейдите **Администрирование** → **Пользователи и роли** → вкладка **Группы** (см. «Рис. 78»).

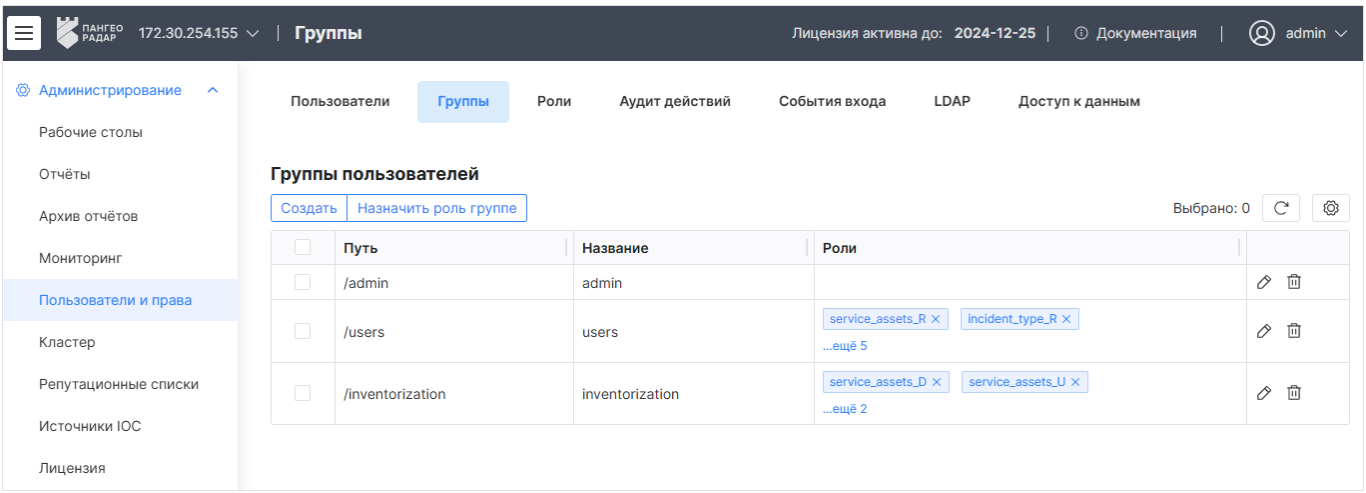


Рис. 78 – Раздел "Пользователи и роли". Вкладка "Группы"

На вкладке отображается следующая информация:

- **Путь**;
- **Название** группы;
- **Роли**, назначенные группе.

9.2.1 Создание группы пользователей

1. Нажмите кнопку **Создать**. Откроется окно "Создать группу" (см. «Рис. 79»).

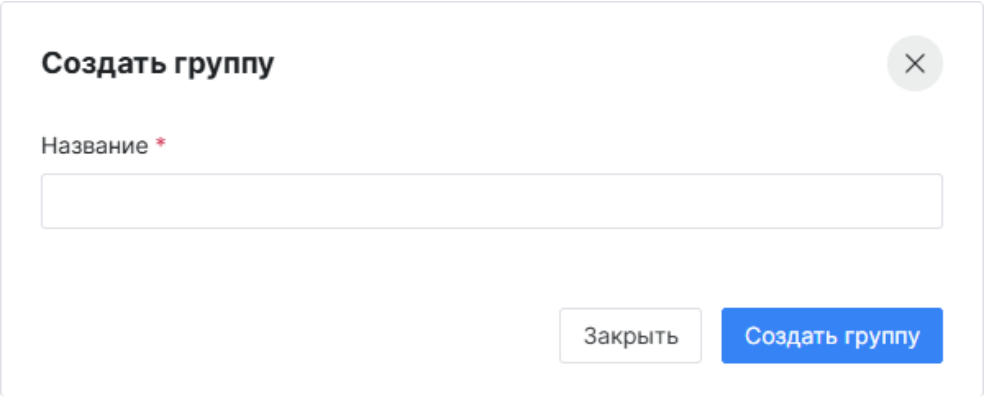


Рис. 79 – Окно "Создать группу"

2. В поле **Название** укажите уникальное наименование группы пользователей.
3. Нажмите кнопку **Создать группу**.

9.2.2 Редактирование группы пользователей

1. В строке нужной группы нажмите кнопку .
2. Измените основную информацию о группе.
3. Нажмите кнопку **Редактировать группу** для сохранения изменений.

9.2.3 Назначение роли группе пользователей

1. Нажмите кнопку **Назначить роль группе**. Откроется окно "Назначить роль группе" (см. «Рис. 80»).

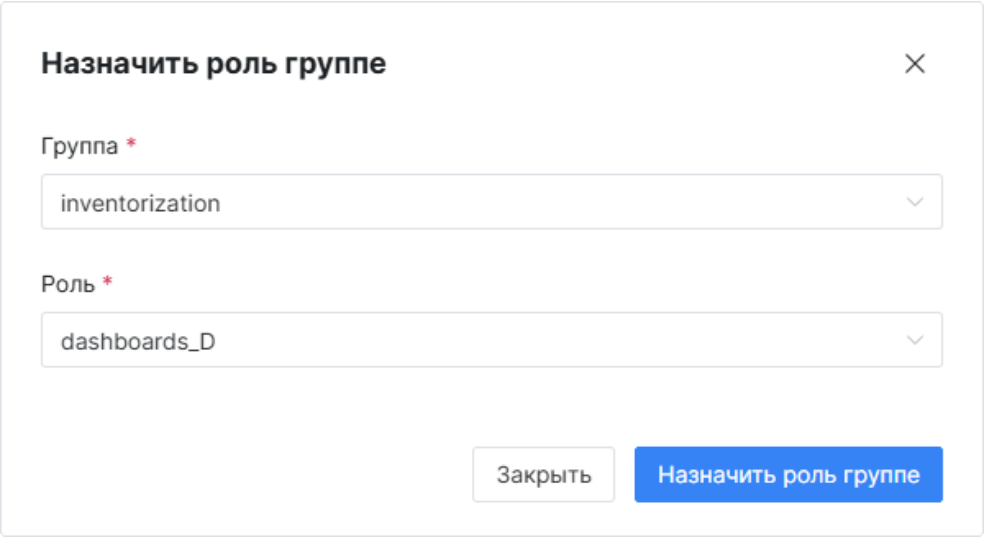


Рис. 80 – Окно "Назначить роль группе"

2. Укажите в окне следующую информацию:
   - в поле **Группа** из выпадающего списка выберите группу, которой будет назначена роль;
   - в поле **Роль** из выпадающего списка выберите роль. Список ролей приведен в разделе «Роли». Выбранная роль будет назначена всем пользователям, состоящим в группе.

3. Нажмите кнопку **Назначить роль группе**.

9.2.4 Удаление роли у группы пользователей

1. Найдите нужную группу в списке на вкладке "Группы".
2. В графе **Роли** нажмите на кнопку ✕ рядом с наименованием нужной роли (см. «Рис. 81»).

Рис. 81 – Удаление роли у группы пользователей"

3. Подтвердите удаление в открывшемся окне.

9.2.5 Удаление группы пользователей

1. В строке нужной группы пользователей нажмите кнопку 🗑.
2. Подтвердите удаление в открывшемся окне.

9.3 Роли

Роль – группа действий, которые пользователь может выполнить в платформе. Действия группируются по функциональной связанности.

Каждому пользователю системы назначается набор ролей. Пользователь получает право на доступ к функциям платформы в соответствии с набором действий, включенных в предоставленные ему роли.

Работа с ролями включает в себя следующие процессы:

1. «Просмотр списка ролей».
2. «Редактирование роли».

9.3.1 Просмотр списка ролей

Для просмотра списка ролей перейдите **Администрирование** → **Пользователи и роли** → вкладка **Роли** (см. «Рис. 82»).

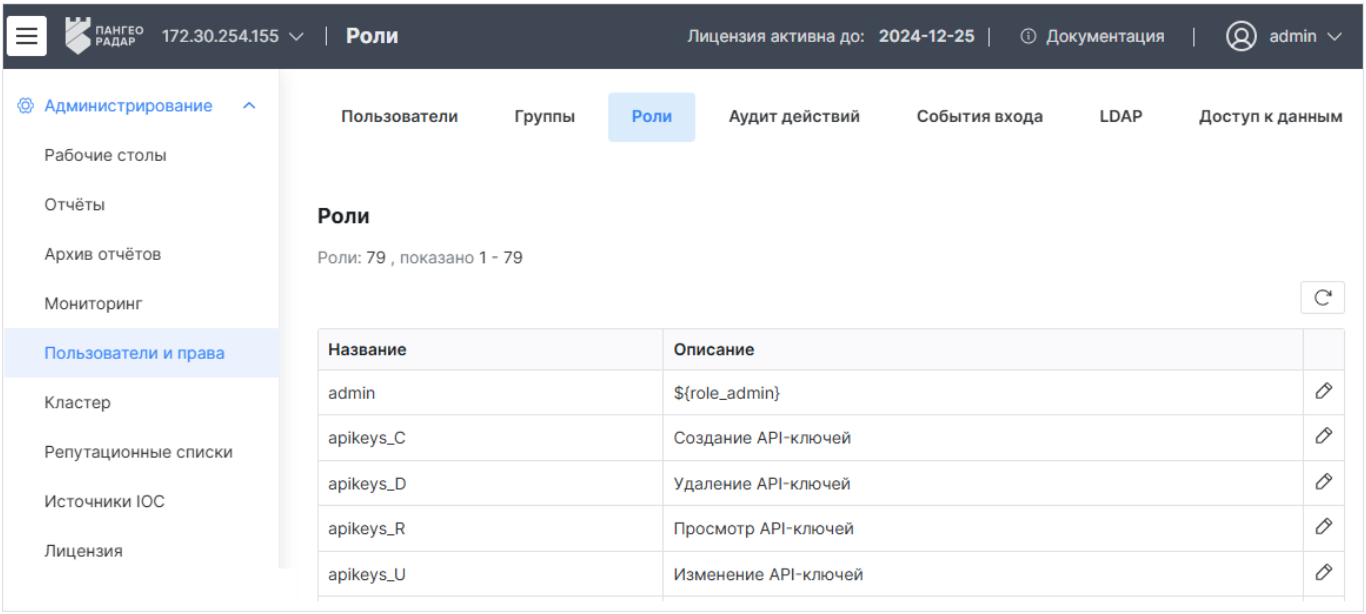


Рис. 82 – Раздел "Пользователи и роли". Вкладка "Роли"

Список предустановленных ролей приведен в «Таблица 2».

Таблица 2 – Предустановленные роли

№ п/п	Название роли	Описание роли
1	admin	Доступ ко всем возможностям платформы
2	apikeys_C	Создание API-ключей
3	apikeys_D	Удаление API-ключей
4	apikeys_R	Просмотр API-ключей
5	apikeys_U	Изменение API-ключей
6	cluster_agent_access	Доступ к API кластер-агента
7	cluster_manager_access	Доступ к API кластер-менеджера
8	config_params_R	Просмотр параметров конфигов
9	config_params_U	Изменение параметров конфигов
10	configs_C	Создание конфигов
11	configs_D	Удаление конфигов
12	configs_R	Просмотр конфигов
13	configs_U	Изменение конфигов

№ п/п	Название роли	Описание роли
14	content_E	Экспорт контента
15	content_I	Импорт контента
16	correlator_A	Управление корреляторами
17	correlator_C	Создание правил корреляции
18	correlator_D	Удаление правил корреляции
19	correlator_R	Просмотр правил корреляции
20	correlator_result_D	Удаление результатов корреляции
21	correlator_U	Изменение правил корреляции
22	create-realm	Возможность создания сущностей
23	dashboards_C	Создание рабочего стола
24	dashboards_D	Удаление рабочего стола
25	dashboards_R	Просмотр рабочего стола
26	dashboards_U	Редактирование рабочего стола
27	events_C	Создание события
28	events_D	Удаление события
29	events_R	Просмотр событий
30	events_U	Редактирование события
31	incident_C	Создание инцидентов
32	incident_D	Удаление инцидентов
33	incident_mass_U	Массовые действия с инцидентами
34	incident_R	Просмотр инцидентов
35	incident_status_U	Изменять статус инцидента
36	incident_type_C	Создание типов инцидентов
37	incident_type_D	Удаление типов инцидента

№ п/п	Название роли	Описание роли
38	incident_type_R	Просмотр типов инцидентов
39	incident_type_U	Изменение типов инциндентов
40	incident_U	Измнение инцидентов
41	incident_users_U	Назначения пользователей для инцидента
42	monitoring	Доступ к мониторингу
43	nodes_C	Добавление узлов
44	nodes_D	Удаление узлов
45	nodes_R	Просмотр узлов
46	nodes_U	Изменение узлов
47	normalizers	Доступ к правилам нормализации
48	offline_access	Доступ без сети интернет
49	parsers	Доступ к правилам разбора
50	report_C	Создание отчета
51	report_D	Удаление отчета
52	report_R	Просмотр отчета
53	reports_C	Создание отчетов
54	reports_D	Удаление отчетов
55	reports_R	Просмотр отчетов
56	reports_U	Изменение отчетов
57	report_U	Редактирование отчета
58	scan_results_C	Загрузка результатов сканирования
59	scan_results_D	Удаление результатов сканирования
60	scan_results_R	Просмотр результатов сканирования
61	scan_results_U	Изменение результатов сканирования

№ п/п	Название роли	Описание роли
62	service_assets_C	Создание активов, групп, интерфейсов, настройка идентификации
63	service_assets_D	Удаление активов, групп, интерфейсов, настройка идентификации
64	service_assets_R	Просмотр активов, групп, интерфейсов, настройка идентификации
65	service_assets_U	Изменение активов, групп, интерфейсов, настройка идентификации
66	software_compliance_checks_C	Создание правил и наборов правил оценки соответствия ПО
67	software_compliance_checks_D	Удаление правил и наборов правил оценки соответствия ПО
68	software_compliance_checks_R	Просмотр всех сущностей оценки соответствия ПО
69	software_compliance_checks_U	Изменение правил и наборов правил оценки соответствия ПО
70	sources_C	Создание источников
71	sources_D	Удаление источников
72	sources_R	Просмотр источников
73	sources_U	Изменение источников
74	system_admin	Администратор системы без доступа к данным
75	table_C	Создание хранилища
76	table_D	Удаление хранилища
77	table_R	Просмотр хранилища
78	table_U	Редактирование хранилища
79	uma_authorization	${role_uma_authorization}

Внимание! *Пользователи с назначенной ролью "admin" будут иметь доступ ко всем разделам и настройкам* ***Платформы Радар***.

9.3.2 Редактирование роли

1. В строке нужной роли нажмите кнопку .
2. Нажмите кнопку **Редактировать роль** для сохранения изменений.

9.4 Аудит действий пользователей

Для обеспечения функций безопасности **Платформа Радар** регистрирует все действия, совершаемые в платформе. Действия делятся на системные и пользовательские. По каждому действию можно посмотреть запрос, который был исполнен во время выполнения действия.

Для просмотра совершенных в платформе действий перейдите **Администрирование** → **Пользователи и роли** → вкладка **Аудит действий** (см. «Рис. 83»).

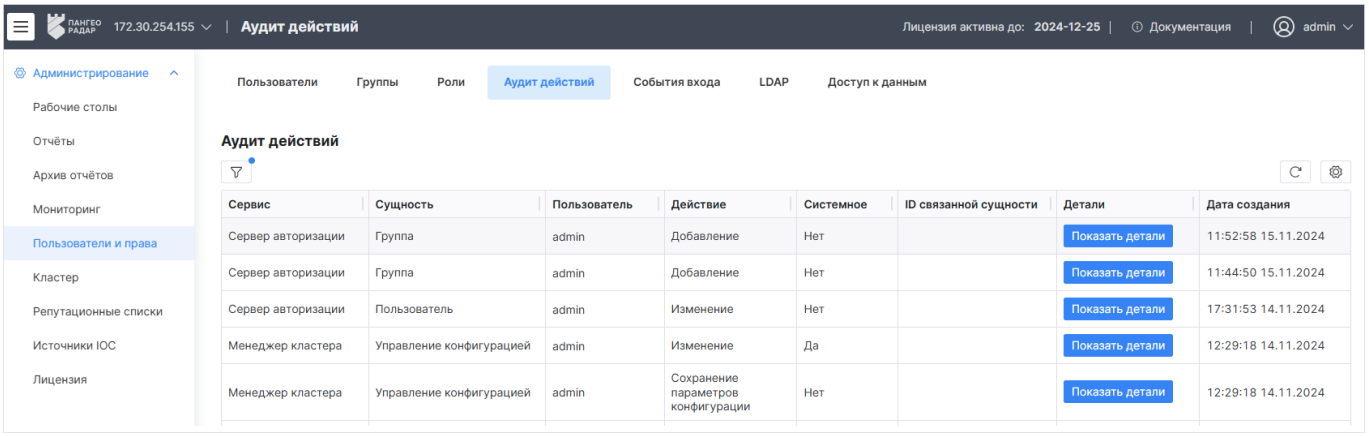


Рис. 83 – Раздел "Пользователи и роли". Вкладка "Аудит действий"

На вкладке отображается следующая информация:

- **Сервис** – наименование сервиса, в котором выполнялось действие;
- **Сущность** – наименование сущности, над которой было выполнено действие;
- **Пользователь** – наименование пользователя, выполнившего действие;
- **Действие** – описание действия;
- **Системное** – признак, выполнялось ли действие платформой: да, нет;
- **ID связанной сущности** – идентификатор сущности, которая также была изменена при выполнении действия над родительской сущностью;
- **Детали** – просмотр тела запроса, который был выполнен;
- **Дата создания** – дата и время создания записи о совершенном действии.

Для просмотра тела запроса, который был выполнен для исполнения действия, в строке нужного действия нажмите кнопку **Показать детали**. Откроется окно "Показать детали" (см. «Рис. 84»).

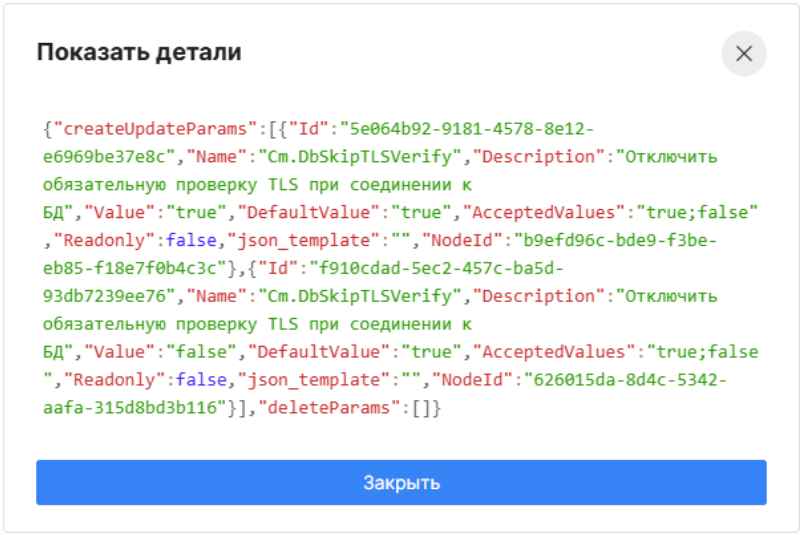


Рис. 84 – Окно "Показать детали"

9.5 Журнал входа пользователей

Для обеспечения функций безопасности **Платформа Радар** регистрирует следующие типы событий входа:

- вход в платформу – был зарегистрирован успешный вход пользователя;
- обмен токена на ключ – особенность реализации сессии пользователя, требующая повторную аутентификацию после определенного периода времени. Данное действие выполняется автоматически, если пользователь выполняет работу в платформе. В случае, если пользователь бездействовал, его сессия будет прервана.

По каждому действию можно посмотреть детальную информацию.

Для просмотра журнала входа пользователей в платформу перейдите **Администрирование** → **Пользователи и роли** → вкладка **События входа** и выберите период, за который нужно сформировать журнал (см. «Рис. 85»).

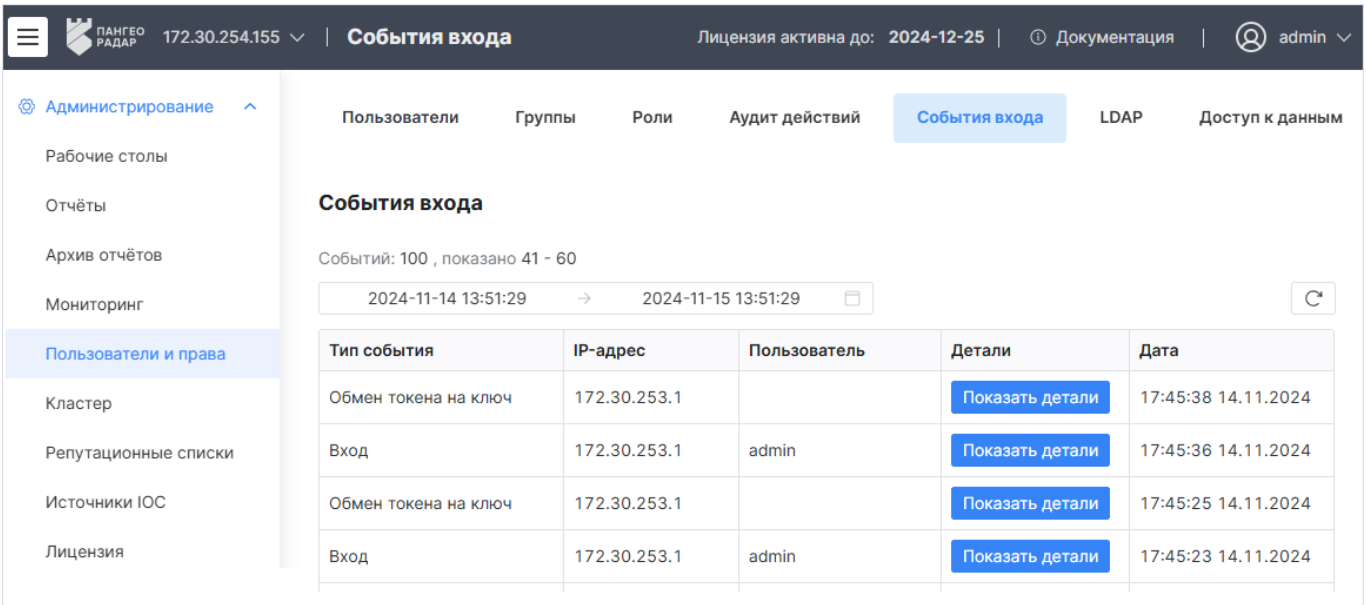


Рис. 85 – Раздел "Пользователи и роли". Вкладка "События входа"

На вкладке отображается следующая информация:

- **Тип события** – событие входа: вход пользователя, обмен токена на ключ;
- **IP-адрес** – IP-адрес, с которого выполнялся вход в платформу;
- **Пользователь** – логин пользователя, выполнившего вход в платформу;
- **Детали** – просмотр детальной информации о событии входа;
- **Дата** – дата и время создания записи о событии входа.

Для просмотра детальной информации о событии входа, в строке нужного действия нажмите кнопку **Показать детали**. Откроется окно "Показать детали" (см. «Рис. 86»).

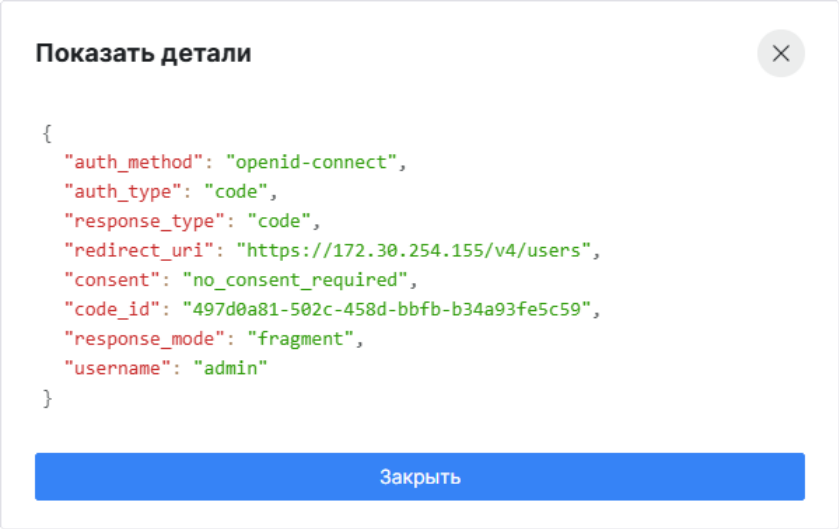


Рис. 86 – Окно "Показать детали"

9.6 Интеграции LDAP

Платформа Радар использует сервис **Keycloak** в качестве системы идентификации и управления доступом.

Платформа позволяет создать интеграцию **Keycloak** с сервером **LDAP**, а затем использовать LDAP в качестве источника пользовательских данных.

Данная интеграция позволяет подключиться к службе каталогов, в которой хранятся данные аутентификации, такие как имена пользователей, пароли, домашние каталоги пользователей, используемые для хранения деловых и других данных, что позволит импортировать пользователей в платформу. Можно синхронизировать учетные записи сотрудников компании между **Платформой Радар** и различными корпоративными сервисами (таких как электронная почта, сайт, VoIP и другое). Благодаря этому одна учётная запись может быть использована для авторизации во всех корпоративных сервисах.

Платформа Радар поддерживает интеграцию со следующими поставщиками услуг:

- Active Directory;
- Red Hat Directory Server;
- Tivoli;
- Novel eDirectory.

Также поддерживается интеграция и с другими поставщиками услуг, но потребуется дополнительная настройка.

Работа с интеграциями включает в себя следующие процессы:

1. «Добавление интеграции LDAP».
2. «Редактирование интеграции LDAP».
3. «Удаление интеграции LDAP».

Для работы с интеграциями LDAP перейдите **Администрирование → Пользователи и роли →** вкладка **LDAP** (см. «Рис. 87»).

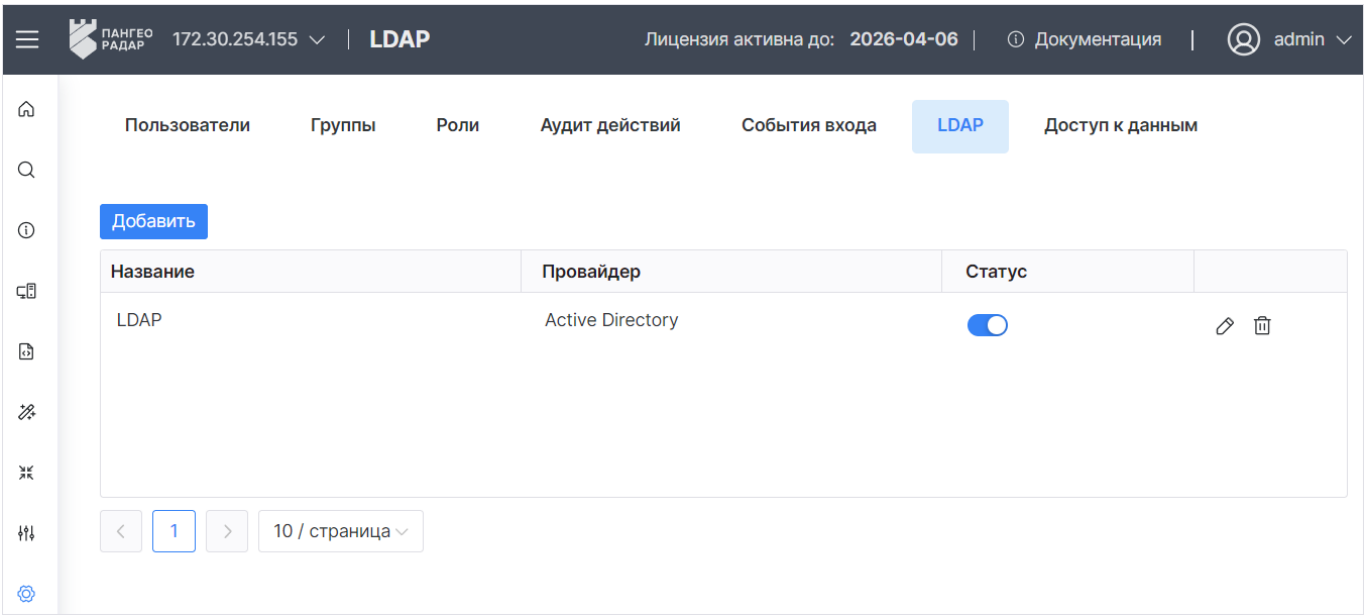


Рис. 87 – Раздел "Пользователи и роли". Вкладка "LDAP"

На вкладке отображается следующая информация:

- **Название** – название интеграции;
- **Провайдер** – поставщик услуг;
- **Статус** – состояние интеграции: активна, не активна.

9.6.1 Добавление интеграции LDAP

Для добавления интеграции LDAP нажмите кнопку **Добавить**. Начнется процесс добавления интеграции, который состоит из следующих шагов:

- «Шаг 1. Основные настройки».
- «Шаг 2. Расширенные настройки».
- «Шаг 3. Пул соединений».
- «Шаг 4. Интеграция с Kerberos».
- «Шаг 5. Синхронизация настроек».
- «Шаг 6. Настройки кэширования».
- «Шаг 7. Завершение добавления интеграции».

9.6.1.1 Шаг 1. Основные настройки

Пример основных настроек приведен на «Рис. 88».

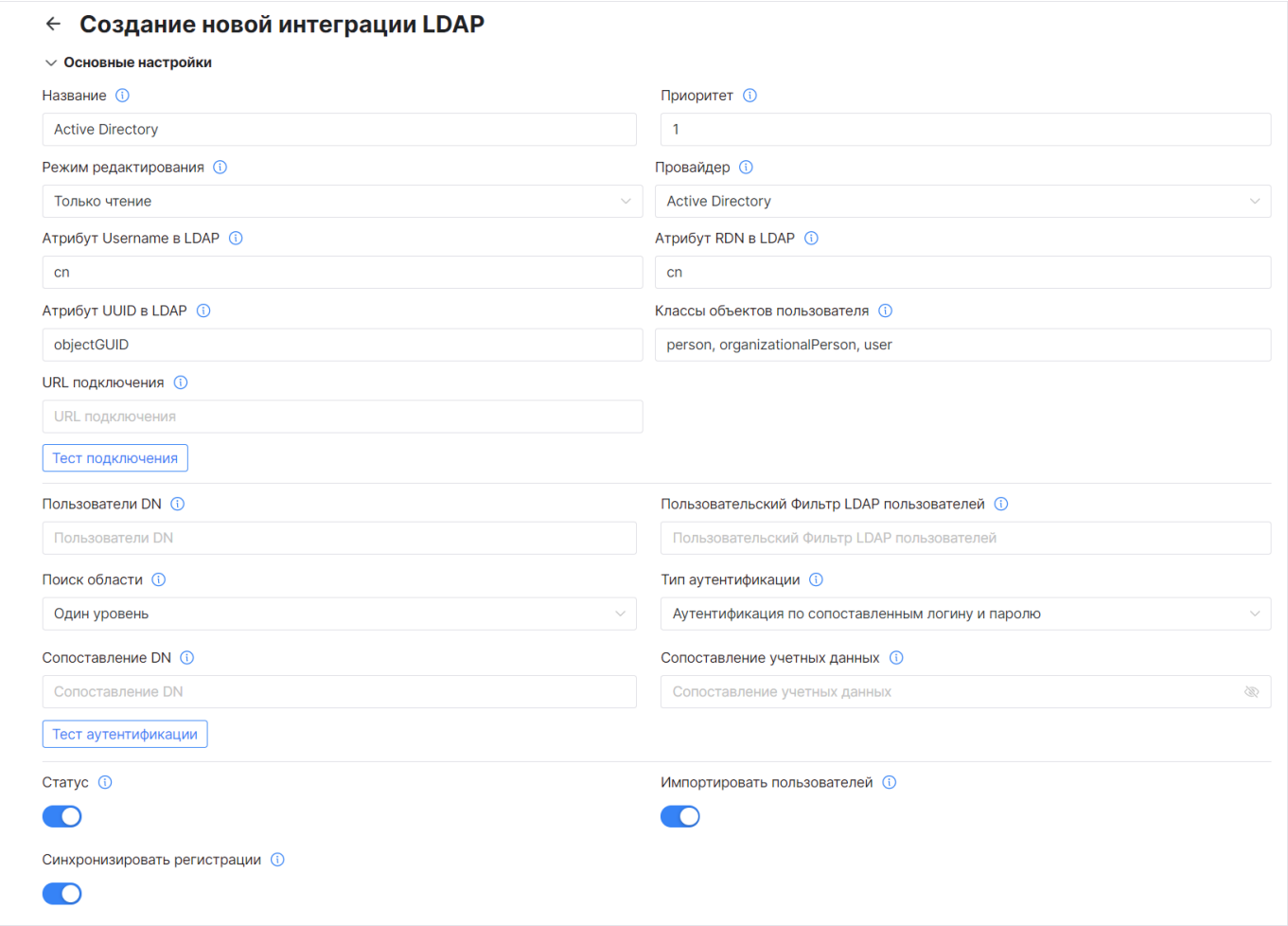


Рис. 88 – Создание интеграции LDAP. Основные настройки

В блоке **Основные настройки** заполните следующие поля:

- **Название** – укажите наименование интеграции;
- **Приоритет** – укажите приоритет службы при поиске пользователя. Вперед идут более низкие значения;
- **Режим редактирования** – выберите режим редактирования из LDAP. Доступны следующие значения:
  - "Только чтение" – доступ только на чтение из LDAP;
  - "Записываемый" – данные будут обратно синхронизированы в LDAP по заявке;
  - "Несинхронизированный" – данные пользователя будут импортированы, но не синхронизированы обратно в LDAP.
- **Провайдер** – выберите поставщика услуг LDAP;
- **Атрибут Username в LDAP** – укажите наименование LDAP атрибута, которое отображается как имя пользователя в "Keycloak":

- для провайдеров Red Hat Directory Server, Tivoli, Novel eDirectory и множества других серверов LDAP это может быть uid.
- для Active Directory это может быть sAMAccountName или cn.

Атрибут должен быть заполнен для всех LDAP записей пользователей, которые вы хотите импортировать из LDAP в Keycloak.

- **Атрибут RDN в LDAP** – укажите наименование атрибутов LDAP, которое используется как RDN (верхний атрибут) обычного пользователя DN. Обычно оно такое же, как атрибут имени пользователя LDAP, однако он не обязателен. Для примера, для Active directory обычно используется cn как атрибут RDN, в то время как атрибут имени пользователя может быть sAMAccountName;
- **Атрибут UUID в LDAP** – укажите наименование LDAP атрибута, которое используется как уникальный идентификатор объектов (UUID) в LDAP:
  - для провайдеров "Red Hat Directory Server", Tivoli, Novel eDirectory и множества других серверов LDAP это может быть entryUUID;
  - для Active directory он должен быть objectGUID.

  Если ваш LDAP сервер не поддерживает понятие UUID, вы можете использовать любой другой атрибут, который должен быть уникальным среди пользователей в дереве LDAP. Например, uid или entryDN;
- **Классы объектов пользователя** – укажите все значения из LDAP objectClass атрибутов для пользователей в LDAP, разделенные запятой. Например: inetOrgPerson, organizationalPerson. Вновь созданные пользователи Keycloak будут записаны в LDAP вместе с этими классами объектов, а существующие записи пользователей LDAP будут найдены только если они содержат все эти классы объектов;
- **URL подключения** – укажите URL соединения с вашим сервером LDAP. Для проверки доступа сервера LDAP нажмите кнопку **Тест подключения**;
- **Пользователи DN** – укажите полный DN из дерева LDAP, где присутствуют ваши пользователи. Этот DN является родителем пользователей LDAP. Например, он может быть ou=users, dc=example, dc=com при условии, что ваш обычный пользователь будет иметь DN похожий на uid=john,ou=users,dc=example,dc=com;
- **Пользовательский Фильтр LDAP пользователей** – укажите дополнительный фильтр LDAP для фильтрации искомых пользователей. Оставьте поле пустым, если не нуждаетесь в дополнительном фильтре.
- **Поиск области** – выберите поиск области. Доступные варианты:
  - "Один уровень" – выполняется поиск пользователей только в DN, определенных как пользовательские DN;
  - "Поддерево" – выполняется поиск полностью в их поддеревьях. Смотрите документацию LDAP для подробных деталей.

- **Тип аутентификации** – выберите способ аутентификации. Доступны следующие варианты:
    - "Анонимная аутентификация";
    - "Аутентификация по сопоставленным логину и паролю". Если выбран данный способ, то укажите дополнительную информацию в следующих полях:
        - **Сопоставление DN** – укажите DN администратора LDAP, которые будут использованы Keycloak для доступа на сервер LDAP;
        - **Сопоставление учетных данных** – укажите пароль администратора LDAP;
        - Для проверки указанных данных нажмите кнопку **Тест аутентификации**.
- **Статус** – выберите состояние интеграции установив переключатель в соответствующее положение:
    - "Включена";
    - "Выключена". Если интеграция выключена, она не будет использована при запросах, а импортированные пользователи будут деактивированы и переведены в состояние "только чтение", пока интеграция не будет включена снова.
- **Импортировать пользователей** – при необходимости включите импортирование пользователей. Если включено, пользователи LDAP будут импортированы в базу данных Keycloak и синхронизированы через сконфигурированные политики синхронизации;
- **Синхронизировать регистрации** – при необходимости включите создание пользователей в хранилище LDAP после процедуры регистрации. Поле **Приоритет** определяет какой из поставщиков будет выбран для синхронизации нового пользователя.

9.6.1.2 Шаг 2. Расширенные настройки

Пример расширенных настроек приведен на «Рис. 89».

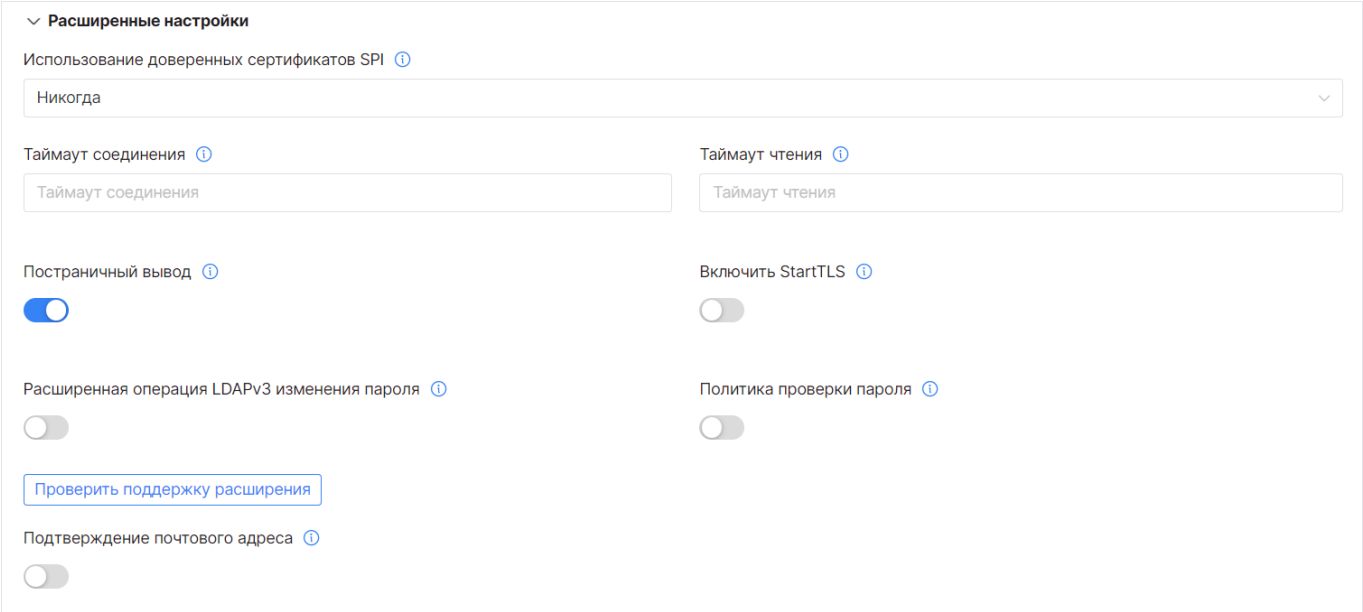


Рис. 89 – Создание интеграции LDAP. Расширенные настройки

В блоке **Расширенные настройки** заполните следующие поля:

- **Использование доверенных сертификатов SPI** – настройка определяет, будет ли соединение с LDAP использовать хранилище доверенных сертификатов SPI вместе с сертификатами, сконфигурированными в keycloak-server.json. Выберите способ использования доверенных сертификатов SPI:
  - "Всегда" – использовать всегда;
  - "Никогда"– не использовать.
  - "Только для LDAP" – использовать вместе с вашими соединениями к LDAP серверам. Если keycloak-server.json не сконфигурирован, то по умолчанию Java будет использовать cacerts или сертификат, определенный в javax.net.ssl.trustStore.
- **Таймаут соединения** – укажите таймаут соединения с LDAP в миллисекундах;
- **Таймаут чтения** – укажите таймаут чтения из LDAP в миллисекундах. Этот таймаут применяется к операциям чтения из LDAP;
- **Постраничный вывод** – при необходимости включите постраничный вывод;
- **Расширенная операция LDAPv3 изменения пароля** – при необходимости включите использование расширенной операции LDAPv3 изменения пароля (RFC-3062). Для расширенной операции изменения пароля обычно требуется, чтобы у LDAP пользователя уже был выставлен пароль на сервере. Когда эта опция используется вместе с "Синхронизацией зарегистрированных пользователей" желательно также добавить "Фиксированный LDAP маппер атрибутов", содержащий случайно сгенерированное начальное значение для пароля.

  Для проверки поддержки настройки нажмите кнопку **Проверить поддержку расширения**;

- **Подтверждение почтового адреса** – при необходимости включите подтверждение почтового адреса. Если включено, то E-mail, предоставленный этим поставщиком, будет требовать подтверждение, даже если оно не включено для области;
- **Включить StartTLS** – при необходимости включите шифрование соединения к LDAP с помощью STARTTLS, которое позволяет создать зашифрованное соединение (TLS или SSL) прямо поверх обычного TCP-соединения. Шифрование отключит пул соединений (подробнее о настройке пула соединений см. «Шаг 3. Пул соединений»).
- **Политика проверки пароля** – определяет должен ли Keycloak, перед тем как обновлять пароль, валидировать его согласно политике паролей области.

9.6.1.3 Шаг 3. Пул соединений

Пример настроек пула соединений приведен на «Рис. 90».

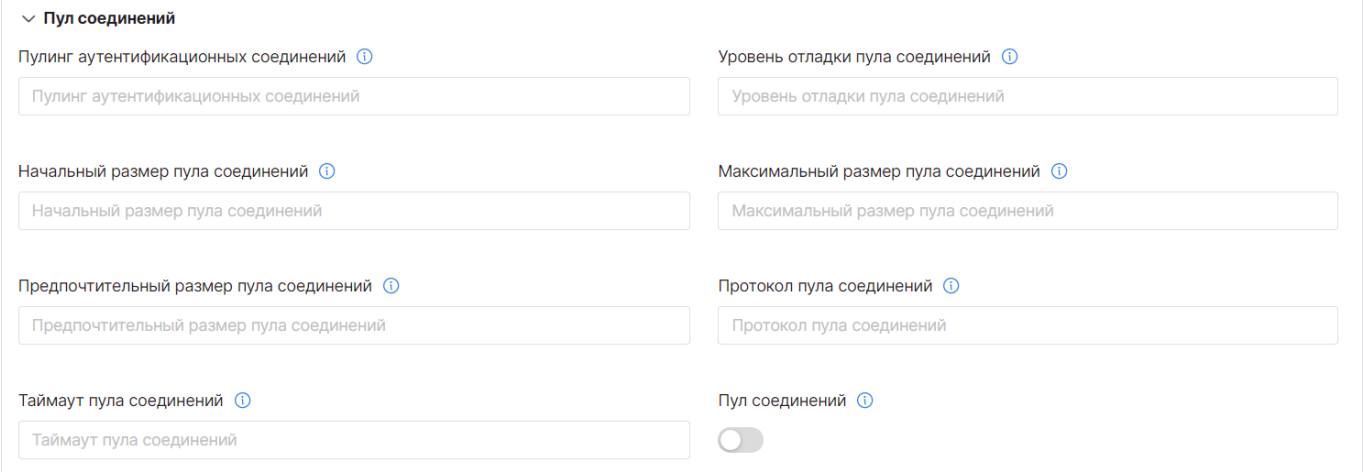


Рис. 90 – Создание интеграции LDAP. Пул соединений

В блоке **Пул соединений** заполните следующие поля:

- **Пулинг аутентификационных соединений** – укажите через пробел список аутентификационных типов соединений, которые могут быть помещены в пул. Валидные значения: "none", "simple" и "DIGEST-MD5";
- **Начальный размер пула соединений** – укажите число начально создаваемых соединений к каждому из узлов;
- **Предпочтительный размер пула соединений** – укажите предпочтительное число одновременных соединений к узлу;
- **Таймаут пула соединений** – укажите количество миллисекунд, в течение которых неактивное соединение может пребывать в пуле перед тем, как оно будет закрыто и удалено из него;
- **Уровень отладки пула соединений** – укажите уровень отладки. Доступные значения:
  - "fine" – журналирует создание и удаление соединений;
  - "all" – полный вывод всей отладочной информации.

- **Максимальный размер пула соединений** – укажите максимальное число одновременных соединений к узлу;
- **Протокол пула соединений** – укажите через пробел список протоколов соединений, которые можно поместить в пул. Допустимые значения: "plain" и "ssl";
- **Пул соединений** – при необходимости включите использование службой Keycloak пула соединений для доступа к LDAP серверу.

9.6.1.4 Шаг 4. Интеграция с Kerberos

Пример настроек интеграции с Kerberos приведен на «Рис. 91».

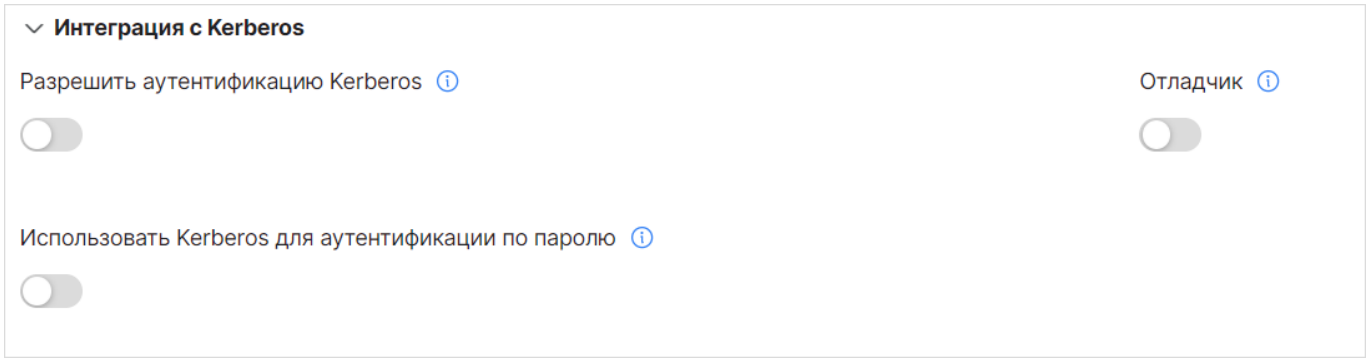


Рис. 91 – Создание интеграции LDAP. Интеграция с Kerberos

В блоке **Интеграция с Kerberos** заполните следующие поля:

- **Разрешить аутентификацию Kerberos** – при необходимости включите аутентификацию HTTP пользователей с токенами SPNEGO/Kerberos. Данные об аутентифицированных пользователях будут предусмотрены из этого LDAP сервера;
- **Использовать Kerberos для аутентификации по паролю** – при необходимости включите использование модуля входа Kerberos, для аутентификации по логину/паролю с сервера Kerberos, вместо аутентификации на сервере LDAP с Directory Service API;
- **Отладчик** – при необходимости включите отладочные журналы в стандартный вывод для Krb5LoginModule.

9.6.1.5 Шаг 5. Синхронизация настроек

Пример настроек синхронизации приведен на «Рис. 92».

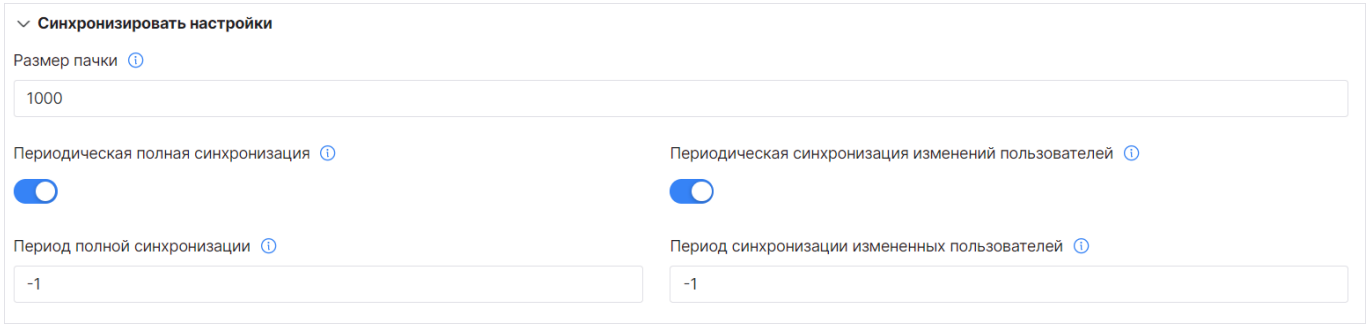


Рис. 92 – Создание интеграции LDAP. Синхронизировать настройки

В блоке **Синхронизация настроек** заполните следующие поля:

- **Размер пачки** – укажите количество пользователей LDAP, которые будут импортированы в Keycloak за одну транзакцию;
- **Периодическая полная синхронизация** – при необходимости включите полную периодическую синхронизацию пользователей LDAP в Keycloak. Если функция включена, то в поле **Период полной синхронизации** укажите период для полной синхронизации в секундах;
- **Периодическая синхронизация изменений пользователей** – при необходимости включите периодическую синхронизацию новых и измененных пользователей LDAP в Keycloak. Если функция включена, то в поле **Период синхронизации измененных пользователей** укажите период для синхронизации измененных или вновь созданных пользователей LDAP в секундах.

9.6.1.6 Шаг 6. Настройки кэширования

Пример настроек кэширования приведен на «Рис. 93».

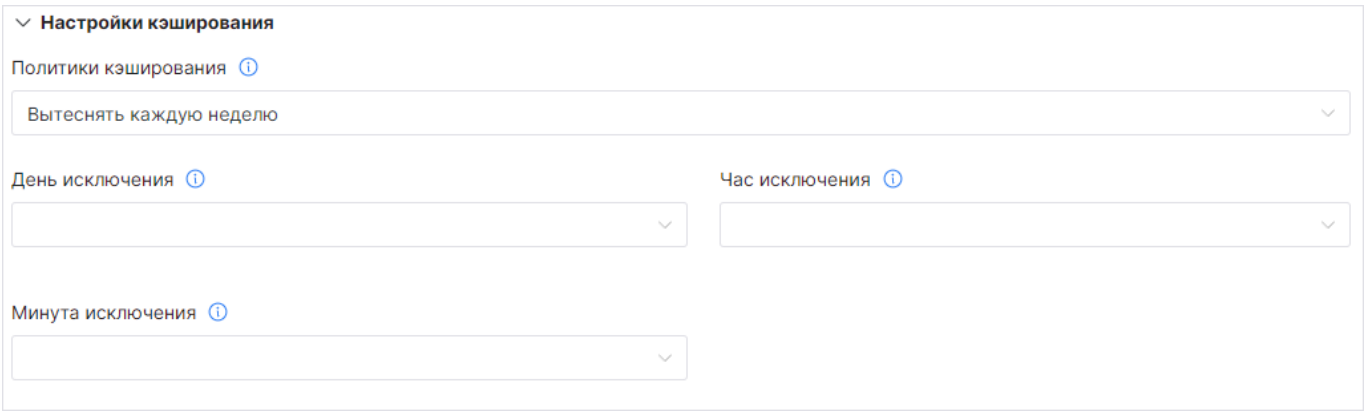


Рис. 93 – Создание интеграции LDAP. Настройки кэширования

В блоке **Синхронизация настроек** выберите политику кэширования и заполните соответствующие поля. Доступны следующие политики кэширования:

- **По умолчанию**. Выставить настройки по умолчанию для глобального пользовательского кэша;
- **Вытеснять каждый день**. Время каждого дня, после которого пользовательский кэш инвалидируется. При выборе данной политики в полях **Час исключения** и **Минута исключения** укажите час и минуту по истечению которых запись станет недействительна;
- **Вытеснять каждую неделю**. Время и день недели после которого пользовательский кэш инвалидируется. При выборе данной политики в полях **День исключения**, **Час исключения** и **Минута исключения** укажите соответствующее время;
- **По максимальному времени жизни**. При выборе данной политики в соответствующем поле укажите время в миллисекундах, в течение которого будет существовать жизненный цикл записи в кэше;
- **Без кэширования**.

9.6.1.7 Шаг 7. Завершение добавления интеграции

После выполнения всех шагов нажмите кнопку **Сохранить**.

9.6.2 Редактирование интеграции LDAP

1. В строке нужной интеграции нажмите кнопку .
2. Измените основную информацию об интеграции.
3. Нажмите кнопку **Редактировать интеграцию LDAP** для сохранения изменений.

9.6.3 Удаление интеграции LDAP

1. В строке нужной интеграции нажмите кнопку .
2. Подтвердите удаление в открывшемся окне.

9.7 Доступ к данным

Управление доступом пользователей к данным включает в себя следующие процессы:

1. «Просмотр сводной информации о пользователе».
2. «Настройка доступа к данным».
3. «Настройка доступа для группы пользователей».

Для просмотра информации о доступе пользователей или групп пользователей к данным перейдите **Администрирование** → **Пользователи и роли** → вкладка **Доступ к данным** и в поле **Инстанс** выберите интересующий инстанс (см. «Рис. 94»).

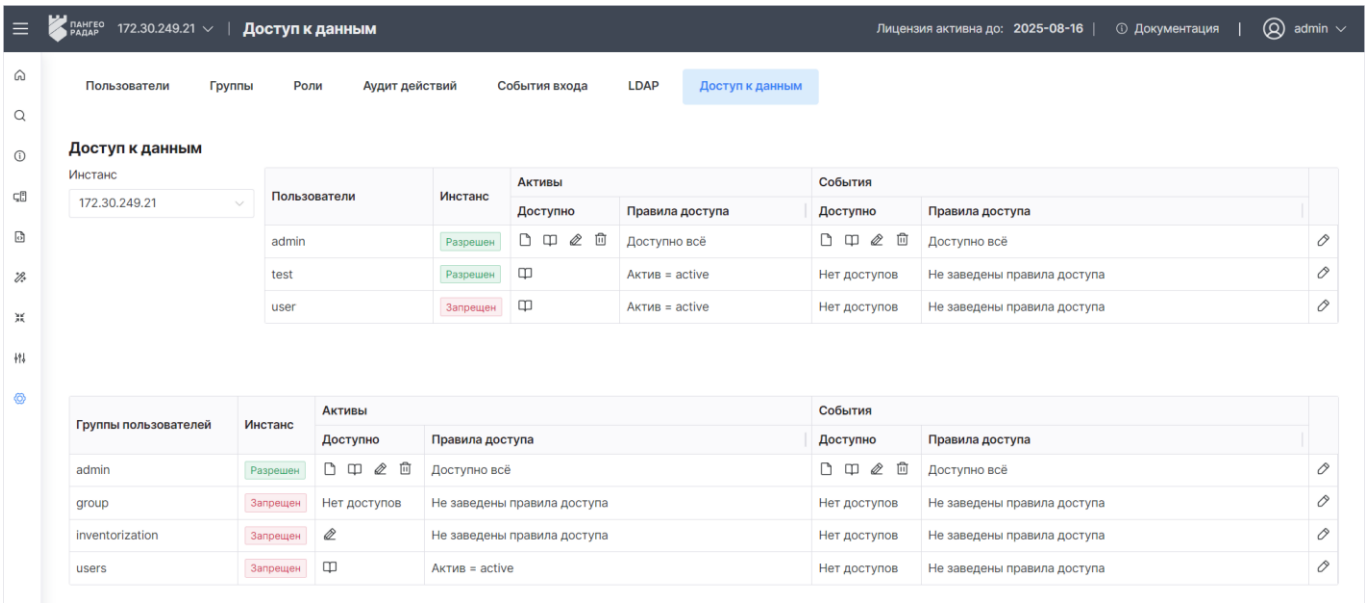


Рис. 94 – Раздел "Пользователи и роли". Вкладка "Доступ к данным"

На вкладке отображаются две таблицы:

- таблица со списком пользователей;
- таблица со списком групп пользователей.

Каждая таблица содержит информацию о доступе к выбранному инстансу, активам и событиям.

Доступ к инстансу может принимать следующие значения: **Разрешен**, **Запрещен**.

Для активов и событий доступ разделен по видам действий:

- – доступ к созданию;
- – доступ к просмотру;
- – доступ к редактированию;
- – доступ к удалению;
- Нет доступа.

Для активов и событий могут быть определены правила доступа, информация о которых отображается в соответствующей графе таблицы.

9.7.1 Просмотр сводной информации о пользователе

Найдите нужного пользователя в списке на вкладке "Доступ к данным" и нажмите кнопку в соответствующей строке. Откроется форма "Сводная информация о пользователе" (см. «Рис. 95»).

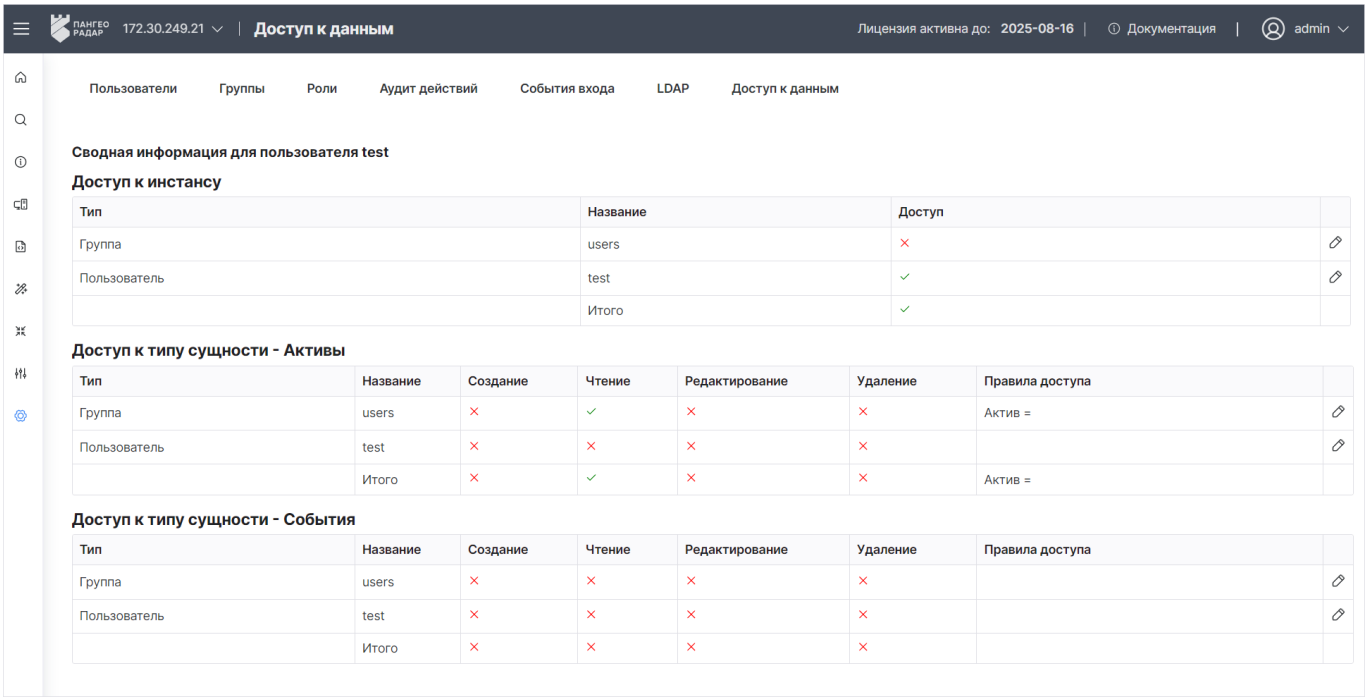


Рис. 95 – Форма "Сводная информация о пользователе"

На форме отображается состояние доступа пользователя к инстансу, активам и событиям.

Если пользователь состоит в группе, то также будет отображена информация о доступах группы и подведен общий итог: разрешен или запрещен доступ.

Иконки доступа обозначают:

- - доступ разрешен;

- ✖ - доступ запрещен.

9.7.2 Настройка доступа к данным

Настройка доступа к данным включает следующие настройки:

- «Настройка доступа к инстансу»;
- «Настройка доступа к активам»;
- «Настройка доступа к событиям».

9.7.2.1 Настройка доступа к инстансу

1. Перейдите на форму "Сводная информация о пользователе" (см. «Рис. 95»).
2. В таблице **Доступ к инстансу** нажмите кнопку ✎. Откроется окно "Настройки доступа для пользователя" (см. «Рис. 96»).

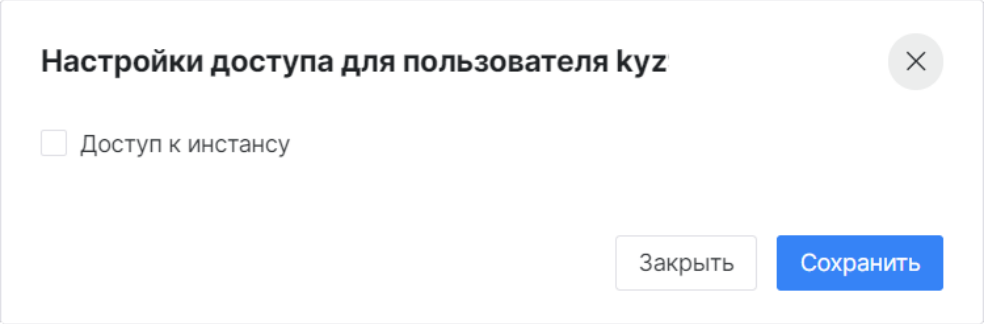


Рис. 96 – Окно "Настройки доступа для пользователя"

3. Для того, чтобы разрешить или запретить доступ к инстансу, установите или снимите соответствующий флаг.
4. Нажмите кнопку **Сохранить**.

9.7.2.2 Настройка доступа к активам

Настройка доступа к активам включает в себя выдачу прав пользователю на чтение, редактирование, создание и удаление актива, а также добавление правил доступа.

Каждое правило выглядит следующим образом:

Выбранная сущность (оператор: равно/не равно) *Значение*

При добавлении правил доступа к активам можно выбрать следующие сущности и соответствующие значения:

- **Актив** – IP-адрес или FQDN актива;
- **Группа активов** – наименование группы активов.

Для настройки доступа пользователя к активам выполните следующие действия:

1. Перейдите на форму "Сводная информация о пользователе" (см. «Рис. 95»).
2. В таблице **Доступ к типу сущности - активы** нажмите кнопку ✎. Откроется окно "Настройки доступа для пользователя" (см. «Рис. 97»).

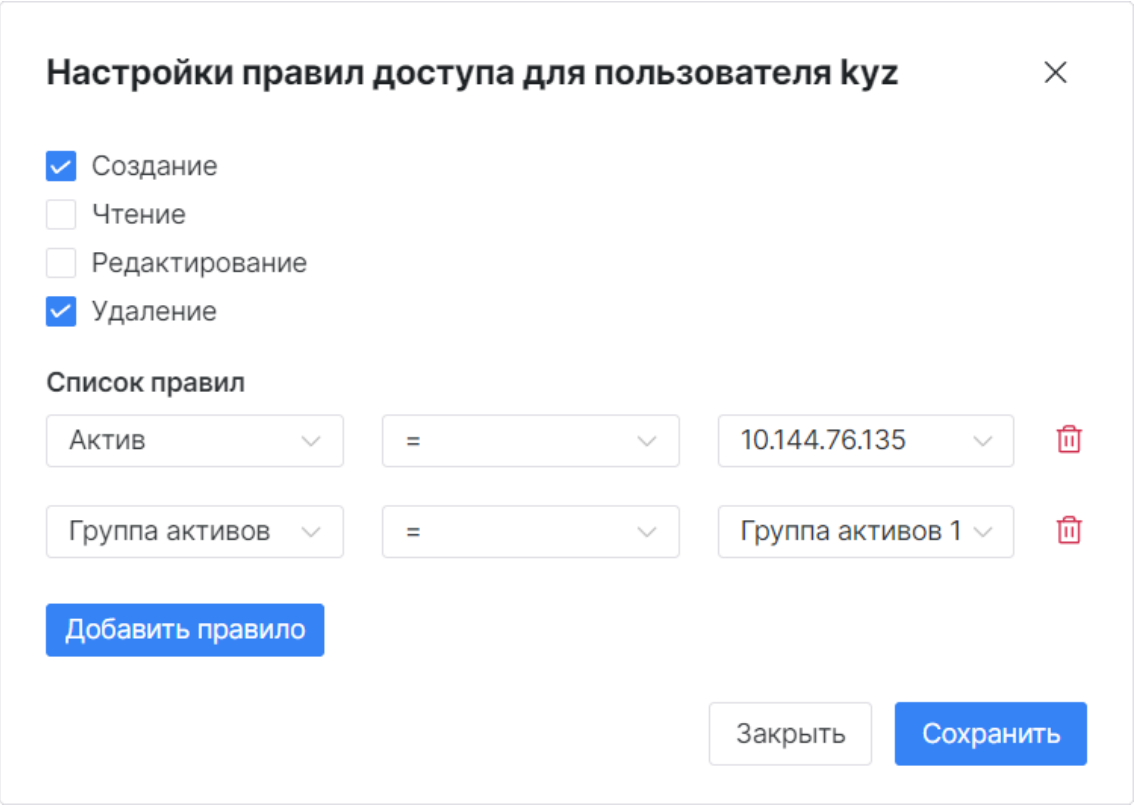


Рис. 97 – Окно "Настройки доступа для пользователя"

3. Установите или запретите доступ к функциям создания, чтения, редактирования, удаления активов, установив/сняв соответствующий флаг.
4. При необходимости добавьте правила доступа. Для этого нажмите кнопку **Добавить правило** и укажите сущность, для которой будет работать правило, оператор и соответствующее значение.
5. Нажмите кнопку **Сохранить**.

9.7.2.3 Настройка доступа к событиям

Настройка доступа к событиям включает в себя выдачу прав пользователю на чтение, редактирование, создание и удаление событий, а также добавление правил доступа.

Каждое правило выглядит следующим образом:

Выбранная сущность (оператор: равно/не равно) *Значение*

При добавлении правил доступа к событиям можно выбрать следующие сущности и соответствующие значения:

- **vendor** – наименование вендора;
- **subsystem** – наименование подсистемы;
- **product** – наименование продукта;
- **name** – наименование события;
- **application** – наименование приложения;
- **fqdn** – наименование домена;

- **hostname** – наименование хоста в сети;
- **ip** – ip-адрес хоста в сети.

Для настройки доступа пользователя к событиям выполните следующие действия:

1. Перейдите на форму "Сводная информация о пользователе" (см. «Рис. 95»).
2. В таблице **Доступ к типу сущности - события** нажмите кнопку . Откроется окно "Настройки доступа для пользователя" (см. «Рис. 98»).

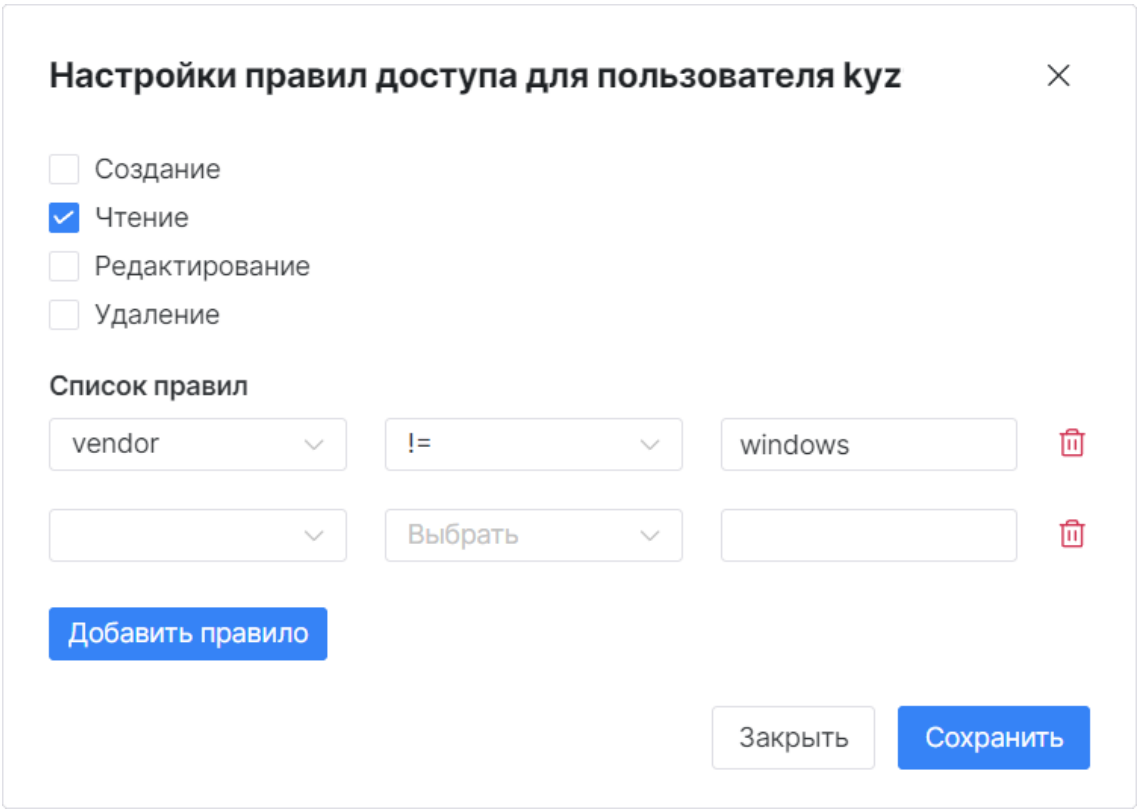


Рис. 98 – Окно "Настройки доступа для пользователя"

3. Установите или запретите доступ к функциям создания, чтения, редактирования, удаления событий, установив/сняв соответствующий флаг.
4. При необходимости добавьте правила доступа. Для этого нажмите кнопку **Добавить правило** и укажите сущность, для которой будет работать правило, оператор и соответствующее значение.
5. Нажмите кнопку **Сохранить**.

9.7.3 Настройка доступа для группы пользователей

Перейти к настройке доступа для группы пользователей можно двумя способами:

- Найдите нужную группу в списке на вкладке "Доступ к данным" (см. «Рис. 94») и нажмите кнопку .
- Перейдите на форму "Сводная информация о пользователе" (см. «Рис. 95») и нажмите кнопку в любой из таблиц, в строке с наименованием группы.

Откроется форма **Сводная информация о группе** (см. «Рис. 99»).

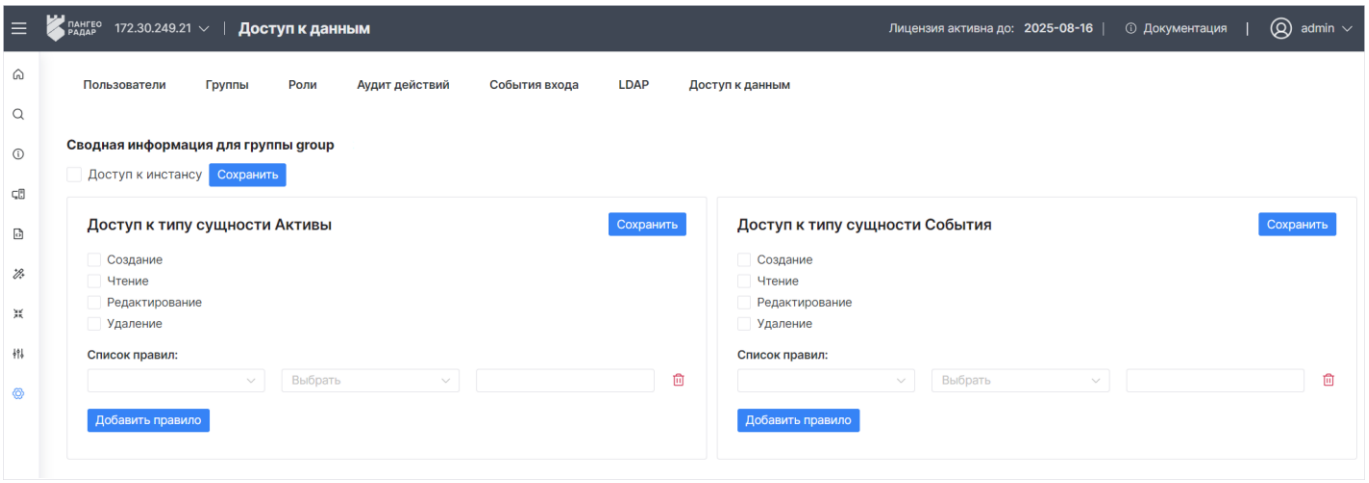


Рис. 99 – Форма "Сводная информация о группе пользователей"

При необходимости измените и сохраните информацию о доступе к данным в соответствующих блоках. Особенности настроек изложены в разделах:

- «Настройка доступа к инстансу»;
- «Настройка доступа к активам»;
- «Настройка доступа к событиям».

10. Управление кластером

10.1 Узлы системы

10.1.1 Общие сведения

Платформа Радар может быть установлена как на одном сервере, так и распределено на нескольких. Каждый сервер - узел кластера, который может осуществлять работу согласно назначенной на него роли.

Платформа Радар позволяет выполнять настройки всех серверов и узлов без необходимости подключения к ним через терминальные соединения.

Кластер **Платформы Радар** состоит из следующих компонентов:

- менеджер кластера;
- агент (-ы) кластера.

При добавлении узла автоматически добавляется агент (-ы), через который будет осуществляться управление и контроль состояния узла. Интерфейс и менеджер кластера находятся на сервере с ролью **MASTER**.

Для работы с узлами кластера перейдите в раздел **Администрирование** → **Кластер** → вкладка **Узлы**. Интерфейс раздела состоит из трех блоков:

- «Карта кластера» – просмотр распределения серверных ролей по узлам кластера;
- «Узлы системы» – управление узлами кластера;
- «Сервисы» – управление сервисами на узлах кластера.

10.1.2 Карта кластера

На карте кластера можно посмотреть распределение серверных ролей по узлам кластера. Пример карты приведен на «Рис. 100».

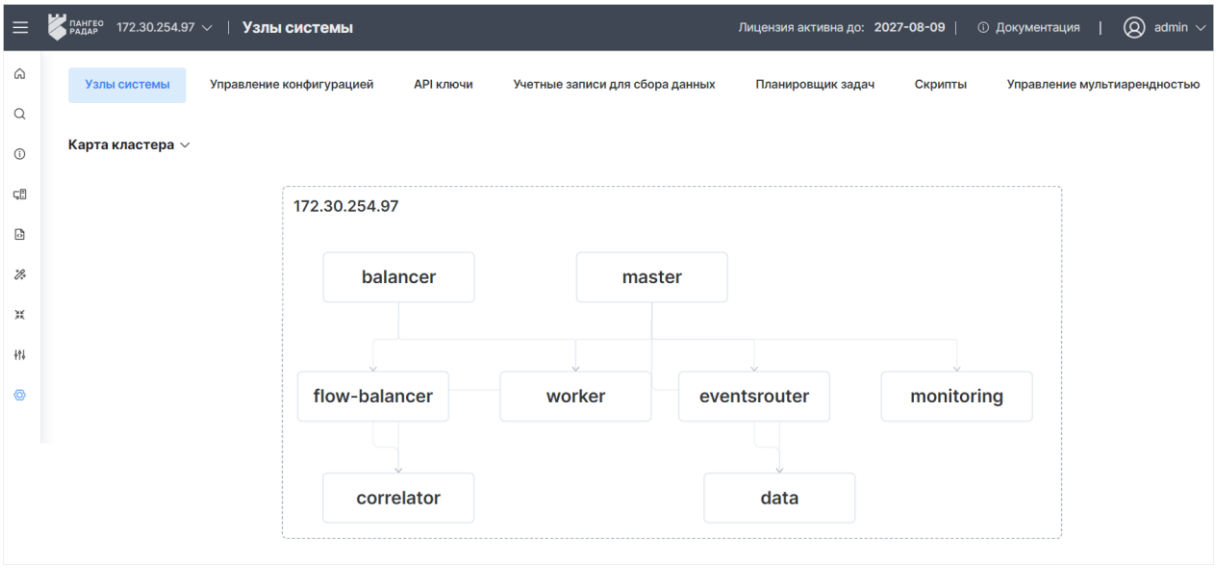


Рис. 100 – Раздел "Кластер". Вкладка "Узлы системы" → "Карта кластера"

10.1.3 Узлы системы

В блоке **Узлы системы** содержаться информация об узлах кластера и доступны следующие действия:

- «Добавление узла»;
- «Просмотр узла кластера»;
- «Добавление роли»;
- «Установка роли»;
- «Удаление роли»;
- «Исполнение скриптов на удаленном хосте»;
- «Удаление узла».

Список серверных ролей, доступных узлам кластера приведен в «Таблица 3».

Таблица 3 – Список серверных ролей

Название роли	Описание роли
MASTER	Управление **Платформой Радар**
DATA	Хранение данных обработанных событий
MONITORING	Мониторинг работоспособности **Платформы Радар**
WORKER	Обработка входящего потока событий
BALANCER	Балансировка входящего потока событий
CORRELATOR	Корреляция обработанного потока событий
EVENTSROUTER	Пересылка событий
FLOW-BALANCER	Балансировка коррелятора
AGENT	Агент управления лог-коллектором
BACKUP	Резервная копия
AGENT_WIN	Агент управления лог-коллектором, установленным на ОС Windows
LOG-COLLECTOR	Сбор событий

Пример блока **Узлы системы** представлен на «Рис. 101».

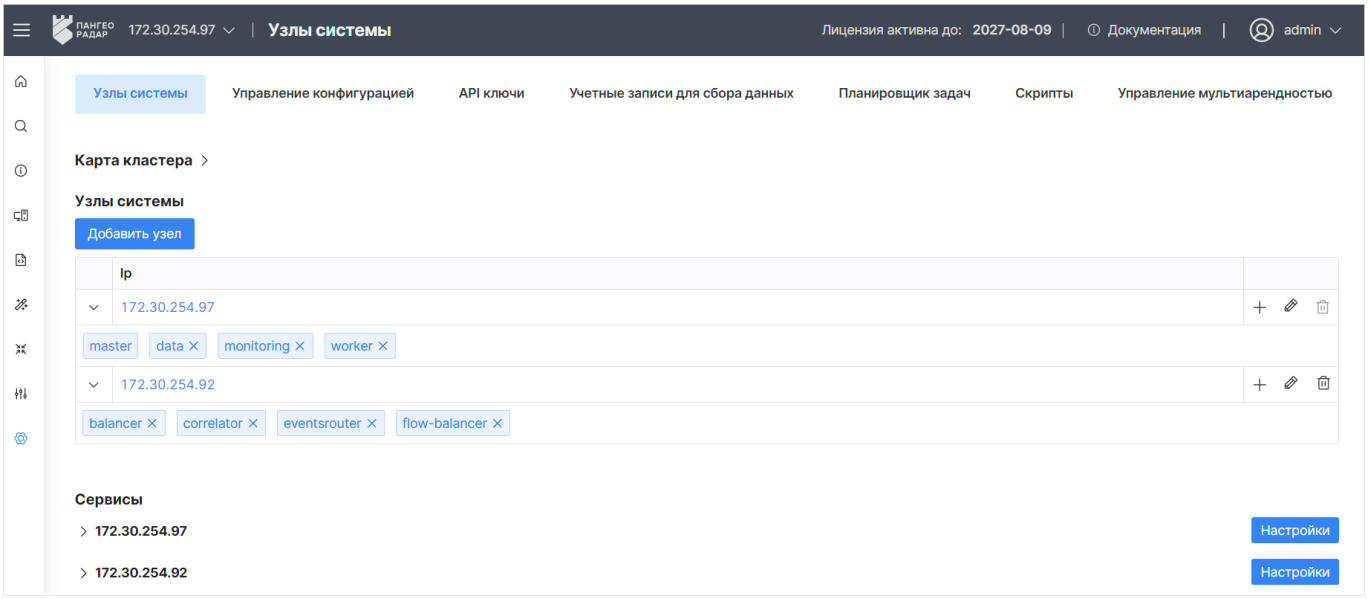


Рис. 101 – Раздел "Кластер". Вкладка "Узлы"

10.1.3.1 Добавление узла

1. Убедитесь, что соблюдены следующие условия для добавления нового узла:
    - узел развернут и готов принимать внешние соединения;
    - на узле установлена ОС - Debian 12 / Astra Linux 1.8 в 64-разрядном режиме;
    - на узле поднят SSH-сервер (см. раздел «Настройка SSH-сервера на Debian 12»);
    - узел разрешает соединения под привилегированным пользователем root.
2. Войдите в веб-интерфейс на узле с ролью **MASTER** и перейдите в раздел **Администрирование** → **Кластер** → вкладка **Узлы** (см. «Рис. 101»).
3. Нажмите кнопку **Добавить узел** (см. «Рис. 102»).

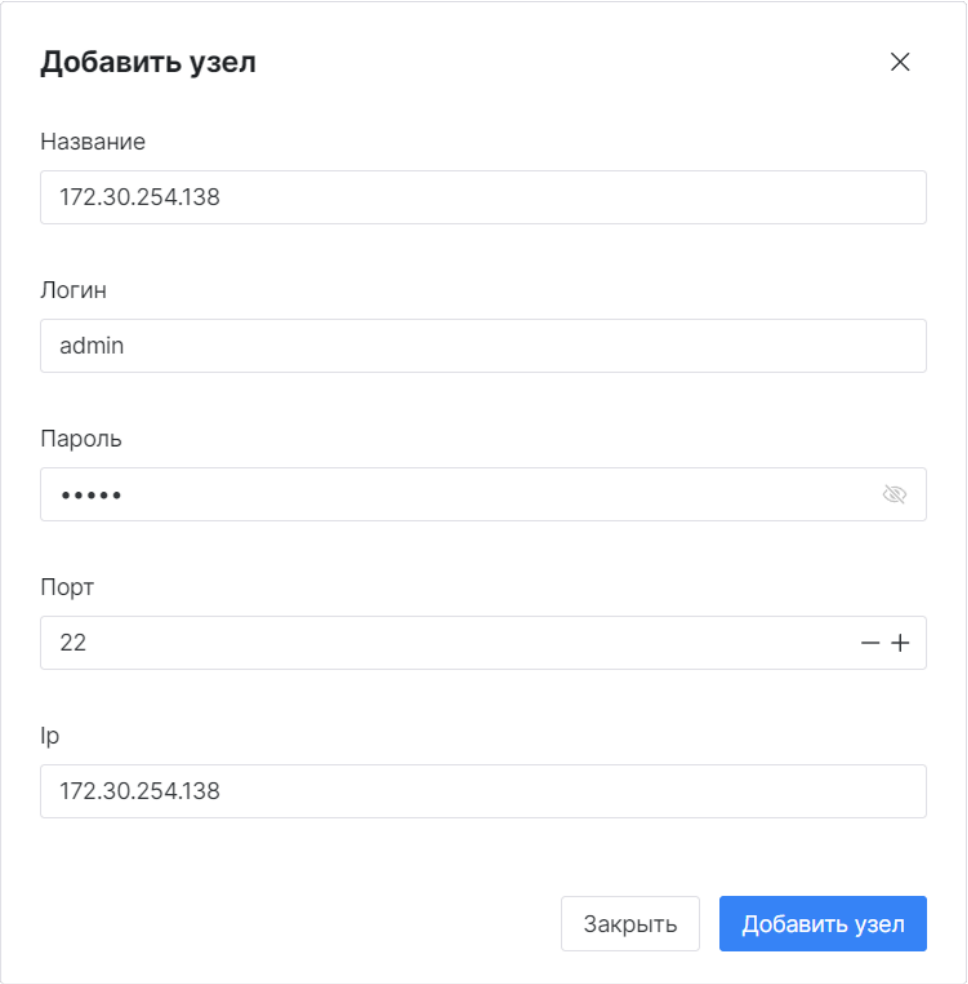


Рис. 102 – Окно "Добавить узел"

4. Укажите в окне следующую информацию:
   - в поле **Название** укажите наименование узла;
   - в полях **Логин** и **Пароль** укажите данные для подключения привилегированного пользователя root к узлу;
   - в полях **IP** и **Порт** укажите IP-адрес и порт подключения к узлу.
5. Нажмите кнопку **Добавить узел**.

10.1.3.2 Просмотр узла кластера

Для просмотра детальной информации об узле кластера нажмите по ссылке с **IP** кластера в блоке **Узлы системы**. Откроется форма просмотра узла кластера см. «Рис. 103».

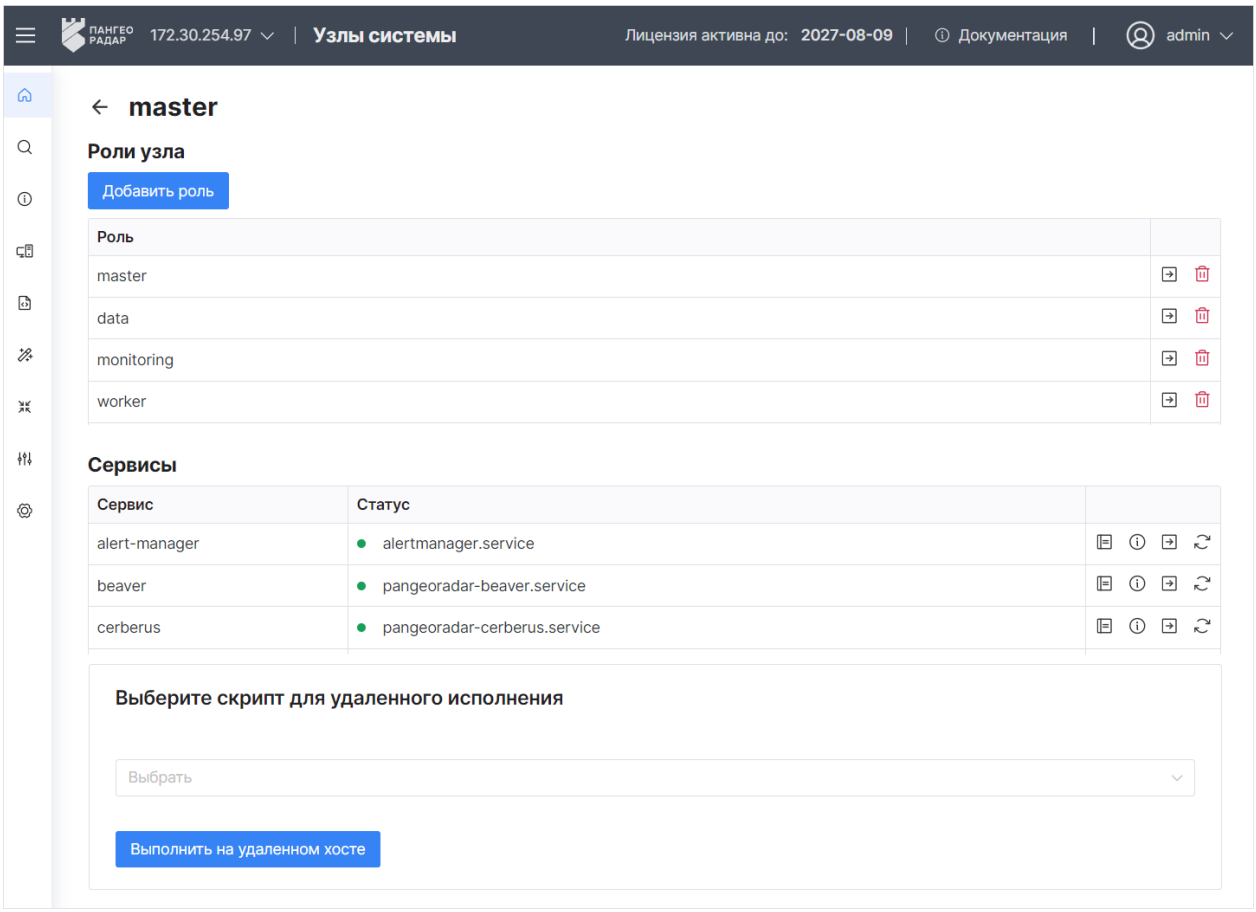


Рис. 103 – Форма просмотра узла кластера

На форме отображается следующая информация:

- Наименование узла;
- Список ролей узла;
- Сервисы, запущенные на узле.

10.1.3.3 Добавление роли

Добавление роли узлу кластера можно выполнить следующими способами:

- В блоке **Узлы системы** (см. «Рис. 101») нажмите кнопку **+**;
- На форме просмотра узла («Рис. 103») нажмите кнопку **Добавить роль**.

Откроется окно "Добавить роль", в котором из выпадающего списка выберите нужную роль и нажмите кнопку **Добавить роль** (см. «Рис. 104»).

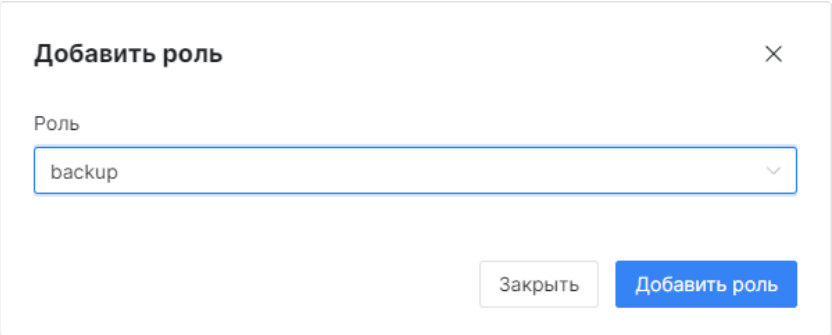


Рис. 104 – Окно «Добавить роль»

10.1.3.4 Установка роли

После добавления роли узлу кластера ее необходимо "раскатить" (установить). Для этого перейдите на форму просмотра узла и нажмите кнопку .

Внимание! *При выполнении операции будут перезапущены все сервисы, установленные на узле.*

10.1.3.5 Удаление роли

Первый способ:

1. Выберите нужный узел из списка в блоке **Узлы системы** (см. «Рис. 101»).
2. В строке со списком ролей нажмите на кнопку рядом с наименованием нужной роли.
3. Подтвердите удаление в открывшемся окне.

Второй способ:

1. Перейдите на форму просмотра нужного узла («Рис. 103»).
2. В блоке **Роли узла** выберите нужную роль и нажмите кнопку .
3. Подтвердите удаление в открывшемся окне.

10.1.3.6 Исполнение скриптов на удаленном хосте

С помощью исполнения скриптов на удаленном хосте вы можете установить/удалить ряд сервисов или выполнить ряд самостоятельных операций. Список скриптов, доступных для выполнения задается в разделе **Администрирование** → **Кластер** → вкладка **Скрипты** (подробнее см. раздел «Скрипты»).

Для выполнения операции выполните следующие действия:

1. Перейдите на форму просмотра нужного узла («Рис. 103»).
2. В блоке **Выберите скрипт для удаленного исполнения** из выпадающего списка выберите необходимый скрипт.
3. Нажмите кнопку **Выполнить на удаленном хосте**. Скрипт будет исполнен, а результат выполнения скрипта отобразится в окне "Результаты выполнения скрипта" (см. «Рис. 105»).

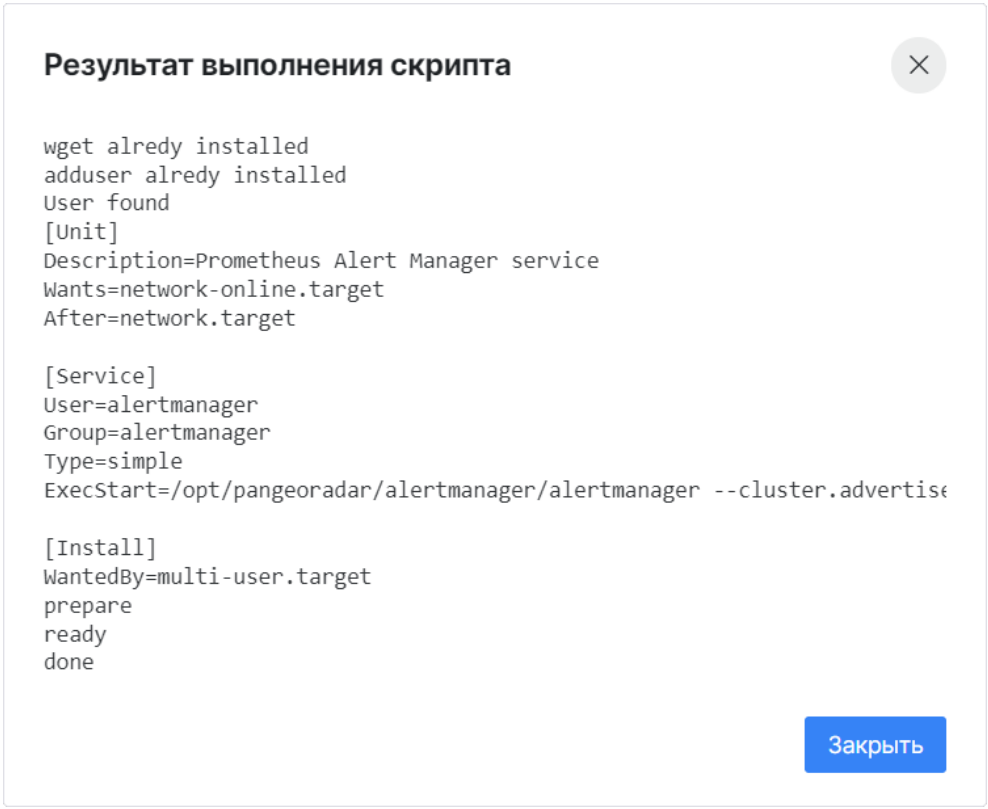


Рис. 105 – Пример результата выполнения скрипта

10.1.3.7 Удаление узла

Примечание: *узел с ролью MASTER удалить нельзя*.

1. Выберите нужный узел в блоке **Узлы системы** и нажмите кнопку .
2. Подтвердите удаление в открывшемся окне.

10.1.4 Сервисы

Список сервисов платформы радар, а также управление параметрами сервисов описано в разделе «Управление конфигурацией».

Пример блока **Сервисы** приведен на «Рис. 106».

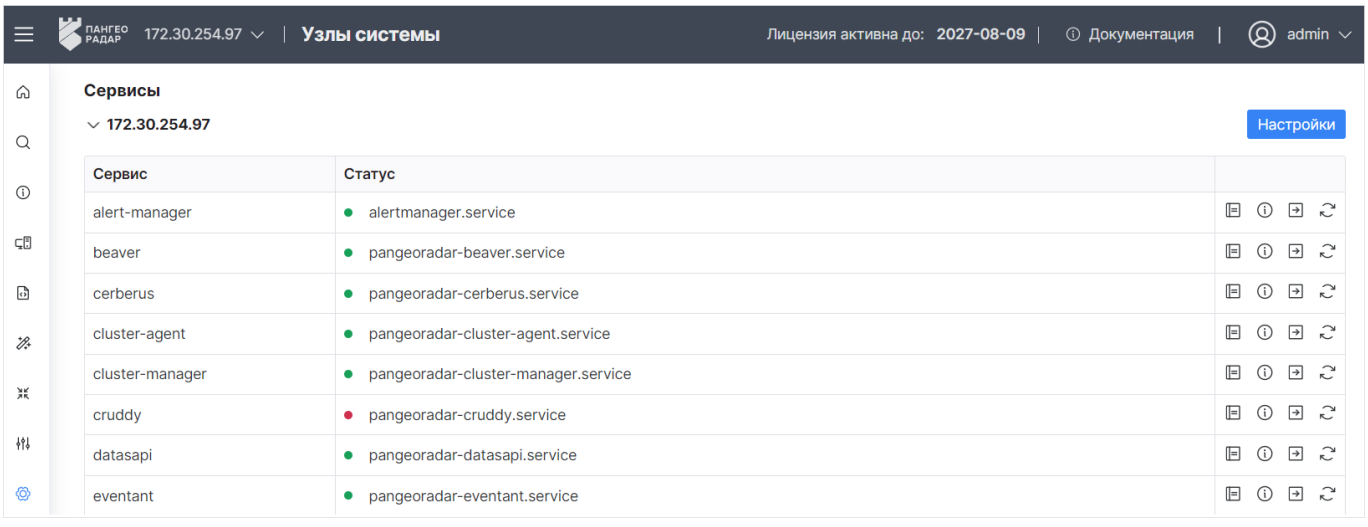


Рис. 106 – Блок "Сервисы"

В графе **Сервис** отображается наименование сервиса.

В графе **Статус** отображается наименование соответствующей службы и ее текущее состояние:

- (зеленый) – сервис работает в штатном режиме;
- (красный) – сервис не отвечает.

При настройке узлов доступны следующие операции над сервисами:

Кнопка	**Действие**
	Просмотр журнала сервиса
	Просмотр статуса сервиса
	Переустановка сервиса на узле
	Перезапуск сервиса на узле
Настройки	Открывает форму просмотра узла (см. «Рис. 103»)

10.1.4.1 Просмотр журнала сервиса

Для просмотра журнала работы сервиса нажмите кнопку . Откроется окно "Логи сервиса" (см. «Рис. 107»).

Рис. 107 – Пример журнала работы сервиса

10.1.4.2 Просмотр статуса сервиса

Для просмотра подробной информации о текущем состоянии сервиса нажмите кнопку . Откроется окно "Статус сервиса" (см. «Рис. 108»).

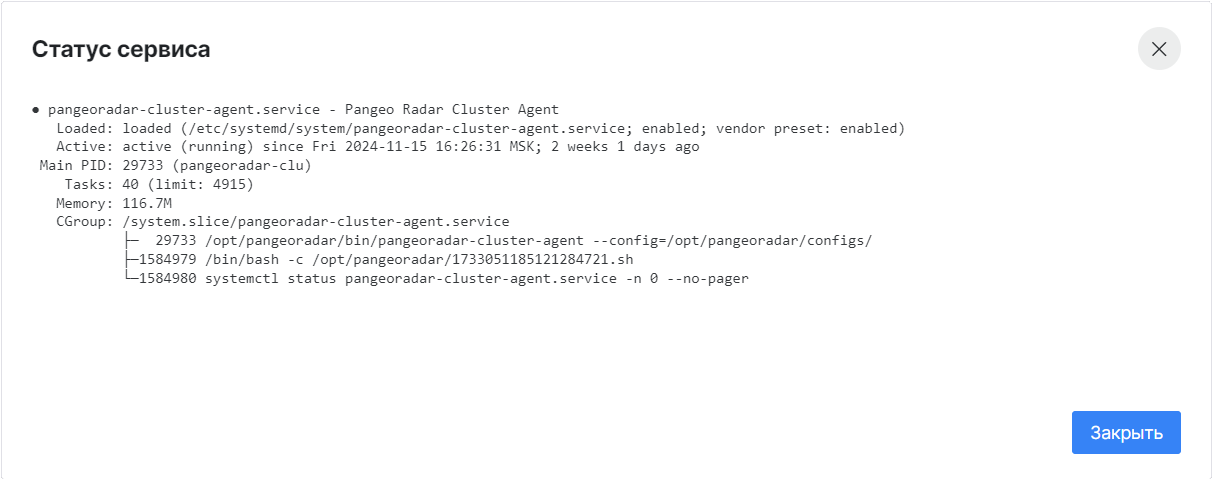


Рис. 108 – Пример статуса сервиса

10.1.4.3 Переустановка и перезапуск сервиса

Переустановка и перезапуск сервиса может потребоваться в случае, если сервис не отвечает.

Для переустановки сервиса нажмите кнопку .

Для переустановки сервиса нажмите кнопку .

10.2 Управление конфигурацией

10.2.1 Общий принцип работы

В разделе **Администрирование → Кластер→** вкладка **Управление конфигурацией** выполняется управление следующими параметрами:

- Глобальный ключ авторизации запросов на сервисе cerberus;
- Список адресов электронной почты для уведомления о внештатном изменении конфигурации системы;
- Список адресов электронной почты для уведомления о штатном изменении конфигурации системы;
- Тонкая настройка всех сервисов **Платформы Радар**. Список сервисов представлен в «Таблица 4».

Таблица 4 – Сервисы Платформы Радар

№	Сервис	Описание	Доступные настройки
1	Beaver	Балансировщик обработчика событий	– уровень логирования маршрутизатора событий – параметры Data – параметры Workers
2	Cerberus	Межсервисный шлюз	– внешний IP адрес сервиса – IP адрес сервиса – режим запуска: стандартный/отладка – внешний порт сервиса на сервере nginx – порт сервиса – отключить обязательную проверку TLS при соединении к БД – использовать TLS шифрование

№	Сервис	Описание	Доступные настройки
			– параметры InputChecker
3	ClusterAgent	Агент управления узлом кластера.	– IP сервиса – уровень логирования – внешний порт сервиса на сервере nginx – порт сервиса
4	Cm	Менеджер кластера	– отключить обязательную проверку TLS при соединении к БД – использовать TLS шифрование – IP адрес сервиса – уровень логирования – порт сервиса – протокол обращения к сервису
5	Cruddy	Центр управления API	– директория хранения загруженных файлов – IP адрес сервиса – уровень логирования – порт сервиса – протокол обращения к сервису – режим работы сервиса – отключить обязательную проверку TLS при соединении к БД – использовать TLS шифрование
6	DatasApi	Отчетность	– использовать ли режим отладки – IP адрес сервиса – порт сервиса – протокол обращения к сервису – таймаут опроса заданий в секундах
7	DNS	Настройка домена и адреса сервиса авторизации	– дополнительные доменные имена – адрес сервиса авторизации – доменное имя
8	Enrich	Обогащение событий	– использовать ли Custom функции – параметры DNS – параметры GeoIp – использовать ли RVS (табличные списки)
9	ESExporter	Экспорт метрик с сервиса, отвечающего за хранение событий	– внешний порт сервиса на сервере nginx – порт сервиса
10	EventAnt	Интеграция с ГосСОПКА	– IP адрес сервиса – уровень логирования – порт сервиса – протокол обращения к сервису – отключить обязательную проверку TLS при соединении к БД – использовать TLS шифрование – параметры Sopka
11	FlowBalancer	Балансировщик коррелятора	– интервал коммита событий (с) – уровень логирования – параметры Head – параметры Frontend – параметры Sender
12	Grafana	Визуализация метрик	– IP адрес сервиса – ключ к доступу API Grafana – внешний порт сервиса на сервере nginx – порт сервиса – протокол обращения к сервису – порт WEB интерфейса

№	Сервис	Описание	Доступные настройки
13	KafkaExporter	Экспорт метрик с сервиса Kafka	– внешний порт сервиса на сервере nginx – порт сервиса
14	Kafka	Передача данных и событий между модулями	– IP адрес сервиса – время хранения сегмента лога Кафки (в минутах)
15	Karaken	Провайдер мультиарендности	– режим отладки – IP адрес сервиса – внешний порт сервиса на сервере nginx – порт сервиса
16	KeyCloak	Аутентификация	– IP адрес сервиса – внешний порт сервиса на сервере nginx – порт сервиса
17	Logmule2	Коррелятор событий	– внешний IP адрес сервиса (по-умолчанию) – интервал малого окна группировки в секундах по умолчанию – IP адрес сервиса – локальные сети – уровень логирования – максимальное количество сработок – период для определения ограничения количества сработок (секунды) – ограничение памяти в Мб – кол-во одновременно выполняемых процедур пересчета группера – порт сервиса – коэффициент для корректирования метрики памяти – интервал синхронизации правил в секундах – интервал обновления счетчика ошибок в секундах – параметры RuleLogs – параметры Frontend
18	Logproxy	Пересылка событий от лог-коллектора в сервис Kafka	– порт приема сообщений – Message ID приема событий верхнеуровневой корреляции – Message ID приема разобранных событий
19	Nginx	Веб-сервер	– путь до файла SSL сертификат – путь до файла ключа SSL сертификата
20	NodeExporter	Сбор метрик с узлов кластера	– внешний порт сервиса на сервере nginx – порт сервиса
21	Opensearch	Хранение и поиск обработанных событий	– путь до файла SSL сертификата opensearch – путь до файла ключа SSL сертификата opensearch – внешний IP адрес сервиса – IP адрес сервиса – внешний порт сервиса на сервере nginx – порт сервиса – путь до файла SSL сертификата Opensearch – версия сервиса Opensearch
22	Pg	База данных	– параметры путей к сертификатам – параметры базы данных для различных сервисов платформы – параметры пользователей базы данных различных сервисов платформы
23	Pluto	Наблюдение за источниками событий	– использовать TLS шифрование – режим отладки – IP адрес сервиса – не проверять подключение к opensearch – порт сервиса

№	Сервис	Описание	Доступные настройки
			– протокол обращения к сервису – секретный ключ – таймаут соединения
24	Prometheus	Сбор и хранение метрик работы **Платформы Радар**	– IP адрес сервиса – порт сервиса – размер хранилища (GB) – срок хранения данных (дни)
26	Sonar	Сканирование активов	– использовать ли режим отладки: да, нет; – IP адрес сервиса – порт сервиса – протокол обращения к сервису
27	Termit	Разбор, нормализация событий	– использовать ли сервис Termit: да, нет – кол-во обработчиков – параметры очереди – параметры Dns – параметры GeoIp
28	Ti	Обновление информации об угрозах	– размер пачки на вставку – отключить обязательную проверку TLS при соединении к БД – использовать TLS шифрование – режим отладки – IP адрес сервиса – порт сервиса – протокол обращения к сервису – интервал обновления
29	Toller	Оповещения	– отключить обязательную проверку TLS при соединении к БД – использовать TLS шифрование – режим отладки – ID инстанса – IP адрес сервиса – порт сервиса – протокол обращения к сервису – адрес WebHook для Slack – включить Slack – параметры SMTP

Интерфейс управления конфигурацией приведен на «Рис. 109».

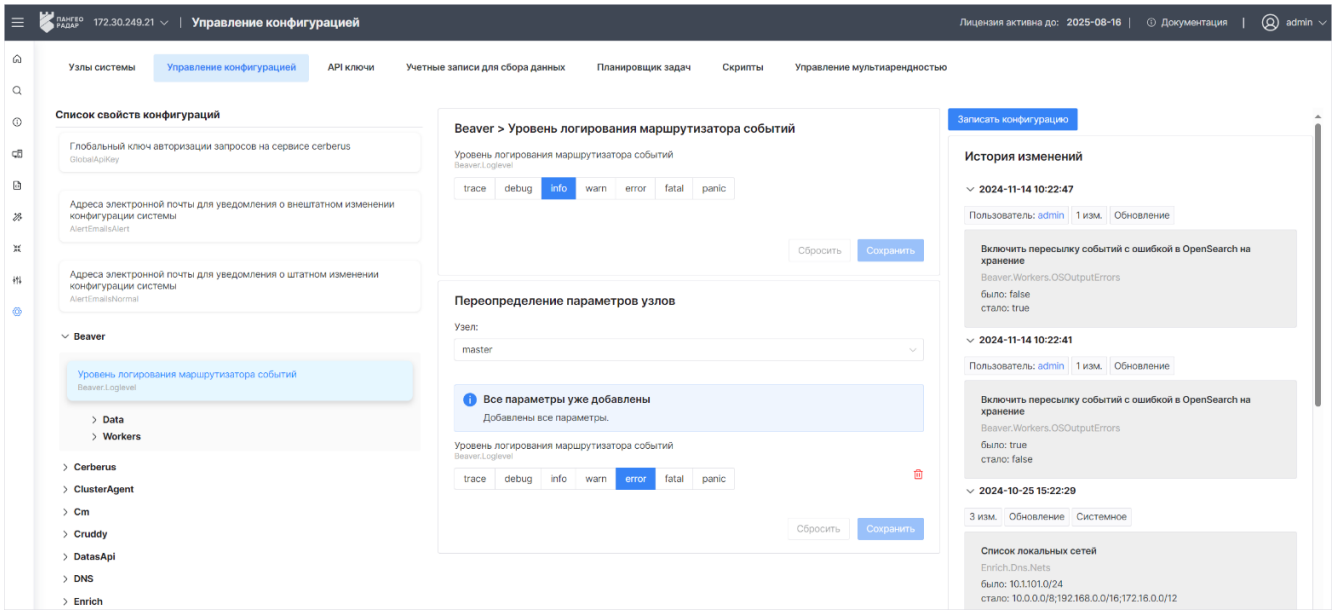


Рис. 109 – Раздел "Кластер". Вкладка "Управление конфигурацией"

Интерфейс вкладки можно разделить на три блока:

- **Слева**. Блок со древовидным списком параметров сервисов.
- **Центр**. Блок, где выполняется настройка выбранного параметра или группы параметров, выбранных слева.
- **Справа**. Блок с общей историей изменения конфигурации платформы.

Вносимые изменения параметров применяются на всех узлах **Платформы Радар**, однако для отдельных узлов можно установить собственные значения параметров. Для этого при редактировании всех параметров предусмотрена область **Переопределение параметров узлов**, которая располагается в центральном блоке (см. «Рис. 109»).

Для изменения конфигурации платформы выполните следующие действия:

1. Внесите изменения в выбранный параметр.
2. При необходимости переопределите параметр (-ы) для выбранного узла системы.
3. Нажмите кнопку **Записать конфигурацию**.

10.2.2 Перезапись параметров из консоли

В случае, если работоспособность **Платформы Радар** при неправильном задании параметров нарушена, существует возможность просмотреть и изменить значения параметров **Платформы Радар** и ее модулей с помощью консоли (на узле **Master**).

Перейдите в каталог /opt/pangeoradar/bin командой cd /opt/pangeoradar/bin.

Для чтения и задания параметров используются следующие команды консоли:

1. Чтение всех не перезаписанных параметров:

   ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --read-param

```
a.kurkov@v-stand-25:/var/tmp$ cd /opt/pangeoradar/bin
a.kurkov@v-stand-25:/opt/pangeoradar/bin$ ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --read-param
Ключ: AlertEmailsAlert Значение: avk@gaz.ru Название: Адреса электронной почты для уведомления о внештатном изменении конфигурации си
темы Значение по умолчанию:
Ключ: AlertEmailsNormal Значение:  Название: Адреса электронной почты для уведомления о штатном изменении конфигурации системы Значен
е по умолчанию:
Ключ: Beaver.Loglevel Значение: info Название: Уровень логирования маршрутизатора событий Значение по умолчанию: info
Ключ: Beaver.Workers Значение:  Название: Настройки обработчиков маршрутизатора событий Значение по умолчанию:
Ключ: Cerberus.ExtIp Значение: 172.30.254.65 Название: Внешний IP адрес сервиса Значение по умолчанию: 127.0.0.1
Ключ: Cerberus.Ip Значение: 127.0.0.1 Название: IP адрес сервиса Значение по умолчанию: 127.0.0.1
Ключ: Cerberus.Mode Значение: release Название: Стандартный запуск/режим отладки Значение по умолчанию: release
Ключ: Cerberus.NginxPort Значение: 9000 Название: Внешний порт сервиса на сервере nginx Значение по умолчанию: 9000 Данный параметр н
 доступен для редактирования из веб интерфейса. Не рекомендуется вносить в него изменения.
Ключ: Cerberus.Port Значение: 9900 Название: Порт сервиса Значение по умолчанию: 9900 Данный параметр не доступен для редактирования
з веб интерфейса. Не рекомендуется вносить в него изменения.
Ключ: Cerberus.SkipTlsVerify Значение: true Название: Отключить обязательную проверку TLS при соединении к БД Значение по умолчанию:
rue
Ключ: Cerberus.UseTls Значение: true Название: Использовать TLS шифрование Значение по умолчанию: true
Ключ: ClusterAgent.Ip Значение: 127.0.0.1 Название: Ip сервиса Значение по умолчанию: 127.0.0.1
Ключ: ClusterAgent.NginxPort Значение: 6677 Название: Внешний порт сервиса на сервере nginx Значение по умолчанию: 6677 Данный параме
р не доступен для редактирования из веб интерфейса. Не рекомендуется вносить в него изменения.
Ключ: ClusterAgent.Port Значение: 6678 Название: Порт сервиса Значение по умолчанию: 6678 Данный параметр не доступен для редактирова
ия из веб интерфейса. Не рекомендуется вносить в него изменения.
Ключ: Cm.DbSkipTLSVerify Значение: true Название: Отключить обязательную проверку TLS при соединении к БД Значение по умолчанию: true
Ключ: Cm.DbUseTLS Значение: true Название: Использовать TLS шифрование Значение по умолчанию: true
Ключ: Cm.Ip Значение: 127.0.0.1 Название: IP адрес сервиса Значение по умолчанию: 127.0.0.1
Ключ: Cm.Port Значение: 6676 Название: Порт сервиса Значение по умолчанию: 6676 Данный параметр не доступен для редактирования из веб
интерфейса. Не рекомендуется вносить в него изменения.
Ключ: Cm.Protocol Значение: http Название: Протокол обращения к сервису Значение по умолчанию: http
Ключ: Cruddy.DocumentsDir Значение: /opt/pangeoradar/comments_files/ Название: Директория хранения загруженных файлов Значение по умо
чанию: /opt/pangeoradar/comments_files/
Ключ: Cruddy.Ip Значение: 127.0.0.1 Название: IP адрес сервиса Значение по умолчанию: 127.0.0.1
Ключ: Cruddy.LogLevel Значение: error Название: Уровень логирования Значение по умолчанию: error
Ключ: Cruddy.Port Значение: 8089 Название: Порт сервиса Значение по умолчанию: 8089 Данный параметр не доступен для редактирования из
веб интерфейса. Не рекомендуется вносить в него изменения.
Ключ: Cruddy.Protocol Значение: http Название: Протокол обращения к сервису Значение по умолчанию: http
Ключ: Cruddy.ServerMode Значение: release Название: Режим работы сервиса Значение по умолчанию: release
Ключ: Cruddy.SkipTlsVerify Значение: true Название: Отключить обязательную проверку TLS при соединении к БД Значение по умолчанию: tr
e
```

Рис. 110 – Чтение всех не перезаписанных параметров

2. Чтение всех перезаписанных параметров:

   ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --read-param --for-overrides

3. Чтение параметра (ключ из запроса 1 выше):

   ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --read-param --param-key=<ключ>

```
a.kurkov@v-stand-25:/opt/pangeoradar/bin$ ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --read-param --param-key=Ti
.Port
Ti.Port : 8082
```

Рис. 111 – Чтение параметра (ключ из запроса 1 выше)

4. Чтение перезаписанного параметра (ключ из запроса 2 выше вида название*параметра > id*ноды):

   ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --read-param --for-overrides --param-key="<ключ>"

5. Запись параметра:

   ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --write-param --param-key=<ключ> --param-value=<значение>

```
a.kurkov@v-stand-25:/opt/pangeoradar/bin$ ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --write-param --param-key=T
i.Port --param-value=8082
Для Ti.Port установлено значение
```

Рис. 112 – Запись параметра

6. Запись перезаписанного параметра (ключ из запроса 2 выше вида название *параметра > id*ноды):

   ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --write-param --param-key="<ключ>" --param-value=<значение> --for-overrides

7. Перезапись конфигурационных файлов в БД:

   ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --refresh-param-files

8. Перезапись конфигурационных файлов в БД для перезаписанных параметров:

   ./pangeoradar-cluster-manager --config=/opt/pangeoradar/configs/ --refresh-param-files --for-overrides

10.3 API ключи

Для межсервисного взаимодействия и для обращения в **Платформу Радар** из сторонних решений посредством публичного API, используются доверенные ключи API.

В платформе предустановлен ключ API с наименованием global_api_key. Данный ключ по умолчанию используется для межсервисного взаимодействия и при выполнении запросов, с полным набором прав, от сторонних решений.

Внимание! *После удаления global_api_key может быть утеряна работоспособность платформы. Не рекомендуется его удалять*.

Работа с ключами API включает в себя следующие процессы:

1. «Добавление API ключа».
2. «Удаление API ключа».

Для работы с ключами API перейдите в раздел **Администрирование** → **Кластер** → вкладка **API ключи** (см. «Рис. 113»).

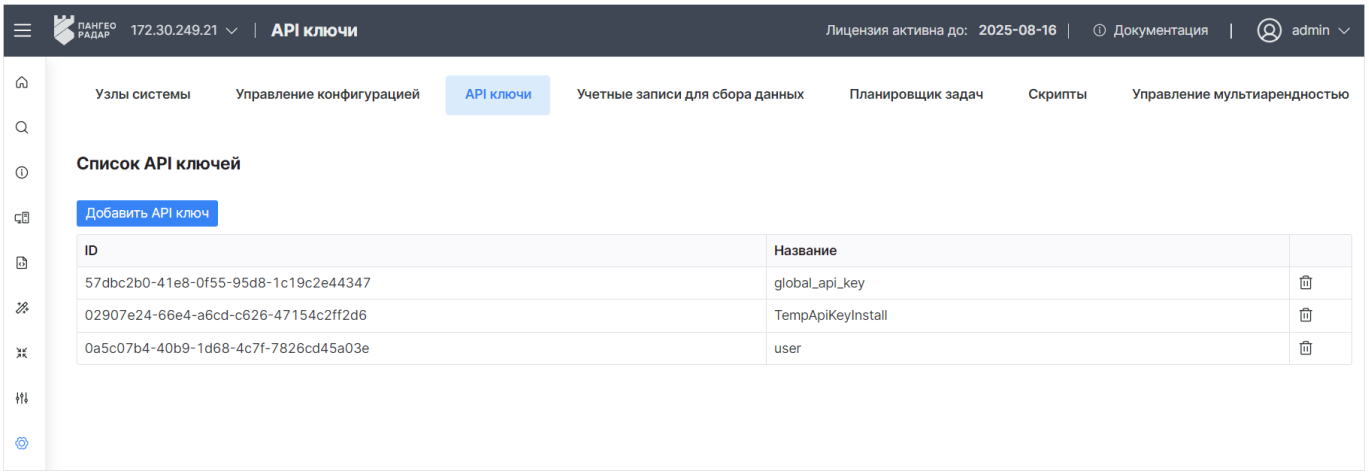


Рис. 113 – Раздел "Кластер". Вкладка "API ключи"

На вкладке отображается следующая информация:

- **ID** – идентификатор API ключа. Данный ID используется при выполнении запросов;
- **Название** – наименование ключа API.

10.3.1 Добавление API ключа

1. Нажмите кнопку **Добавить API ключ**. Откроется окно "Добавить API ключ" (см. «Рис. 114»).

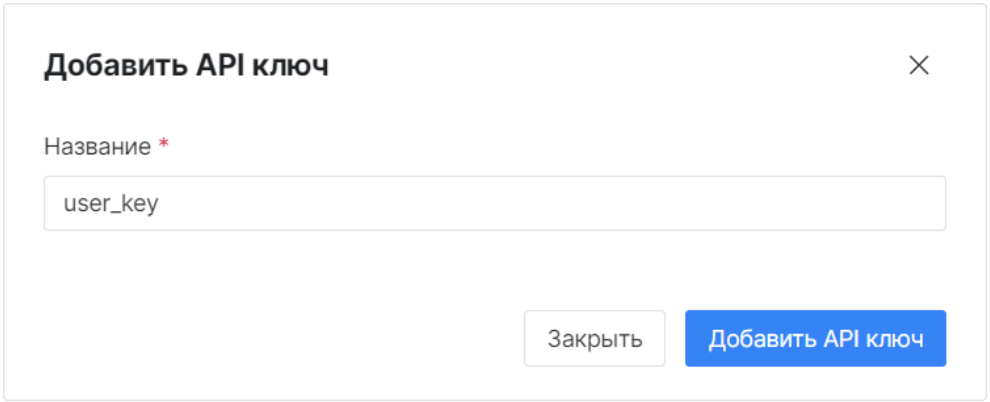


Рис. 114 – Окно "Добавить API ключ"

2. В поле **Название** укажите наименование ключа API.
3. Нажмите кнопку **Добавить API ключ**.

10.3.2 Удаление API ключа

1. В строке нужного ключа нажмите кнопку .
2. Подтвердите удаление в открывшемся окне.

10.4 Учетные записи для сбора данных

Учетные записи используются для сбора данных с хостов и активов при выполнении следующих процессов:

- Обнаружение хостов;
- Обнаружение сервисов;
- Сбор данных;
- Реализации API-взаимодействия с лог-коллектором.

Для учетной записи можно выбрать один или несколько протоколов взаимодействия, по которому (-ым) учетная запись будет обращаться к активу. Поддерживаются следующие протоколы:

- wmi – используется для получения данных с помощью Windows Management Instrumentation. Доступен для Windows-активов;
- rpc – позволяет программе на одном компьютере вызвать функцию на другом компьютере так, будто эта функция находится на первом компьютере;
- ssh – позволяет производить удалённое управление операционной системой и туннелирование TCP-соединений.

Работа с учетными записями для сбора данных включает в себя следующие процессы:

1. «Добавление учетной записи для сбора данных».
2. «Удаление учетной записи для сбора данных».

Для работы с учетными записями для сбора данных перейдите в раздел **Администрирование** → **Кластер**→ вкладка **Учетные записи для сбора данных** (см. «Рис. 115»).

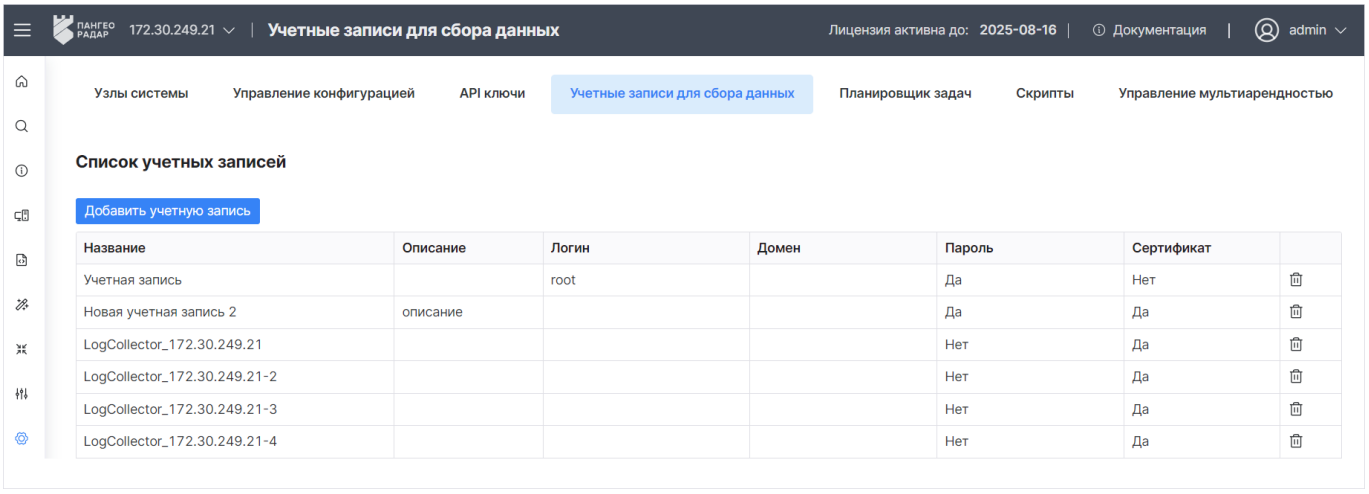


Рис. 115 – Раздел "Кластер". Вкладка "Учетные записи для сбора данных"

На вкладке отображается следующая информация:

- **Название** –наименование учетной записи для сбора данях;
- **Описание** –дополнительные сведения об учетной записи для сбора данных;

- **Домен** –домен, в котором собираются данные;
- **Пароль** –используется ли пароль для авторизации учетной записи: да, нет;
- **Сертификат** – используется ли сертификат для авторизации учетной записи: да, нет.

10.4.1 Добавление учетной записи для сбора данных

1. Нажмите кнопку **Добавить учетную запись**. Откроется окно "Добавить учетную запись" (см. «Рис. 116»).

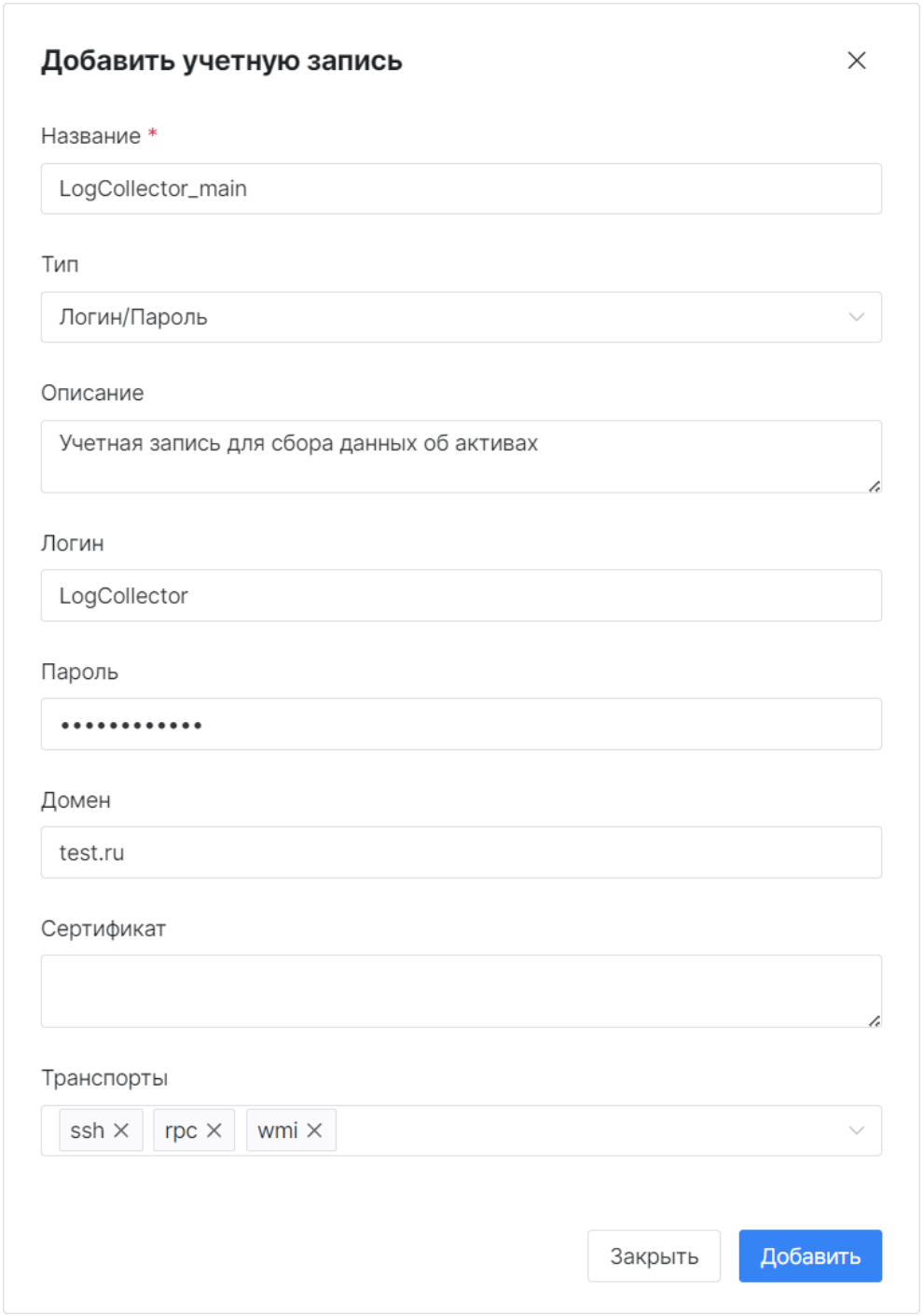


Рис. 116 – Окно "Добавить учетную запись"

2. Укажите в окне следующую информацию:
    - в поле **Название** укажите наименование учетной записи;

- в поле **Тип** выберите способ авторизации учетной записи: Пароль, Логин/Пароль или Сертификат.;
- в поле **Логин** укажите уникальное имя учетной записи;
- в поле **Пароль** укажите пароль от учетной записи;
- в поле **Домен** укажите домен, в котором будет выполняться сбор данных;
- в поле **Сертификат** укажите хэш значение сертификата от учетной записи;
- в поле **Транспорты** из выпадающего списка выберите протокол взаимодействия, по которому учетная запись будет обращаться к активу.

3. Нажмите кнопку **Добавить**.

10.4.2 Удаление учетной записи для сбора данных

1. Выберите нужную учетную запись на вкладке "Учетные записи для сбора данных" и нажмите кнопку .
2. Подтвердите удаление в открывшемся окне.

10.5 Планировщик задач

В **Платформе Радар** реализован инструмент по управлению и организации периодических задач кластера. Инструмент позволяет эффективно распределить ресурсы кластера для достижения поставленных целей.

Для реализации механизма используются CRON-выражения. Подсказу по CRON-выражениям см. на **сайте**.

Работа с планировщиком задач включает в себя следующие процессы:

1. «Добавление задачи в планировщик».
2. «Быстрое редактирование (быстрая смена статусов задач)».
3. «Редактирование задачи».
4. «Просмотр журнала выполнения задачи».
5. «Удаление задачи».

Управление задачами планировщика выполняется в разделе **Администрирование** → **Кластер** → вкладка **Планировщик задач** (см. «Рис. 117»).

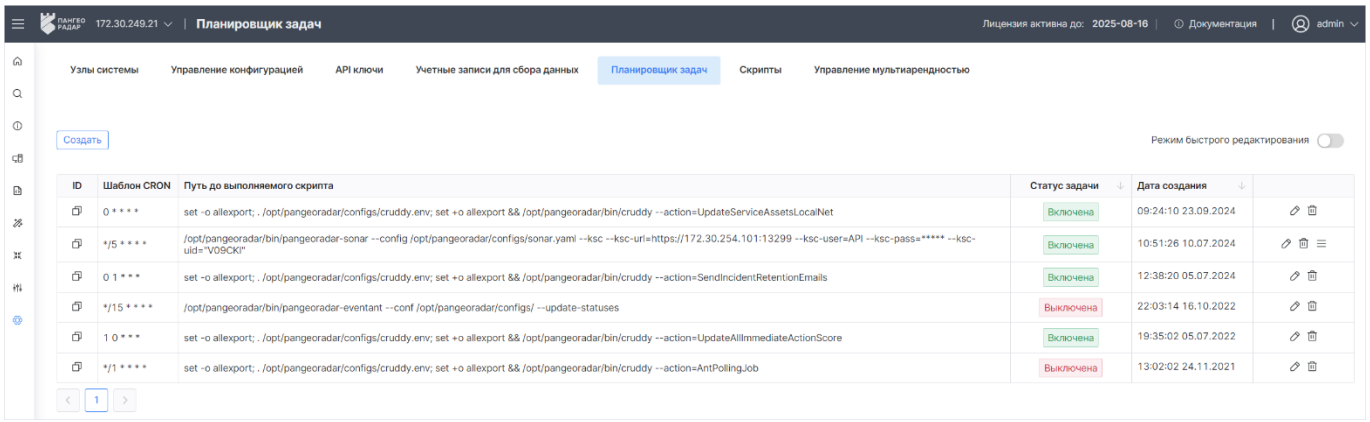


Рис. 117 – Раздел "Кластер". Вкладка "Планировщик задач"

На вкладке отображается следующая информация:

- **Шаблон CRON** – CRON-выражение, описывающее периодичность задачи;
- **Путь до выполняемого скрипта** – команда на bash, которая исполняется при выполнении задачи планировщика;
- **Статус задачи**. Задача может находиться в следующих статусах:
  - **Включена** – задача ожидает выполнения;
  - **Выполняется** – задача выполняется в данный момент;
  - **Выключена** – выполнение задачи приостановлено.
- **Дата создания** – дата и время создания задачи планировщика.

10.5.1 Добавление задачи в планировщик

1. Нажмите кнопку **Создать**. Откроется окно **Создание задачи** (см. «Рис. 118»).

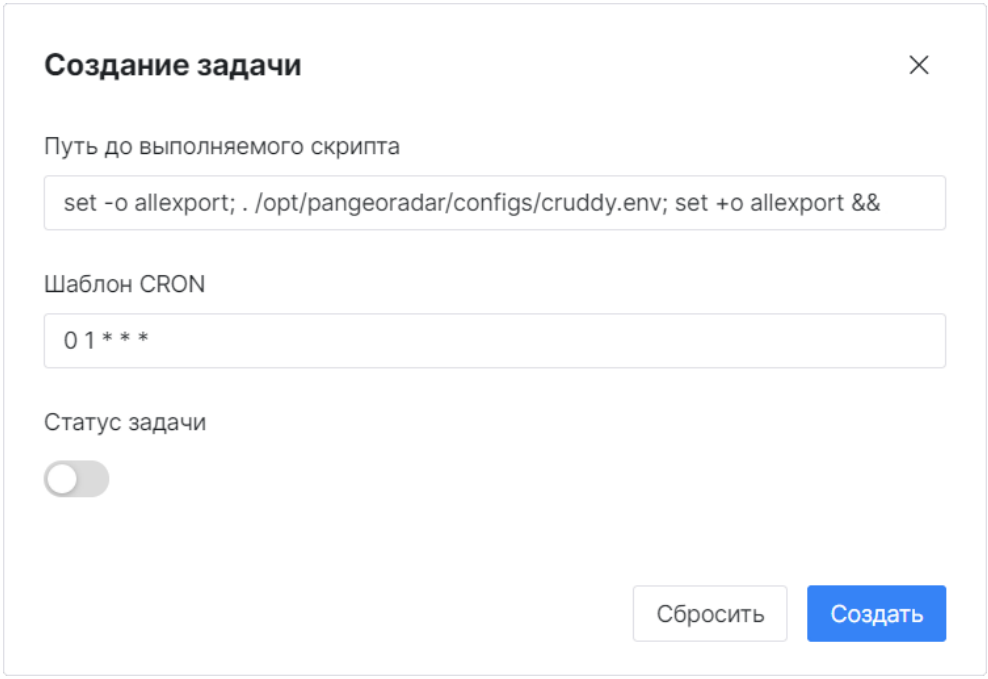


Рис. 118 – Окно "Создание задачи"

2. Укажите в окне следующую информацию:

- в поле **Путь до выполняемого скрипта** укажите bash команду, которая будет исполняться при запуске задачи;
- в поле **Шаблон CRON** укажите CRON-выражение;
- в поле **Статус задачи** включите/выключите выполнение задачи.

3. Нажмите кнопку **Создать**.

10.5.2 Быстрое редактирование (быстрая смена статусов задач)

1. Включите переключатель **Режим быстрого редактирования**. На вкладке **Планировщик задач** появится возможность менять статусы задач (см. «Рис. 119»).

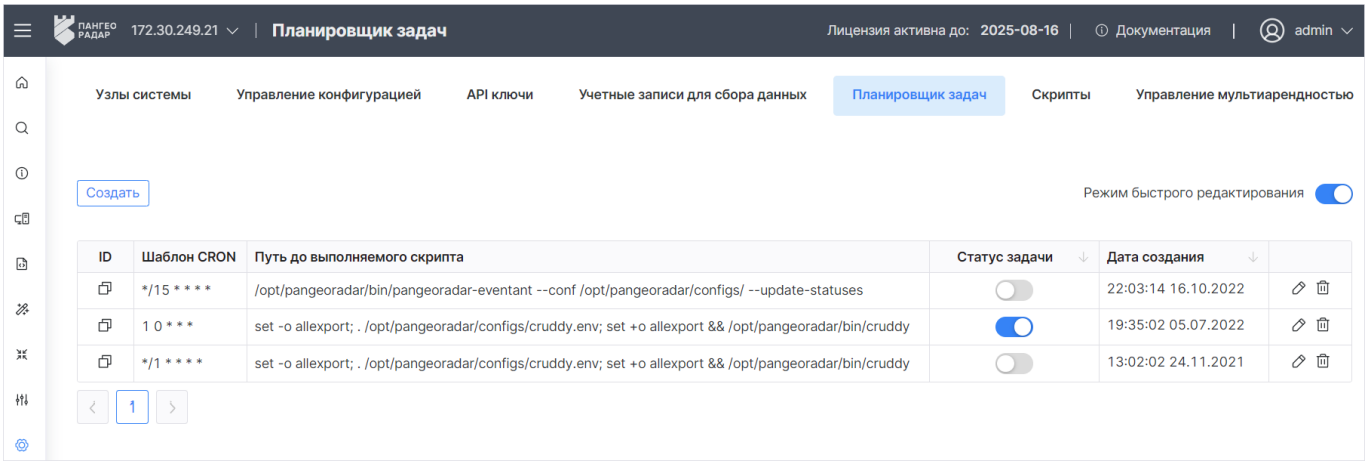


Рис. 119 – Режим быстрого редактирования

2. Измените статусы задач включив/выключив соответствующие переключатели.

10.5.3 Редактирование задачи

1. Выберите нужную задачу из списка на вкладке "Планировщик задач" и нажмите кнопку .
2. Измените информацию о задаче.
3. Нажмите кнопку **Сохранить**.

10.5.4 Просмотр журнала выполнения задачи

Выберите нужную задачу из списка на вкладке "Планировщик задач" и нажмите кнопку . Откроется журнал выполнения задачи (см. «Рис. 120»).

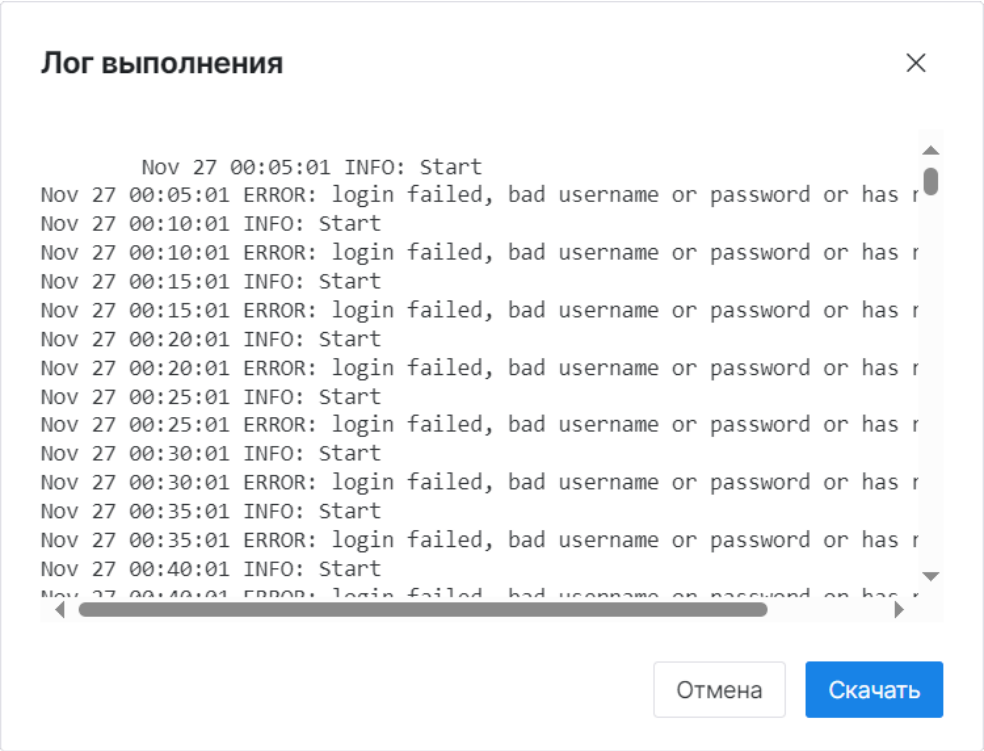


Рис. 120 – Окно "Лог выполнения"

При необходимости можно скачать журнал в формате .txt нажав на соответствующую кнопку.

10.5.5 Удаление задачи

1. Выберите нужную задачу из списка на вкладке "Планировщик задач" и нажмите кнопку .
2. Подтвердите удаление в открывшемся окне.

10.6 Скрипты

Для реализации функции установки/обновления сервисов и ролей **Платформы Радар** используются скрипты, написанные на bash.

В платформе используется ряд предустановленных скриптов для выполнения основных задач.

Внимание! *Не рекомендуется вносить в скрипты изменения без консультации со службой технической поддержки*.

Исполнение скриптов выполняется в процессе настройки узлов кластера (см. раздел «Исполнение скриптов на удаленном хосте»).

Работа со скриптами включает в себя следующие процессы:

1. «Добавление скрипта».
2. «Выставление связи скрипта с серверными ролями и/или с сервисами».
3. «Редактирование скрипта».

4. «Удаление скрипта».

Для работы со скриптами перейдите **Администрирование** → **Кластер** → вкладка **Скрипты** (см. «Рис. 121»).

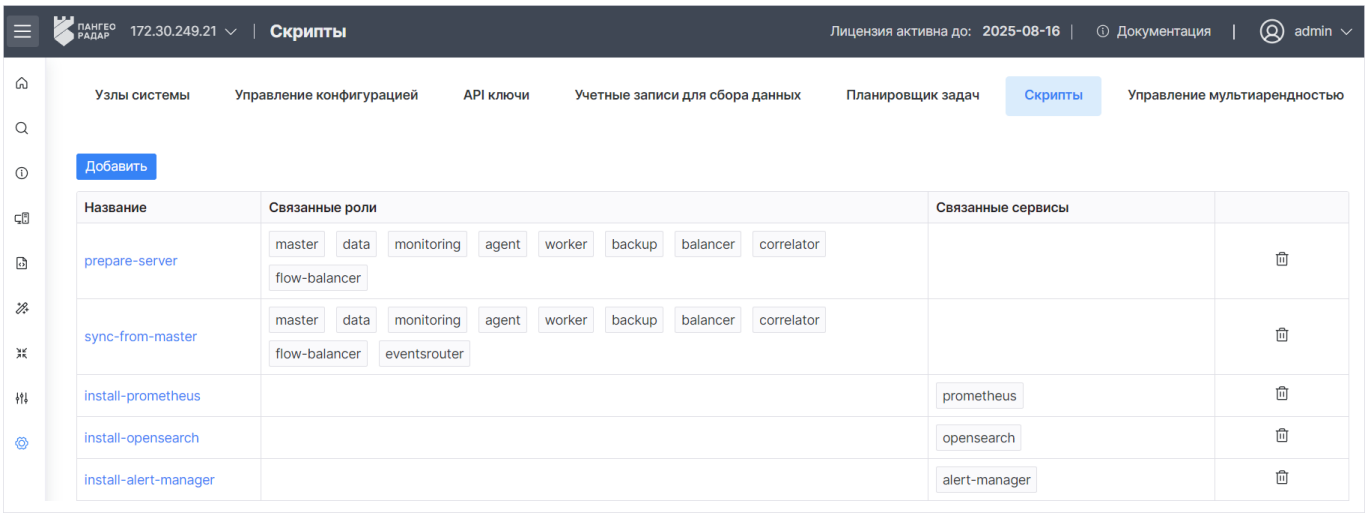


Рис. 121 – Раздел "Кластер". Вкладка "Скрипты"

На вкладке отображается следующая информация:

- **Название** – название скрипта;
- **Связанные роли** – список серверных ролей платформы, на работу которых влияет выполнение скрипта;
- **Связанные сервисы** – список сервисов платформы, на работу которых влияет выполнение скрипта.

10.6.1 Добавление скрипта

1. Нажмите кнопку **Добавить**. Откроется окно "Добавление скрипта" (см. «Рис. 122»).

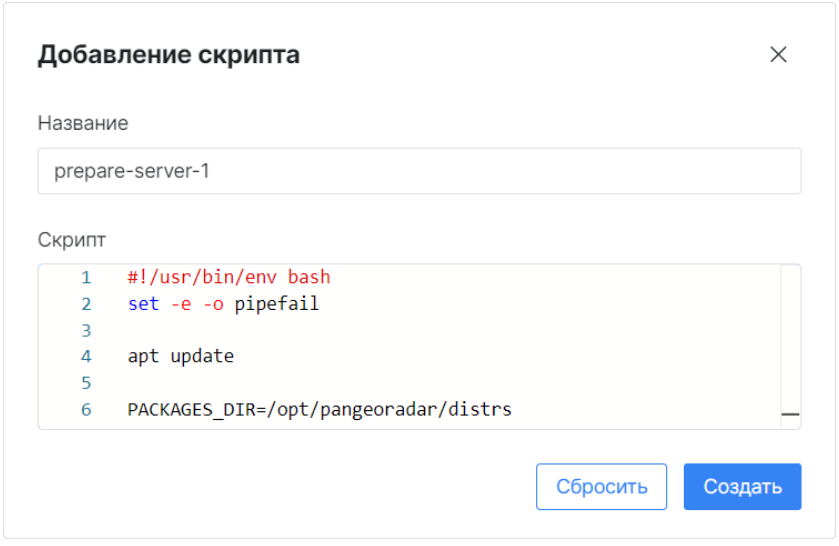


Рис. 122 – Окно "Добавление скрипта"

2. Укажите в окне информацию о скрипте:
    - в поле **Название** укажите уникальное наименование скрипта;

- в поле **Скрипт** укажите тело скрипта на bash.

3. Нажмите кнопку **Создать**.

10.6.2 Выставление связи скрипта с серверными ролями и/или с сервисами

1. Выберите нужный скрипт из списка на вкладке "Скрипты" и нажмите кнопку . Откроется форма "Редактирование скрипта" (см. «Рис. 123»).

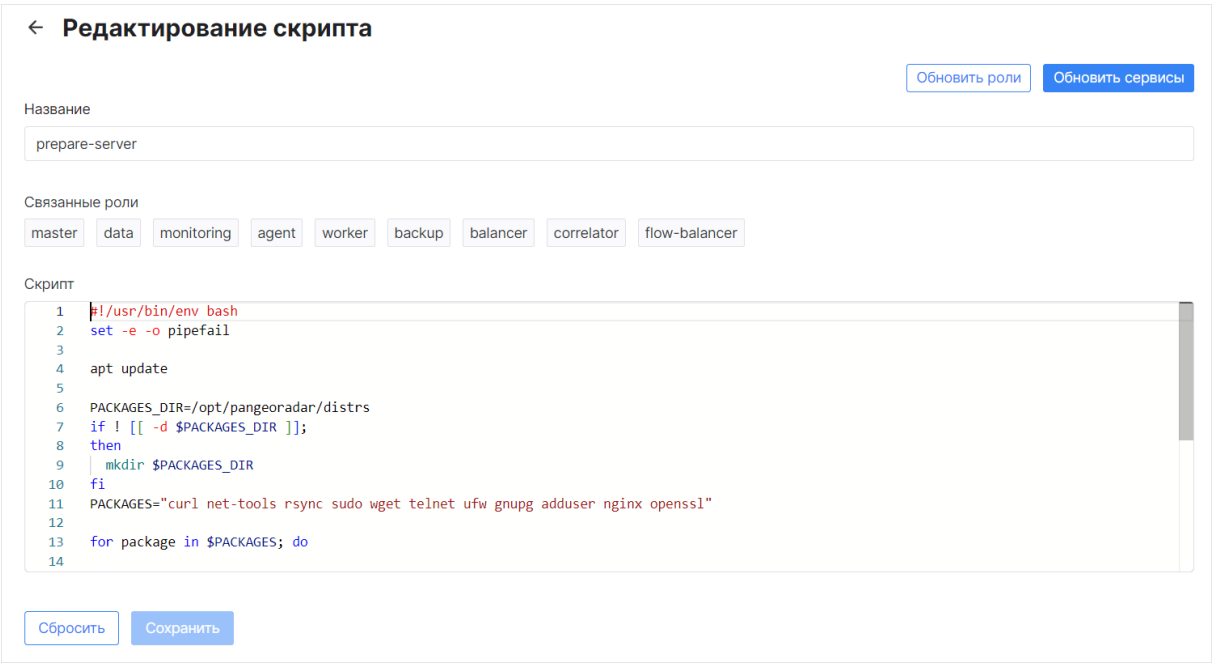


Рис. 123 – Окно "Редактирование скрипта"

2. Для настройки связи скрипта с серверными ролями платформы выполните следующие действия:

- нажмите кнопку **Обновить роли**. Откроется окно "Связанные роли" (см. «Рис. 124»);

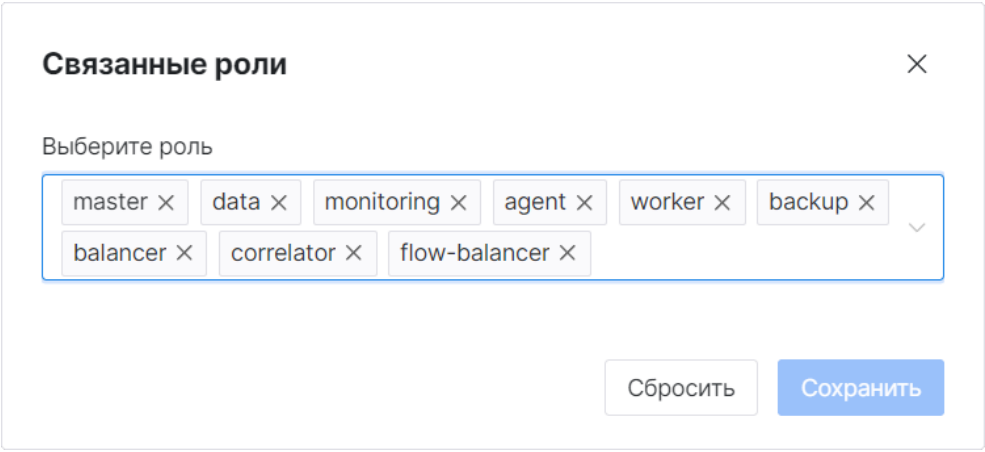


Рис. 124 – Окно "Связанные роли"

- в поле **Выберите роль** из выпадающего списка выберите серверные роли;
- нажмите кнопку **Сохранить**.

3. Для настройки связи скрипта с сервисами платформы выполните следующие действия:
    - нажмите кнопку **Обновить сервисы**. Откроется окно "Связанные сервисы" (см. «Рис. 125»);

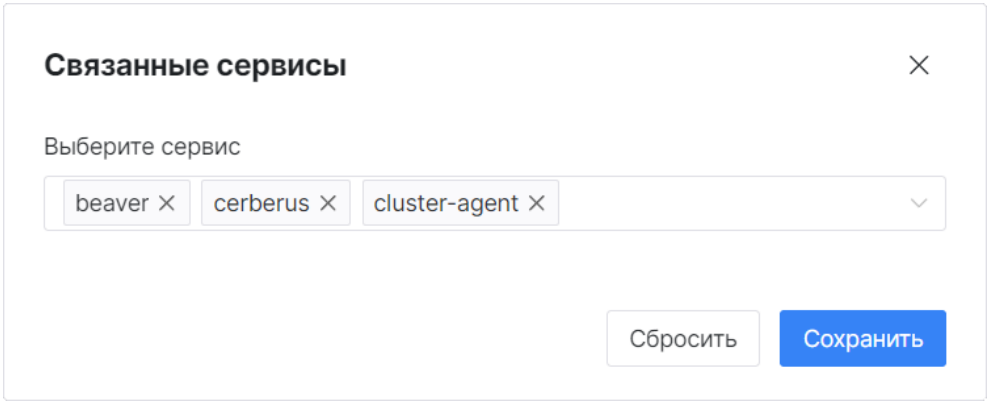


Рис. 125 – Окно "Связанные сервисы"

    - в поле **Выберите сервисы** из выпадающего списка выберите сервисы;
    - нажмите кнопку **Сохранить**.
4. Нажмите кнопку **Сохранить**.

10.6.3 Редактирование скрипта

1. Найдите нужный скрипт в списке на вкладке "Скрипты" и нажмите кнопку .
2. Измените информацию о скрипте.
3. Нажмите кнопку **Сохранить**.

10.6.4 Удаление скрипта

1. Найдите нужный скрипт в списке на вкладке "Скрипты" и нажмите кнопку .
2. Подтвердите удаление в открывшемся окне.

10.7 Управление мультиарендностью

Особенность архитектуры **Платформы Радар** позволяет работать в инфраструктуре мультитенант или мультиарендность.

Экземпляры платформы устанавливаются на инстансы, которые делятся на основной и подчиненные.

Основной инстанс может быть только один. Обычно через веб-интерфейс платформы основного инстанса, выполняется добавление подчиненных инстансов.

Работа с инстансами включает в себя следующие процессы:

1. «Добавление подчиненного инстанса».
2. «Изменение адреса авторизации подчиненного инстанса».
3. «Переключение между инстансами».

4. «Редактирование подчиненного инстанса».
5. «Удаление инстанса».

Управления инстансами выполняется в разделе **Администрирование** → **Кластер** → вкладка **Управление мультиарендностью** (см. «Рис. 126»).

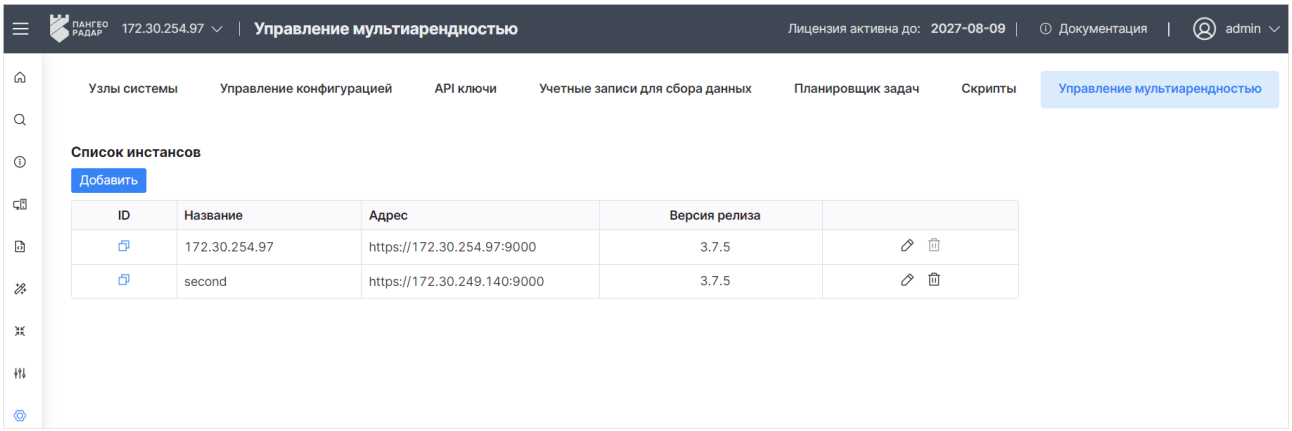


Рис. 126 – Раздел "Кластер". Вкладка "Управление мультиарендностью"

На вкладке отображается следующая информация:

- **Название** – название инстанса;
- **Адрес** – IP-адрес инстанса;
- **Версия релиза** – версия **Платформы Радар**, установленная на инстансе.

10.7.1 Добавление подчиненного инстанса

1. Нажмите кнопку **Добавить**. Откроется окно "Добавление инстанса" (см. «Рис. 127»).

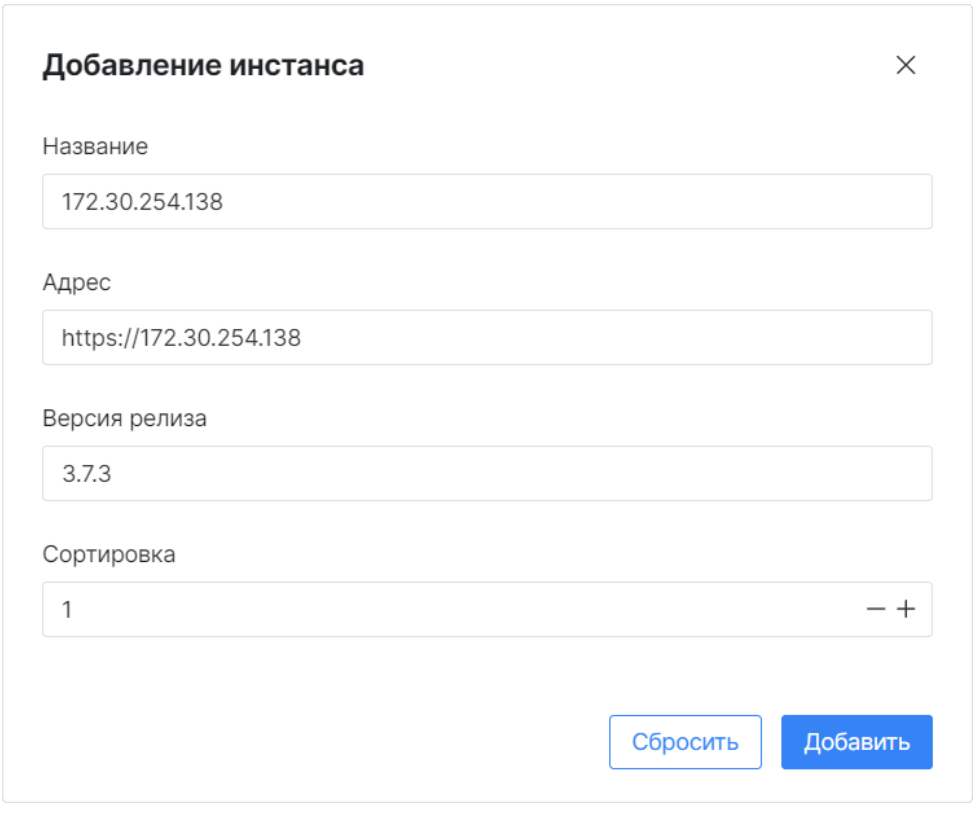


Рис. 127 – Окно "Добавление инстанса"

2. Укажите в окне информацию об инстансе:
    - в поле **Название** укажите наименование инстанса. Данное наименование будет отображаться при переключении между инстансами.
    - в поле **Адрес** укажите IP-адрес и при необходимости порт инстанса, на котором установлен экземпляр платформы;
    - в поле **Версия** релиза укажите номер установленной на инстансе версии платформы;
    - в поле **Сортировка** укажите порядковый номер инстанса. При переключении инстансов список будет формироваться в соответствии с заданной сортировкой.
3. Нажмите кнопку **Добавить**.

10.7.2 Изменение адреса авторизации подчиненного инстанса

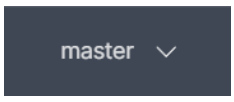
1. Перейдите в веб-интерфейс подчиненного инстанса.
2. Перейдите в раздел **Администрирование** → **Кластер** → вкладка **Управление конфигурацией**.
3. В свойствах **DNS** измените **Адрес сервиса авторизации** на url-адрес управляющего инстанса в формате https://<ip-адрес управляющего инстанса>:8180.

10.7.3 Переключение между инстансами

После добавления инстанса и изменения его адреса авторизации появится возможность переключиться на другой инстанс через веб-интерфейс управляющего инстанса.

Для этого в шапке сайта нажмите на кнопку с наименованием инстанса и из выпадающего списка выберите подчиненный инстанс.

Пример кнопки с наименованием инстанса:



10.7.4 Редактирование подчиненного инстанса

1. Найдите нужный инстанс в списке на вкладке "Управление мультиарендностью" и нажмите кнопку .
2. Измените информацию об инстансе.
3. Нажмите кнопку **Сохранить**.

10.7.5 Удаление инстанса

1. Найдите нужный инстанс в списке на вкладке "Управление мультиарендностью" и нажмите кнопку .
2. Подтвердите удаление в открывшемся окне.

11. Репутационные списки

Репутационные списки предназначены для обогащения событий данными. Репутационные списки можно сформировать, указав индикаторы компрометации.

Индикатор компрометации это наблюдаемый в сети или на конкретном устройстве объект (или активность), который с большой долей вероятности указывает на несанкционированный доступ к системе (то есть её компрометацию).

В качестве индикатора компрометации в репутационных списках могут выступать следующие данные:

- Домен-URL;
- IP;
- SSL хэш;
- Хэш файл.

Репутационные списки делятся на системные и пользовательские. Системные создаются автоматически по результатам работы сервиса **Ti**.

Управление репутационными списками выполняется в разделе **Администрирование** → **Репутационные списки**. Пример раздела приведен на «Рис. 128».

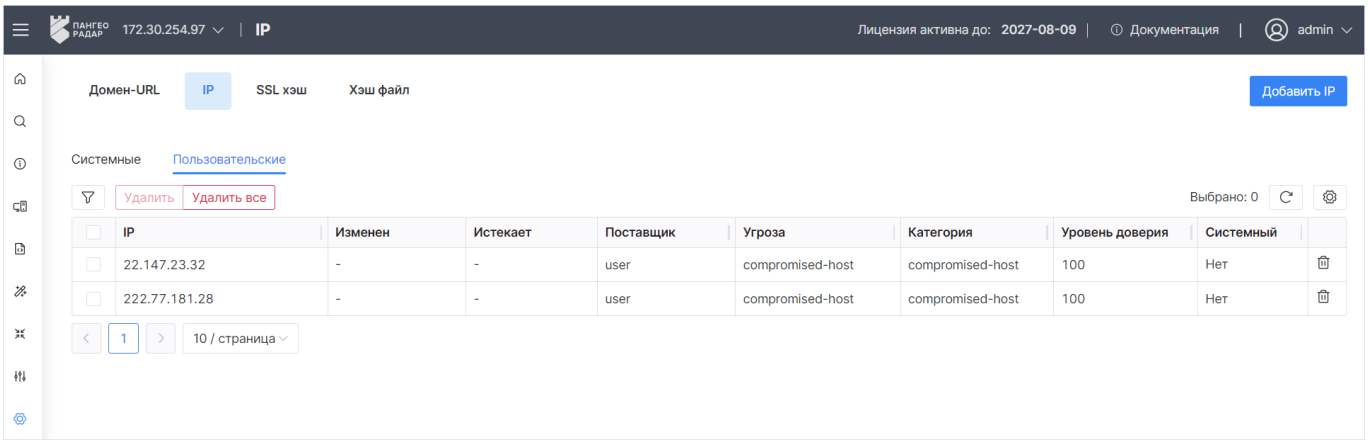


Рис. 128 – Раздел "Репутационные списки". Вкладка "IP"

В разделе информация разделена по соответствующим вкладкам. В общем случае в разделе отображается следующая информация:

- **Домен**, **IP**, **SSL** – индикатор компрометации. Отображаемый индикатор формируется в зависимости от выбранной вкладки;
- **Изменен** – дата и время изменения сведений об индикаторе компрометации;
- **Истекает** – дата и время устаревания индикатора компрометации. Например, если владелец сайта обнаруживает взлом и устраняет уязвимость, индикатор, который указывал на вредоносный домен неделю назад, может потерять свою актуальность;
- **Поставщик** – наименование поставщика, который предоставляет сведения об индикаторе компрометации. Например, **Alien Vault**, **Kaspersky** (подробнее см.

раздел «Источники IOC»). Если указано значение user, то это значит, что индикатор добавлен пользователем;

- **Угроза** – наименование угрозы;
- **Категория** – наименование категории, к которой относится угроза;
- **Уровень доверия** – это рейтинг индикатора компрометации, который рассчитывается с учётом характеристик источника данных и самого индикатора. Также при определении уровня доверия к индикатору учитывается **актуальность индикатора с течением времени**;
- **Системный** – добавлены ли сведения об индикаторе безопасности системой: да, нет;
- **URL** (только для вкладки **Домен**) – адрес URL скомпрометированного домена;
- **Алгоритмы хэширования MD5, SHA1, SHA256.** (только для вкладки **Хэш файл**) – значение индикатора компрометации по соответствующему алгоритму хэширования.

11.1 Добавление индикатора компрометации "Домен-URL"

1. Перейдите на вкладку "Домен-URL" и нажмите кнопку **Добавить домен-URL**. Откроется окно "Создание домена-URL" (см. «Рис. 129»).

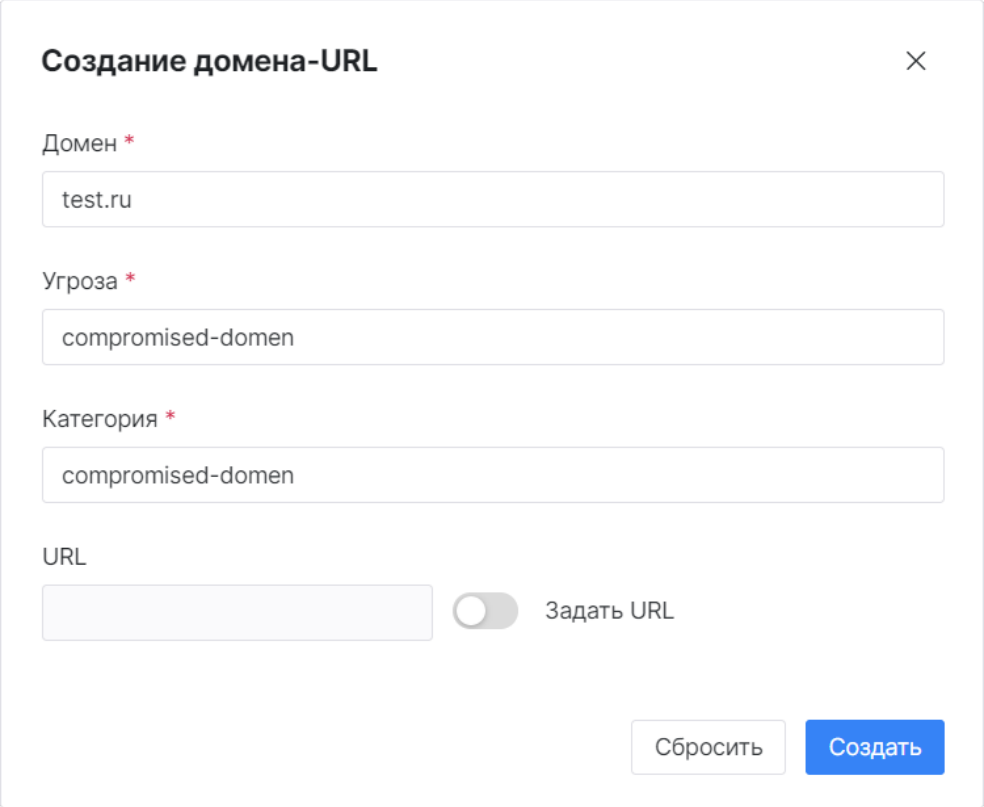


Рис. 129 – Окно "Создание домена-URL"

2. Укажите в окне следующую информацию:
   - в поле **Домен** укажите скомпрометированный домен;
   - в поле **Угроза** укажите наименование потенциальной угрозы, которая может возникнуть в результате компрометации домена;

- в поле **Категория** укажите категорию, к которой относится угроза;
- в поле **URL** при необходимости включите переключатель **Задать URL** и укажите значение скомпрометированного URL домена.

3. Нажмите кнопку **Создать**.

11.2 Добавление индикатора компрометации "IP"

1. Перейдите на вкладку "IP" и нажмите кнопку **Добавить IP**. Откроется окно "Создание IP записи" (см. «Рис. 130»).

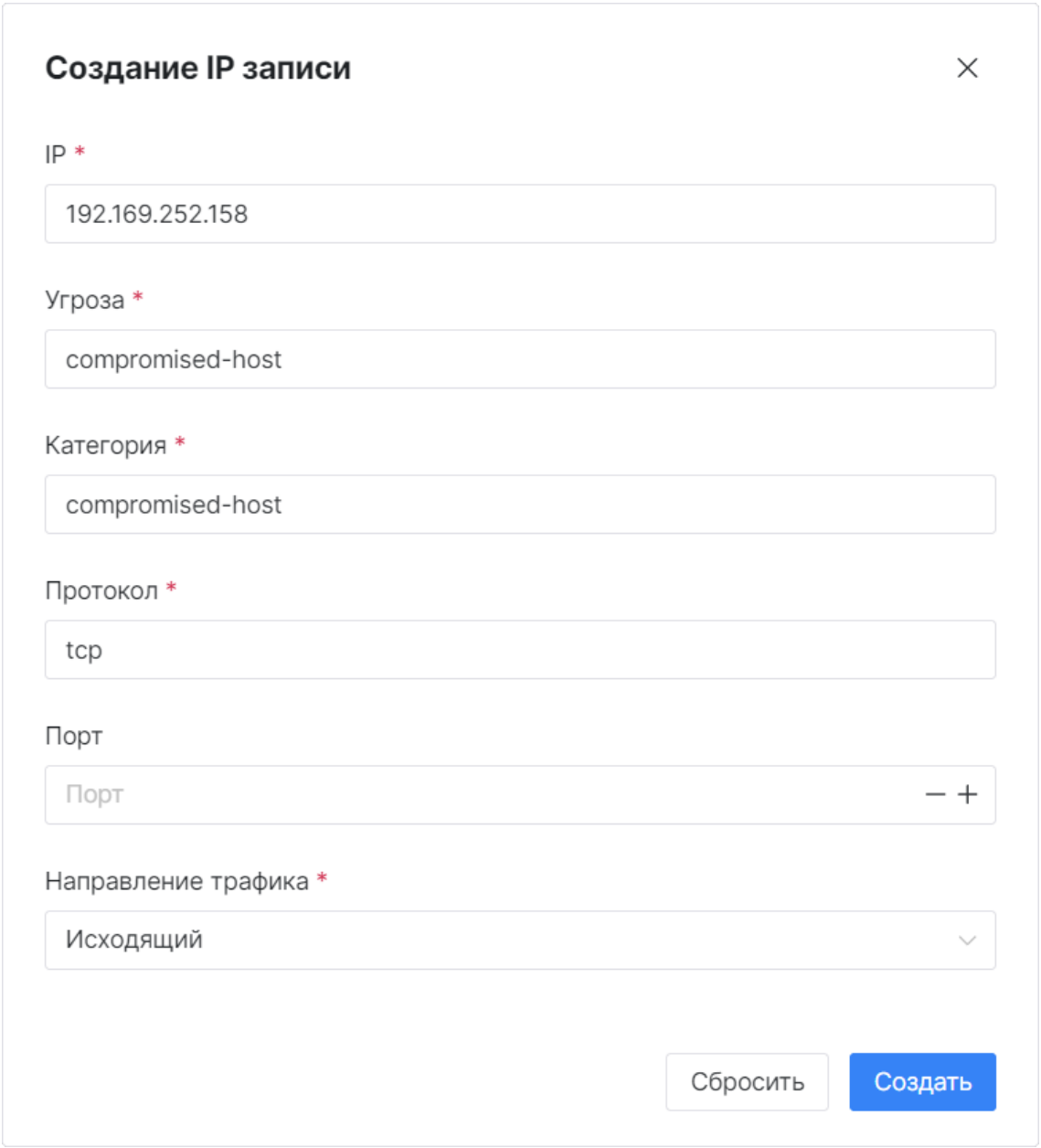


Рис. 130 – Окно "Создание IP записи"

2. Укажите в окне следующую информацию:
   - в поле **IP** укажите скомпрометированный IP-адрес;
   - в поле **Угроза** укажите наименование потенциальной угрозы, которая может возникнуть в результате компрометации IP-адреса;

- в поле **Категория** укажите категорию, к которой относится угроза;
- в поле **Протокол** укажите протокол соединения с IP-адресом;
- в поле **Порт** при необходимости укажите конкретный порт, на котором произошла компрометация;
- в поле **Направление трафика** из выпадающего списка выберите направление потока данных.

3. Нажмите кнопку **Создать**.

11.3 Добавление индикатора компрометации "SSL хэш"

1. Перейдите на вкладку "SSL хэш" и нажмите кнопку **Добавить ssl-хэш**. Откроется окно "Создание ssl-хэша" (см. «Рис. 131»).

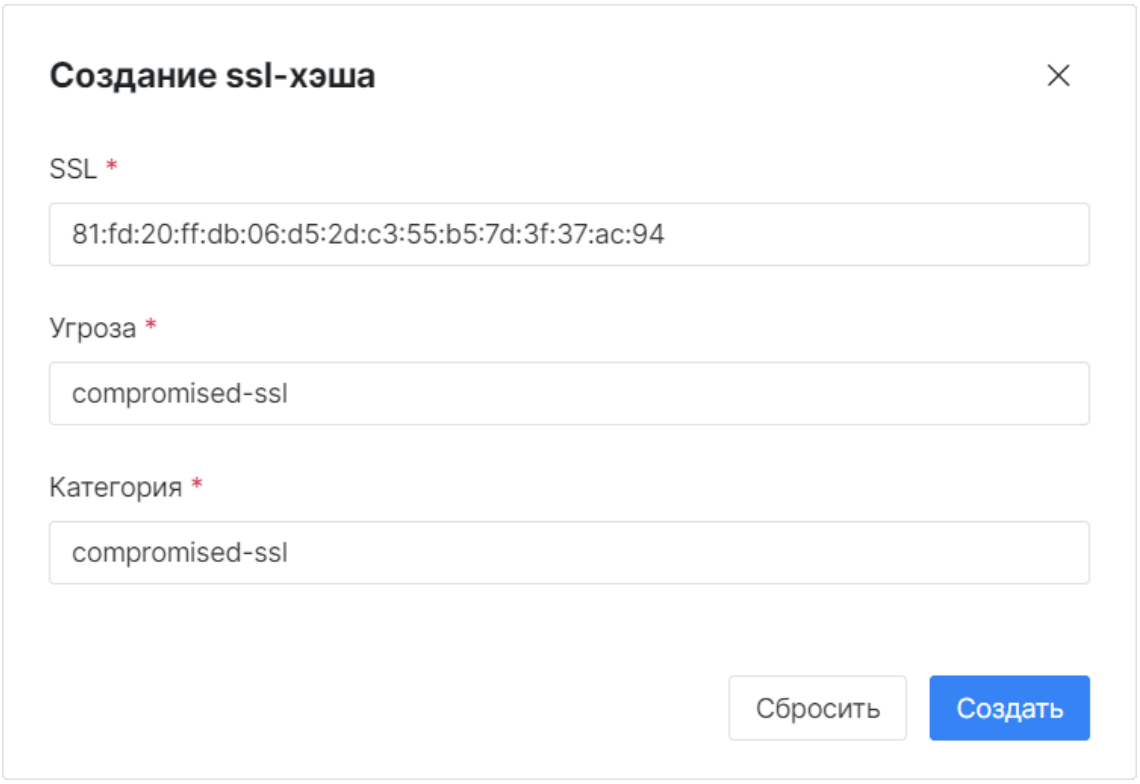


Рис. 131 – Окно "Создание ssl-хэша"

2. Укажите в окне следующую информацию:
   - в поле **SSL** укажите хэш значение скомпрометированного SSL-сертификата;
   - в поле **Угроза** укажите наименование потенциальной угрозы, которая может возникнуть в результате компрометации сертификата;
   - в поле **Категория** укажите категорию, к которой относится угроза.
3. Нажмите кнопку **Создать**.

11.4 Добавление индикатора компрометации "Хэш файл"

1. Перейдите на вкладку "SSL хэш" и нажмите кнопку **Добавить хэш файл**. Откроется окно "Создать пользовательский файл" (см. «Рис. 132»).

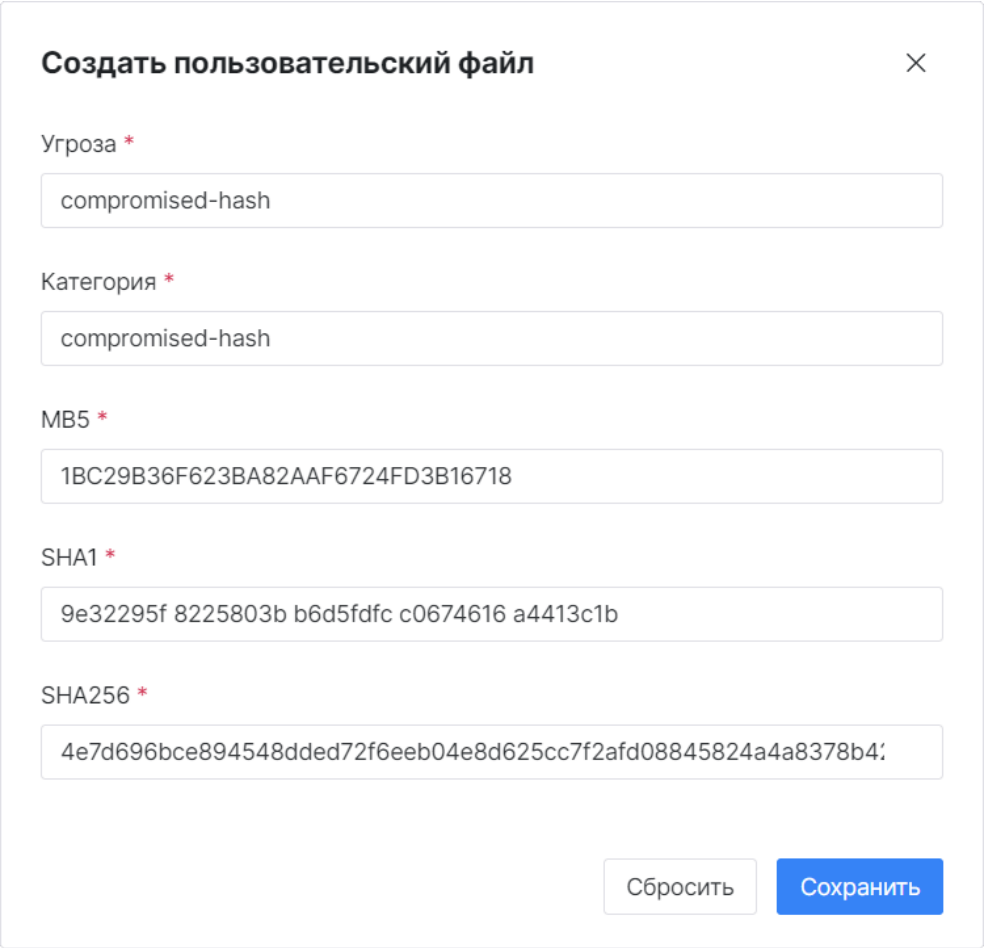


Рис. 132 – Окно "Создать пользовательский файл"

2. Укажите в окне следующую информацию:
   - в поле **Угроза** укажите наименование потенциальной угрозы, которая может возникнуть в результате компрометации файла;
   - в поле **Категория** укажите категорию, к которой относится угроза.
   - в поле **MD5** укажите хэш значение скомпрометированного файла по алгоритму "MD5";
   - в поле **SHA1** укажите хэш значение скомпрометированного файла по алгоритму "SHA1";
   - в поле **SHA256** укажите хэш значение скомпрометированного файла по алгоритму "SHA256";
3. Нажмите кнопку **Создать**.

11.5 Удаление индикатора компрометации

1. Перейдите на нужную вкладку: "Домен-URL", "IP", "SSL хэш", "Хэш файл".
2. Выберите тип индикатора компрометации: системный или пользовательский.
3. В строке нужного индикатора компрометации нажмите кнопку .
4. Подтвердите удаление в открывшемся окне.

12. Источники IOC

Источники IOC – это поставщики индикаторов компрометации, которые используются при работе репутационных списков (см. раздел «Репутационные списки»).

Индикатор компрометации (IOC) является свидетельством того, что кто-то мог создать брешь в сети организации. Эти данные экспертизы не просто указывают на потенциальную угрозу. Они сигнализируют, что уже произошла атака, например проникновение вредоносных программ, компрометация учетных сведений или кража данных.

Индикаторами компрометации могут выступать, например, IP-адрес или доменное имя узла, на котором зарегистрирована подозрительная активность, хеш-сумма вредоносного файла.

Источники IOC собирают информацию об индикаторах компрометации из открытых баз данных, которые предоставляются такими компаниями как **Alien Vault**, **Kaspersky** и т.д. Затем передают полученные сведения в репутационные списки.

Источники IOC делятся на системные и пользовательские.

Системные источники IOC необходимы для корректной работы платформы, поэтому их нельзя изменить или удалить.

При настройке пользовательских источников IOC можно настроить формат сопоставления данных. Это необходимо для корректной передачи индикаторов компрометации в репутационные списки. Формат сопоставления может быть настроен, как и для стандартной формы (обычно это CSV файл), так и для формы с дополнительными параметрами.

Поскольку базы данных постоянно обновляются, **Платформа Радар** позволяет настроить периодичность получения индикаторов компрометации.

Работа с источниками IOC включает в себя следующие процессы:

1. «Создание источника IOC».
2. «Просмотр источника IOC».
3. «Редактирование источника IOC».
4. «Изменение состояния источника IOC».
5. «Запуск и остановка источников IOC».
6. «Настройка периода запуска источников IOC».
7. «Удаление источников IOC».

Для работы с источниками IOC перейдите **Администрирование** → **Источники IOC** (см. «Рис. 133»).

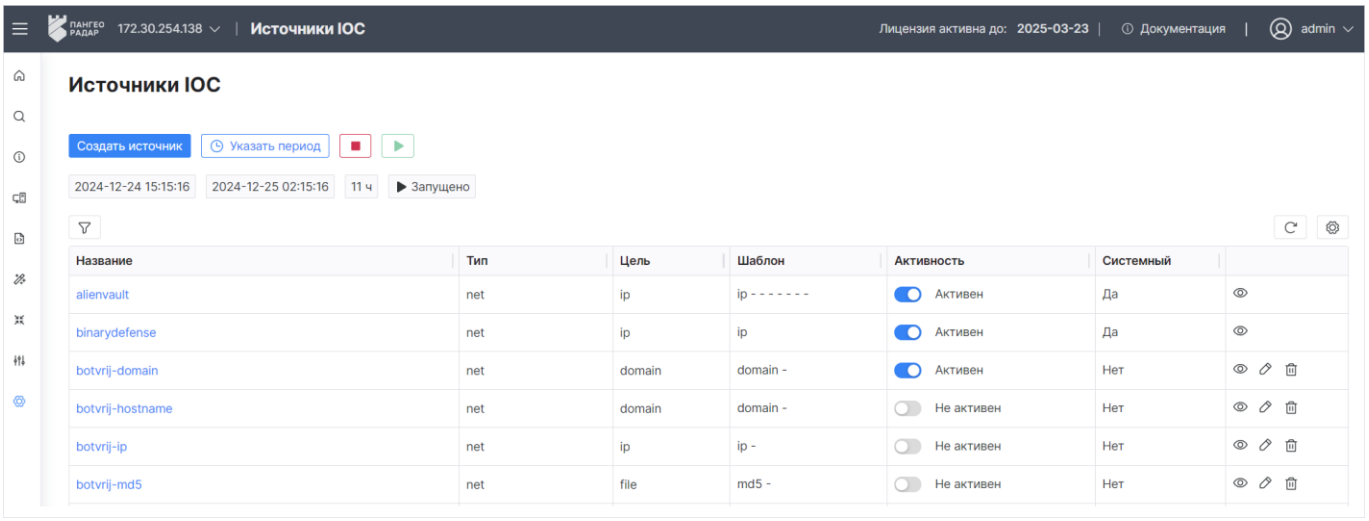


Рис. 133 – Раздел "Источники IOC"

В разделе отображается следующая информация:

- **Название** – наименование источника IOC в платформе;
- **Тип** – тип источника компрометации. По умолчанию в платформе доступен тип "NET" (аномалии трафика);
- **Цель** – потенциальная цель атаки: IP-адрес, доменное имя узла, хеш-сумма файла;
- **Шаблон** – шаблон, по которому будут извлекаться данные из открытых баз данных и передаваться в репутационные списки;
- **Активность** – состояние источника, которое показывает используется ли источник для передачи индикаторов компрометации в репутационные списки. Может принимать следующие значения: Активен, Не активен;
- **Системный** – является ли источник системным: да, нет.

При работе с источниками IOC доступны следующие элементы управления:

Кнопка	Действие
	просмотр информации об источнике IOC
	редактирование источника IOC
	удаление источника IOC
	запустить все активные источники для получения/обновления индикаторов компрометации
	остановить получение/обновление индикаторов компрометации всеми активными источниками
Указать период	настроить период автоматического запуска и остановки всех активных источников для получения/обновления индикаторов компрометации
Создать источник	создание пользовательского источника IOC

12.1 Создание источника IOC

1. Нажмите кнопку **Создать**. Откроется форма "Создать источник" (см. «Рис. 134»).

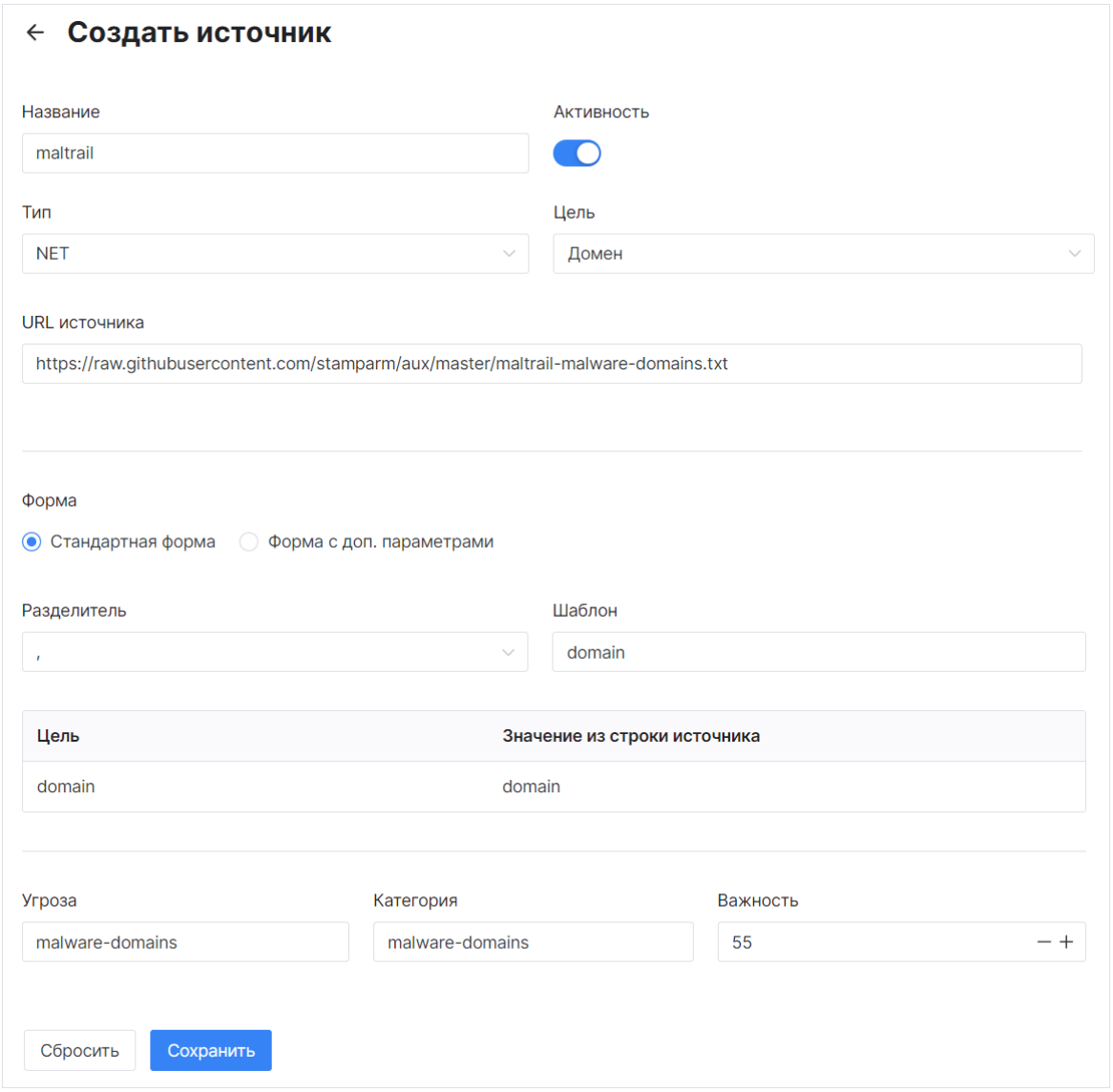


Рис. 134 – Форма "Создать источник"

2. Укажите в окне информацию об источнике:

   - в поле **Название** укажите наименование источника в платформе. В разделе «Репутационные списки» наименование источника будет отображать в графе **Поставщик**;
   - установите переключатель **Активность** в положение "Включен" если необходимо использовать источник для передачи индикаторов компрометации в репутационные списки;
   - в поле **Тип** из выпадающего списка выберите тип источника IOC;
   - в поле **Цель** из выпадающего списка выберите потенциальную цель атаки;
   - в поле **URL источника** укажите адрес, на котором располагается база данных индикаторов компрометации;

- в зависимости от указанной базы данных индикаторов компрометации, настройте параметры сопоставления данных при передаче в репутационные списки:
    - для стандартной формы (см. пункт 3);
    - для формы с дополнительными параметрами (см. пункт 4).
- в поле **Угроза** укажите наименование потенциальной угрозы, которая может возникнуть в результате компрометации;
- в поле **Категория** укажите категорию, к которой относится угроза;
- в поле **Важность** укажите числовой показатель важности угрозы. Данный показатель будет учитываться в процессе создания инцидента и будет влиять на показатель "срочность инцидента"

3. Для стандартной формы исходника индикаторов компрометации укажите следующие данные:
    - в поле **Разделитель** из выпадающего списка выберите способ разделения колонок исходника;
    - в поле **Шаблон** укажите шаблон, по которому будут извлекаться значения из строки источника. Например, шаблон ip - - - - - - будет означать, что будет извлекаться параметр IP-адрес из первой колонки.
4. Для нестандартной формы исходника индикаторов компрометации в поле **Форма** выберите вариант "Форма с доп. параметрами". На форме создания источника IOC появятся дополнительные поля для заполнения (см. «Рис. 135»).

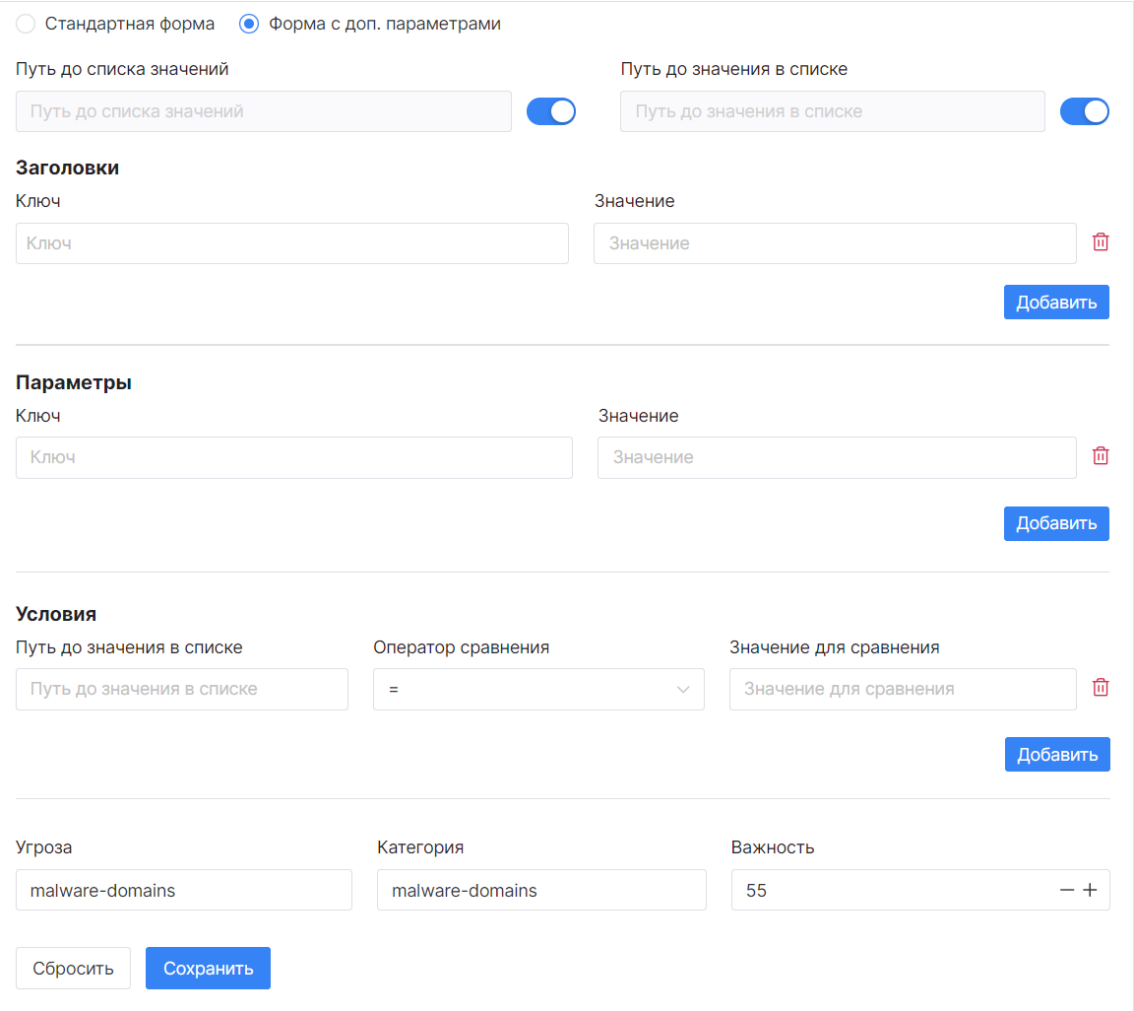


Рис. 135 – Форма "Создать источник". Настройка формы исходника с доп. параметрами

Укажите на форме следующую информацию:

- При необходимости укажите путь до исходника со списком значений индикаторов компрометации и соответствующий путь до значения в списке. Для этого активируйте соответствующие переключатели и укажите нужные пути;
- Добавьте и укажите необходимо количество пар "Ключ-Значение" для сопоставления **заголовков** и **параметров** из списка значений индикаторов компрометации;
- Добавьте и настройте необходимое количество условий сравнения для значений в списке:
    - в поле **Путь до значения** укажите путь до значения в списке значений индикаторов компрометации;
    - в поле **Оператор сравнения** выберите один из операторов, по которому будет выполняться сравнение: "равно", "не равно";
    - в поле **Значение для сравнения** укажите значение, с которым будет выполняться сравнение значения из списка.

5. Нажмите кнопку **Сохранить**.

12.2 Просмотр источника IOC

Для просмотра источника IOC нажмите по ссылке с наименованием источника или кнопку в соответствующей строке (см. «Рис. 136»).

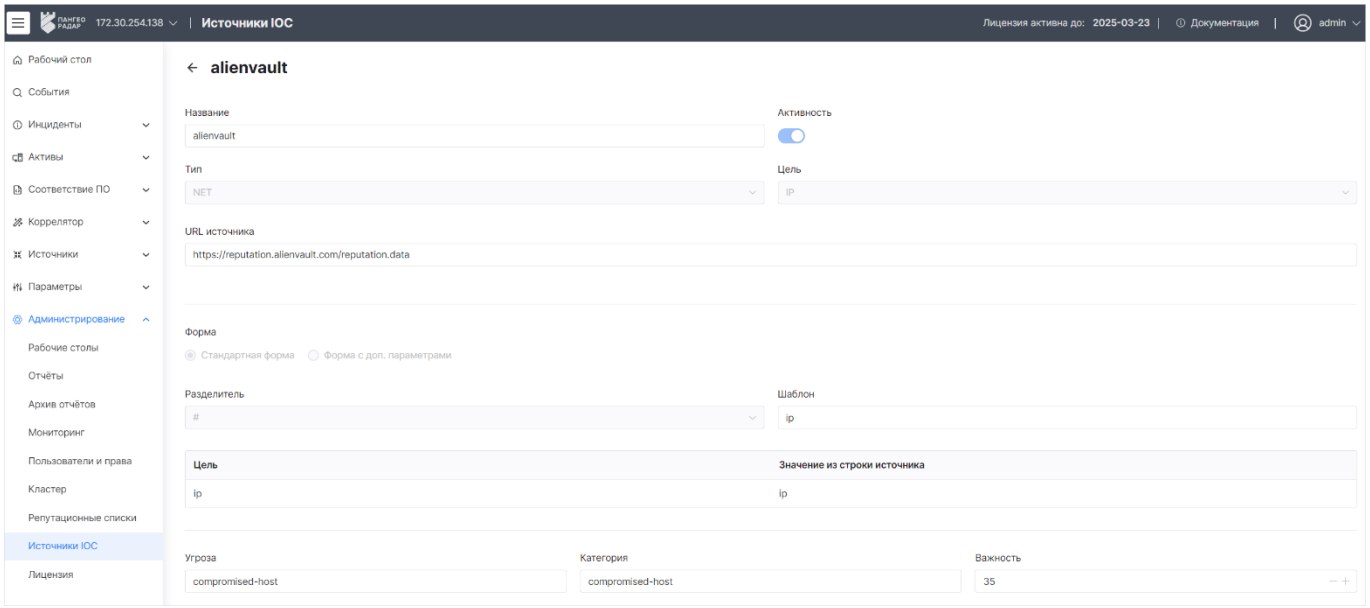


Рис. 136 – Форма "Просмотр источника IOC"

Набор данных, отображаемых на форме просмотра источника IOC, аналогичен данным, которые указываются при его создании.

12.3 Редактирование источника IOC

1. В строке нужного источника IOC нажмите кнопку .
2. Измените информацию об источнике IOC.
3. Нажмите кнопку **Сохранить**.

12.4 Изменение состояния источника IOC

Состояние источника показывает используется ли источник для передачи индикаторов компрометации в репутационные списки. Может принимать следующие значения:

- Активен – источник передает индикаторы компрометации в репутационные списки
- Не активен – не передает.

Изменение состояния источника IOC можно выполнить следующими способами:

Способ 1. Используйте переключатель в графе **Активен** на основной странице раздела.

Способ 2. Используйте переключатель **Активность** на формах создания/редактирования источника IOC.

12.5 Запуск и остановка источников IOC

Процедура запуска источников IOC служит для получения/обновления индикаторов компрометации из исходников.

Для запуска процесса нажмите кнопку .

Для остановки процесса нажмите кнопку .

Текущее состояние процесса отображается на основной странице раздела над таблицей со списком источников IOC (см. «Рис. 136»).

12.6 Настройка периода запуска источников IOC

Чтобы не обновлять информацию об индикаторах компрометации вручную, платформа позволяет настроить периодичность запуска данного процесса.

Для этого выполните следующие действия:

1. Нажмите кнопку **Указать период**. Откроется окно "Изменение периода запуска" (см. «Рис. 137»).

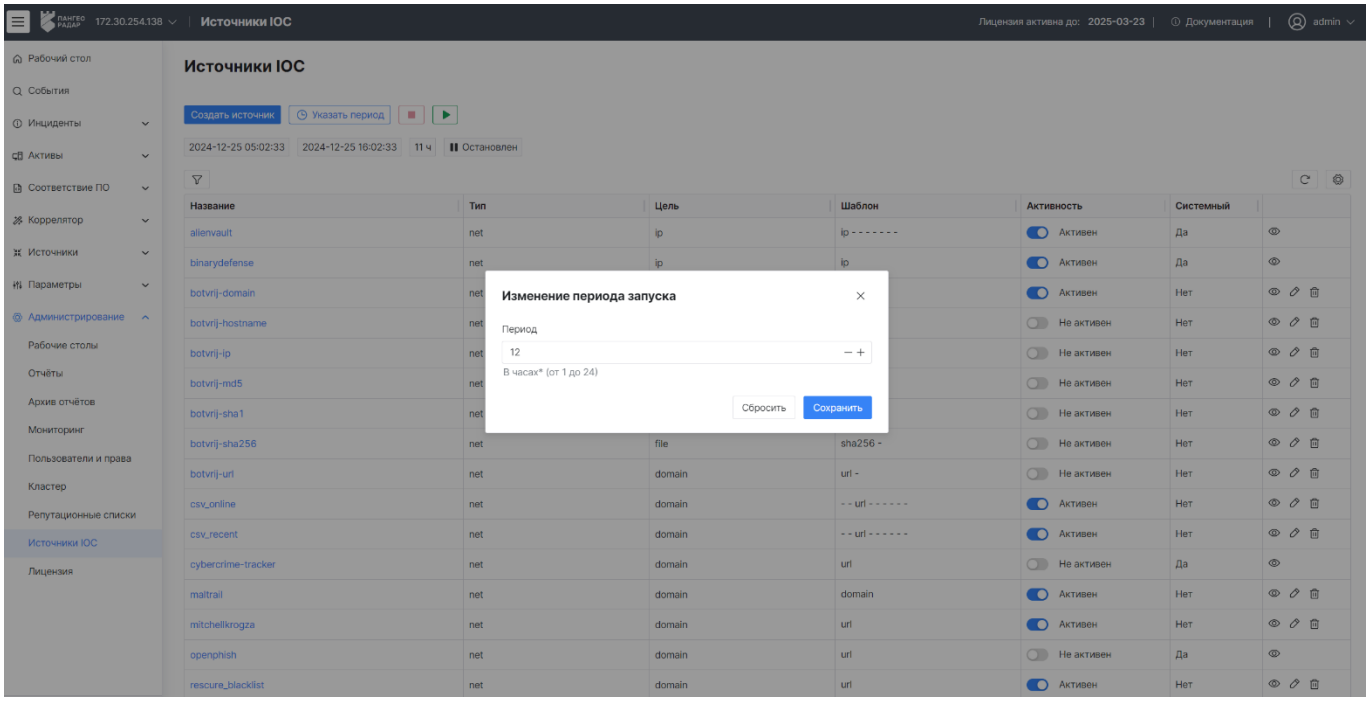


Рис. 137 – Окно "Изменение периода запуска"

2. В окне укажите количество часов (от 1-го до 24-х), по истечении которых будет запускаться процесс получения/обновления источников компрометации.
3. Нажмите кнопку **Сохранить**.

12.7 Удаление источников IOC

1. В строке нужного источника нажмите кнопку .
2. Подтвердите удаление в открывшемся окне.

13. Лицензия

Раздел интерфейса **Лицензия** предназначен для просмотра параметров лицензии и повторной активации лицензии.

Пример раздела приведен на «Рис. 138».

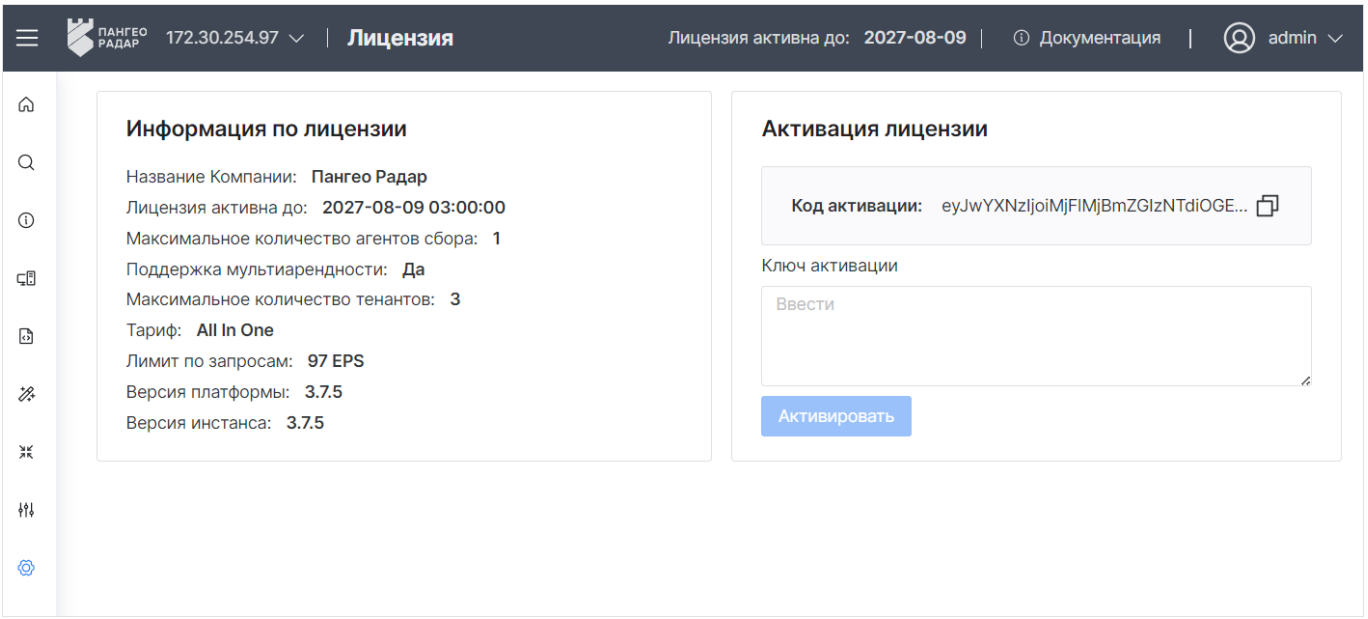


Рис. 138 – Раздел "Лицензия"

В блоке **Информация по лицензии** отображается следующая информация:

- **Название компании** – наименование компании, которой выдана лицензия;
- **Лицензия активна до** –- срок активности лицензии, по истечении которого, если не будет получена новая лицензия, не будет доступен интерфейс **Платформы Радар**, за исключением текущего раздела;
- **Максимальное количество агентов сбора** – максимальное количество агентов сбора журналов с источников;
- **Поддержка мультиарендности** – включена ли в состав лицензии поддержка режима мультиарендности: да, нет.
- **Максимальное количество тенантов** – максимальное количество экземпляров **Платформы Радар**, которые можно установить в режиме мультиарендности;
- **Тариф** – наименование тарифа;
- **Лимит по запросам** – ограничение по количеству запросов в EPS;
- **Версия платформы** – версия платформы, активированная по данной лицензии;
- **Версия инстанса** – версия экземпляра платформы, установленного на данном инстансе.

В блоке **Активация лицензии** выполняется повторная активация лицензии:

1. Скопируйте код активации. Для этого достаточно кликнуть по соответствующему полю. Рекомендуется сохранить скопированный код в текстовый файл.
2. Перейдите в личный кабинет клиентского портала **Платформы Радар** (см. «Рис. 139»).

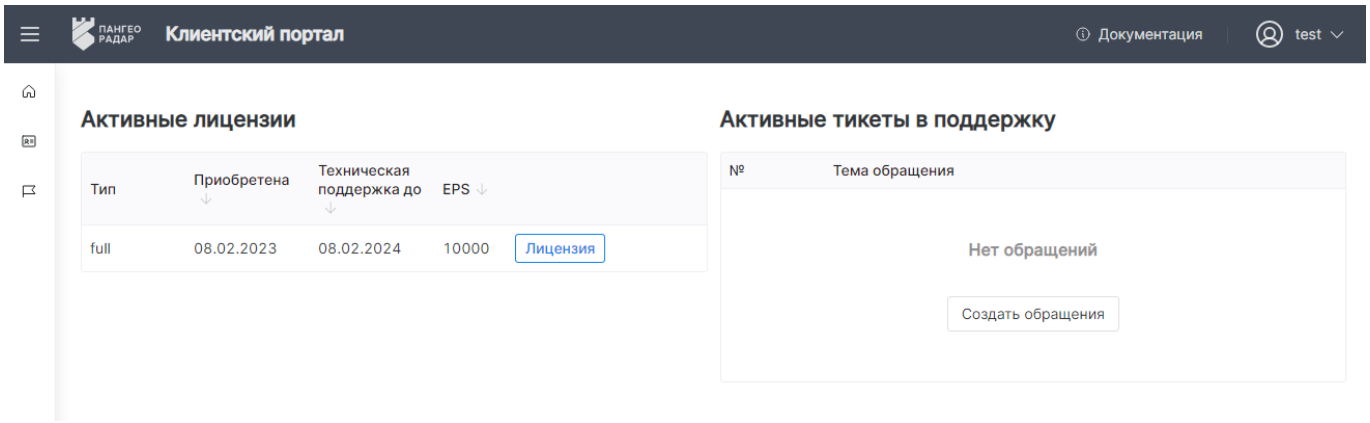


Рис. 139 -- Клиентский портал Платформы Радар

3. Нажмите кнопку **Создать обращение**.
4. В обращении опишите причину и вставьте ранее скопированный код активации.
5. Дождитесь ответа от службы технической поддержки **Платформы Радар** по результатам которого вам будет выдан Ключ активации.
6. В разделе "Лицензия" (см. «Рис. 138») укажите ключ активации в соответствующем поле и нажмите кнопку **Активировать**.

14. Сообщения

Платформа Радар поддерживает обмен сообщений между пользователями платформы.

Например, при изменении информации об инцидентах или активах можно **написать ответственному**. Сообщения, отправленные подобным образом, отображаются в разделе **Сообщения**. Доступна возможность написать другому пользователю, из данного раздела.

Работа с сообщениями включает в себя следующие процессы:

- «Создание сообщения»;
- «Просмотр сообщения»;
- «Ответ на сообщение»;
- «Отметить сообщения прочитанными»;
- «Отметить прочитанные сообщения как непрочитанные»;
- «Экспорт сообщений»;
- «Удаление сообщений».

Для работы с сообщениями нажмите на наименование учетной записи в правом верхнем углу и выберите пункт **Сообщения**. Откроется страница "Сообщения" (см. «Рис. 140»).

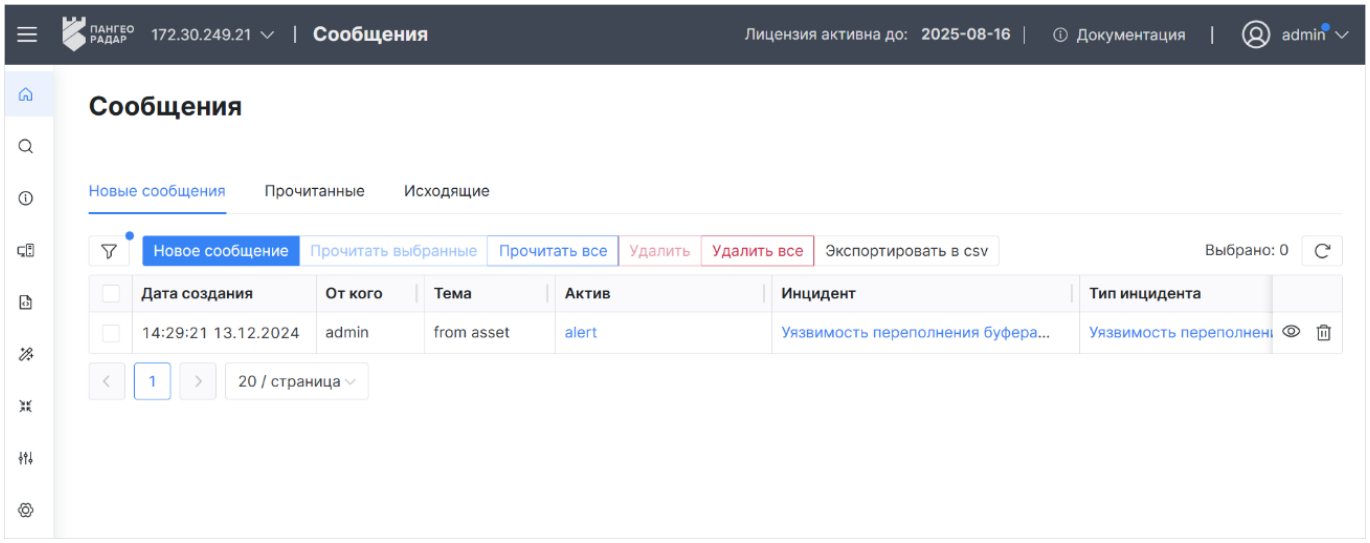


Рис. 140 – Раздел "Сообщения"

Примечание: *если есть непрочитанные сообщения, то рядом с учетной записью появится индикатор* 🔵.

Сообщения в разделе разделены по следующим вкладкам:

- **Новые сообщения** – список новых сообщений;
- **Прочитанные** – список прочитанных сообщений;
- **Исходящие** – список исходящих сообщений.

На вкладках отображается следующая информация:

- **Дата создания** – дата и время создания сообщения;
- **От кого/Кому** – адресант/адресат сообщения;
- **Тема** – тема сообщения;
- **Актив** – наименование актива, при изменении информации о котором было создано сообщение. По ссылке откроется страница просмотра актива;
- **Инцидент** – наименование инцидента, при изменении информации о котором было создано сообщение. По ссылке откроется страница просмотра инцидента;
- **Тип инцидента** – наименование типа инцидента. По ссылке откроется страница просмотра типа инцидента.

14.1 Создание сообщения

1. Нажмите кнопку **Новое сообщение**. Откроется окно "Новое сообщение" (см. «Рис. 141»)

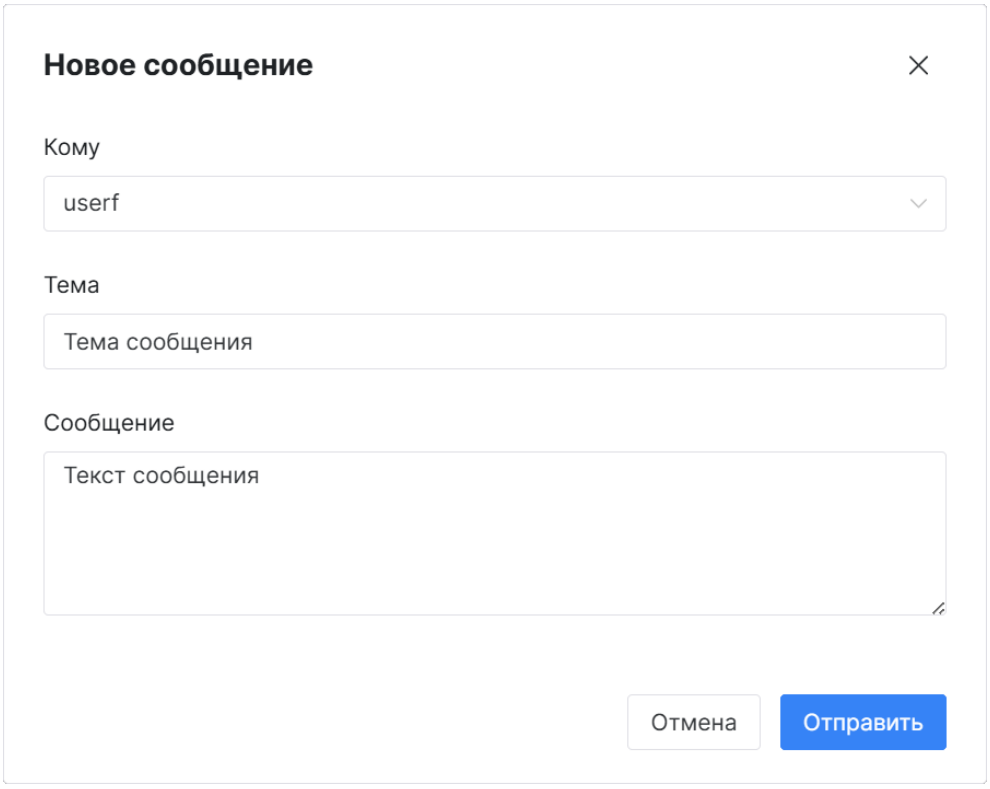


Рис. 141 – Окно "Новое сообщение"

2. Укажите в окне следующую информацию:
   - в поле **Кому** из выпадающего списка выберите адресата сообщения;
   - в поле **Тема** укажите тему сообщения;
   - в поле **Сообщение** укажите текст сообщения.
3. Нажмите кнопку **Отправить**.

14.2 Просмотр сообщения

1. В строке нужного сообщения нажмите кнопку . Откроется окно "Просмотр сообщения" (см. «Рис. 142»).

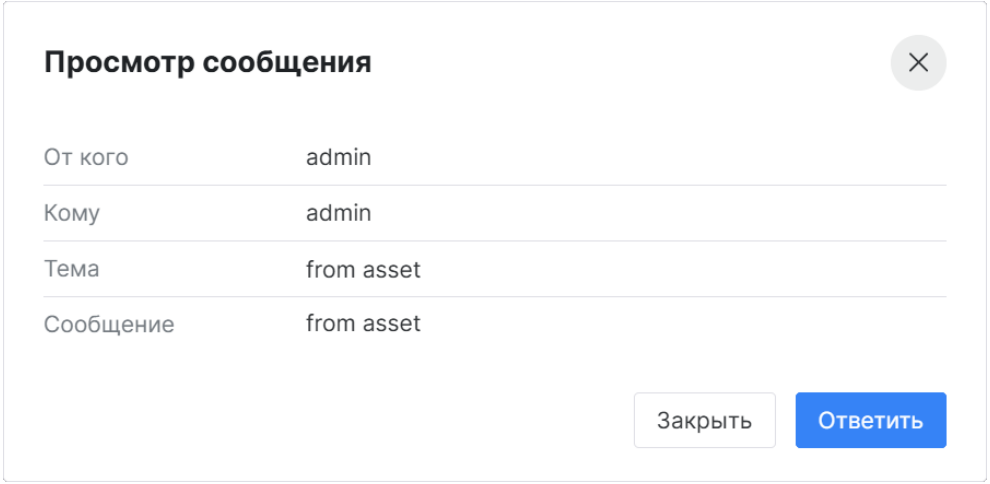


Рис. 142 – Окно "Просмотр сообщения"

2. Если сообщение было просмотрено из вкладки "Новые сообщения", то оно сменит статус на "прочитано" и автоматически переместиться на соответствующую вкладку.

14.3 Ответ на сообщение

1. Откройте сообщение на просмотр (см. «Рис. 142») и нажмите кнопку **Ответить**. Откроется окно "Новое сообщение" (см. «Рис. 141»).
2. Укажите в окне необходимую информацию и нажмите кнопку **Отправить**.

14.4 Отметить сообщения прочитанными

Действие выполняется на вкладке **Новые сообщения**.

Чтобы отметить все новые сообщения прочитанными, нажмите кнопку **Прочитать все**.

Чтобы отметить конкретные сообщения прочитанными, установите нужные флаги и нажмите кнопку **Прочитать выбранные**.

14.5 Отметить прочитанные сообщения как непрочитанные

Действие выполняется на вкладке **Прочитанные**.

Чтобы отметить все прочитанные сообщения не прочитанными, нажмите кнопку **Пометить все непрочитанным**.

Чтобы отметить конкретные сообщения непрочитанными, установите нужные флаги и нажмите кнопку **Пометить выбранные как непрочитанные**.

14.6 Экспорт сообщений

1. Перейдите на нужную вкладку.
2. Нажмите на кнопку **Экспортировать в csv**.

3. Будет сформирован документ в формате .csv.
4. Нажмите кнопку **Скачать** и укажите путь для сохранения файла.

14.7 Удаление сообщений

Для удаления сообщения нажмите кнопку  в соответствующей строке.

Для удаление всех сообщений с выбранной вкладки нажмите кнопку **Удалить все**.

Для удаления конкретных сообщений, установите нужные флаги и нажмите кнопку **Удалить**.

15. Профиль пользователя

В разделе пользователю доступны следующие действия:

- «Изменение информации о своей учетной записи»;
- «Изменение пароля»;
- «Подключение аутентификатора»;
- «Выход из всех сессий»;
- «Просмотр журнала изменений учетной записи»;
- «Настройка оповещений»;
- «Просмотр истории действий в платформе».

Для перехода в профиль пользователя нажмите на наименование учетной записи в правом верхнем углу и выберите пункт **Профиль**. Откроется страница "Профиль" (см. «Рис. 143»).

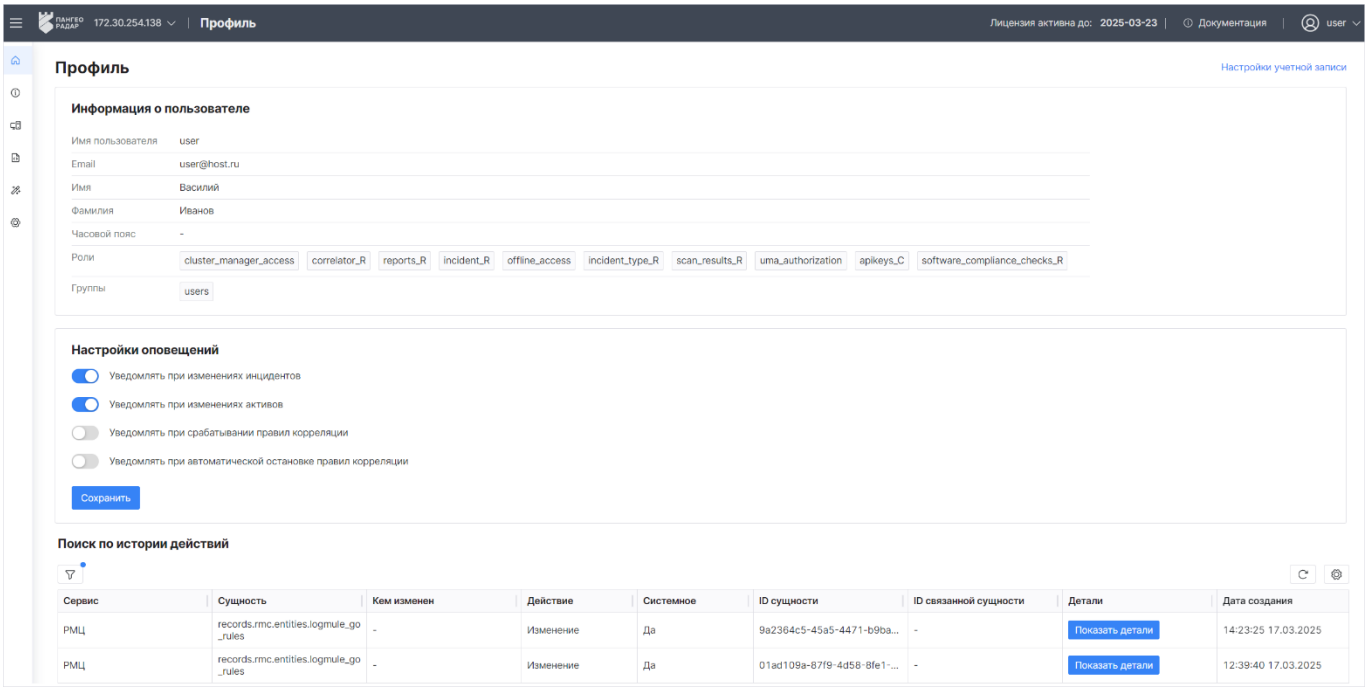


Рис. 143 – Раздел "Профиль"

Информация в разделе отображается в следующих блоках:

- **Информация о пользователе** – в блоке отображаются персональные данные пользователя:
  - логин для входа в платформу;
  - адрес электронной почты;
  - имя пользователя;
  - фамилия пользователя;
  - часовой пояс;

- список ролей, которые назначены пользователю;
- список групп, в которые добавлен пользователь.

- **Настройка оповещений** – в блоке выполняется настройка оповещений;
- **Поиск по истории действий** – в блоке выполняется поиск и просмотр истории действий в платформе.

15.1 Изменение информации о своей учетной записи

1. Перейдите в профиль пользователя.
2. Нажмите кнопку **Настройки учетной записи**. Откроется форма "Изменение учетной записи" (см. «Рис. 144»).

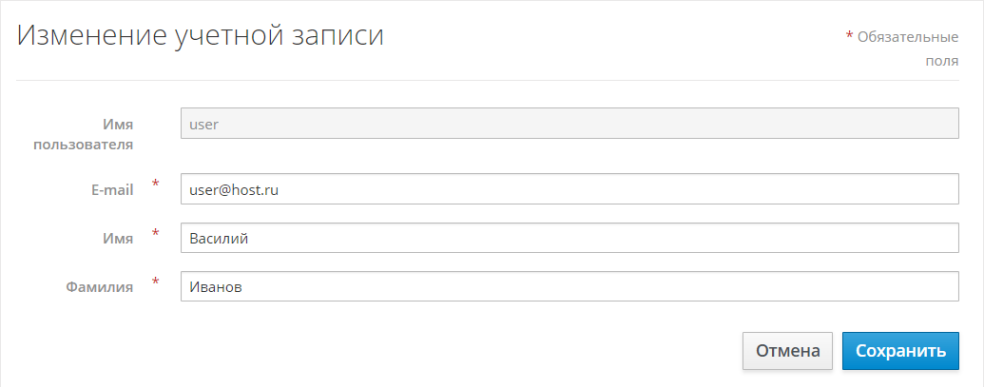


Рис. 144 – Форма "Изменение учетной записи"

3. Укажите в окне следующую информацию:
   - в поле **E-mail** измените адрес электронной почты;
   - в полях **Имя** и **Фамилия** измените соответствующие данные пользователя.
4. Нажмите кнопку **Сохранить**.

15.2 Изменение пароля

1. Перейдите в профиль пользователя.
2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Пароль**. Откроется форма "Смена пароля" (см. «Рис. 145»).

Рис. 145 – Форма "Смена пароля"

3. Укажите в окне следующую информацию:
    - в поле **Пароль** укажите текущий пароль;
    - в полях **Новый пароль** и **Подтверждение пароля** укажите новый пароль.
4. Нажмите кнопку **Сохранить**.

15.3 Подключение аутентификатора

1. Перейдите в профиль пользователя.
2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Аутентификатор**. Откроется форма "Смена пароля" (см. «Рис. 146»).

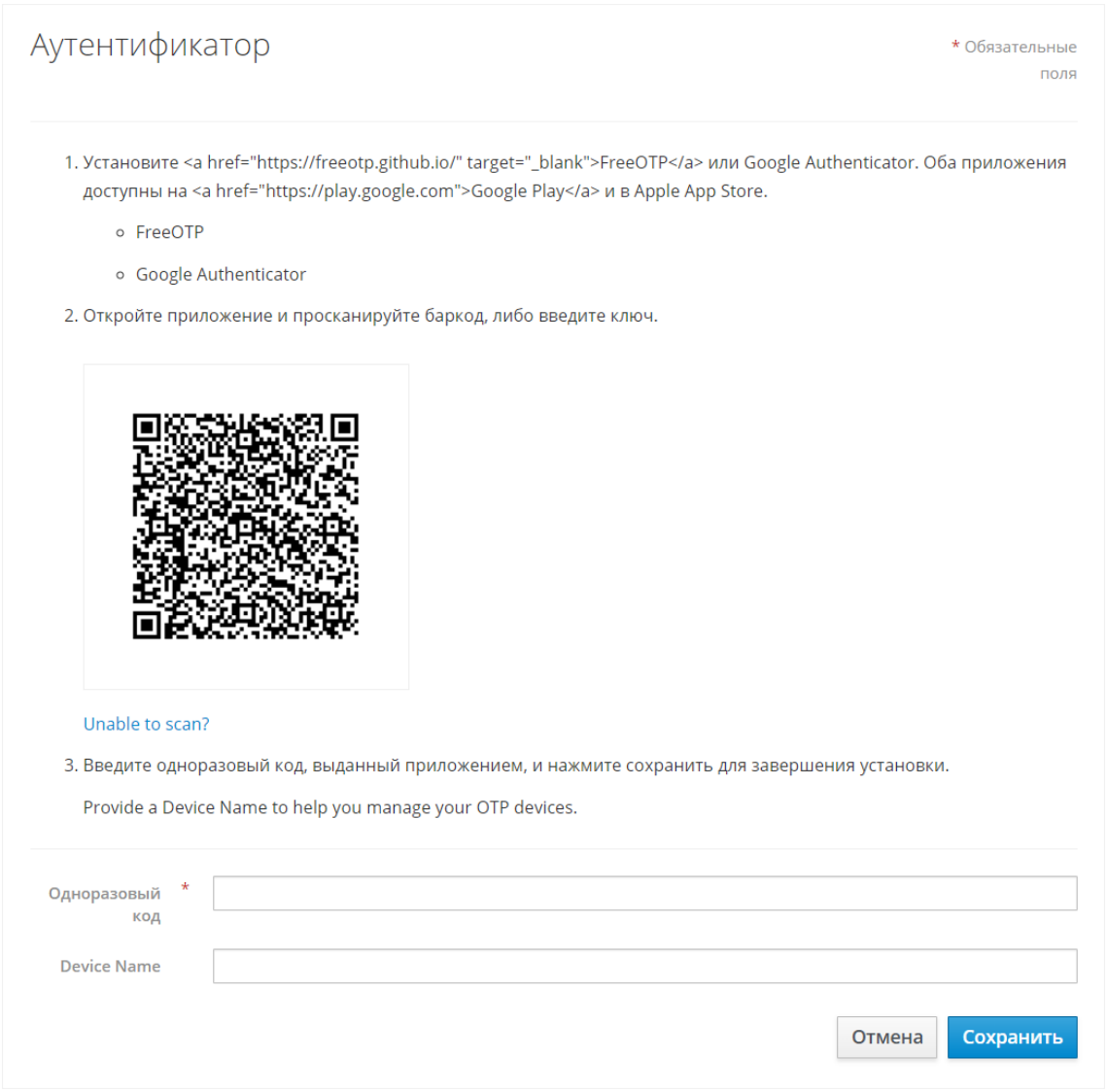


Рис. 146 – Форма "Аутентификатор"

3. Выполните инструкцию, указанную на форме.
4. Нажмите кнопку **Сохранить**.

15.4 Выход из всех сессий

1. Перейдите в профиль пользователя.

2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Сессии**. Откроется страница "Сессии" (см. «Рис. 147»).

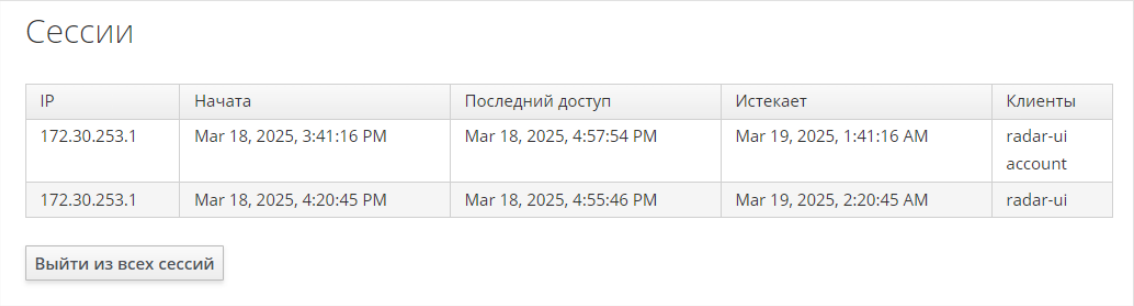


Рис. 147 – Страница "Сессии"

3. Нажмите кнопку **Выйти из всех сессий**.

15.5 Просмотр журнала изменений учетной записи

1. Перейдите в профиль пользователя.
2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Журнал**. Откроется страница "Лог учетной записи" (см. «Рис. 148»).

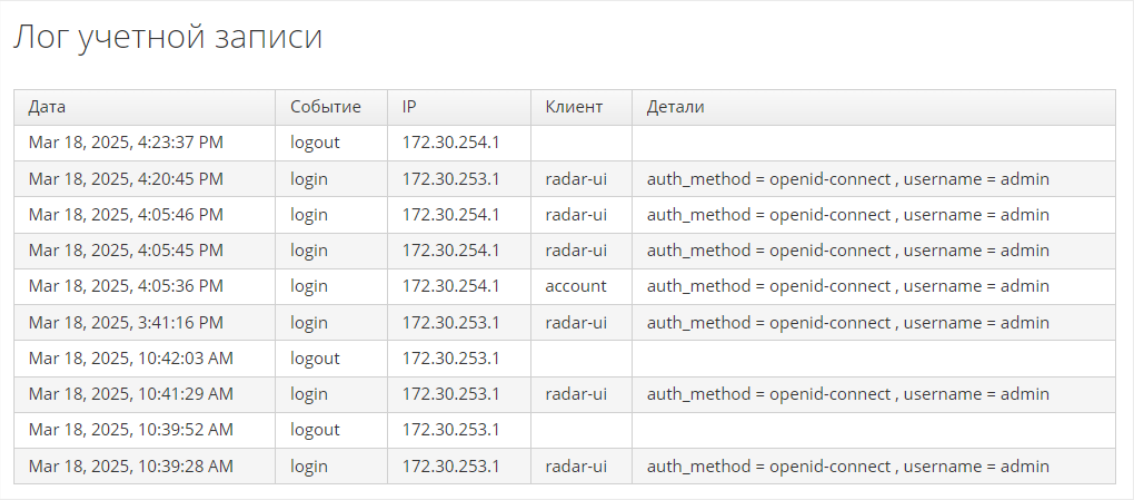


Рис. 148 – Страница "Лог учетной записи"

На странице отображается следующая информация:

- **Дата** – дата и время события;
- **Событие** – тип события;
- **IP** – IP-адрес, с которого выполнено событие;
- **Клиент** – наименование сервиса;
- **Детали** – детали события.

15.6 Настройка оповещений

1. Перейдите в профиль пользователя.

2. В блоке **Настройка оповещений** включите/выключите уведомления о следующих событиях:
    - изменение инцидентов;
    - изменение активов;
    - произошла "сработка" правила корреляции;
    - произошла автоматическая остановка правила корреляции.
3. Нажмите кнопку **Сохранить**.

15.7 Просмотр истории действий в платформе

Пример блока **Поиск по истории действий** приведен на «Рис. 149».

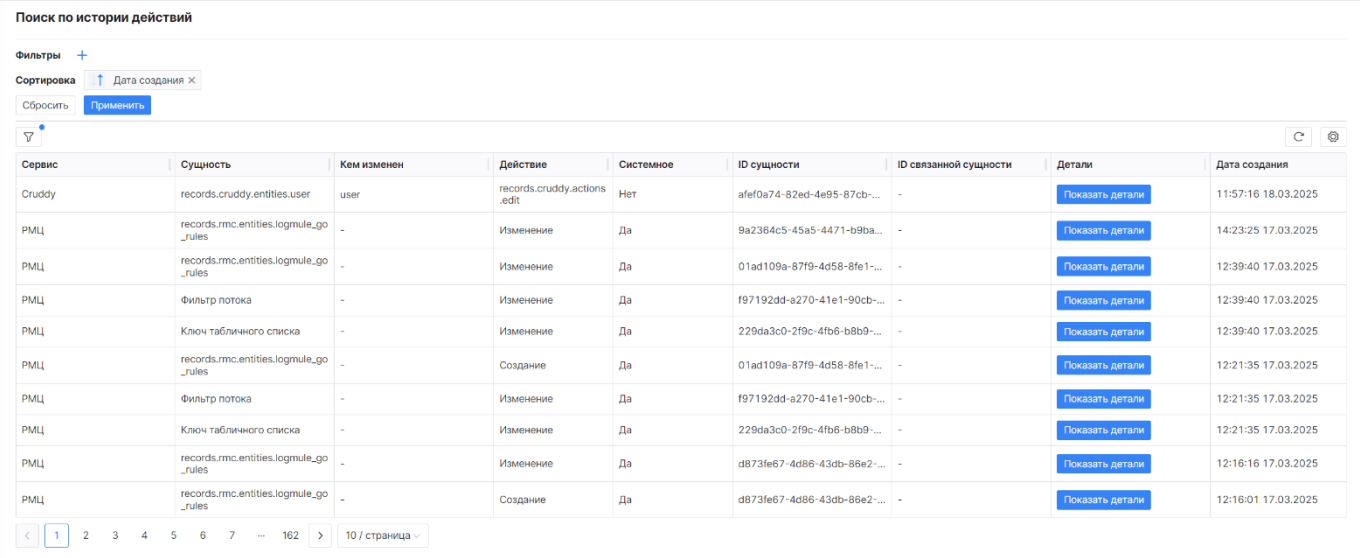


Рис. 149 – Блок "Поиск по истории действий"

В блоке отображается следующая информация:

- **Сервис** – наименование сервиса, в котором было выполнено действие;
- **Сущность** – наименование сущности, над которой было выполнено действие;
- **Кем изменен** – логин пользователя, выполнившего действие. Если пользователь не указан, то действие было выполнено платформой;
- **Действие** – описание выполненного действия;
- **Системное** – признак, выполнено ли действие платформой: Да, Нет;
- **ID сущности** – идентификатор сущности, над которой было выполнено действие;
- **ID связанной сущности** – идентификатор связанной сущности;
- **Дата создания** – дата и время создания записи о выполненном действии.

По кнопке **Детали** можно посмотреть подробную информацию о действии (см. «Рис. 150»).

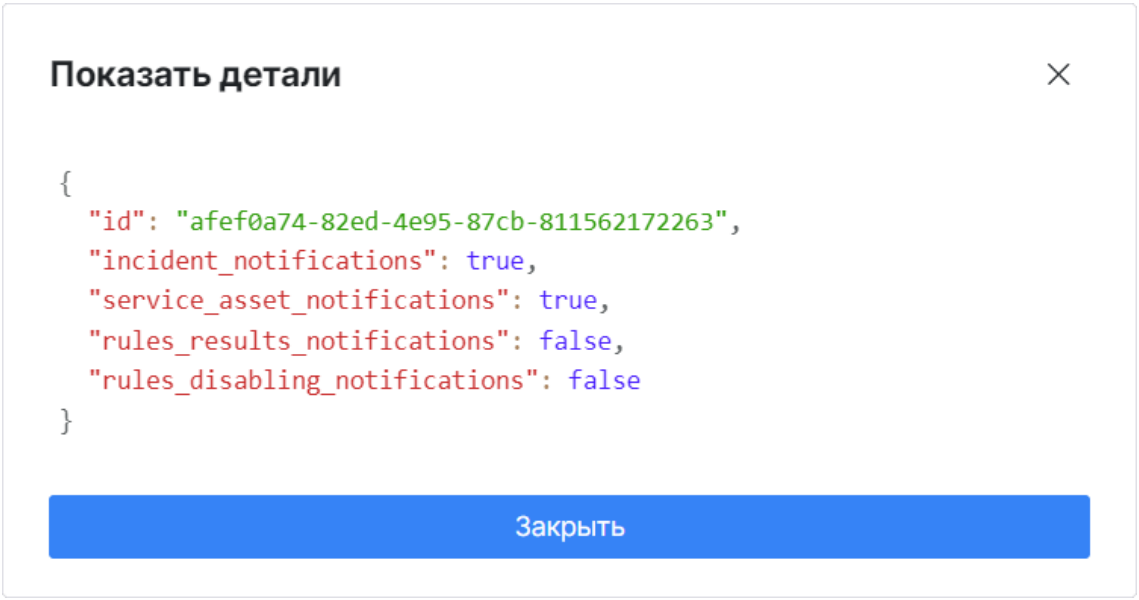


Рис. 150 – Окно "Показать детали"

16. Дополнительные задачи администратора

16.1 Диагностика состояния Платформы Радар

16.1.1 Общие данные

Диагностика состояния **Платформы Радар** осуществляется с помощью специального скрипта диагностики. Скрип диагностики *cluster_diagnostic.sh* обеспечивает проверку состояния всех сервисов и компонентов **Платформы Радар**. Скрипт проводит диагностику установок как на один сервер, так и распределенную (кластер).

В случае обнаружения ошибок скрипт собирает данные диагностики, относящие к данному сервису и окружению узла, на котором обнаружены ошибки работы, при этом не собирая данные с других узлов кластера или узлов, не относящихся к проблеме.

Скрипт не собирает данные диагностики, относящиеся к работе лог-коллектора, как Linux так и Windows.

16.1.2 Параметры командной строки скрипта

- -h - вывести список доступных параметров;
- --diag - собрать данные диагностики по всем сервисам и узлам кластера **Платформы Радар**;
- --open-err - выгрузить в архив ошибки парсинга. В случае использования ключа --diag данные так же выгружаются;
- --export-rule - экспортирует активные правила корреляци;
- --export-prometheus- экспортирует данные диагностики в архив;
- --encrypted - шифрование архива данных диагностики;
- --diag-data - сбор данных диагностики с data nodes;
- --diag-master - сбор данных диагностики с master node;
- --diag-monitoring - сбор данных диагностики с monitoring;
- --diag-worker - сбор данных диагностики с worker nodes;
- --diag-infra - сбор данных диагностики с infra node;
- --diag-balancer - сбор данных диагностики с balancer node;
- --diag-correlator - сбор данных диагностики с correlator nodes;
- --diag-eventsrouter - сбор данных диагностики с eventsrouter nodes.

16.1.3 Перечень сведений, выгружаемых скриптом диагностики

Сервисы:

- статус сервиса (*systemctl status*);

- журнал работы (*journalctl*);
- доступность портов.

Дополнительные журналы по сервисам (ролям):

- Data - Журналы работы ноды (/var/log/opensearch/)
- Data - Ошибки парсинга и нормализации (при использовании соответствующих параметров)
- Worker - Журналы работы и ошибки
- Correlator - Журналы работы (без журналов работы правил корреляции)
- Веб-сервер - Журналы доступа и ошибки
- Master (База данных) - Журналы работы и ошибки

С узла с ролью MASTER:

- Доступность серверов и их IP адреса
- Список ролей и их IP адреса
- Контрольные суммы установленных пакетов **Платформы радар**
- Параметры настройки **Платформы Радар**
- Шаблоны файлов конфигурации **Платформы Радар**
- SSH список известных хостов (known_hosts)
- Состояние (размер очереди) уведомлений правил корреляции
- Открытые ключи доступа SSH (закрытые ключи не затрагиваются)

Окружение для всех узлов:

- Информация о используемом процессоре
- Информация об оперативной памяти и ее использовании
- Файлы конфигурации сервисов **Платформы Радар**
- Файлы конфигурации системы (/etc/)
- Журналы работы (journalctl)
- Список активных процессов
- Версию операционной системы
- Журнал установки компонентов **Платформы Радар**
- Список примонтированных устройств и файловой системе
- Историю выполняемых команд
- Журналы установки пакетов (APT, DPKG)
- Список установленных пакетов
- Текущие маршруты (route)

- Настройки сети
- Доступную память
- Информацию о дисковом пространстве и именах дисков
- Журналы авторизации
- Информация о настройках окружения (env)
- Ошибки работы скрипта диагностики (в случае использования параметра --diag)
- Список подключенных репозиториев Debian (etc/apt/sources.list)
- Настройки ядра Linux (sysctl)
- Список запланированных задач (Cron)

16.1.4 Сбор диагностической информации при установке на один сервер

Платформа Радар позволяет выгрузить всю необходимую диагностическую информацию при установке на один сервер.

Для сбора диагностической информации необходимо выполнить команду:

```
/opt/pangeoradar/support_tools/diagnostics/aio_diagnostic.sh --diag
```

По окончанию выполнения данной команды на экран будет выведена информация об имени архива с диагностической информацией и его месторасположении.

16.2 Установка сертификата TLS для Nginx с помощью MS CA

Если в организации используется собственный корпоративный удостоверяющий центр, его можно использовать для выпуска сертификата веб-сервера **Платформы Радар**.

В данном примере рассмотрен выпуск сертификата с использованием Microsoft Certification Authority.

16.2.1 Выпуск сертификата

Сначала необходимо создать файл закрытого ключа. Для этого необходимо запустить утилиту openssl и указать имя создаваемого файла, а также используемый алгоритм шифрования:

```
# openssl genrsa -out pangeo_custom.key -aes256 2048
```

в результате на экран будет выведено следующее сообщение:

```
Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
Enter pass phrase for pangeo_custom.key:
Verifying - Enter pass phrase for pangeo_custom.key:
```

После появления приглашения Enter pass phrase for radar_custom.key следует ввести пароль для файла закрытого ключа (дважды). Пароль необходимо запомнить.

В текущем каталоге необходимо создать файл openssl.cnf и записать в него следующие данные:

Значения полей: **countryName_default**, **stateOrProvinceName_default**, **localityName_default**, **0.organizationName_default**, **organizationalUnitName_default**, **commonName_default**, **emailAddress_default**, **DNS.0**, **IP.0** необходимо заполнить самостоятельно в соответствии с параметрами инсталляции и инфраструктуры. После внесения изменений файл необходимо сохранить.

Пример:

```
[ req ]
req_extensions = v3_req
distinguished_name = req_distinguished_name
promt = yes

[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = RU

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Moscow

localityName = Locality Name (eg, city)
localityName_default = Moscow

0.organizationName = Organization Name (eg, company)
0.organizationName_default = Pangeo

organizationalUnitName = Organizational Unit Name (eg, section)
organizationalUnitName_default = ITSec

commonName = Common Name (eg, your name or your server\'s hostname)
commonName_default = radar-353-aio.test.lab

emailAddress = Email Address
emailAddress_default = support@pangeoradar.ru

[ v3_req ]
basicConstraints = critical, CA:true
#basicConstraints = CA:false
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.0 = radar-353-aio.test.lab

IP.0 = 192.168.2.147
```

Необходимо сгенерировать запрос на подпись сертификата, выполнив следующую команду:

```
# openssl req -new -key radar_custom.key -out cert_request.csr -config openssl.cnf
```

В процессе выполнения команда запросит ввод пароля, указанного в шаге 1.

После создания файла запроса cert_request.csr необходимо зайти в веб-интерфейс УЦ MS CA и перейти по ссылке "*Request a certificate*":

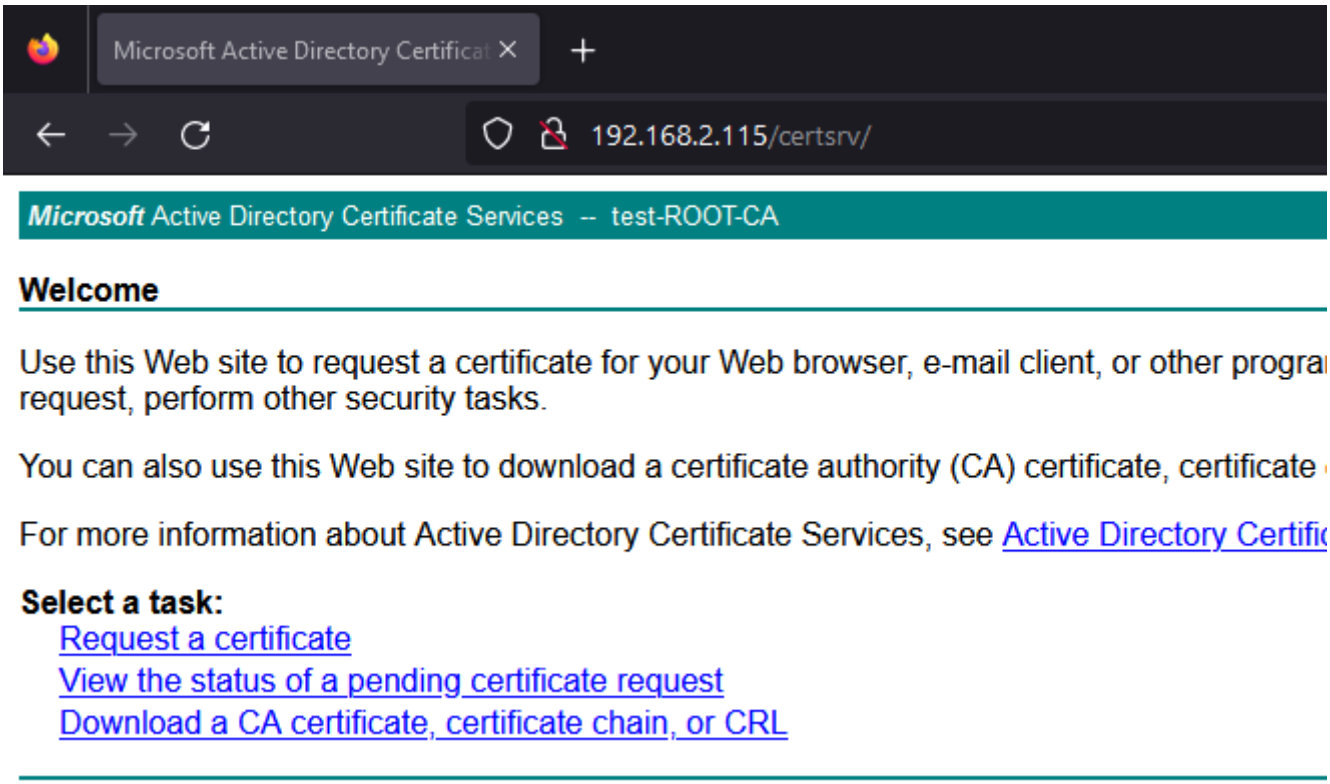


Рис. 151 – Веб-интерфейс УЦ MS CA

На следующем этапе необходимо выбрать "*advanced certificate request*":

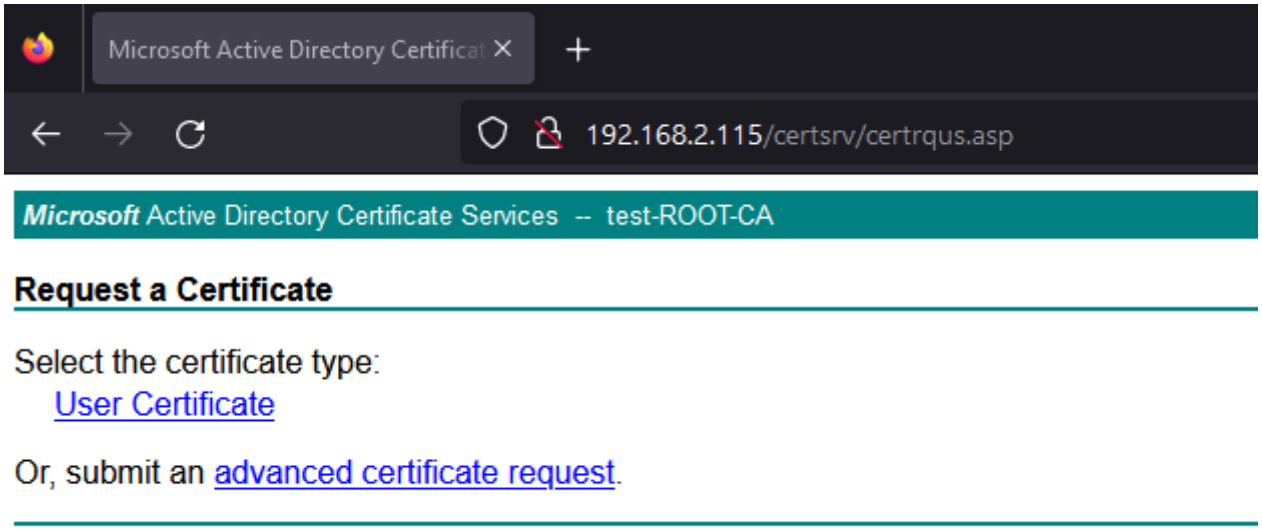


Рис. 152 – advanced certificate request

В поле "**Saved Request**" необходимо скопировать содержимое файла request.csr, для поля "**Certificate Template**" выбрать тип "**Web Server**". Нажать кнопку "**Submit**".

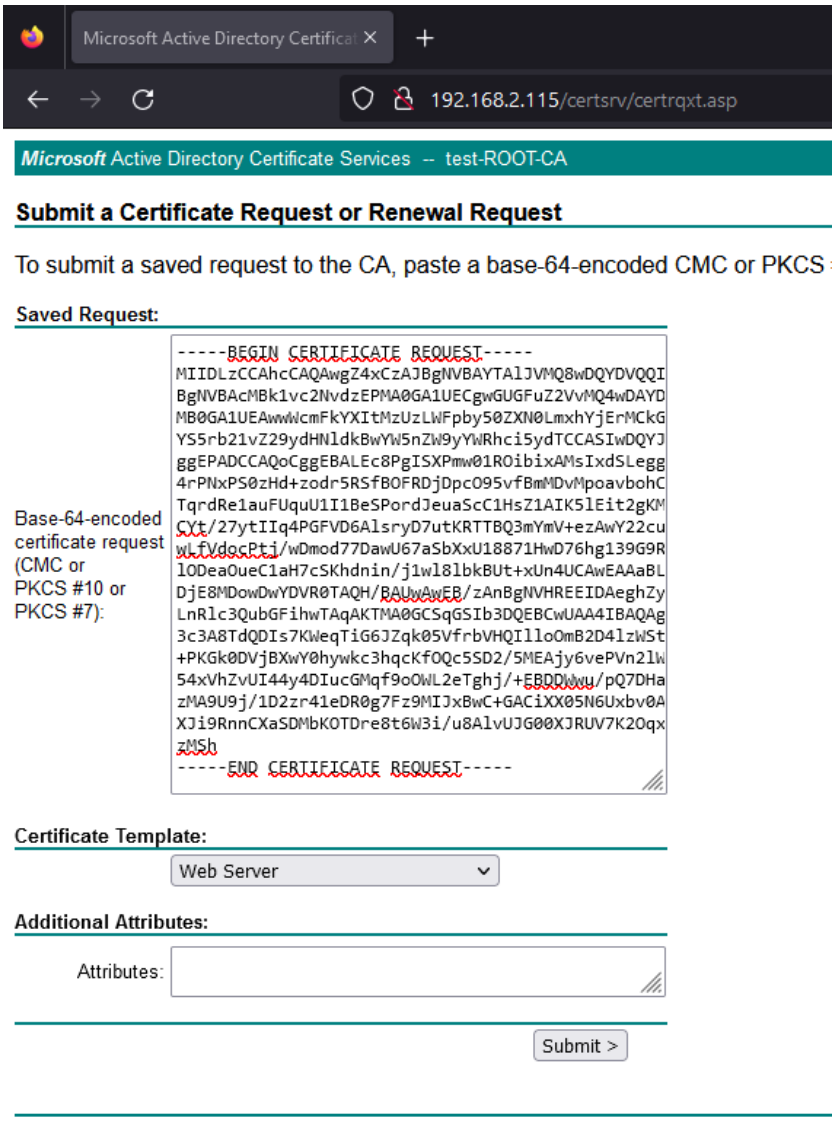


Рис. 153 – Submit certificate request

После успешного выпуска необходимо скачать сертификат ("*Download certificate*") и загрузить файл на сервер, где функционирует служба Nginx.

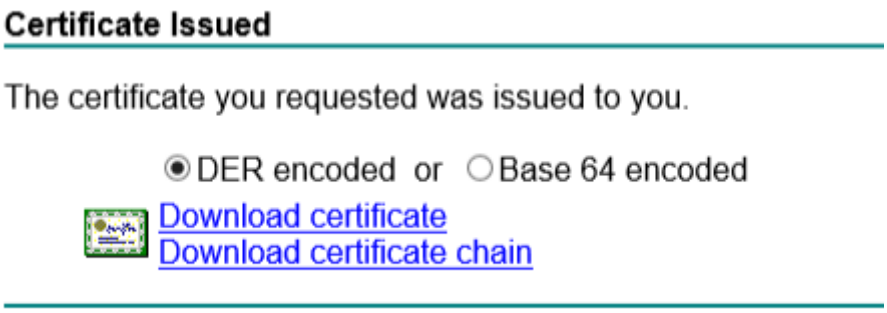


Рис. 154 – Выгрузка сертификата

16.2.2 Установка сертификата

К моменту установки сертификата в наличии должны быть следующие файлы (пример):

- pangeo_custom.key (файл закрытого ключа);

- pangeo_custom.cer (файл сертификата).

Далее:

1. Сконвертируйте файл *.cer в* .crt.

   Если сертификат скачивался в формате DER:

   openssl x509 -inform DER -in pangeo_custom.cer -out pangeo_custom.crt

   Если сертификат скачивался в формате PEM (Base64):

   openssl x509 -inform PEM -in pangeo_custom.cer -out pangeo_custom.crt

2. Далее удалите пароль для файла закрытого ключа (команда потребует ввод пароля):

   openssl rsa -in pangeo_custom.key -out pangeo_custom_unencrypted.key

3. Затем, файлы pangeo_custom.crt и pangeo_custom_unencrypted.key скопируйте в директорию /opt/pangeoradar/certs/:

```
# cp pangeo_custom_unencrypted.key /opt/pangeoradar/certs/
# cp pangeo_custom.crt /opt/pangeoradar/certs/
# chmod 644 /opt/pangeoradar/certs/pangeo_custom_unencrypted.key
# chmod 644 /opt/pangeoradar/certs/pangeo_custom.crt
```

4. В разделе ***Кластер - Управление конфигурацией*** выбрать Nginx и указать использование нестандартных сертификатов, выполните сохранение и применение настроек:

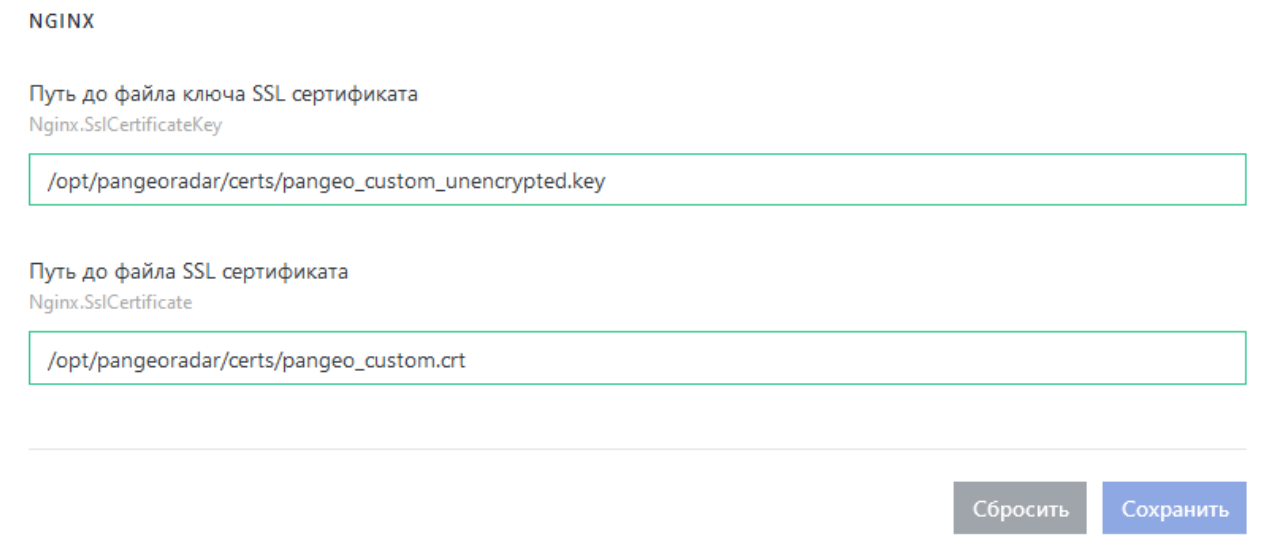


Рис. 155 – Кластер. Управление конфигурацией «NGINX»

5. Для подмены сертификата в Keycloak отредактируйте файл шаблона /opt/pangeoradar/bin/service_config_templates/ui.nginx.tmpl, раскомментировав вторую секцию конфигурации:

```
server {
        location /fonts  {
                alias /opt/pangeoradar/bin/dist/fonts;
        }
        location / {
                proxy_pass http://{{.Ui.Ip}}:{{ .Ui.Port }};
        }{{ if .DNS.DomainName | IsDomain }}
        server_name {{ .DNS.UiDomain}};{{ end }}
{{ if .DNS.DomainName | IsIp }}   listen 443 ssl default_server;{{ else }}   listen 443 ssl;{{ end }}
        ssl on;
        ssl_protocols TLSv1.2 TLSv1.3;
        ssl_prefer_server_ciphers on;
        ssl_certificate {{ .Nginx.SslCertificate }};
        ssl_certificate_key {{ .Nginx.SslCertificateKey }};
}

server {
        location /fonts  {
                alias /opt/pangeoradar/bin/dist/fonts;
        }
        location / {
                proxy_pass http://127.0.0.1:{{ .Ui.Port }};
        }
        listen 8080 ssl default_server;
        ssl on;
        ssl_protocols TLSv1.2 TLSv1.3;
        ssl_prefer_server_ciphers on;
        ssl_certificate {{ .Nginx.SslCertificate }};
        ssl_certificate_key {{ .Nginx.SslCertificateKey }};

}
```

6. Перезапустите службу Nginx и проверьте результат:

```
# systemctl restart nginx
```

На этом, установка сертификата веб-интерфейса завершена. Для Grafana на порте 6630/TCP сертификат будет заменен автоматически.

16.3 Список доступных таймзон

Таблица 5 – Список доступных таймзон

Africa/Abidjan	America/Indiana/Winamac	Asia/Ho_Chi_Minh
Africa/Accra	America/Indianapolis	Asia/Hong_Kong
Africa/Addis_Ababa	America/Inuvik	Asia/Hovd
Africa/Algiers	America/Iqaluit	Asia/Irkutsk
Africa/Asmara	America/Jamaica	Asia/Istanbul
Africa/Asmera	America/Jujuy	Asia/Jakarta
Africa/Bamako	America/Juneau	Asia/Jayapura
Africa/Bangui	America/Kentucky/Louisville	Asia/Jerusalem
Africa/Banjul	America/Kentucky/Monticello	Asia/Kabul

Africa/Bissau	America/Knox_IN	Asia/Kamchatka
Africa/Blantyre	America/Kralendijk	Asia/Karachi
Africa/Brazzaville	America/La_Paz	Asia/Kashgar
Africa/Bujumbura	America/Lima	Asia/Kathmandu
Africa/Cairo	America/Los_Angeles	Asia/Katmandu
Africa/Casablanca	America/Louisville	Asia/Khandyga
Africa/Ceuta	America/Lower_Princes	Asia/Kolkata
Africa/Conakry	America/Maceio	Asia/Krasnoyarsk
Africa/Dakar	America/Managua	Asia/Kuala_Lumpur
Africa/Dar_es_Salaam	America/Manaus	Asia/Kuching
Africa/Djibouti	America/Marigot	Asia/Kuwait
Africa/Douala	America/Martinique	Asia/Macao
Africa/El_Aaiun	America/Matamoros	Asia/Macau
Africa/Freetown	America/Mazatlan	Asia/Magadan
Africa/Gaborone	America/Mendoza	Asia/Makassar
Africa/Harare	America/Menominee	Asia/Manila
Africa/Johannesburg	America/Merida	Asia/Muscat
Africa/Juba	America/Metlakatla	Asia/Nicosia
Africa/Kampala	America/Mexico_City	Asia/Novokuznetsk
Africa/Khartoum	America/Miquelon	Asia/Novosibirsk
Africa/Kigali	America/Moncton	Asia/Omsk
Africa/Kinshasa	America/Monterrey	Asia/Oral
Africa/Lagos	America/Montevideo	Asia/Phnom_Penh
Africa/Libreville	America/Montreal	Asia/Pontianak
Africa/Lome	America/Montserrat	Asia/Pyongyang
Africa/Luanda	America/Nassau	Asia/Qatar
Africa/Lubumbashi	America/New_York	Asia/Qyzylorda
Africa/Lusaka	America/Nipigon	Asia/Rangoon
Africa/Malabo	America/Nome	Asia/Riyadh
Africa/Maputo	America/Noronha	Asia/Saigon
Africa/Maseru	America/North_Dakota/Beulah	Asia/Sakhalin
Africa/Mbabane	America/North_Dakota/Center	Asia/Samarkand
Africa/Mogadishu	America/North_Dakota/New_Salem	Asia/Seoul
Africa/Monrovia	America/Ojinaga	Asia/Shanghai
Africa/Nairobi	America/Panama	Asia/Singapore
Africa/Ndjamena	America/Pangnirtung	Asia/Srednekolymsk
Africa/Niamey	America/Paramaribo	Asia/Taipei
Africa/Nouakchott	America/Phoenix	Asia/Tashkent
Africa/Ouagadougou	America/Port	au
Africa/Porto	Novo	America/Port_of_Spain
Africa/Sao_Tome	America/Porto_Acre	Asia/Tel_Aviv
Africa/Timbuktu	America/Porto_Velho	Asia/Thimbu
Africa/Tripoli	America/Puerto_Rico	Asia/Thimphu
Africa/Tunis	America/Punta_Arenas	Asia/Tokyo
Africa/Windhoek	America/Rainy_River	Asia/Tomsk
America/Adak	America/Rankin_Inlet	Asia/Ujung_Pandang
America/Anchorage	America/Recife	Asia/Ulaanbaatar
America/Anguilla	America/Regina	Asia/Ulan_Bator

America/Antigua	America/Resolute	Asia/Urumqi
America/Araguaina	America/Rio_Branco	Asia/Ust
America/Argentina/Buenos_Aires	America/Rosario	Asia/Vientiane
America/Argentina/Catamarca	America/Santa_Isabel	Asia/Vladivostok
America/Argentina/ComodRivadavia	America/Santarem	Asia/Yakutsk
America/Argentina/Cordoba	America/Santiago	Asia/Yangon
America/Argentina/Jujuy	America/Santo_Domingo	Asia/Yekaterinburg
America/Argentina/La_Rioja	America/Sao_Paulo	Asia/Yerevan
America/Argentina/Mendoza	America/Scoresbysund	Atlantic/Azores
America/Argentina/Rio_Gallegos	America/Shiprock	Atlantic/Bermuda
America/Argentina/Salta	America/Sitka	Atlantic/Canary
America/Argentina/San_Juan	America/St_Barthelemy	Atlantic/Cape_Verde
America/Argentina/San_Luis	America/St_Johns	Atlantic/Faeroe
America/Argentina/Tucuman	America/St_Kitts	Atlantic/Faroe
America/Argentina/Ushuaia	America/St_Lucia	Atlantic/Jan_Mayen
America/Aruba	America/St_Thomas	Atlantic/Madeira
America/Asuncion	America/St_Vincent	Atlantic/Reykjavik
America/Atikokan	America/Swift_Current	Atlantic/South_Georgia
America/Atka	America/Tegucigalpa	Atlantic/St_Helena
America/Bahia	America/Thule	Atlantic/Stanley
America/Bahia_Banderas	America/Thunder_Bay	Australia/ACT
America/Barbados	America/Tijuana	Australia/Adelaide
America/Belem	America/Toronto	Australia/Brisbane
America/Belize	America/Tortola	Australia/Broken_Hill
America/Blanc	Sablon	America/Vancouver
America/Boa_Vista	America/Virgin	Australia/Currie
America/Bogota	America/Whitehorse	Australia/Darwin
America/Boise	America/Winnipeg	Australia/Eucla
America/Buenos_Aires	America/Yakutat	Australia/Hobart
America/Cambridge_Bay	America/Yellowknife	Australia/LHI
America/Campo_Grande	Antarctica/Casey	Australia/Lindeman
America/Cancun	Antarctica/Davis	Australia/Lord_Howe
America/Caracas	Antarctica/DumontDUrville	Australia/Melbourne
America/Catamarca	Antarctica/Macquarie	Australia/NSW
America/Cayenne	Antarctica/Mawson	Australia/North
America/Cayman	Antarctica/McMurdo	Australia/Perth
America/Chicago	Antarctica/Palmer	Australia/Queensland
America/Chihuahua	Antarctica/Rothera	Australia/South
America/Coral_Harbour	Antarctica/South_Pole	Australia/Sydney
America/Cordoba	Antarctica/Syowa	Australia/Tasmania
America/Costa_Rica	Antarctica/Troll	Australia/Victoria
America/Creston	Antarctica/Vostok	Australia/West
America/Cuiaba	Arctic/Longyearbyen	Australia/Yancowinna
America/Curacao	Asia/Aden	Brazil/Acre
America/Danmarkshavn	Asia/Almaty	Brazil/DeNoronha
America/Dawson	Asia/Amman	Brazil/East
America/Dawson_Creek	Asia/Anadyr	Brazil/West
America/Denver	Asia/Aqtau	CET

America/Detroit	Asia/Aqtobe	CST6CDT
America/Dominica	Asia/Ashgabat	Canada/Atlantic
America/Edmonton	Asia/Ashkhabad	Canada/Central
America/Eirunepe	Asia/Atyrau	Canada/Eastern
America/El_Salvador	Asia/Baghdad	Canada/Mountain
America/Ensenada	Asia/Bahrain	Canada/Newfoundland
America/Fort_Nelson	Asia/Baku	Canada/Pacific
America/Fort_Wayne	Asia/Bangkok	Canada/Saskatchewan
America/Fortaleza	Asia/Barnaul	Canada/Yukon
America/Glace_Bay	Asia/Beirut	Chile/Continental
America/Godthab	Asia/Bishkek	Chile/EasterIsland
America/Goose_Bay	Asia/Brunei	Cuba
America/Grand_Turk	Asia/Calcutta	EET
America/Grenada	Asia/Chita	EST
America/Guadeloupe	Asia/Choibalsan	EST5EDT
America/Guatemala	Asia/Chongqing	Egypt
America/Guayaquil	Asia/Chungking	Eire
America/Guyana	Asia/Colombo	Etc/GMT
America/Halifax	Asia/Dacca	Etc/GMT+0
America/Havana	Asia/Damascus	Etc/GMT+1
America/Hermosillo	Asia/Dhaka	Etc/GMT+10
America/Indiana/Indianapolis	Asia/Dili	Etc/GMT+11
America/Indiana/Knox	Asia/Dubai	Etc/GMT+12
America/Indiana/Marengo	Asia/Dushanbe	Etc/GMT+2
America/Indiana/Petersburg	Asia/Famagusta	Etc/GMT+3
America/Indiana/Tell_City	Asia/Gaza	Etc/GMT+4
America/Indiana/Vevay	Asia/Harbin	Etc/GMT+5
America/Indiana/Vincennes	Asia/Hebron	Etc/GMT+6
Europe/Amsterdam	GB	Etc/GMT+7
Europe/Andorra	GB-Eire	Etc/GMT+8
Europe/Astrakhan	GMT	Etc/GMT+9
Europe/Athens	GMT+0	Etc/GMT-0
Europe/Belfast	GMT-0	Etc/GMT-1
Europe/Belgrade	GMT0	Etc/GMT-10
Europe/Berlin	Greenwich	Etc/GMT-11
Europe/Bratislava	HST	Etc/GMT-12
Europe/Brussels	Hongkong	Etc/GMT-13
Europe/Bucharest	Iceland	Etc/GMT-14
Europe/Budapest	Indian/Antananarivo	Etc/GMT-2
Europe/Busingen	Indian/Chagos	Etc/GMT-3
Europe/Chisinau	Indian/Christmas	Etc/GMT-4
Europe/Copenhagen	Indian/Cocos	Etc/GMT-5
Europe/Dublin	Indian/Comoro	Etc/GMT-6
Europe/Gibraltar	Indian/Kerguelen	Etc/GMT-7
Europe/Guernsey	Indian/Mahe	Etc/GMT-8
Europe/Helsinki	Indian/Maldives	Etc/GMT-9
Europe/Isle_of_Man	Indian/Mauritius	Etc/GMT0
Europe/Istanbul	Indian/Mayotte	Etc/Greenwich

Europe/Jersey	Indian/Reunion	Etc/UCT
Europe/Kaliningrad	Iran	Etc/UTC
Europe/Kiev	Israel	Etc/Universal
Europe/Kirov	Jamaica	Etc/Zulu
Europe/Lisbon	Japan	Pacific/Norfolk
Europe/Ljubljana	Kwajalein	Pacific/Noumea
Europe/London	Libya	Pacific/Pago_Pago
Europe/Luxembourg	MET	Pacific/Palau
Europe/Madrid	MST	Pacific/Pitcairn
Europe/Malta	MST7MDT	Pacific/Pohnpei
Europe/Mariehamn	Mexico/BajaNorte	Pacific/Ponape
Europe/Minsk	Mexico/BajaSur	Pacific/Port_Moresby
Europe/Monaco	Mexico/General	Pacific/Rarotonga
Europe/Moscow	NZ	Pacific/Saipan
Europe/Nicosia	NZ	CHAT
Europe/Oslo	Navajo	Pacific/Tahiti
Europe/Paris	PRC	Pacific/Tarawa
Europe/Podgorica	PST8PDT	Pacific/Tongatapu
Europe/Prague	Pacific/Apia	Pacific/Truk
Europe/Riga	Pacific/Auckland	Pacific/Wake
Europe/Rome	Pacific/Bougainville	Pacific/Wallis
Europe/Samara	Pacific/Chatham	Pacific/Yap
Europe/San_Marino	Pacific/Chuuk	Poland
Europe/Sarajevo	Pacific/Easter	Portugal
Europe/Saratov	Pacific/Efate	ROC
Europe/Simferopol	Pacific/Enderbury	ROK
Europe/Skopje	Pacific/Fakaofo	Singapore
Europe/Sofia	Pacific/Fiji	Turkey
Europe/Stockholm	Pacific/Funafuti	UCT
Europe/Tallinn	Pacific/Galapagos	US/Alaska
Europe/Tirane	Pacific/Gambier	US/Aleutian
Europe/Tiraspol	Pacific/Guadalcanal	US/Arizona
Europe/Ulyanovsk	Pacific/Guam	US/Central
Europe/Uzhgorod	Pacific/Honolulu	US/East
Europe/Vaduz	Pacific/Johnston	US/Eastern
Europe/Vatican	Pacific/Kiritimati	US/Hawaii
Europe/Vienna	Pacific/Kosrae	US/Indiana
Europe/Vilnius	Pacific/Kwajalein	US/Michigan
Europe/Volgograd	Pacific/Majuro	US/Mountain
Europe/Warsaw	Pacific/Marquesas	US/Pacific
Europe/Zagreb	Pacific/Midway	US/Pacific
Europe/Zaporozhye	Pacific/Nauru	US/Samoa
Europe/Zurich	Pacific/Niue	UTC

16.4 Настройка интеграции со службой Active Directory

В **Платформе Радар** предусмотрена возможность использования доменных учетных записей посредством интеграции с Active Directory.

Для настройки интеграции необходимо:

- указать адрес LDAP сервера;
- указать аккаунт и пароль для поиска по LDAP в настройках KeyCloak.

Если на контроллере(ах) домена LDAP ранее не настраивался, то необходимо установить **Microsoft Identity Management for UNIX Role Service** (см. «Рис. 156»).

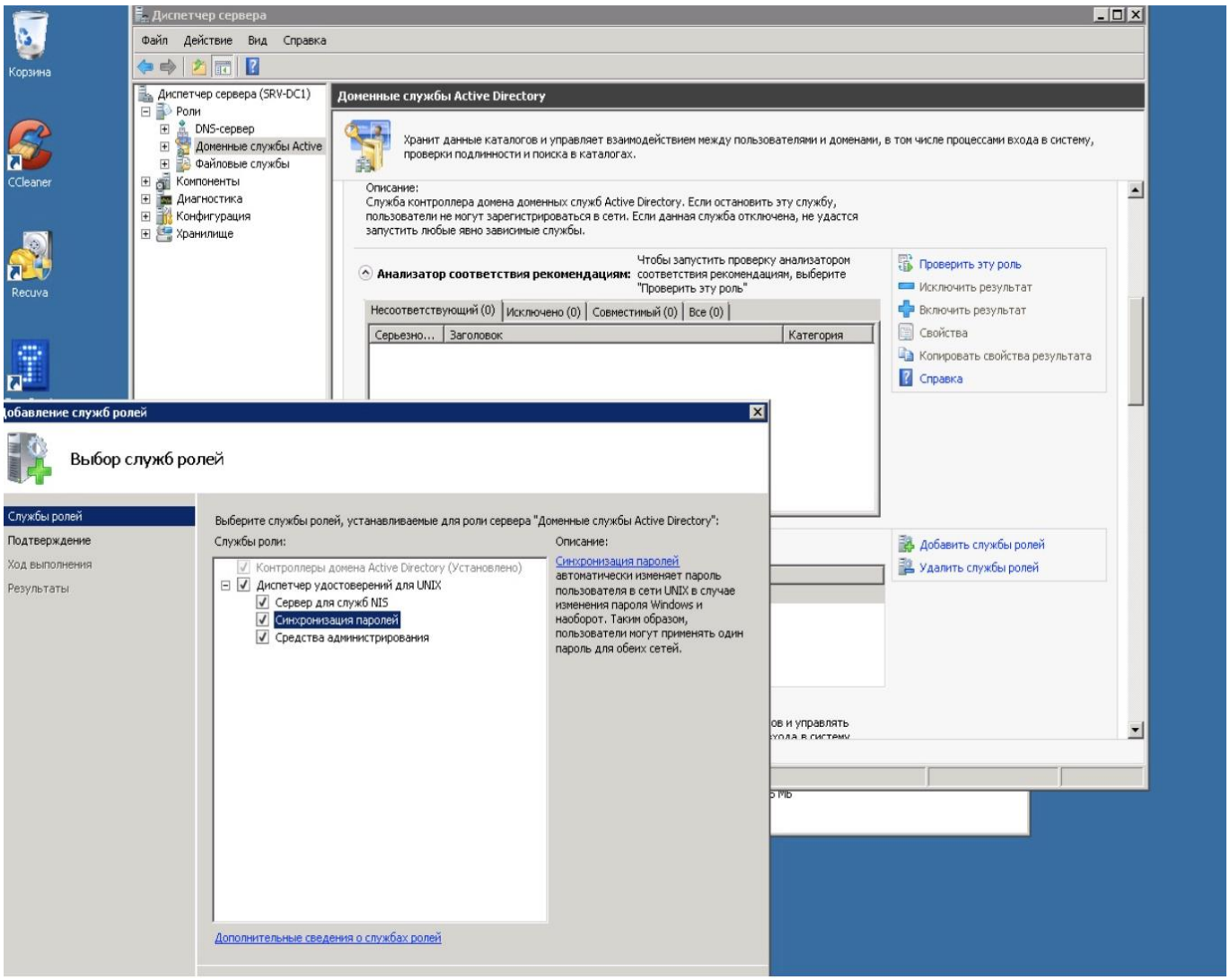


Рис. 156 – Выбор служб ролей в Microsoft Identity Management for UNIX Role Service

Примечание: *данная настройка необходима на контроллерах домена под управлением Windows Server 2008 и ниже. На контроллерах домена под управлением Windows Server 2012 и выше установка* ***Microsoft Identity Management for UNIX Role Service*** *не требуется*.

16.4.1 Настройка LDAP

Примечание: *начиная с версии 4.0.0 настройку LDAP можно выполнить в разделе платформы* ***Администрирование → Пользователи и роли →*** *вкладка* ***LDAP***.

После установки службы перейдите в KeyCloak и начните настройку LDAP, выполнив следующие действия:

1. Откройте консоль администрирования **KeyCloak** (*https://<адрес Платформы Радар>:8180*),выберите "**Administration Console**" и перейдите в пункт меню "**Федерация пользователей**" (см. «Рис. 157»).
2. Откройте список "**Добавить поставщика**" (см. «Рис. 157»).

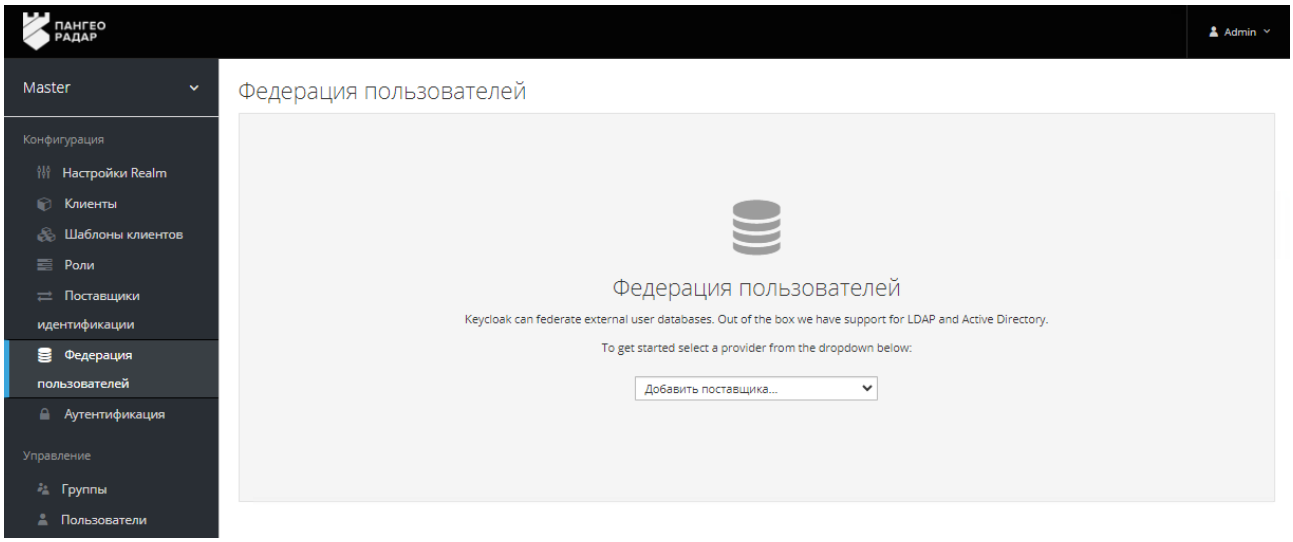


Рис. 157 – Консоль администрирования KeyCloak, раздел меню "Федерация пользователей", список "Добавить поставщика"

3. В открывшемся списке "**Добавить поставщика**" выберите раздел "**LDAP**" и заполните поля на вкладке "**Требуемые настройки**" (см. «Рис. 158»).

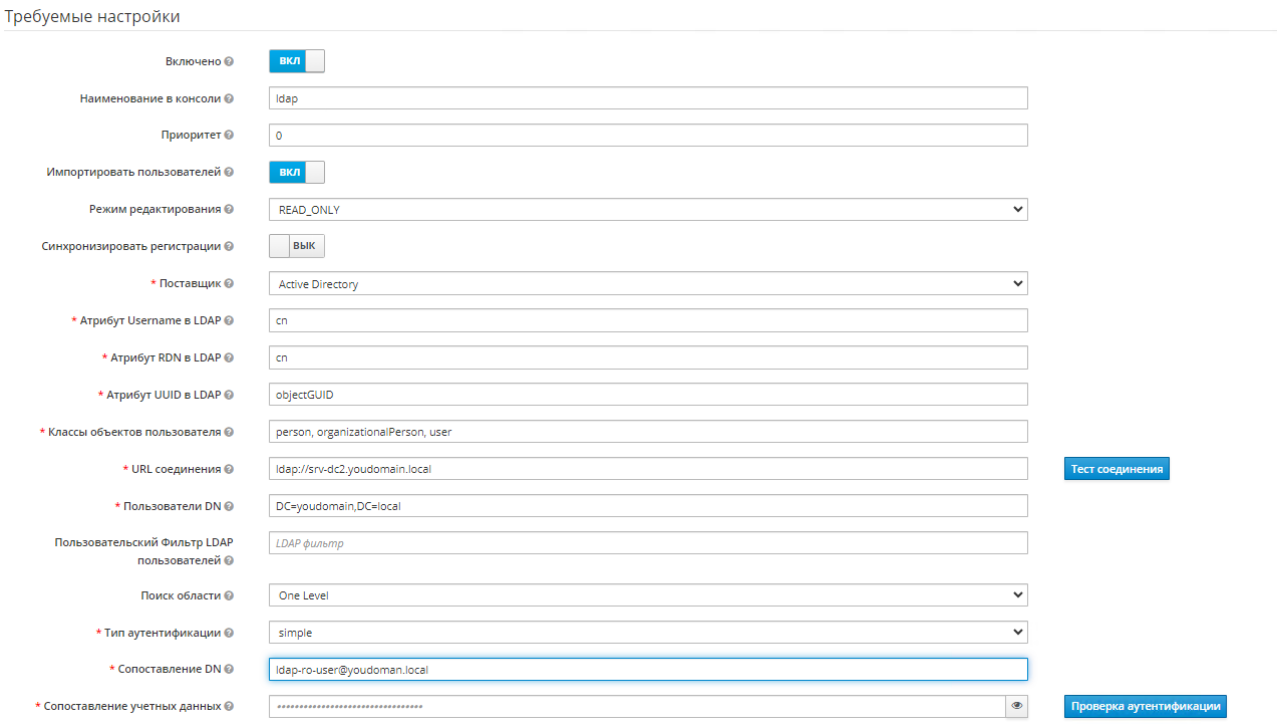


Рис. 158 - Заполнение данных по LDAP

Следующие поля обязательны для заполнения:

- **Включено** - значение ВКЛ (устанавливается по умолчанию);
- **Наименование в консоли** - ldap (устанавливается по умолчанию);
- **Приоритет** - 0 (устанавливается по умолчанию);
- **Импортировать пользователей** - значение ВКЛ (устанавливается по умолчанию);
- **Режим редактирования** - READ_ONLY (выбрать из списка);
- **Синхронизировать регистрации** - значение ВЫК (устанавливается по умолчанию);
- **Поставщик** - указать Active Directory;
- **Атрибут Username в LDAP** - указать sAMAccountName или cn;
- **Атрибут RDN в LDAP** - значение cn (установлено по умолчанию);
- **Атрибут UUID в LDAP** - значение objectGUID (установлено по умолчанию);
- **Классы объектов пользователя** - значения person, organizationPerson, user (установлены по умолчанию);
- **URL соединения** - указать IP-адрес сервера Active Directory, например - ldap://srv-dc2.youdomain.local ;
- **Пользователи DN** - в соответствии с примером DC=youdomain,DC=local;
- **Пользовательский Фильтр LDAP пользователей** - оставить пустым, если не требуется фильтрация списка пользователей;
- **Поиск области** - выберите One level;
- **Тип аутентификации** - выбрать Simple;
- **Сопоставление DN** - указать системный аккаунт в Active Director для чтения данных из LDAP (например, ldap-ro-user@youdoman.local) ;
- **Сопоставление учетных данных** - пароль системного аккаунта.

4. При необходимости можно протестировать введенные параметры LDAP, нажав кнопки "**Тест соединения**" и "**Проверка аутентификации**" (см. «Рис. 158»).
5. Для сохранения введённых настроек LDAP нажмите кнопку "**Сохранить**", расположенную в самом низу экрана.

После сохранения отобразятся кнопки синхронизации пользователей. Нажмите кнопку "**Синхронизировать всех пользователей**", чтобы загрузить список пользователей:

Рис. 159 – Синхронизация пользователей

Если синхронизация пользователей не произошла, то для определения причины сбоя в первую очередь надо смотреть лог плагина /opt/wildfly/standalone/log/keycloak.log. В логе следует

просмотреть события, зафиксированные в момент нажатия тестовых кнопок или кнопок синхронизации пользователей.

16.5 Настройка оповещений

Сервис **Toller** предназначен для формирования уведомлений от **Платформы Радар** и пересылки сформированных уведомлений пользователям и администраторам.

16.5.1 Конфигурация сервиса

Конфигурация сервиса выполняется в разделе «Управление конфигурацией».

Доступные настройки сервиса **Toller**:

Параметр	**Описание**
Отключить обязательную проверку TLS при соединении к БД	Опция, которая позволяет пропустить проверку сертификата при безопасном соединении. Возможные значения: - true – опция включена; - false – опция выключена.
Использовать TLS шифрование	Опция, которая позволяет включить TLS шифрование. Возможные значения: - true – опция включена; - false – опция выключена.
Режим отладки	Опция, которая позволяет использовать сервис в режиме отладки. Возможные значения: - true – опция включена; - false – опция выключена.
ID инстанса	Идентификатор инстанса на котором располагается сервис
IP адрес сервиса	IP-адрес инстанса на котором располагается сервис
Порт сервиса	Порт для обращения к сервису. По умолчанию 6699
Протокол обращения к сервису	Протокол, по которому должно выполняться обращение к сервису. Возможные значения: - http; - https.
Адрес WebHook для Slack	Уникальный URL, предоставляемый Slack, который позволяет внешним приложениям или службам отправлять сообщения в конкретный канал в рабочей области Slack
Включить Slack	Опция, включающая поддержку внешней системы Slack. Возможные значения: - true – опция включена; - false – опция выключена.
SMTP адрес	Адрес SMTP сервера
SMTP default to	Порт SMTP сервера, по умолчанию
Включить SMTP	Опция, включающая отправку сообщений через SMTP сервер. Возможные значения: - true – опция включена; - false – опция выключена.
SMTP поле "от кого"	Наименование адресанта оповещений при использовании SMTP
SMTP Identity	Способ аутентификации на SMTP сервере

Параметр	Описание
SMTP пароль	Пароль для аутентификации на SMTP сервере
SMTP порт	Порт для аутентификации на SMTP сервере
SMTP имя пользователя	Имя пользователя для аутентификации на SMTP сервере

16.5.2 Настройка пользователей

Для настройки получения уведомлений от **Платформы Радар** конкретными пользователями необходимо указать необходимый адрес электронной почты при создании/редактировании пользователя (см. раздел «Пользователи»).

16.5.3 Настройка оповещений о работе сервисов

Для настройки оповещений о работе сервисов необходимо сделать следующее (все действия необходимо выполнять под привилегированным пользователем):

1. Произвести настройку службы *node_exporter*. Расположение конфигурационного файла: /etc/systemd/system/node_exporter.service;

   В конец строки ExecStart добавить --collector.systemd;

   После чего конфигурационный файл должен выглядеть следующим образом:

```
[Unit]
Description=Node Exporter
Wants=network-online.target
After=network-online.target

[Service]
User=node_exporter
Group=node_exporter
Type=simple
ExecStart=/opt/pangeoradar/node_exporter/node_exporter --web.listen-address=":9101" --collector.systemd

[Install]

WantedBy=multi-user.target
```

2. Далее необходимо выполнить команду sudo systemctl daemon-reload
3. После чего, перезапустить службу node_exporter командой sudo service node_exporter restart

Оповещения будут отправляться на адрес, указанный в параметре SmtpDefaultTo" конфигурационного файла /opt/pangeoradar/configs/pangeoradar-toller.yaml.

16.6 Резервное копирование

Ниже представлен один из способов работы со снятием резервных копий индексов OpenSearch путем архивирования индексов. Важно помнить, что для корректной работы потребуется *curator* версии старше 5.0.

16.6.1 Архивирование индексов

В файле /etc/opensearch/opensearch.yml прописан путь до файлового репозитория:

```
path.repo: /opt/opensearch/snapshots
```

Если такой строки нет, необходимо прописать и перезагрузить OpenSearch.

Далее необходимо создать репозиторий, в котором будут размещены снапшоты:

```
mkdir -p /opt/opensearch/snapshots/repository
curl -k -XPUT 'https://localhost:9200/_snapshot/repository' -H 'Content-Type: application/json' -d '{
  "type": "fs",
  "settings": {
    "location": "repository",
    "compress": true
  }
}'
```

Также необходимо создать ещё один репозиторий с именем "*recovery*", который понадобится для восстановления индексов:

```
mkdir -p /opt/opensearch/snapshots/recovery
curl -k -XPUT 'https://localhost:9200/_snapshot/recovery' -H 'Content-Type: application/json' -d '{
  "type": "fs",
  "settings": {
    "location": "recovery",
    "compress": true
  }
}'
```

Далее представлен пример скрипта для архивирования индексов.

Логика работы скрипта описана в комментариях. Не забудьте поправить значения переменных, если ваши настройки будут отличаться от дефолтных.

```
#!/bin/bash

DAYS=31 #Количество дней, от текущей даты, старше которого индексы будут архивироваться
SNAPSHOT_DIRECTORY="/opt/opensearch/snapshots"
BACKUP_DIR="/opt/opensearch/opensearch_backup"
REPOSITORY="repository"
LOG="/var/log/opensearch/opensearch_backup.log"
DATE=`date`
```

Продолжение на следующей странице:

```
#Проверим существование папки для архивов и если нет, создадим её
if ! [ -d $BACKUP_DIR ]; then
  mkdir -p $BACKUP_DIR
fi

#Получаем массив индексов, которые старше $DAYS
INDICES=`curator_cli --config /etc/opensearch/curator-config.yml --host localhost --port 9200 show_indices --filter_list
"[{\"filtertype\":\"age\",\"source\":\"creation_date\",\"direction\":\"older\",\"unit\":\"days\",\"unit_count\":\"$DAYS\"
},{\"filtertype\":\"kibana\",\"exclude\":\"True\"},{\"filtertype\":\"pattern\",\"kind\":\"regex\",\"value\":\"elastalert_stat
us\",\"exclude\":\"True\"}]"`

#Проверим, не пустой ли список
TEST_INDICES=`echo $INDICES | grep -q -i "error" && echo 1 || echo 0`

if [ $TEST_INDICES == 1 ]
then
  echo "$DATE Не найдено индексов для обработки" >> $LOG
  exit
else
# Составляем цикл для каждого индекса в массиве $INDICES
for i in $INDICES
  do
    # Создаём снапшот для индекса $i
    curator_cli --config /etc/opensearch/curator-config.yml --timeout 600 --host localhost --port 9200 snapshot --
repository $REPOSITORY --filter_list "{\"filtertype\":\"pattern\",\"kind\":\"regex\",\"value\":\"$i\"}"

    # Заносим в переменную имя снапшота для индекса $i
    SNAPSHOT=`curator_cli --config /etc/opensearch/curator-config.yml --host localhost --port 9200 show_snapshots --
repository $REPOSITORY`

    # Архивируем папку репозитория и складываем архив в хранилище
    cd $SNAPSHOT_DIRECTORY/$REPOSITORY && tar cjf $BACKUP_DIR"/"$i".tar.bz" ./*

    # Удаляем snapshot
    curator_cli --config /etc/opensearch/curator-config.yml --host localhost --port 9200 delete_snapshots --repository
$REPOSITORY --filter_list "{\"filtertype\":\"pattern\",\"kind\":\"regex\",\"value\":\"$SNAPSHOT\"}"

    # Удаляем индекс
    curator_cli --config /etc/opensearch/curator-config.yml --host localhost --port 9200 delete_indices --filter_list
"{\"filtertype\":\"pattern\",\"kind\":\"regex\",\"value\":\"$i\"}"

    # Очищаем папку репозитория
    rm -rf $SNAPSHOT_DIRECTORY/$REPOSITORY/*
  done
fi
```

16.6.2 Удаление устаревших архивов

Ниже представлен скрипт для удаления устаревших архивов индексов.

```
#!/bin/bash

# Удаление бекапов старше $DAYS дней
# ВАЖНО! В имени файла архива может быть только один знак "-" перед датой. Дата должна быть в формате "yyyy.mm.dd".
# Например: aaa_bbb.ccc-yyyy.mm.dd.tar.bz

DAYS=91
BACKUP_DIR="/opt/opensearch/opensearch_backup"

#Определяем пороговую дату для удаления архивов
THRESHOLD=$(date -d "$DAYS days ago" +%Y%m%d)

#echo "THRESHOLD=$THRESHOLD"

FILES=`ls -1 $BACKUP_DIR`

TODELETE=`for i in $FILES; do echo $i | awk -F- '{printf "%s\n",$2 ;}' | awk -F. '{printf "%s%s%s \n",$1,$2,$3 ;}' | sed "s/$/$i/"; done`

echo -e "$TODELETE" |\
while read DATE FILE
  do
    [[ $DATE -le $THRESHOLD ]] && rm -rf $BACKUP_DIR/$FILE
  done
```

Как правило, удалять устаревшие копии необходимо регулярно, и обычно это делается в периоды наименьшей нагрузки на сервер. Вы можете задать команду на запуск выше представленного скрипта как задачу планировщика (cron).

16.6.3 Восстановление индексов из архива

Ниже представлен скрипт для восстановления индекса из архива. Скрипт принимает первым аргументом путь до архива.

```
#!/bin/bash

#Зададим переменные
ARCHIVE=$1
BACKUP_DIR="/opt/opensearch/opensearch_backup"
RECOVERY_DIR="/opt/opensearch/snapshots/recovery/"

# На всякий случай очищаем папку репозитория
rm -rf $RECOVERY_DIR/*

# Разархивируем индекс в папку репозитория
tar xjf $BACKUP_DIR/$ARCHIVE -C $RECOVERY_DIR

# Заносим в переменную $SNAPSHOT имя снапшота в репозитории
SNAPSHOT=`curl -s -XGET "localhost:9200/_snapshot/recovery/_all?pretty" | jq '.snapshots[0].snapshot' | sed 's/\"//g'`
```

Продолжение на следующей странице

```
# Восстанавливаем индекс из снапшота
curl -XPOST "localhost:9200/_snapshot/recovery/$SNAPSHOT/_restore?pretty"

# Нужно выставить небольшую задержку, чтобы Opensearch не ругался на удаление восстанавливаемого снапшота
sleep 30

# Удалим снапшот из репозитория
curl -XDELETE "localhost:9200/_snapshot/recovery/$SNAPSHOT?pretty"

# Очистим папку репозитория
rm -rf $RECOVERY_DIR/*
```

16.6.4 Утилиты для снятия резервной копии PostgreSQL

16.6.4.1 Утилита pg_dumpall

Утилита *pg_dumpall* реализует резервное копирование всего экземпляра (кластера или инстанса) базы данных без указания конкретной базы данных на инстансе. По принципу схожа с *pg_dump*. Добавим, что только утилиты *pg_dump* и *pg_dumpall* предоставляют возможность создания логической копии данных, остальные утилиты, рассматриваемые в этой статье, позволяют создавать только бинарные копии.

```
# pg_dumpall > /tmp/instance.bak
```

Чтобы сразу сжать резервную копию экземпляра базы данных, нужно передать вывод на архиватор *gzip*:

```
# pg_dumpall | gzip > /tmp/instance.tar.gz
```

Ниже приведены параметры, с которыми может вызываться утилита *pg_dumpall*:

-d <имябд>, --dbname=имябд — имя базы данных.

-h <сервер>, --host=сервер — имя сервера.

-p <порт>, --port=порт — TCP-порт, на который принимаются подключения.

-U <пользователь>, --username=пользователь — имя пользователя для подключения.

-w, --no-password — деактивация требования ввода пароля.

-W, --password — активация требования ввода пароля.

-role=<имя роли> — роль, от имени которой генерируется резервная копия.

-a, --data-only — создание резервной копии без схемы данных.

-c, --clean — добавление операторов DROP перед операторами CREATE.

-f <имяфайла>, --file=имяфайла — активация направления вывода в указанный файл.

-g, --globals-only — выгрузка глобальных объектов без баз данных.

-o, --oids — выгрузка идентификаторов объектов (OIDs) вместе с данными таблиц.

-O, --no-owner — деактивация генерации команд, устанавливающих принадлежность объектов, как в исходной базе данных.

-r, --roles-only — выгрузка только ролей без баз данных и табличных пространств.

-s, --schema-only — выгрузка только схемы без самих данных.

-S <имя*пользователя*>, --*superuser=имя*пользователя — привилегированный пользователь, используемый для отключения триггеров.

-t, --tablespaces-only — выгрузка табличных пространства без баз данных и ролей.

-v, --verbose — режим подробного логирования.

-V, --version — вывод версии утилиты pg_dumpall.

16.6.4.2 Утилита pg_restore

Утилита позволяет восстанавливать данные из резервных копий. Например, чтобы восстановить только определенную БД (в нашем примере zabbix), нужно запустить эту утилиту с параметром *-d*:

```
# pg_restore -d zabbix /tmp/zabbix.bak
```

Чтобы этой же утилитой восстановить определенную таблицу, нужно использовать ее с параметром *-t*:

```
# pg_restore -a -t history /tmp/zabbix.bak
```

Также утилитой pg_restore можно восстановить данные из бинарного или архивного файла. Соответственно:

```
# pg_restore -Fc zabbix.bak
```

```
# pg_restore -Ft zabbix.tar
```

При восстановлении можно одновременно создать новую базу:

```
# pg_restore -Ft -C zabbix.tar
```

Восстановить данные из дампа также возможно при помощи *psql*:

```
# psql zabbix < /tmp/zabbix.dump
```

Если для подключения нужно авторизоваться, вводим следующую команду:

```
# psql -U zabbix -W zabbix < /tmp/zabbix.dump
```

Ниже приведен синтаксис утилиты *pg_restore*.

-h <сервер>, --host=сервер — имя сервера, на котором работает база данных.

-p <порт>, --port=порт — TCP-порт, через базу данных принимает подключения.

-U <пользователь>, --username=пользователь — имя пользователя для подключения.

-w, --no-password — деактивация требования ввода пароля.

-W, --password — активация требования ввода пароля.

-role=<имя роли> — роль, от имени которой выполняется восстановление резервная копия.

<имя_файла> — расположение восстанавливаемых данных.

-a, --data-only — восстановление данных без схемы.

-c, --clean — добавление операторов DROP перед операторами CREATE.

-C, --create — создание базы данных перед запуском процесса восстановления.

-d <имя*бд>, --dbname=имя*бд — имя целевой базы данных.

-e, --exit-on-error — завершение работы в случае возникновения ошибки при выполнении SQL-команд.

-f <имя*файла>, --file=имя*файла — файл для вывода сгенерированного скрипта.

-F <формат>, --format=формат — формат резервной копии. Допустимые форматы:

- p, plain — формирует текстовый SQL-скрипт;
- c, custom — формирует резервную копию в архивном формате;
- d, directory — формирует копию в directory-формате;
- t, tar — формирует копию в формате tar.

-I <индекс>, --index=индекс — восстановление только заданного индекса.

-j <число-заданий>, --jobs=число-заданий — запуск самых длительных операций в нескольких параллельных потоках.

-l, --list — активация вывода содержимого архива.

-L <файл-список>, --use-list=файл-список — восстановление из архива элементов, перечисленных в файле-списке в соответствующем порядке.

-n <пространство_имен>, --schema=схема — восстановление объектов в указанной схеме.

-O, --no-owner — деактивация генерации команд, устанавливающих владение объектами по образцу исходной базы данных.

-P <имя-функции(тип-аргумента[, ...])>, --function=имя-функции(тип-аргумента[, ...]) — восстановление только указанной функции.

-s, --schema-only — восстановление только схемы без самих данных.

-S <пользователь>, --superuser=пользователь — учетная запись привилегированного пользователя, используемая для отключения триггеров.

-t <таблица>, --table=таблица — восстановление определенной таблицы.

-T <триггер>, --trigger=триггер — восстановление конкретного триггера.

-v, --verbose — режим подробного логирования.

-V, --version — вывод версии утилиты pg_restore.

16.6.4.3 Утилита pg_basebackup

Утилитой *pg_basebackup* можно выполнять резервное копирования работающего кластера баз данных PostgreSQL. Результирующий бинарный файл можно использовать для

репликации или восстановления на определенный момент в прошлом. Утилита создает резервную копию всего экземпляра базы данных и не дает возможности создавать слепки данных отдельных сущностей. Подключение pg_basebackup к PostgreSQL выполняется при помощи протокола репликации с полномочиями суперпользователя или с правом REPLICATION.

Для выполнения резервного копирования локальной базы данных достаточно передать утилите *pg_basebackup* параметр *-D*, обозначающий директорию, в которой будет сохранена резервная копия:

```
# pg_basebackup -D /tmp
```

Чтобы создать сжатые файлы из табличных пространств, добавим параметры *-Ft* и *-z*:

```
# pg_basebackup -D /tmp -Ft -z
```

То же самое, но со сжатием bzip2 и для экземпляра базы с общим табличным пространством:

```
# pg_basebackup -D /tmp -Ft | bzip2 > backup.tar.bz2
```

Ниже приведен синтаксис утилиты *pg_basebackup.*

-d <строка*подключения>, --dbname=строка*подключения — определение базы данных в виде строки для подключения.

-h <сервер>, --host=сервер — имя сервера с базой данных.

-p <порт>, --port=порт — TCP-порт, через базу данных принимает подключения.

-s <интервал>, --status-interval=интервал — количество секунд между отправками статусных пакетов.

-U <пользователь>, --username=пользователь — установка имени пользователя для подключения.

-w, --no-password — отключение запроса на ввод пароля.

-W, --password — принудительный запрос пароля.

-V, --version — вывод версии утилиты *pg_basebackup*.

-?, --help — вывод справки по утилите pg_basebackup.

-D каталог, --pgdata=каталог — директория записи данных.

-F <формат>, --format=формат — формат вывода. Допустимые варианты:

- p, plain — значение для записи выводимых данных в текстовые файлы;
- t, tar — значение, указывающее на необходимость записи в целевую директорию в формате tar.

-r <скорость*передачи>, --max-rate=скорость*передачи — предельная скорость передачи данных в Кб/с.

-R, --write-recovery-conf — записать минимальный файл *recovery.conf* в директорию вывода.

-S <имя*слота>, --slot=имя*слота — задание слота репликации при использовании WAL в режиме потоковой передачи.

-T <каталог_1=каталог_2>, --tablespace-mapping=каталог_1=каталог_2 — активация миграции табличного пространства из одного каталога в другой каталог при копировании.

--xlogdir=каталог_xlog — директория хранения журналов транзакций.

-X <метод>, --xlog-method=метод — активация вывода файлов журналов транзакций WAL в резервную копию на основе следующих методов:

- f, fetch — включение режима сбора файлов журналов транзакций при окончании процесса копирования;
- s, stream — включение передачи журнала транзакций в процессе создания резервной копии.

-z, --gzip — активация gzip-сжатия результирующего tar-файла.

-Z <уровень>, --compress=уровень — определение уровня сжатия механизмом gzip.

-c , --checkpoint=fast|spread — активация режима реперных точек.

-l <метка>, --label=метка — установка метки резервной копии.

-P, --progress — активация в вывод отчета о прогрессе.

-v, --verbose — режим подробного логирования.

16.7 Резервное копирование пользовательского контента

Для выполнения резервного копирования пользовательского контента необходимо выполнить экспорт необходимых объектов.

Платформа Радар позволяет выполнить массовый экспорт, как и всех объектов, так и выбранных. Экспорт выполняется посредством механизмов, предоставляемых боковой панелью и универсальными таблицами (подробнее см. раздел «Интерфейс платформы»).

Для восстановления пользовательского контента необходимо выполнить импорт, сохраненного ранее контента. Операция выполняется посредством механизмов, предоставляемых боковой панелью и универсальными таблицами (подробнее см. раздел «Интерфейс платформы»).

Экспорт и импорт пользовательского контента доступен в следующих разделах:

- Типы инцидентов;
- Правила корреляции;
- Пересылка событий;
- Фильтры потока событий;
- Макросы;
- Табличные списки;
- Источники;
- Правила разбора;
- Обогащение;

- Рабочие столы;
- Отчеты.

16.8 Настройка времени сессий пользователя

Перейдите в административный раздел управления сервисом авторизации.

Для этого откройте консоль администрирования **KeyCloak** (*https://<адрес Платформы Радар>:8180*),выберите "**Administration Console**" и перейдите в пункт меню "**Настройки Realm - Токены**".

Затем выберите необходимую настройку:

- **Таймаут сессии SSO** (по умолчанию 30 минут);

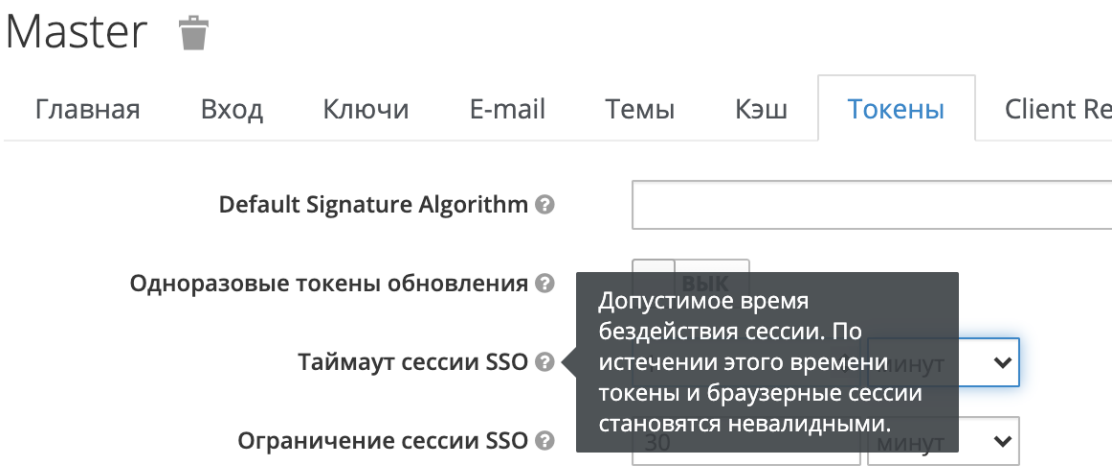


Рис. 160 – Таймаут сессии SSO

- **Ограничение сессии SSO** (по умолчанию 10 часов).

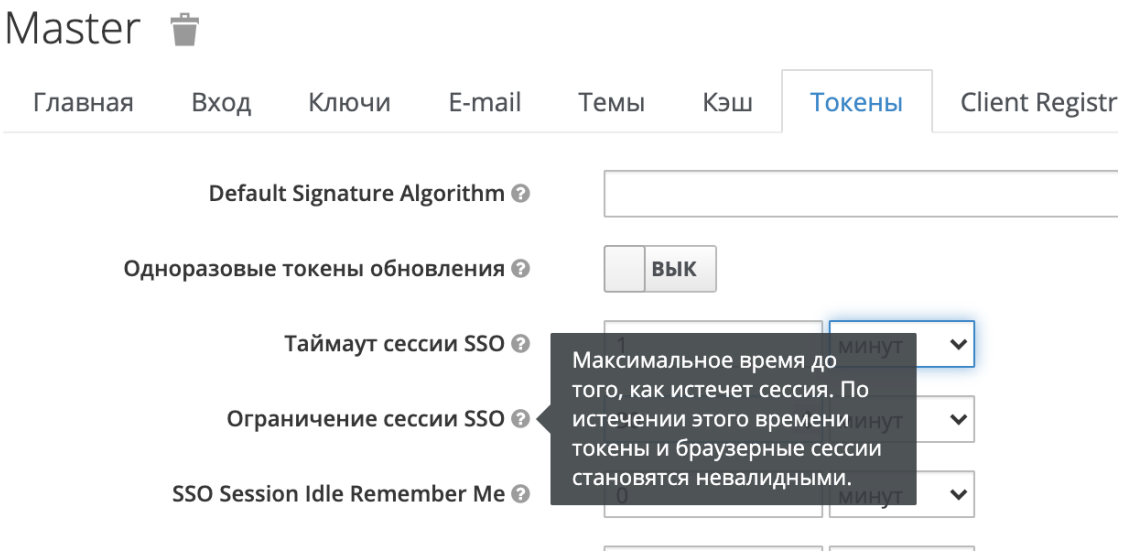


Рис. 161 – Ограничение сессии SSO

16.9 Настройка архивации событий

16.9.1 Проверка настроек политики архивации устаревших событий

Для проверки текущего состояния политики архивации выполните следующие действия:

1. Подключитесь по SSH на сервер архивации событий (узел **Платформы Радар** с ролью **DATA**).
2. Откройте конфигурационный файл

   /opt/pangeoradar/support_tools/elastic/indices_route.sh.
3. Посмотрите значения параметров **cold_day** и **delete_day**. По умолчанию они должны иметь значение 27 (27 дней оперативного хранения).

Для проверки работы политики архивации выполните следующие действия:

1. В веб-интерфейсе **Платформы Радар** перейдите в раздел "**Просмотр событий**".
2. Для формирования отчета выставите в области задания временного интервала промежуток времени длиннее, чем заданный промежуток в политиках архивации, например, 30 дней считая от сегодняшнего дня.

На экране в статистике по событиям не должны отображаться события старше 27 дней.

16.9.2 Изменение политики архивации устаревших событий

Для изменения политики архивации выполните следующие действия:

1. Зайдите по SSH на сервер архивации событий (узел **Платформы Радар** с ролью **DATA**).
2. Откройте конфигурационный файл узла

   /opt/pangeoradar/support_tools/elastic/indices_route.sh.
3. Установите для параметров **cold_day** и **delete_day** новое значение оперативного хранения данных.
4. Принудительно запустите архивацию, выполнив команду:

   bash /usr/bin/bash /opt/pangeoradar/support_tools/elastic/indices_route.sh
5. Дождитесь окончания выполнения скрипта.

Для проверки введённых изменений выполните следующие действия:

1. В веб-интерфейсе **Платформы Радар** перейдите в раздел "**Просмотр событий**".
2. Проверьте, что нет индексов старше 20 дней (алгоритм проверки описан в предыдущем подразделе).
3. Вернитесь в терминал сервера архивации событий (узел **DATA**).
4. Перейдите в директорию /data/archive.
5. Выведите листинг директории командой:

   ls -lah

6. Убедитесь в появлении новых архивов.
7. Для просмотра запланированных заданий выполните команду:

   ```
   crontab -l
   ```

8. Убедитесь в наличии запланированного задания по ротированию и архивации событий.

В результате проведенных действий в веб-интерфейсе **Платформы Радар** должны отсутствовать записи об индексах и событиях старше заданного количества дней в политике архивации.

Должны быть созданы новые архивы с названиями индексов, экспортированных из системы для архивации и долгосрочного хранения.

16.9.3 Восстановление данных из архива

В **Платформе Радар** предусмотрена возможность обращения к устаревшим событиям, находящимся на архивном хранении.

Для того, чтобы получить доступ к архивным данным, необходимо сначала выполнить восстановление данных из архива:

1. Подключитесь по SSH на сервер архивации событий (узел **Платформы Радар** с ролью **DATA**).
2. Запустите скрипт восстановления данных командой:

   ```
   bash /opt/pangeoradar/support_tools/elastic/restore.sh
   ```

3. В появившемся окне укажите фильтр ***** и нажмите "**ОК**".
4. Выберите интересующий индекс из списка, выделите напротив него чек-бокс (запомните имя восстанавливаемого индекса) и нажмите "**ОК**".
5. Дождитесь окончания восстановления (восстановление осуществляется в фоновом режиме).

Для просмотра восстановленных данных необходимо:

1. Перейдите в веб-интерфейс **Платформы Радар** в раздел "**Просмотр событий**".
2. В поле "**Время**" укажите временной диапазон восстанавливаемого индекса.
3. В поле "**Индекс**" укажите имя восстанавливаемого индекса.
4. Нажмите кнопку "**Поиск**".

На экран должен быть выведен список событий (включая диаграмму), относящийся к восстанавливаемому индексу и указанному временному периоду.

16.10 Настройка и проверка интеграции через API

В **Платформе Радар** реализована интеграция посредством API с IRP-системами - R-Vision и Security Vision.

16.10.1 Передача через API информации об инциденте во внешнюю систему

Для настройки интеграции с внешними системами через API необходимой выполнить следующие действия:

1. Подключитесь по SSH к узлу **Платформы Радар** с ролью **Master**.
2. Внесите следующие изменения в конфигурационный файл узла

   /opt/pangeoradar/configs/pangeoradar-pgr-wal-listener.yaml:

   - Добавьте реквизиты интегрируемой системы (R-Vision) — ключ доступа к API R-Vision и IP-адрес R-Vision;
   - Измените схему соответствия полей согласно требованиям интеграции.
3. Запустите сервис **pangeoradar-pgr-wal-listener**:

   service pangeordar-pgr-wal-listener start

Для проверки проведенного подключения выполнить следующие действия:

1. Зайдите в веб-интерфейс **Платформы Радар** (с правами администратора).
2. Зайдите в раздел ***Инциденты - Инциденты***.
3. Создайте инцидент вручную, нажав кнопку "**Создать инцидент**".

При настроенном API новый инцидент передается во внешнюю систему в автоматическом режиме в процессе создания. Созданный инцидент автоматически создан в IRP.

16.10.2 Генерация ключа для доступа к API

Для работы по API необходимо сгенерировать ключ для доступа к API. Для этого выполните следующие действия:

1. Перейдите в веб-интерфейс **Платформы Радар** в раздел **Администрирование** → **Кластер** → вкладка **API ключи** (см. раздел «API ключи»).
2. Добавьте ключ с наименованием, например, integration.
3. Подключитесь по SSH к узлу **Платформы Радар** с ролью **Master**.
4. Выполните с использованием ключа "**integration**" следующую команду:

```
curl -k -H "PgrApiKey:<ключ, сгенерированный на шаге 2 >" "https://<IP-адрес ПлатформыРадар>:9000/cruddy/public/api/v1/incidents?page=1&per_page=1&order=id%20DESC"
```

На экран будут выведена запись по одному инциденту в формате JSON.

16.11 Настройка политики противодействия попыткам подбора пароля

Платформа Радар обладает встроенными механизмами противодействия попыткам подбора пароля (BruteForce атаки) на базе открытого ПО **Keycloak** (идентификационный брокер).

Для настройки политики противодействия попыткам подбора пароля выполните следующие действия:

1. С правами администратора войдите в специализированный веб-интерфейс **Keycloak Платформы Радар** *https://<адрес Платформы Радар>:8180* (см. «Рис. 162»).

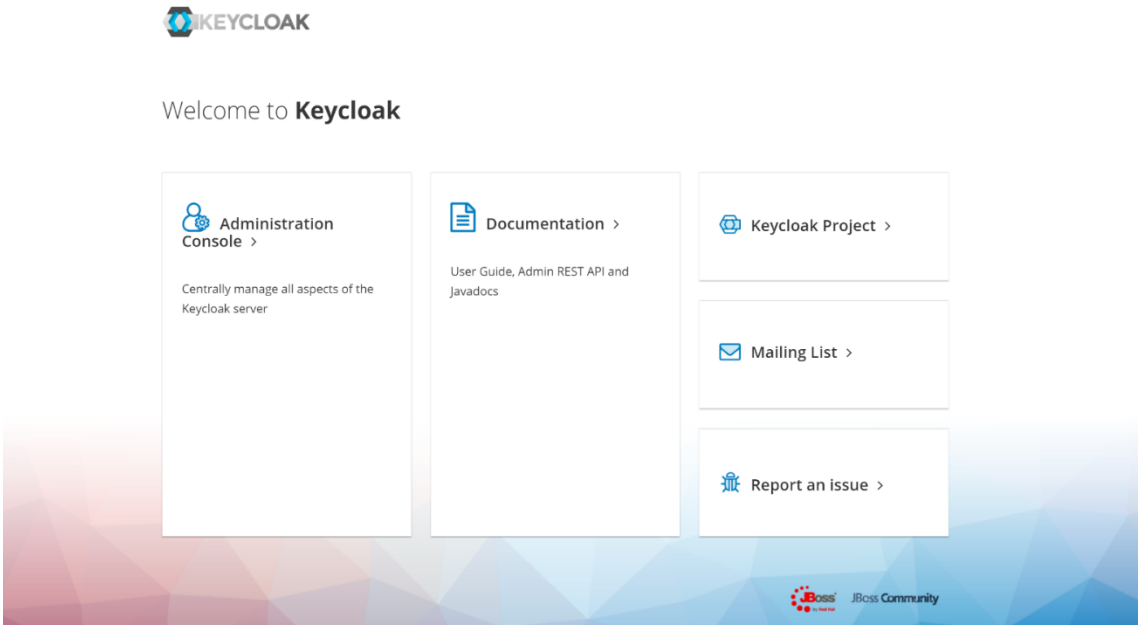


Рис. 162 – Интерфейс "идентификационного брокера" Keycloak

2. Перейдите в раздел ***Administration Console - Защита безопасности - Определение Brute Force*** (см. «Рис. 163»).

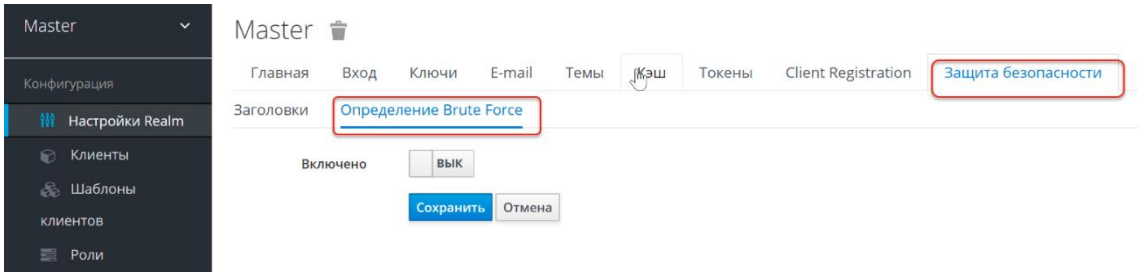


Рис. 163 – Раздел "Определение Brute Force" при отключенных политиках.

3. Включите политику "**Определение Brute Force**", установив переключатель в поле "**Включено**" в положение "**вкл**". Откроются параметры настройки политики (см. «Рис. 164»).

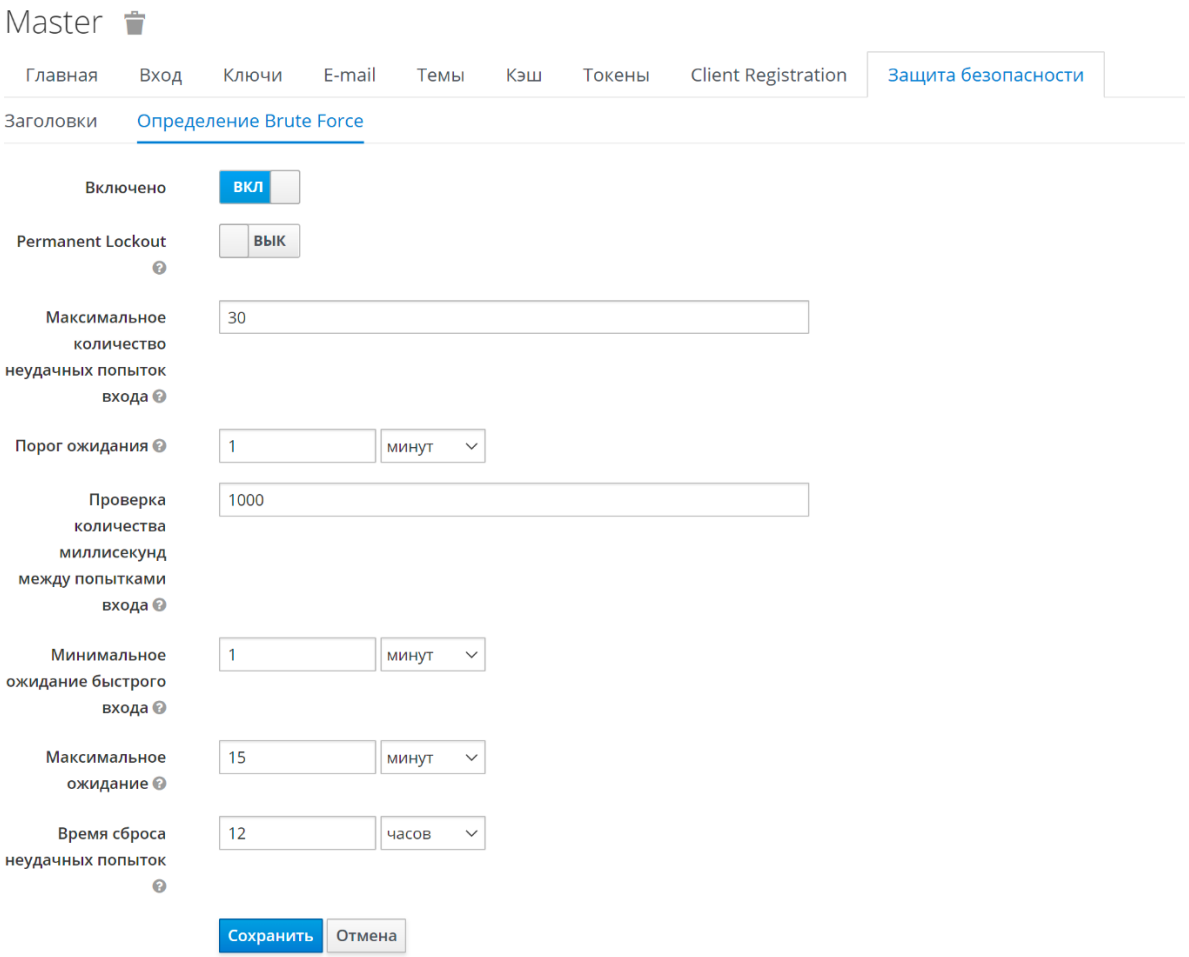


Рис. 164 – Параметры настройки политики

4. При необходимости установите следующие параметры:
   - **Максимальное количество неудачных попыток входа** (основная настройка) — количество неудачных попыток входа до блокировки пользователя;
   - **Порог ожидания** (основная настройка) — если порог ошибок превышен, сколько времени пользователь будет заблокирован;
   - **Проверка количества миллисекунд между попытками входа** — если попытки аутентификации происходят слишком часто, то пользователя необходимо заблокировать;
   - **Минимальное ожидание быстрого входа** — как долго ждать после неудачной попытки быстрого входа;
   - **Максимальное ожидание** — максимальное время, на которое пользователь будет заблокирован;
   - **Время сброса неудачных попыток** — через какое время счетчик неудачных попыток будет сброшен.
5. Сохраните настройки, нажав кнопку "**Сохранить**".

16.12 Проверка работы сервисов

16.12.1 Проверка работы сервисов платформы

Для выполнения проверки выполните следующие действия:

1. Перейдите в раздел **Администрирование** → **Кластер** → **Узлы системы** (см. «Рис. 165»).

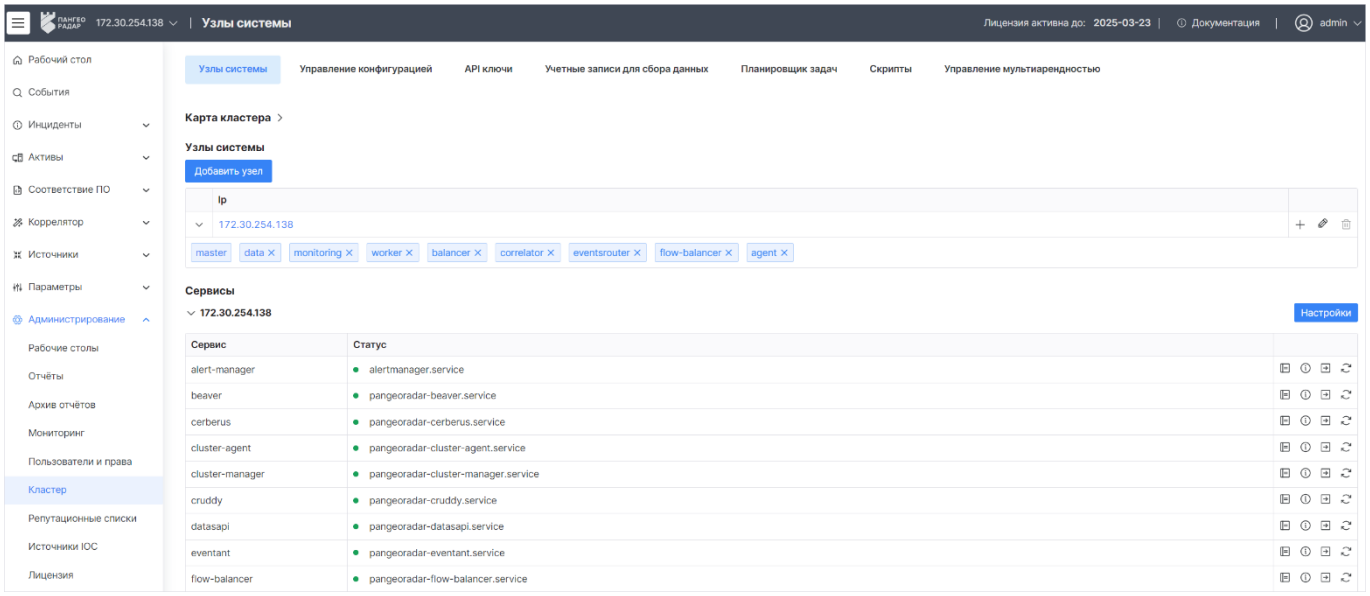


Рис. 165 -- Раздел Кластер. Вкладка "Узлы системы"

Текущее состояние сервиса отображается с помощью индикатора:

- 🟢 (зеленый) – сервис работает в штатном режиме;
- 🔴 (красный) – сервис не отвечает.

2. Для детального просмотра и проверки состояния сервисов на узле, необходимо нажать кнопку **Настройки** в поле с IP-адресом узла, на котором развернуты сервисы. Откроется форма просмотра узла кластера (см. «Рис. 166»).

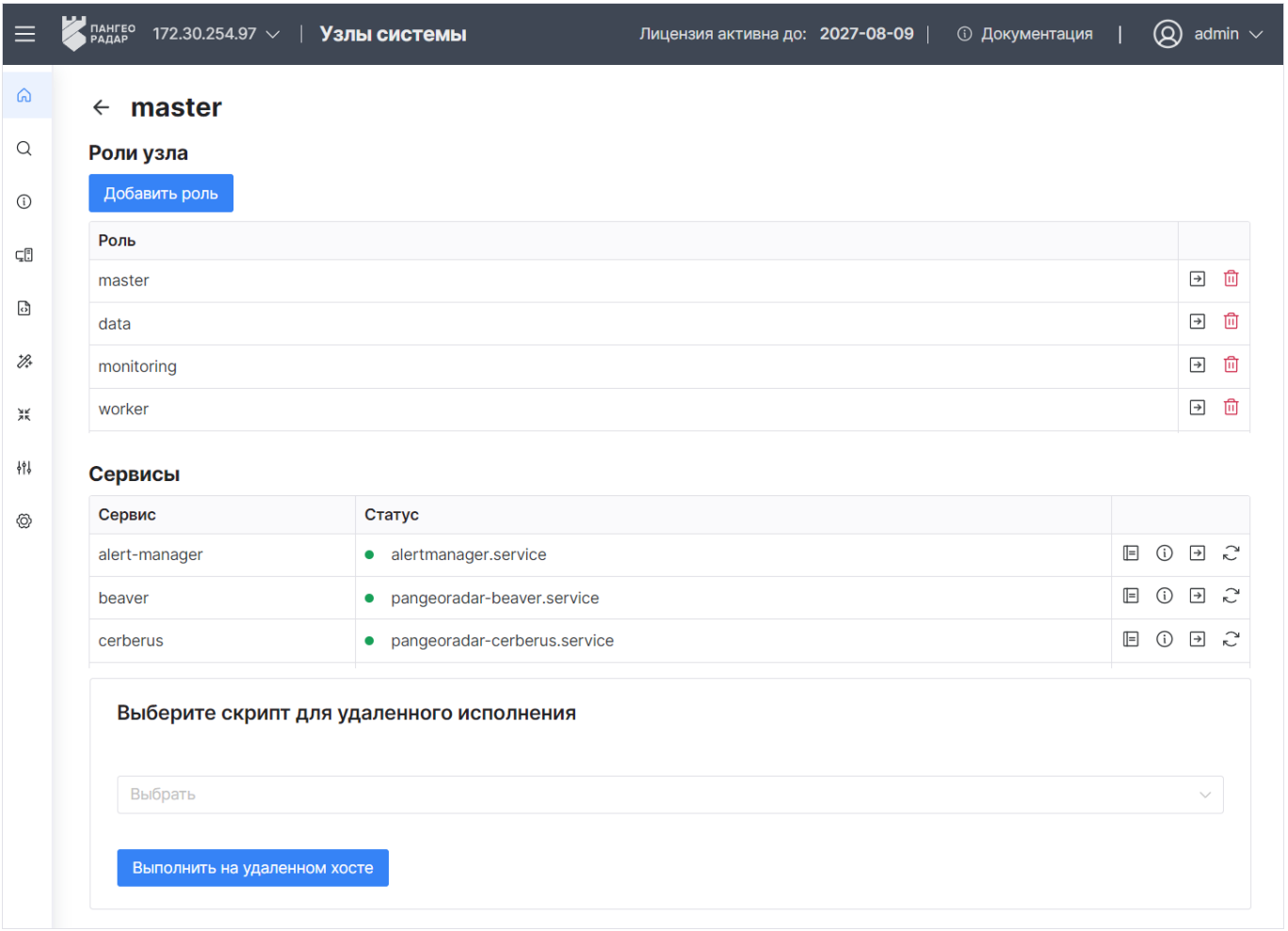


Рис. 166 – Форма настройки узла кластера

На форме отображается следующая информация:

- Наименование узла;
- Список ролей узла;
- Сервисы, запущенные на узле.

3. Для просмотра журнала работы сервиса нажмите кнопку . Откроется окно "Логи сервиса" (см. «Рис. 167»).

Рис. 167 – Пример журнала работы сервиса

4. Для просмотра подробной информации о текущем состоянии сервиса нажмите кнопку . Откроется окно "Статус сервиса" (см. «Рис. 168»).

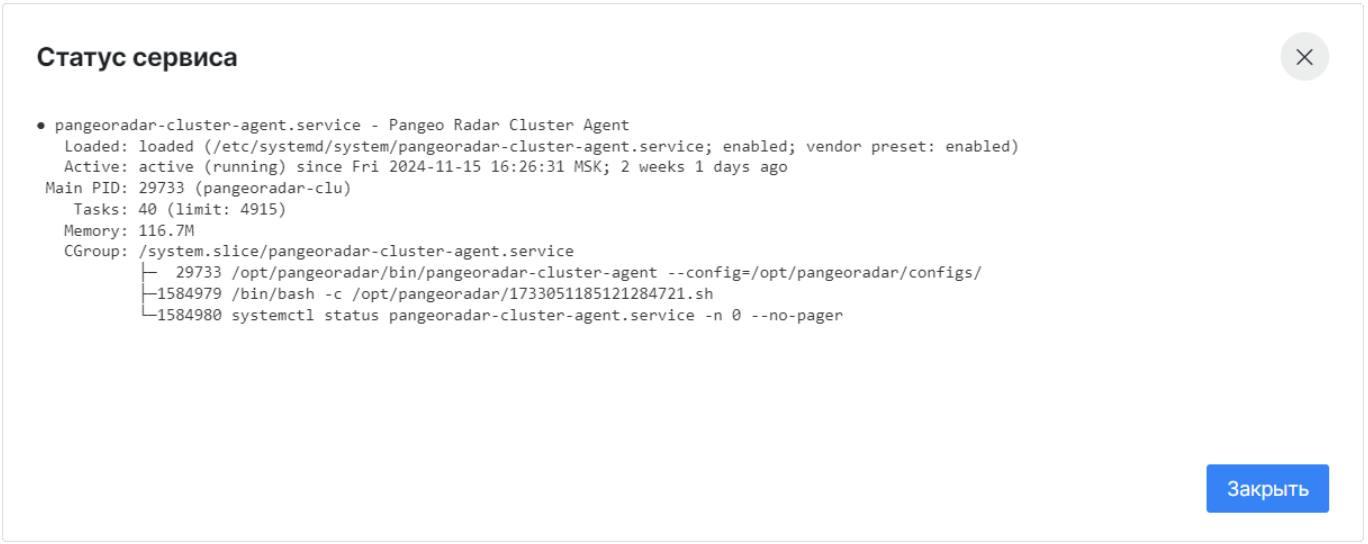


Рис. 168 – Пример статуса сервиса

16.12.2 Проверка распределенной установки

Перейдите в раздел **Администрирование → Кластер → Узлы системы** и убедитесь, что список узлов и их ролей, совпадает с тем, что был задан на этапе распределенной установки (см. «Рис. 169»).

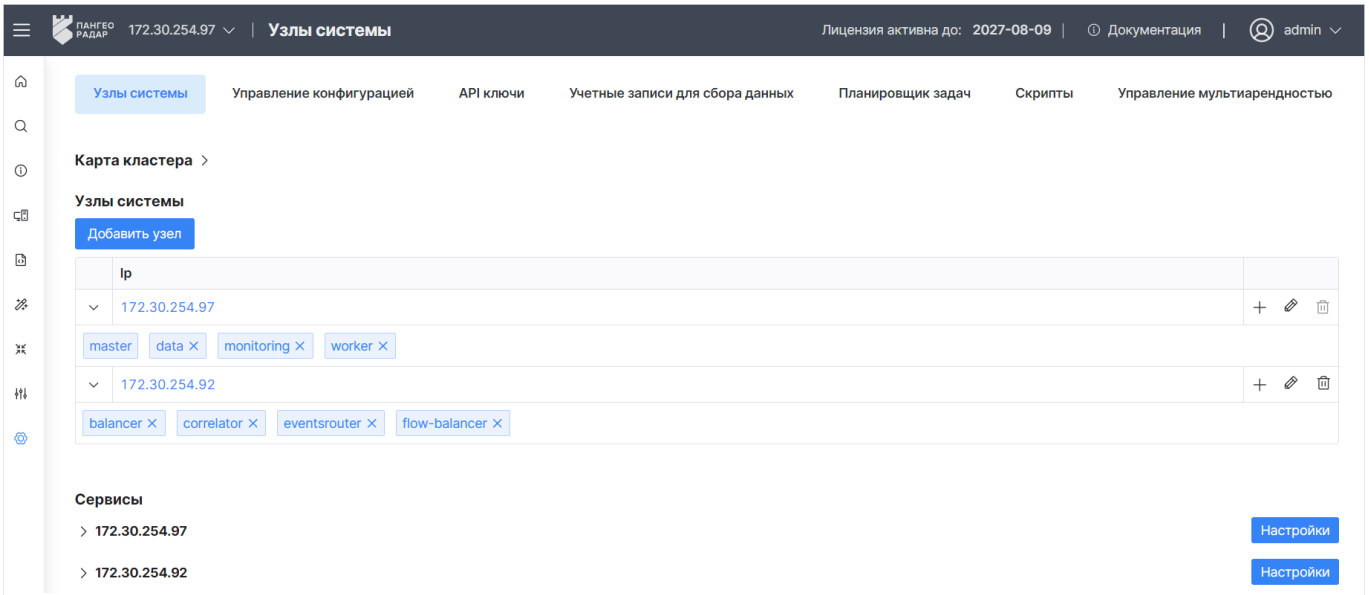


Рис. 169 – Раздел "Кластер". Список узлов платформы

Проверьте индикацию, состояние и журналы работы сервисов на всех узлах. Проверка выполняется по аналогии с «Проверка работы сервисов платформы».

Для подтверждения достоверности информации, полученной через веб-интерфейс **Платформы Радар**, можно подключиться к выбранному для проверки узлу и выполнить команду:

```
# service pangeoradar-<наименование сервиса, например kafka> status
```

В результате выполнения команды в окне терминала должна отобразиться та же информация о сервисе, что и в окне веб-интерфейса при просмотре состояния сервиса (кнопка ⓘ).

Для проверки IP-адреса узла выполните команду:

```
# ip a
```

Полученный в результате выполнения команды IP-адрес должен совпадать с IP-адресом узла в веб-интерфейсе.

16.12.3 Добавление нового узла кластера

При необходимости расширения производительных возможностей **Платформы Радар** существует возможность добавить дополнительный экземпляр узла с той или иной ролью.

1. Убедитесь, что соблюдены следующие условия для добавления нового узла:
    - узел развернут и готов принимать внешние соединения;
    - на узле установлена ОС - Debian 12 / Astra Linux 1.8 в 64-разряднсти;
    - на узле поднят SSH-сервер (см. раздел «Настройка SSH-сервера на Debian 12»);
    - узел разрешает соединения под привилегированным пользователем root.
2. Войдите в веб-интерфейс на узле с ролью **MASTER** и перейдите в раздел **Администрирование** → **Кластер** → вкладка **Узлы** (см. «Рис. 169»).
3. Нажмите кнопку **Добавить узел** (см. «Рис. 170»).

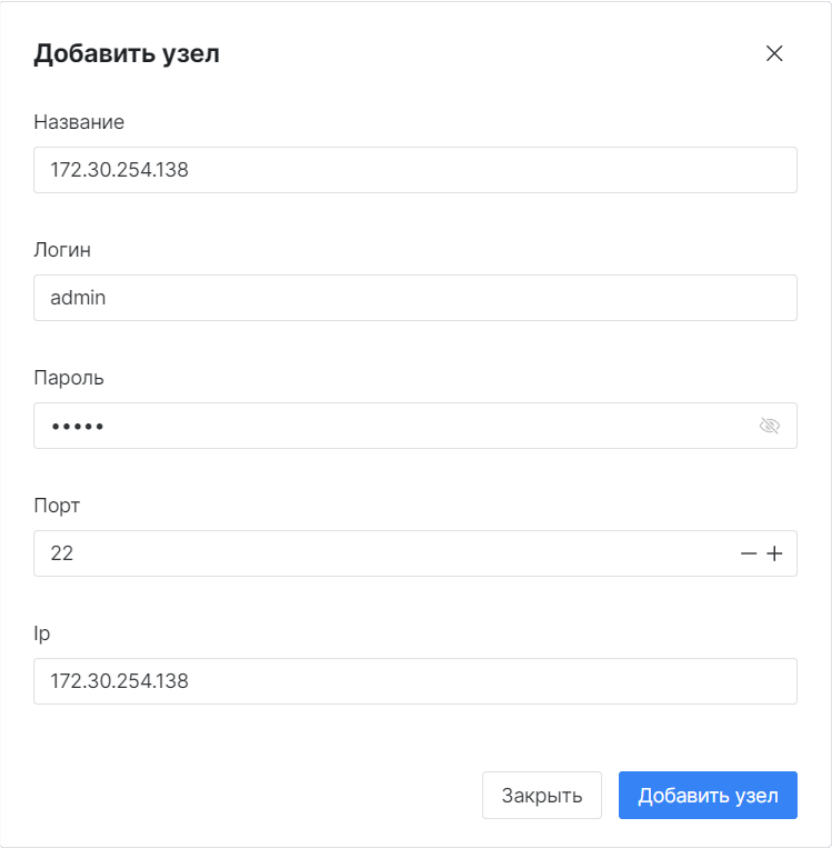


Рис. 170 – Окно "Добавить узел"

4. Укажите в окне следующую информацию:
    - в поле **Название** укажите наименование узла;

- в полях **Логин** и **Пароль** укажите данные для подключения привилегированного пользователя root к узлу;
- в полях **IP** и **Порт** укажите IP-адрес и порт подключения к узлу.

5. Нажмите кнопку **Добавить узел**.

16.12.4 Устранение проблем в работе сервисов

Переустановка и перезапуск сервиса может потребоваться в случае, если сервис не отвечает (индикатор ●).

Для переустановки сервиса нажмите кнопку .

Для перезапуска сервиса нажмите кнопку .

При возникновении непредвиденных ошибок обратитесь к разделу «Режимы работы Платформы Радар».

16.12.5 Изменение конфигурации сервисов Платформы Радар

Для выполнения тонкой настройки сервисов, для нужд и особенностей вашей организации, в **Платформе Радар** предусмотрена возможность изменения конфигурации сервисов платформы.

Примечание: *конфигурация сервисов по умолчанию подходит для большинства сценариев использования. Не рекомендуется менять конфигурацию без лишней необходимости, если это явно не указано в отдельных инструкциях*.

Изменение конфигурации можно выполнить следующими способами:

- **Централизованно** – через веб-интерфейс платформы. Подробнее см. раздел «Управление конфигурацией»;
- **Вручную** – непосредственное изменение конфигурационного файла сервиса. Данный способ будет разобран в данном разделе.

Конфигурационные файлы сервисов располагаются по следующему пути:

opt/pangeoradar/configs/<Наименование сервиса>/config.json

Например, opt/pangeoradar/configs/logproxy/config.json.

Наименования сервисов и соответствующих служб можно посмотреть в разделе **Администрирование** → **Кластер** → вкладка **Узлы** (см. раздел «Сервисы»).

Для ручного изменения конфигурационных файлов выполните следующие действия:

1. Откройте на редактирование необходимый конфигурационный файл и внесите изменения.
2. Перейдите в раздел **Администрирование** → **Кластер** → вкладка **Узлы** и найдите сервис, параметры которого были изменены.
3. Перезапустите сервис, нажав кнопку .

4. Удостоверьтесь, что после перезапуска сервис работает в штатном режиме (индикатор ●).

16.13 Режимы работы Платформы Радар

16.13.1 Общие данные

Платформа Радар может работать в следующих режимах:

- **Штатный режим** – работают все сервисы, события собираются со всех подключённых источников. Используется по умолчанию.
- **Сервисный режим** – позволяет перевести узел с соответствующей серверной ролью в режим обслуживания. Используется в следующих случаях:
  - неработоспособности отдельных сервисов;
  - требуется выполнить работы по обновлению и обслуживанию сервисов;
  - обновление операционной системы и её компонентов;
  - другие работы, требующие перезагрузки ОС или выключения сервера с последующим длительным периодом недоступности.

16.13.2 Режим обслуживания узла с ролью MASTER

Для перевода узла **MASTER** в режим обслуживания требуется приостановить сбор событий со всех источников.

Для этого в интерфейсе платформы перейдите в раздел **Администрирование** → **Кластер** → вкладка **Узлы**.

Откройте форму просмотра узла, на котором установлен агент сбора (например, **MASTER**, **AGENT** или **AGENT WIN**) и перейдите к блоку **Управление агентом** (см. Рис. 171»).

В поле **Сборщики и отправители** нажмите кнопку **Остановить**.

После проведения обслуживания необходимо запустить остановленный ранее сбор событий и при необходимости перезапустить агент.

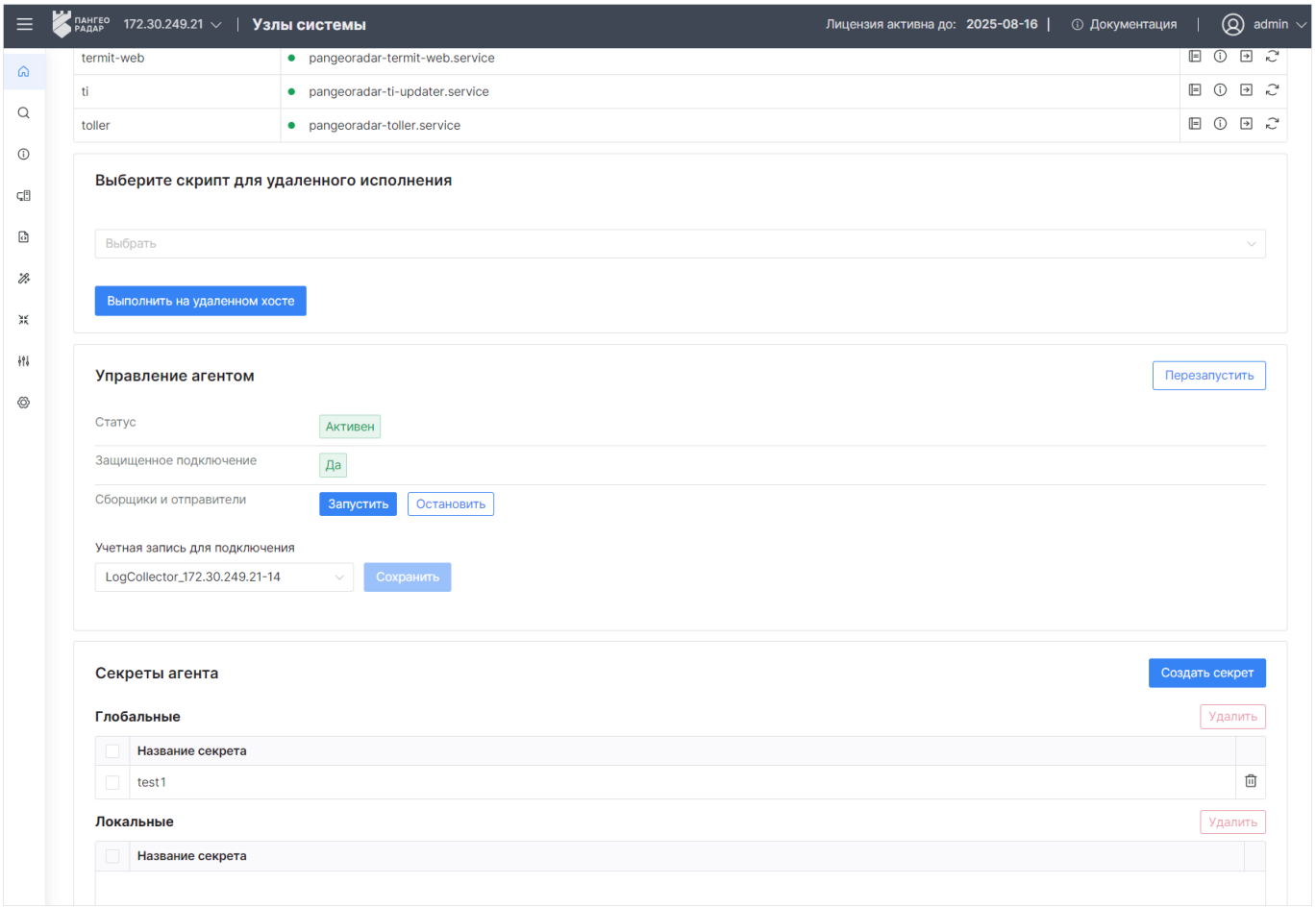


Рис. 171 – Форма просмотра узла. Блок "Управление агентом"

16.13.3 Режим обслуживания узла с ролью BALANCER

Для перевода узла с ролью **BALANCER** в режим обслуживания необходимо остановить сервис **pangeoradar-logproxy.service**:

```
# sudo service pangeoradar-logproxy.service stop
```

В случаях, когда планируемое время обслуживания превышает 1 час, то также рекомендуется перевести в режим обслуживания LOG-COLLECTOR.

После завершения работ по обслуживанию запустите сервис **pangeoradar-logproxy.service**:

```
# sudo service pangeoradar-logproxy.service start
```

16.13.4 Режим обслуживания узла с ролью WORKER

Для перевода узла с ролью **WORKER** в режим обслуживания необходимо остановить сервис **pangeoradar-termit.service**:

```
# sudo service pangeoradar-termit.service stop
```

В случаях, когда планируемое время обслуживания превышает 1 час, то также рекомендуется перевести в режим обслуживания узел с ролью BALANCER.

После завершения работ по обслуживанию запустите сервис **pangeoradar-termit.service**:

```
# sudo service pangeoradar-termit.service start
```

16.13.5 Режим обслуживания узла с ролью DATA

Для перевода узла с ролью **DATA** в режим обслуживания необходимо остановить сервис **opensearch.service**:

```
# sudo service pangeoradar-termit.service stop
```

И остановить узел с ролью MASTER.

После завершения работ по обслуживанию требуется запустить сервис **opensearch.service**:

```
# sudo service opensearch.service start
```

16.13.6 Режим обслуживания узла с ролью CORRELATOR

Для перевода узла с ролью **CORRELATOR** в режим обслуживания необходимо остановить сервис **pangeoradar-logmule2.service**:

```
# sudo service pangeoradar-logmule2.service stop
```

В случаях, когда на кластере всего один узел корреляции событий и планируемое время обслуживания превышает период в 1 час рекомендуется также перевести в режим обслуживания узел с ролью.

После завершения работ по обслуживанию требуется запустить сервис **pangeoradar-logmule2.service**:

```
# sudo service pangeoradar-logmule2.service start
```

16.13.7 Режим обслуживания компонента LOG-COLLECTOR

Для перевода компонента **LOG-COLLECTOR** в режим обслуживания необходимо остановить сервис **pangeoradar-logcollector.service**.

```
# sudo service pangeoradar-logcollector.service stop
```

После завершения работ по обслуживанию требуется запустить сервис **pangeoradar-logcollector.service**:

```
# sudo service pangeoradar-logcollector.service start
```

16.14 Установка контента, поставляемого с платформой

В комплект поставки платформы включен контент, который предназначен для добавления в платформу данных по умолчанию.

В рамках поставки данный контент называется expert-pack (далее эксперт пак).

В общем случае эксперт пак может содержать следующий контент:

- Правила корреляции;
- Фильтры потока событий;
- Табличные списки;
- Макросы;

- Типы инцидентов;
- Источники;
- Правила разбора;
- Правила обогащения.

Эксперт пак поставляется в репозитории, который устанавливается на узел с ролью **MASTER**.

Для выполнения установки выполните команду:

```
# sudo apt install pangeoradar-expert-packs
```

При выполнении обновления платформы, эксперт пак будет автоматически обновлен до актуальной версии.

16.15 Возможные проблемы при эксплуатации платформы

16.15.1 Проблема доступа к базе данных

Описание проблемы:

При выполнении **жесткого сброса (hard reset)** может произойти потеря соединения с базой данных, что приведет к неработоспособности продукта.

Условия возникновения:

- Выполнение жесткого сброса устройства/системы.
- Аварийное отключение питания.

Последствия:

- Продукт становится неработоспособным.
- Данные могут быть недоступны или повреждены.
- Требуется ручное восстановление базы данных.

Рекомендации по исправлению:

- Восстановите базу данных из резервной копии.
- Обратитесь в службу технической поддержки.

Рекомендации по предотвращению:

- Выполняйте выключение/перезагрузку штатными средствами ОС.
- Используйте бесперебойные источники питания.

16.15.2 Проблема сбора данных с активов

Описание проблемы:

При попытке сбора данных с узлов на ОС Windows, возникают ошибки следующего вида:

```
"Feb 18 14:42:02 newplatform pangeoradar-sonar[920]:
{"file":"/build/cmd/sonar/main.go:1229","func":"main.processDaemon.func1","level":
"error","msg":"Handler /scan/software completed with error: get OS:
[172.30.250.102] Failed to run cmd: exit status 127","time":"2025-02-
18T14:42:02+03:00"}"

Mar 05 11:46:18 v-qa-cl1-master.pgr.local pangeoradar-sonar[1364213]:
{"file":"/build/cmd/sonar/main.go:1229","func":"main.processDaemon.func1","level":
"error","msg":"Handler /scan/hardware completed with error: get hardware info:
[172.30.254.101] failed to get processor info: [172.30.254.101] Failed to run cmd:
exit status 1","time":"2025-03-05T11:46:18+03:00"}

Mar 05 11:46:55 v-qa-cl1-master.pgr.local pangeoradar-sonar[1364213]:
{"file":"/build/cmd/sonar/main.go:1229","func":"main.processDaemon.func1","level":
"error","msg":"Handler /scan/software completed with error: get OS:
[172.30.254.101] Failed to run cmd: exit status 1","time":"2025-03-
05T11:46:55+03:00"}
```

Условия возникновения:

- Версия платформы 4.0.0 и выше.
- На машинах, с которых выполняется сбор данных, установлена ОС Windows.
- Язык ОС - русский.

Последствия:

Данные с машин не собираются или собираются сведения только об аппаратном ПО.

Рекомендации по исправлению:

1. Установите протокол SMB на Windows-сервер.
2. Создайте пользователя.
3. Добавьте пользователя в группу **Administrators/Администраторы**.
4. Добавьте пользователя в группу **Remote Desktop Users**.
5. Добавьте пользователя в **Remote Management Users**.
6. Откройте SMB порты (winexe): TCP 445, TCP 139.
7. Откройте RPC порты (wmic): TCP 135.
8. Отключите фильтрацию токенов для локальных учетных записей:

```
# reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
/v "LocalAccountTokenFilterPolicy" /t REG_DWORD /d 1 /f
```

16.16 Настройка SSH-сервера на Debian 12

1. Откройте терминал.
2. При необходимости обновите списки пакетов и установленные пакеты с помощью команд:

```
# sudo apt update

# sudo apt upgrade
```

3. Установить пакет OpenSSH сервера, если он ещё не установлен. Для этого нужно выполнить команду:

```
# sudo apt-get install openssh-server
```

4. OpenSSH сервер по умолчанию использует порт 22 для удаленных подключений. Если вы используете службу UFW, нужно разрешить удаленное подключение к порту 22. Для этого выполните команду:

```
# sudo ufw allow ssh
```

5. Удостоверьтесь, что в конфигурации OpenSSH сервера разрешен **root-логин**. Для этого откройте конфигурационный файл `/etc/ssh/sshd_config` и проверьте настройки следующих параметров:

```
PasswordAuthentication yes

PermitRootLogin yes
```

6. Проверьте работу SSH-сервера с помощью команды:

```
# sudo systemctl status ssh
```