# Платформа Радар

Руководство оператора

Версия 3.6.7

**ООО «Пангео Радар»**

# Оглавление

# 1. Вход в веб-интерфейс Платформы Радар

По умолчанию интерфейс пользователя доступен по URL `http://<адрес сервера>`.

Если пользователь не был авторизован, то при открытии интерфейса **Платформы Радар** на экране отобразится окно входа (см. рисунок 1).

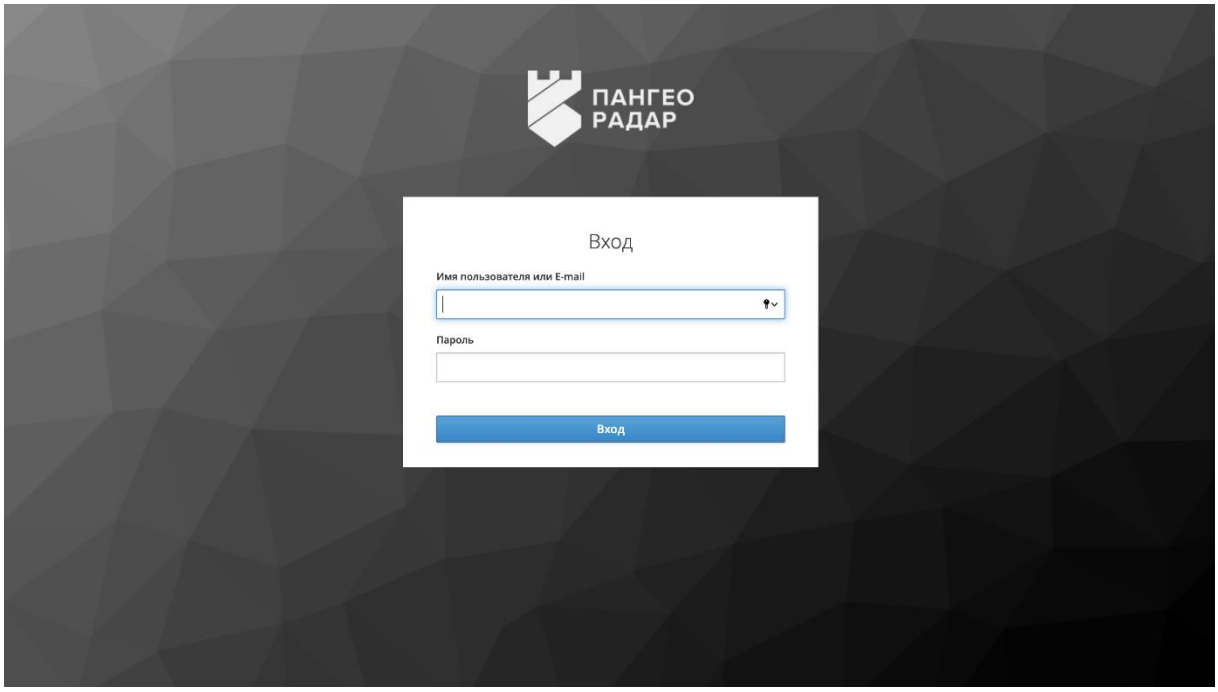



**Рисунок 1 – Окно входа в веб-интерфейс Платформы Радар**

После входа пользователя на экране откроется рабочий стол пользовательского интерфейса **Платформы Радар** (см. раздел «Основные элементы интерфейса»).

При первой аутентификации **Платформа Радар** может потребовать от пользователя сменить пароль (см. рисунок 2).

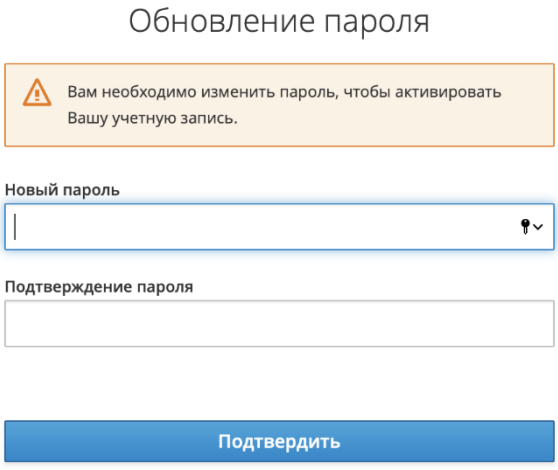



**Рисунок 2 – Форма ввода нового пароля**

Если при вводе логина и пароля были допущены ошибки, то **Платформа Радар** выдаст соответствующее предупреждение.

# 2. Рабочий стол

При входе пользователя в графический пользовательский интерфейс **Платформы Радар** открывается рабочий стол пользователя (см. рисунок 3).

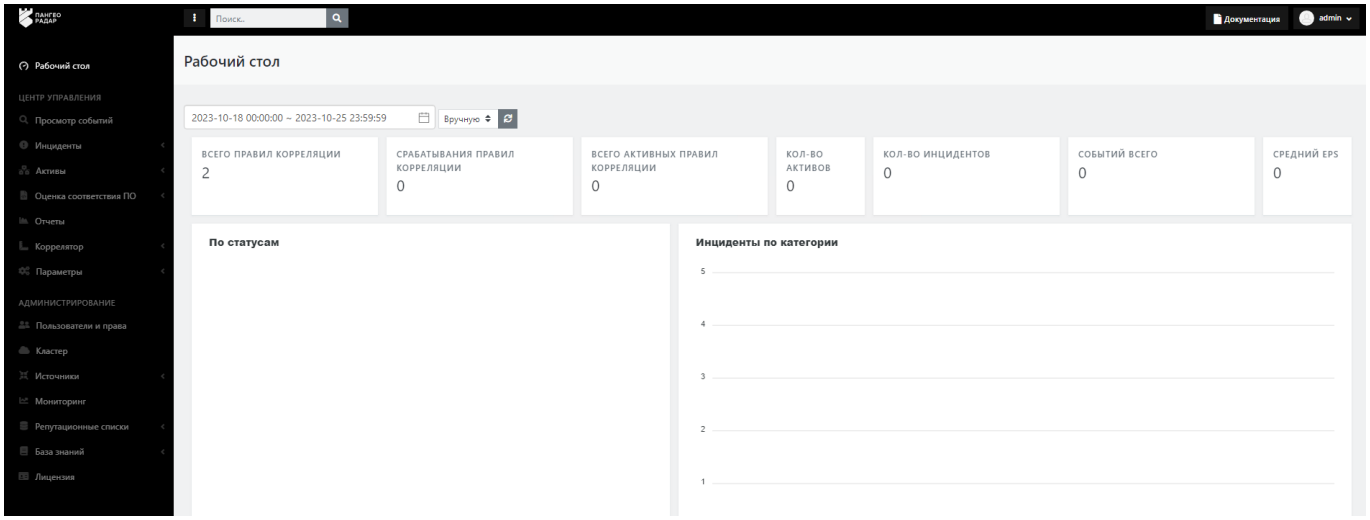
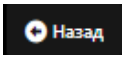
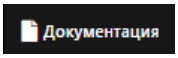


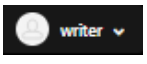

**Рисунок 3 – Рабочий стол пользовательского интерфейса Платформы Радар**

**Платформа Радар** поддерживает разные часовые пояса. Для отображения информации, зависящей от времени, учитывается локальное время и часовой пояс работающего оператора.

На верхней панели интерфейса располагаются следующие элементы:

-  - пиктограмма для скрытия/разворачивания основного меню **Платформы Радар**. В свернутом виде отображаются только пиктограммы меню, в развернутом - пиктограммы и надписи;
- Функция поиска - стандартное поле ввода поискового запроса (см. рисунок 3);
- 

- пиктограмма возврата на предыдущую страницу;
- 

- пиктограмма перехода к документации на **Платформу Радар***. При нажатии на пиктограмму откроется раздел с документацией;
- 

- пиктограмма профиля пользователя с индикацией наличия новых сообщений. При нажатии на пиктограмму открывается меню работы с профилем пользователя. Подробное описание работы с профилем пользователя см. в разделе «Пользовательские настройки».

Слева располагается основное меню **Платформы Радар**, которое может находиться в свернутом или развернутом состоянии.

Основное меню **Платформы Радар** содержит три раздела:

- **Рабочий стол**;
- **Центр управления**;
- **Администрирование**.

Раздел "**Рабочий стол**" - главная страница **Платформы Радар** с выбранным отчетом для публикации виджетов.

Раздел "**Центр управления**" содержит следующие подразделы:

- Просмотр событий - просмотра событий информационной безопасности;
- Инциденты - управление инцидентами;
- Активы - управление активами и группами активов;
- Оценка соответствия ПО - конфигурирование правил контроля соответствия установленного программного обеспечения различным политикам;
- Отчеты - управление отчетностью и виджетами рабочего стола;
- Коррелятор - управление правилами корреляции;
- Параметры - управление настройками.

Раздел "**Администрирование**" содержит следующий пункты:

- Пользователи и права - управление пользователями;
- Кластер - управление **Платформой Радар**;
- Источники - управление подключением источников событий;
- Мониторинг - просмотр метрик работоспособности компонентов **Платформы Радар**;
- Репутационные списки - управление списками индикаторов компрометации;
- База знаний - управление базой знаний по типам инцидентов и правилам корреляции;
- Лицензия - управление лицензией и просмотра параметров лицензии.

Непосредственно на рабочем поле располагается актуальная информация (см. рисунок 3) разных типов и разных способов представления, скомпонованная по принципу приборной доски (дашборда). Информация предоставляется за период времени, который устанавливается в специальном поле в верхней части "Рабочего стола".

Для установки периода отображения информации кликните в поле установки периода и с помощью календаря задайте необходимый период времени.

Рядом располагается список выбора интервала обновления приборной панели рабочего стола:

- вручную
- 5с
- 15с
- 30с
- 60с

С помощью иконки  можно в любой момент обновить информацию на приборной панели "**Рабочего стола**". При установленном ручном обновлении приборной панели иконка будет серого цвета, при автоматическом - зеленого.

Приборная панель "**Рабочего стола**" содержит следующие блоки данных:

- диаграмма распределения инцидентов по статусам;
- график распределения инцидентов по категориям;
- таблица распределения инцидентов по типу категории и важности;
- таблица распределения инцидентов по источнику;
- таблица распределения инцидентов по уровню опасности;
- в верхней части приборной панели отображаются данные по следующим параметрам:
    - "всего правил корреляции";
    - "срабатывание правил корреляции" за указанный период времени;
    - "всего активных правил корреляции";
    - "количество активов";
    - "количество инцидентов";
    - "событий всего" ;
    - "средний EPS".

# 3. Пользовательские настройки

## 3.1 Меню профиля пользователя

На верхней панели интерфейса в правом углу располагается пиктограмма профиля пользователя с индикацией наличия новых сообщений - 

.

При нажатии на пиктограмму открывается меню работы с профилем пользователя, которое содержит следующие пункты (см. рисунок 4):

- **Сообщения** - просмотр списков сообщений пользователя, создание и отправка нового сообщения. Подробнее см. в разделе «Сообщения»;
- **Профиль** - доступ к настройкам профиля;
- **Выйти из системы** - завершение текущего сеанса работы.

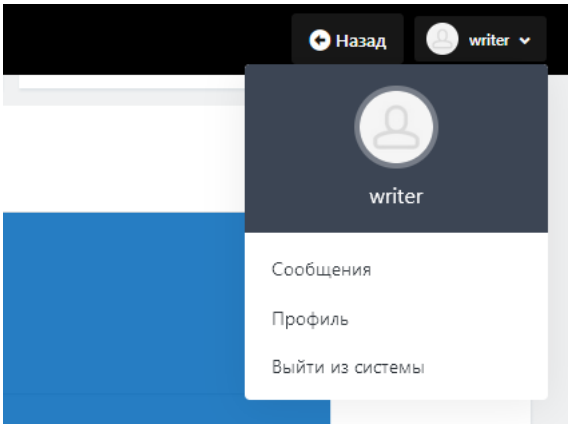



**Рисунок 4 – Меню работы с профилем пользователя**

## 3.2 Профиль – Сообщения

### 3.2.1 Основные элементы подраздела "Сообщения"

Раздел "**Сообщения**" предназначен для просмотр списков сообщений пользователя, создания и отправка новых сообщений.

В рабочей области отображаются следующие элементы (см. рисунок 5):

- табличные списки сообщений пользователя следующих типов (см. рисунок 5):
  - **Непрочитанные сообщения**;
  - **Прочитанные сообщения**;
  - **Отправленные сообщения**.
- Набор фильтров для поиска сообщений в списках – кнопка  ;
- Функция создания нового сообщения -- кнопка "**Написать**";
- Функция смены статуса Прочитанное все/ Непрочитанное все:

- кнопка "**Отметить прочитанным всё**" для списка непрочитанных сообщений;
- кнопка "**Отметить непрочитанным всё**" для списка прочитанных сообщений.

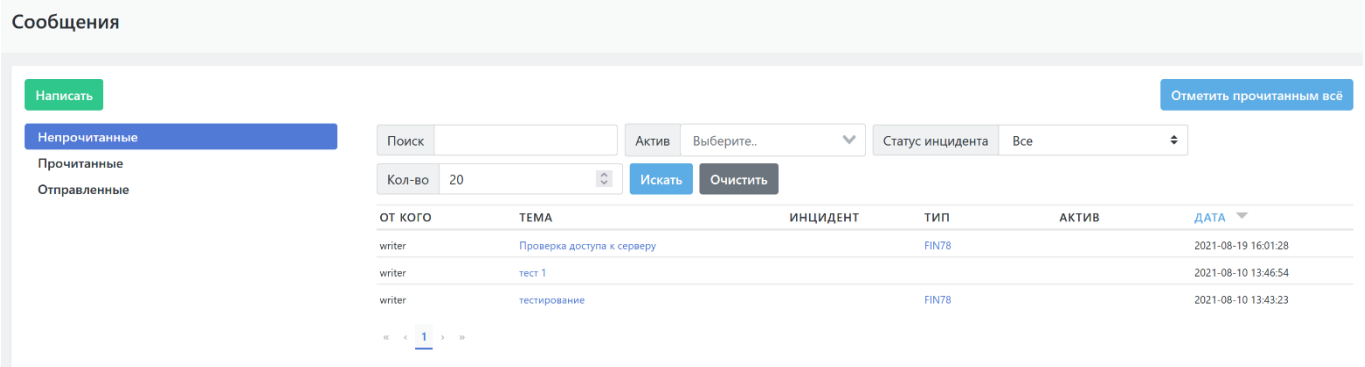



**Рисунок 5 – Сообщения пользователя**

## 3.2.2 Списки сообщений. Параметры списков

Список сообщений представлен в виде таблицы с полями:

- **От кого** - имя отправителя в **Платформе Радар**;
- **Тема** - тема сообщения: активная ссылка, по которой открывается текст сообщения;
- **Инцидент** - название инцидента: активная ссылка, по которой открывается страница с данными инцидента;
- **Тип** - тип инцидента: активная ссылка, по которой открывается страница с описанием типа инцидента;
- **Актив** - актив, на котором произошел инцидент: активная ссылка, по которой открывается страница с данными актива;
- **Дата** - дата получения сообщения или оповещения.

## 3.2.3 Настраиваемые фильтры списков сообщений

При нажатии на кнопку  открывается область фильтров для списков сообщений, которая включает в себя следующие фильтры:

- Фильтр с полем для свободного текстового ввода, ищет вхождение искомой фразы в поле "**Тема**";
- Фильтр по активам - раскрывающийся список, содержит текущий перечень активов;
- Фильтр по статусу инцидента - раскрывающийся список с возможными значениями статуса инцидента.

## 3.2.4 Просмотр деталей сообщения

Для просмотра сообщения кликните по теме сообщения в поле "**Тема**". Откроется форма просмотра сообщения.

Более подробное описание работы с сообщениями приведено в разделе «Просмотр деталей сообщения».

### 3.2.5 Создание и отправка нового сообщения

При нажатии на кнопку "**Написать**" откроется форма создания и отправки нового сообщения.

Подробное описание создания и отправки нового сообщения приведено в отдельном разделе «Работа с сообщениями. Просмотр деталей сообщения».

## 3.3 Профиль - Настройка оповещений

### 3.3.1 Основные элементы подраздела

В разделе "**Профиль**" отображается (см. рисунок 6):

- **Настройка оповещений** - настройки режимов отправки оповещений;
- **Поиск по истории действий**, в которую входят:
    - табличный список действий пользователя, повлекших за собой изменения в системе - далее история действий пользователя;
    - фильтры для поиска действий в истории – кнопка  ;
    - функция просмотра деталей действий пользователя - кнопки "**Показать детали**" / "**Скрыть детали**";
    - функция выгрузки данных по действиям пользователя - кнопка "**Выгрузить CSV**".
- Кнопка "**Перейти к настройкам профиля**" - функция перехода к настройкам профиля пользователя.

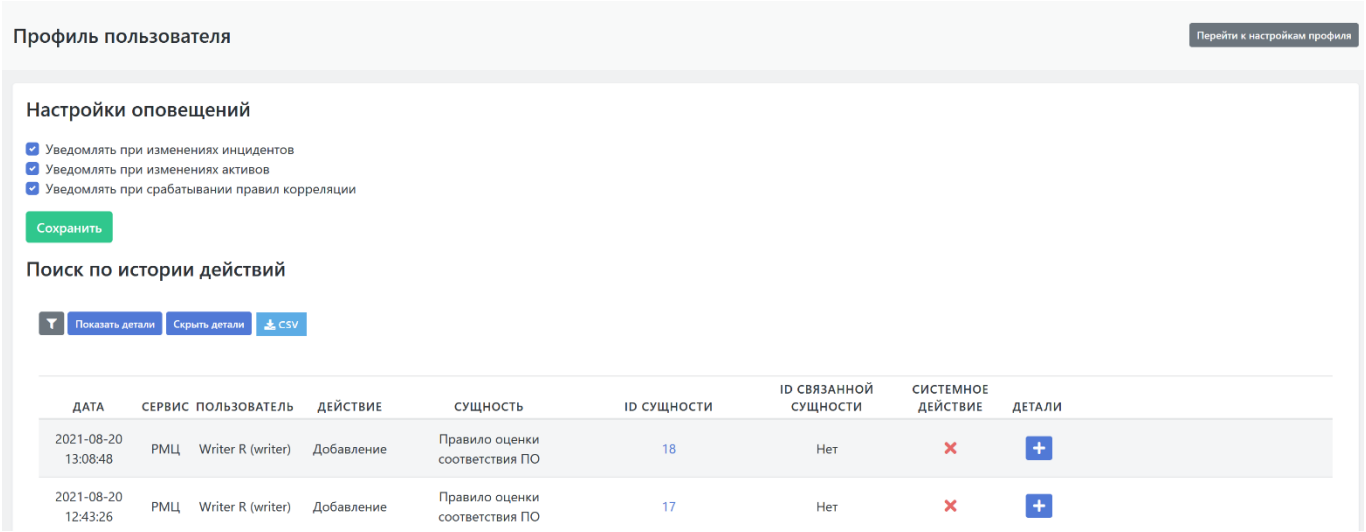



**Рисунок 6 – Работа с оповещениями**

### 3.3.2 Настройка режимов оповещения

Пользователь может получать от **Платформы Радар** оповещения при регистрации в **Платформе Радар** следующих событий:

- Изменение статуса инцидента - для этого установите флажок в поле "**Уведомлять при изменениях инцидентов**" ;

- Изменение статуса актива - для этого установите флажок в поле "**Уведомлять при изменениях активов**";
- Срабатывание правил корреляции - для этого установите флажок в поле "**Уведомлять при срабатывании правил корреляции**".

Для сохранения указанных настроек оповещений нажмите на кнопку "**Сохранить**".

### 3.3.3 История действий пользователя. Параметры списка

История действий пользователя, повлекших за собой изменения в системе, представлена в виде табличного списка действий пользователя со следующими параметрами:

- **Дата** - дата и время совершения действия;
- **Сервис** - сервис, на активах которого было совершено действие пользователем;
- **Пользователь** - пользователь, совершивший действие (владелец профиля);
- **Действие** - тип действия пользователя;
- **Сущность** - краткая характеристика действия;
- **ID сущности** - идентификатор действия в **Платформе Радар**;
- **ID связанной сущности** - идентификатор связанной с данным действием сущности (если есть);
- **Системное действие** - ответ системы на действие пользователя (если есть);
- **Детали** (  ) - функция просмотра "сырых" данных действия: кнопка.

### 3.3.4 Настраиваемые фильтры поиска по истории действий

При нажатии на кнопку  откроется область фильтров для истории действий, которая включает в себя следующие фильтры:

- фильтр по заданному временному интервалу - вывод на экран списка действий, совершенных за указанный промежуток времени;
- фильтр по сервису, на котором произошло действие - раскрывающийся список, содержит текущий перечень сервисов.

### 3.3.5 Просмотр детализации действий пользователя

Для просмотра детализации действия кликните на пиктограмму  в строке интересующего действия. Непосредственно в строке откроются "сырые" данные действия (см. рисунок 7). Для сворачивания окна с "сырыми" данными нажмите на пиктограмму  .

При нажатии на кнопку "**Показать детали**" "сырые" данные будут открыты одновременно для всех действий в истории пользователя.

При нажатии на кнопку **"Скрыть детали"** будут скрыты все открытые на текущий момент "сырые" данные.

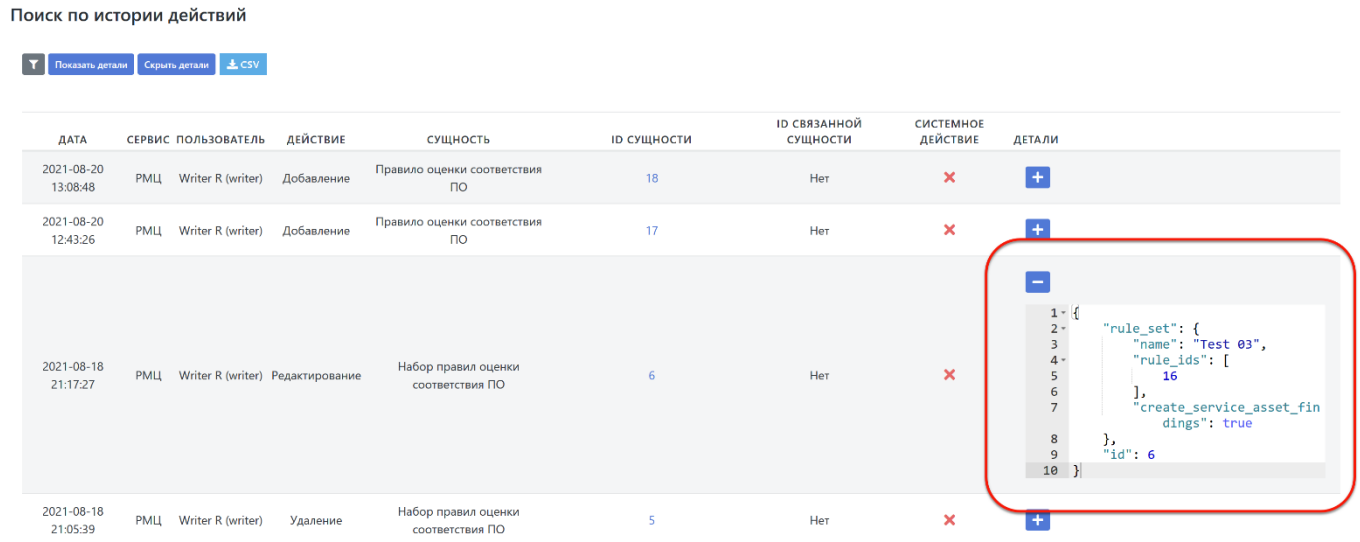



**Рисунок 7 – Детализация действия пользователя**

# 3.4 Профиль - Настройка профиля

## 3.4.1 Основные элементы подраздела

Для получения доступа к данным пользователя в разделе "**Профиль**" нажмите на кнопку "**Перейти к настройкам профиля**". Откроется раздел, который содержит средства просмотра и редактирования данных пользователя (см. рисунок 8).

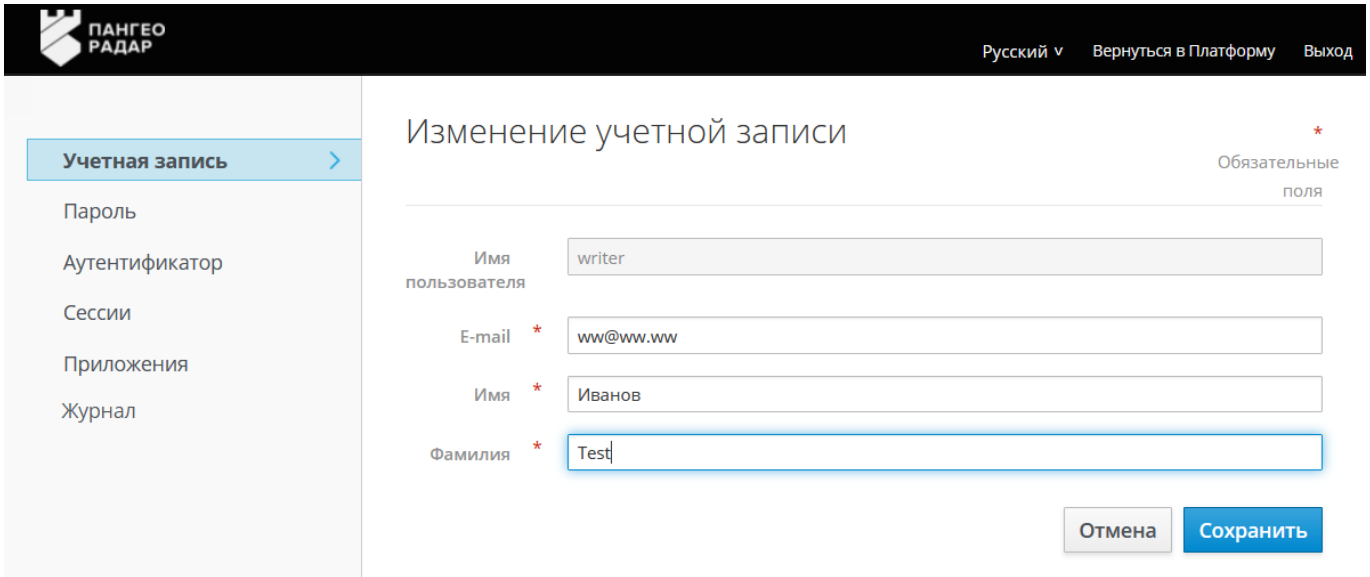



**Рисунок 8 – Данные пользователя. Подраздел "Учетная запись"**

Раздел состоит из следующих подразделов:

- **Учетная запись** - стандартный для пользовательских интерфейсов подраздел, предназначенный для редактирования имени, фамилии и электронной почты пользователя;
- **Пароль** - стандартный для пользовательских интерфейсов подраздел, предназначенный для смены текущего пароля пользователя;
- **Аутентификатор** - подраздел предназначен для получения кода аутентификации;

- **Сессии** - подраздел предназначен для просмотра перечня и параметров текущих сессий пользователя, а также для выхода из сессий;
- **Приложения** - подраздел предназначен для просмотра перечня и параметров приложений **Платформы Радар**, к которым имеет доступ пользователь.

### 3.4.2 Настройка доступа через мобильное приложение

Подраздел "**Аутентификатор**" содержит пошаговую инструкцию для настройки доступа к **Платформе Радар** с мобильных устройств через одно из следующих мобильных приложений аутентификации (см. рисунок 9):

- FreeOTP - мобильное приложение для двухфакторной аутентификации для систем, использующих протоколы одноразовых паролей с поддержкой Android (3.0 или более поздней версии) и iOS (7 или более поздней версии);
- Google Authenticator - мобильное приложение для создания кодов двухэтапной аутентификации помощью Time-based One-time Password Algorithm (TOTP) и HMAC-based One-time Password Algorithm (HOTP).

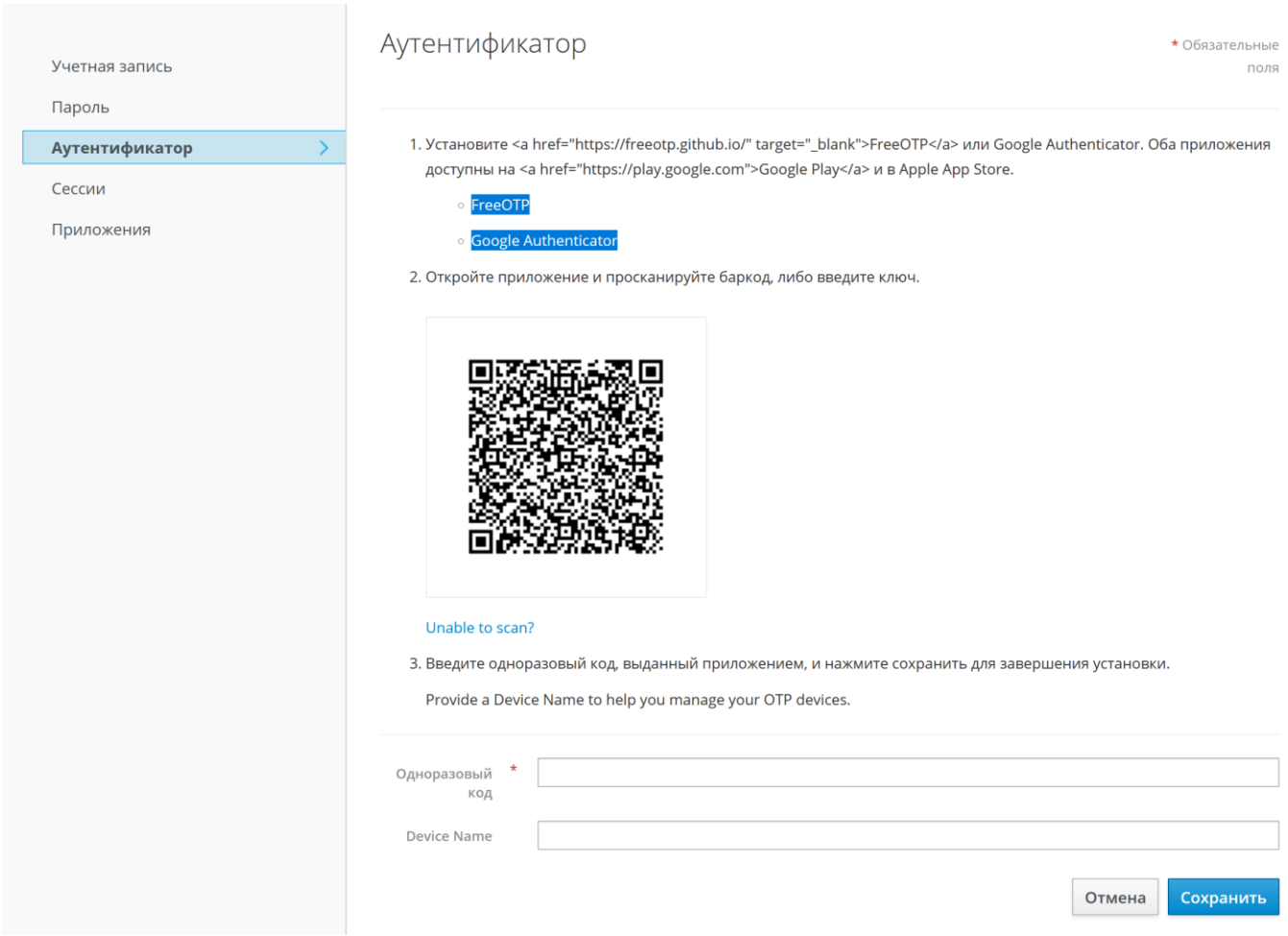



**Рисунок 9 – Настройка доступа к Платформе Радар с мобильных устройств**

### 3.4.3 Управление сессиями пользователя

Подраздел "**Сессии**" предназначен для:

- Просмотра перечня текущих сессий пользователя и следующих параметров сессии (см. рисунок 10):
    - IP - ip-адрес актива;
    - дата и время начала сессии;
    - дата и время последнего доступа;
    - дата и время, когда сессия истекает;
    - клиенты.
- Для выхода из сессий - кнопка "**Выйти из всех сессий**".

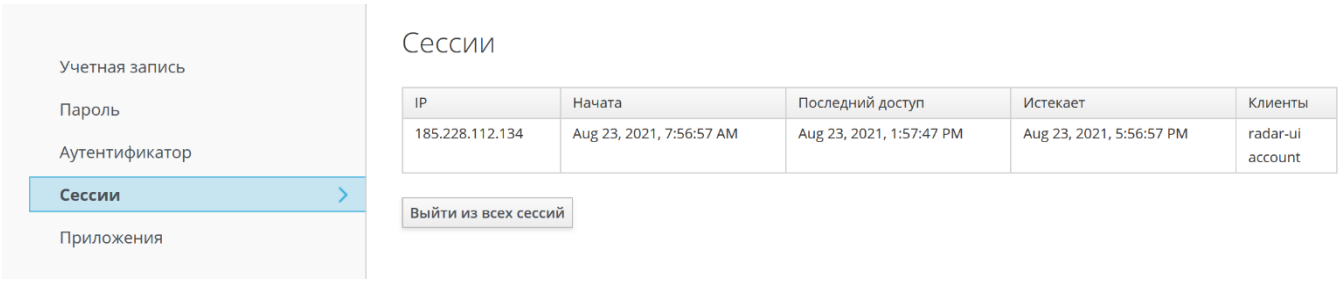



**Рисунок 10 – Сессии пользователя**

## 3.4.4 Приложения

Подраздел "**Приложения**" предназначен для просмотра перечня и параметров приложений **Платформы Радар**, к которым пользователь имеет доступ (см. рисунок 11).

Кликните по названию приложения для перехода непосредственно на страницу указанного приложения для работы с ним.

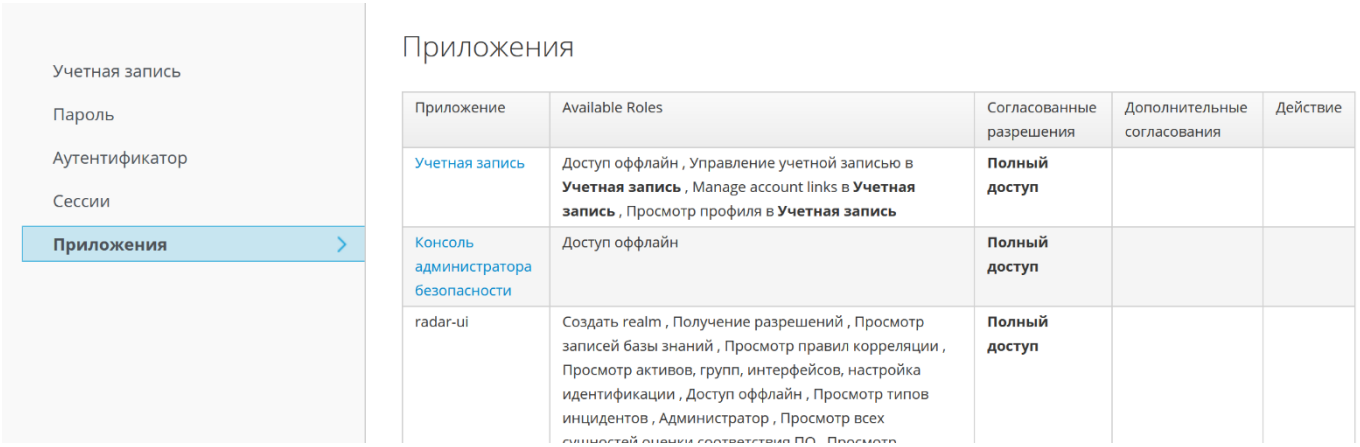



**Рисунок 11 – Приложения пользователя**

## 3.4.5 Журнал

Подраздел "Журнал" предназначен для просмотра перечня действий пользователя в Платформе Радар (см. рисунок 12).

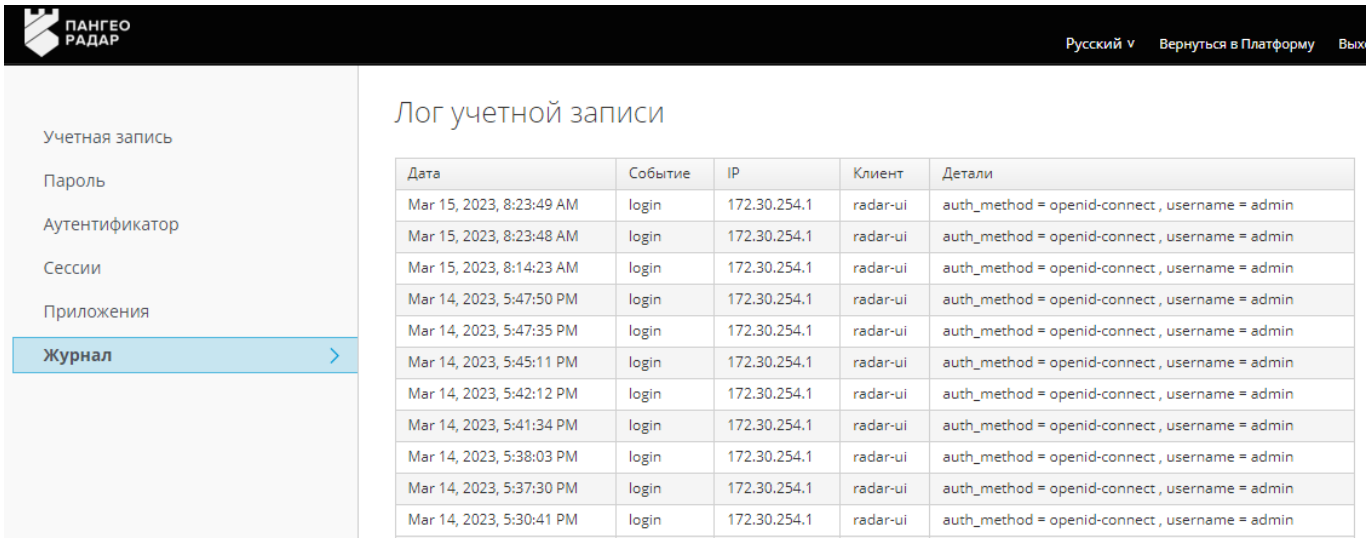



**Рисунок 12 – Просмотр действий пользователя**

### 3.4.6 Выход из системы

При выборе пункта меню **"Выйти из системы"** происходит выход пользователя из **Платформы Радар** и переход на страницу входа в **Платформу Радар**.

**Внимание!** *Выход пользователя из **Платформы Радар** производится без окна подтверждения выхода*.

# 4. Просмотр событий

**Внимание**! *Данный раздел основного меню доступен только пользователям с соответствующими правами на просмотр событий.*

Раздел "**Просмотр событий**" предназначен для поиска, просмотра и анализа зафиксированных событий, вызвавших инцидент, включая сырые данные событий (см. рисунок 13):

- Набор настраиваемых фильтров для вывода событий по заданным параметрам:
  - **Время** - задание временного интервала, на котором надо просмотреть события;
  - **Индекс** - указание индекса ElasticSearch;
  - Поле текстового ввода поискового запроса;
  - Ползунок с установкой количества отображаемых событий (от 50 до 10 000).
- Функция фильтрации выведенных на экран событий по полям из сырых данных:
  - Кнопка "**Новый фильтр**" - для указания нового поля для фильтрации;
  - Список полей слева от диаграммы (см. рисунок 13)
- Область отображения диаграммы событий - количество событий за заданный интервал времени;
- Область отображения сырых данных по каждому из событий, расположена под диаграммой событий.

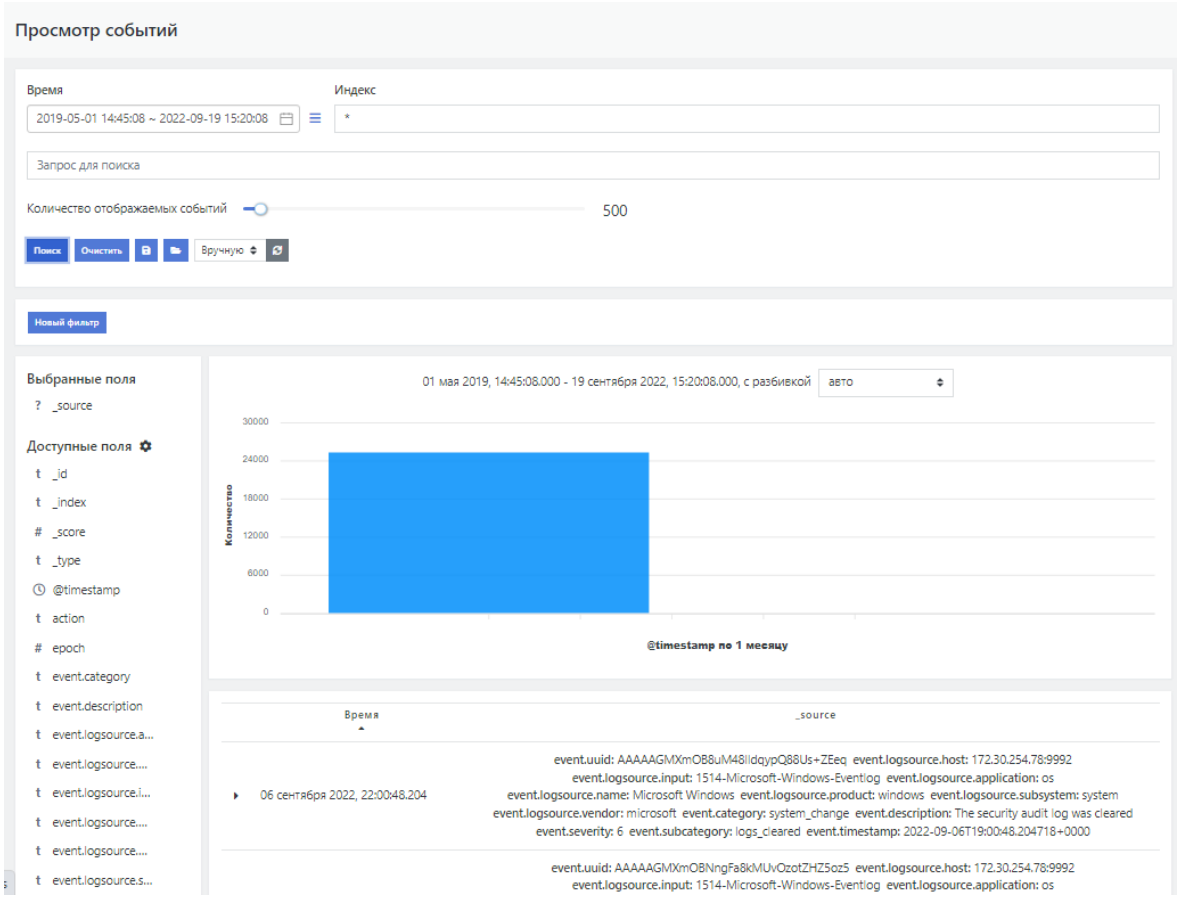



**Рисунок 13 – Рабочая область подраздела «Просмотр событий»**

# 5. Инциденты

## 5.1 Состав раздела

Раздел "**Инциденты**" содержит следующие подразделы:

- **Инциденты** - предназначен для работы с инцидентами;
- **Группы инцидентов** - предназначен для управления инцидентами, объединенными в группы;
- **Типы инцидентов** - предназначен для работы с типами инцидентов;
- **Происшествия на отправку** - предназначен для выбора происшествий на отправку в ГосСОПКА (подробнее см. в разделе «Работа с НКЦКИ»);
- **Дополнительные поля** - предназначен для управления создаваемыми пользователями полями.

## 5.2 Подраздел "Инциденты"

Зарегистрированные инциденты информационной безопасности хранятся в системе в отдельном хранилище.

### 5.2.1 Основные элементы подраздела

Подраздел "**Инциденты**" предназначен для оперирования инцидентами.

Подраздел содержит следующие элементы (см. рисунок 14):

- Текущий список инцидентов.
- Общее количество инцидентов.
- Календарь происшествий - область "**Происшествия**";
- Набор фильтров для просмотра списка инцидентов – кнопка  ;
- Область быстрого переключения списка по статусам инцидентов - предустановленные фильтры по статусам инцидентов;
- Функция создания нового инцидента в системе - кнопка "**Создать инцидент**";
- Функция редактирования параметров инцидентов – кнопка  ;
- Функция выгрузки данных во внешний файл в формате CSV - кнопка "**Выгрузить CSV**";
- Функция настройки временного периода обновления данных - раскрывающийся список "**Вручную**" (где "Вручную" значение по умолчанию);
- Кнопка для запуска обновления данных -  ;
- Функции назначения инцидентов пользователю или группе - раскрывающиеся списки "**Назначить пользователю**" и "**Назначить группе**";

- Функция объединения выбранных инцидентов в группу инцидентов - раскрывающийся список "**Объединить в группу**";
- Функция смены статуса - раскрывающийся список "**Сменить статус**".

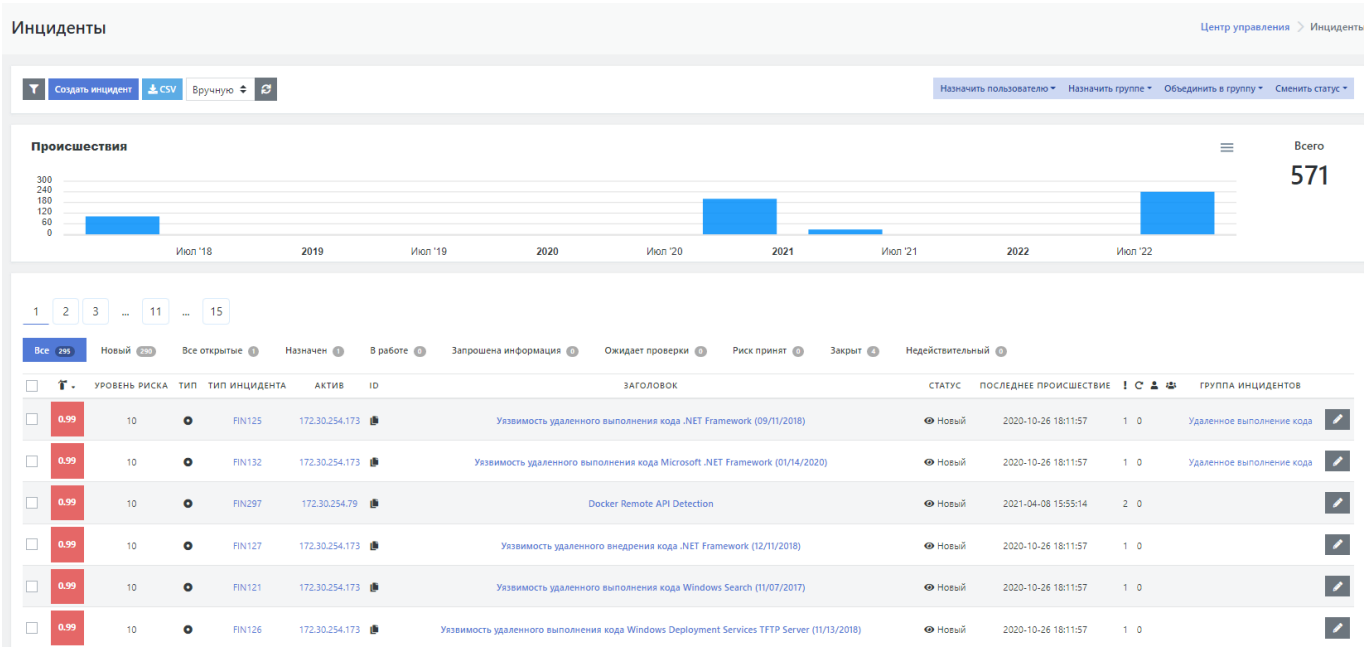



**Рисунок 14 – Рабочая область подраздела «Инциденты»**

## 5.2.2 Список инцидентов. Параметры списка

Система поддерживает изменение сортировки в списке инцидентов. По умолчанию используется сортировка по оценке срочности инцидента. Для выбора параметра сортировки нажмите на заголовок необходимого столбца. После нажатия сортировка списка будет изменена на выбранный параметр.

Текущий список инцидентов представлен в виде табличного списка со следующими основными параметрами:

- Поле ( / ) - флаговое поле для выбора строк с инцидентами для проведения с ними каких-то действий;
- **Оценка срочности** ( ) - содержит оценку срочности отработки инцидента;
- **Уровень риска** - содержит численную оценку уровня риска;
- **Тип** - содержит пиктограмму - идентификатор типа, к которому принадлежит инцидент;
- **Тип инцидента** - содержит идентификатор инцидента;
- **Актив** - идентификатор сетевого актива на котором произошел инцидент (IP-адрес актива или сетевое имя);
- **Заголовок** - текстовый заголовок инцидента, под которым он был зафиксирован в **Платформе Радар**;
- **Статус** - содержит статус в котором находится инцидент в настоящее время;
- **Последнее происшествие** - дата и время когда было зафиксировано последнее происшествие в рамках инцидента;

- **Кол-во происшествий** ( ! ) - счетчик количества происшествий в рамках инцидента;
- **Кол-во повторных открытий** ( ↻ ) - счетчик количества повторных открытий инцидента;
- **Пользователь** ( 👤 ) - назначенный ответственный пользователь;
- **Группа** ( 👥 ) - назначенная группа ответственных;
- **Группа инцидентов** - принадлежность инцидента к группе инцидентов (если есть). Клик по полю откроет окно просмотра всех инцидентов в группе (см. раздел Управление группой инцидентов);
- Кнопка ( ✎ ) - функция редактирования параметров инцидента.

При необходимости разработчиками **Платформы Радар** могут быть введены дополнительные поля списка.

### 5.2.3 Статусы инцидентов. Быстрое переключение списка инцидентов по статусам

Область быстрого переключения по статусам инцидентов представляет собой набор предустановленных фильтров по статусам со счетчиками инцидентов (строк таблицы) в каждом из статусов (см. рисунок 15):

- **Все** - вывод на экран всех строк списка инцидентов;
- **Новый** - вывод на экран списка новых инцидентов;
- **Все открытые** - вывод на экран списка открытых инцидентов;
- **Назначена** - вывод на экран списка назначенных инцидентов;
- **В работе** - вывод на экран списка инцидентов, находящихся в работе;
- **Запрошена информация** - вывод на экран списка инцидентов, по которым была запорошена информация;
- **Ожидает проверки** - вывод на экран списка инцидентов, находящихся в ожидании проверки;
- **Риск принят** - вывод на экран списка инцидентов, для которых приняты риски;
- **Закрыт** - вывод на экран списка закрытых инцидентов;
- **Недействительный** - вывод на экран списка недействительных инцидентов.

Для вывода на экран списка инцидентов с определенным статусом щелкните по нужному статусу в области быстрого переключения (см. рисунок 15).

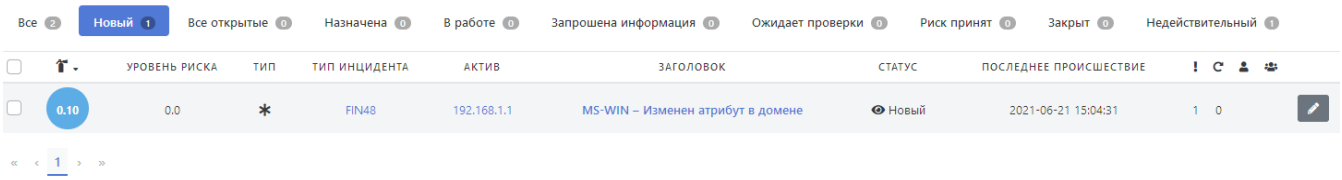



**Рисунок 15 - Область быстрого переключения между списками инцидентов, отфильтрованных по текущему статусу**

### 5.2.4 Настраиваемые фильтры списка инцидентов

При нажатии на кнопку  открывается область с настраиваемыми фильтрами для табличного списка инцидентов. Фильтр списка инцидентов разбит на группы и позволяет провести фильтрацию списка по следующим параметрам:

1. Вкладка "**Фильтр**" содержит следующие возможности (см. рисунок 16):
    - Фильтр по заголовку инцидента - свободный текстовый ввод;
    - Фильтр по идентификатору инцидента - свободный текстовый ввод;
    - Фильтр по типу инцидента - раскрывающийся список типов инцидентов;
    - Фильтр по группе инцидентов - раскрывающийся список групп инцидентов;
    - Фильтр по времени обработки инцидента - выбор времени из предустановленного в **Платформе Радар** списка (раскрывающийся список):
        - Нормальное;
        - Небольшая задержка;
        - Задержка;
        - Неприемлемый.

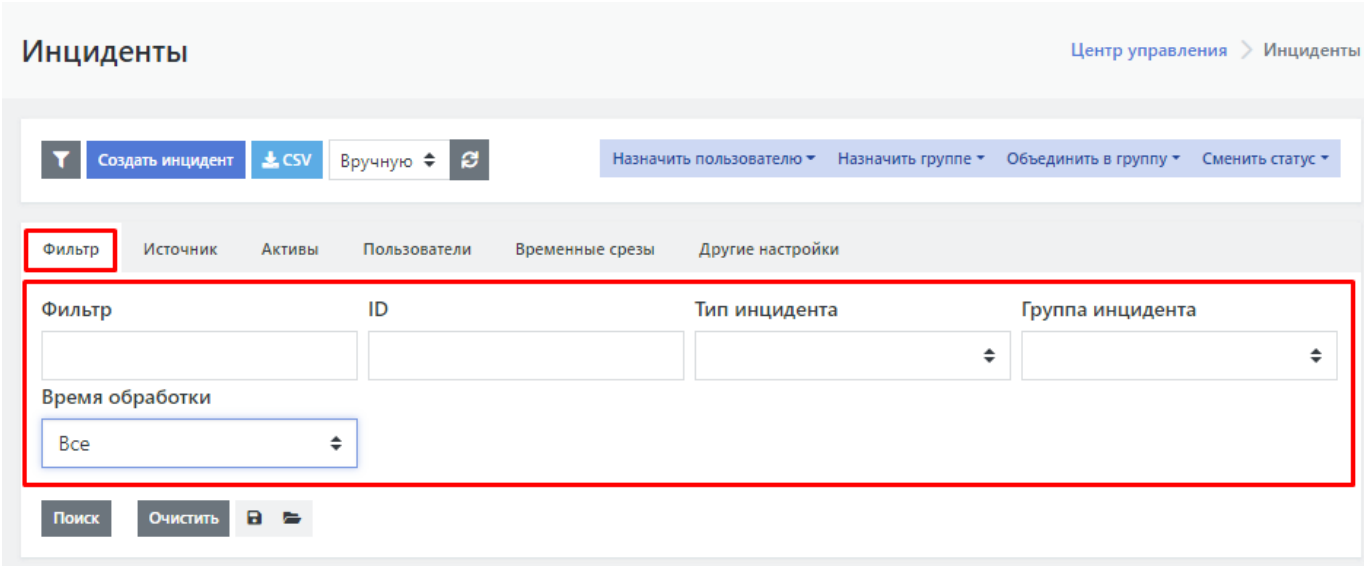



**Рисунок 16 – Фильтры для списка инцидентов на вкладке "Фильтры"**

2. Вкладка "**Источник**" содержит следующие возможности (см. рисунок 17):
    - Фильтр по категории, к которой относится инцидент - раскрывающийся список со следующими значениями:
        - Уязвимость;
        - Сетевая аномалия;
        - Нарушение политики.
    - Фильтр по источнику, создавшему инцидент в **Платформе Радар** - раскрывающийся список со следующими значениями:

- Сканер уязвимостей;
- Устаревший инцидент;
- Коррелятор событий;
- Введён вручную;
- Контроль соответствия;
- Контроль потока событий.

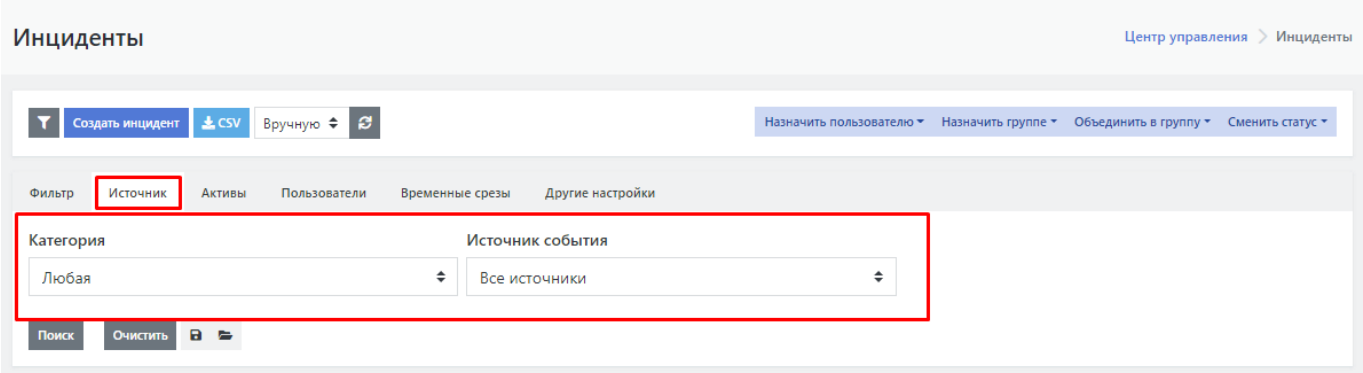



**Рисунок 17 – Фильтры для списка инцидентов на вкладке "Источник"**

3. Вкладка "**Активы**" содержит следующие возможности (см. рисунок 18):

- Фильтр по группам активов - раскрывающийся список, состав списка групп активов определяется Администраторами **Платформы Радар** и правами доступа пользователя;
- Фильтр по активам - раскрывающийся список, содержит текущий перечень активов;
- Фильтр по значимости актива - раскрывающийся список со следующими значениями:
  - Ключевой актив;
  - Важный актив;
  - Нормальный актив;
  - Распределенный или некритичный актив;
  - Тестовый актив.
- Фильтр по сетевой видимости актива - раскрывающийся список со следующими значениями:
  - Прямое подключение к Интернет;
  - DMZ, частичный доступ из Интернет;
  - Штатный доступ в Интернет через Proxy;
  - Ограниченный доступ в Интернет;
  - Не подключенный к сети.

- Фильтр по расположению актива - раскрывающийся список предустановленных мест расположения активов (например названия городов, где располагаются сетевые активы).

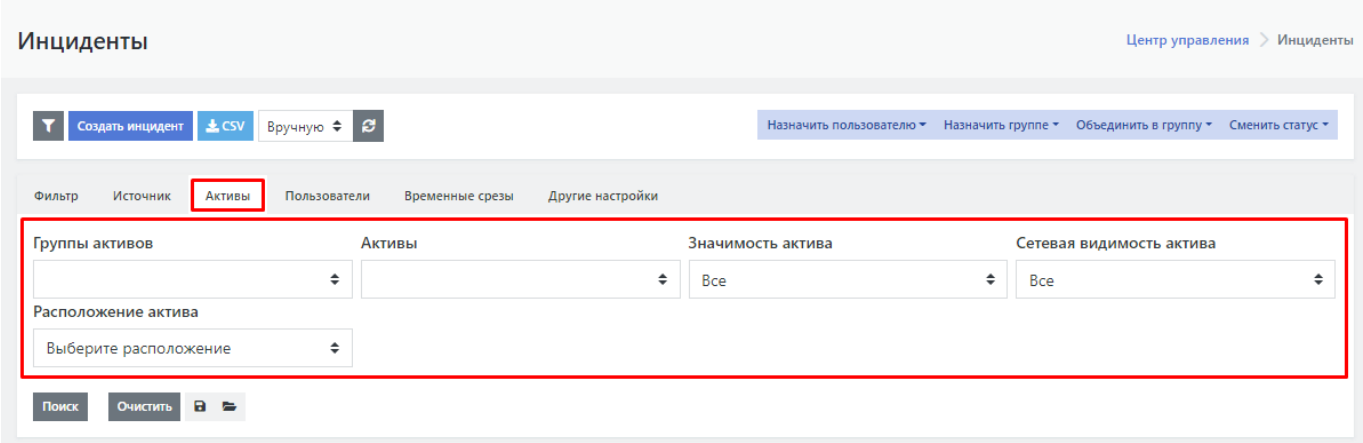



**Рисунок 18 – Фильтры для списка инцидентов на вкладке "Активы"**

4. Вкладка "**Пользователи**" содержит следующие возможности (см. рисунок 19):
   - Фильтр по логину пользователя, отвечающего за инциденты - раскрывающийся список логинов пользователей, зарегистрированных в **Платформе Радар**;
   - Фильтр по названию группы, отвечающей за инциденты - раскрывающийся список групп пользователей, созданных в **Платформе Радар**.

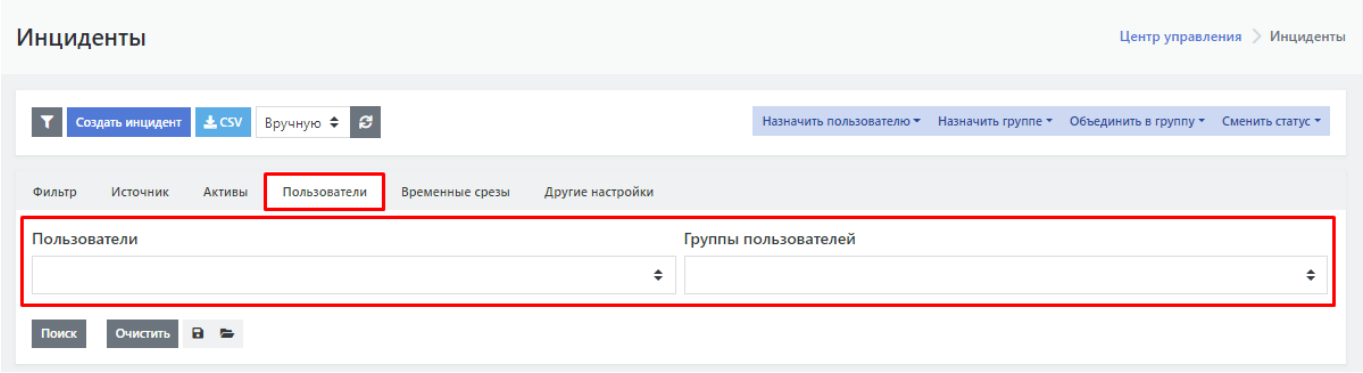



**Рисунок 19 – Фильтры для списка инцидентов на вкладке "Пользователи"**

5. Вкладка "**Временные срезы**" позволяет задать следующие временные срезы (см. рисунок 20):
   - "**Последнее происшествие с**" - "**Последнее происшествие до**";
   - "**Последнее сканирование от**" - "**Последнее сканирование до**";
   - "**Сменился статус с**" - "**Сменился статус по**".

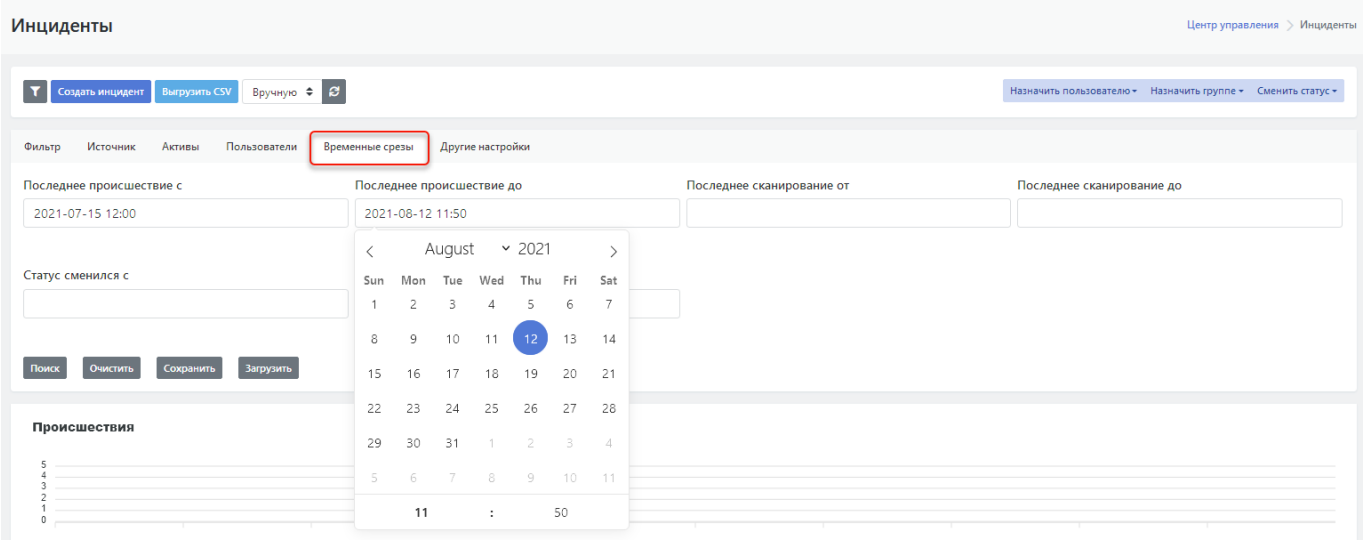



**Рисунок 20 – Фильтрация инцидентов по временным срезам. Вкладка "Временные срезы"**

6. Вкладка "**Другие настройки**" содержит следующие возможности (см. рисунок 21):
    - Фильтр по уровню риска - раскрывающийся список со следующими значениями:
        - Высокий;
        - Средний;
        - Низкий;
        - Нет.
    - Фильтр по наличию удаленной эксплуатации актива - раскрывающийся список "Да/ Нет/ Не важно";
    - Фильтр по типу сканирования "Внешнее сканирование" - раскрывающийся список "Да/ Нет/ Не важно";
    - Фильтр по типу инцидента "Обработанный?" - раскрывающийся список "Да/ Нет/ Не важно".

Так же на данной вкладке расположена функция редактирования количества строк табличного списка на одной экранной странице - "**Кол-во на странице**".

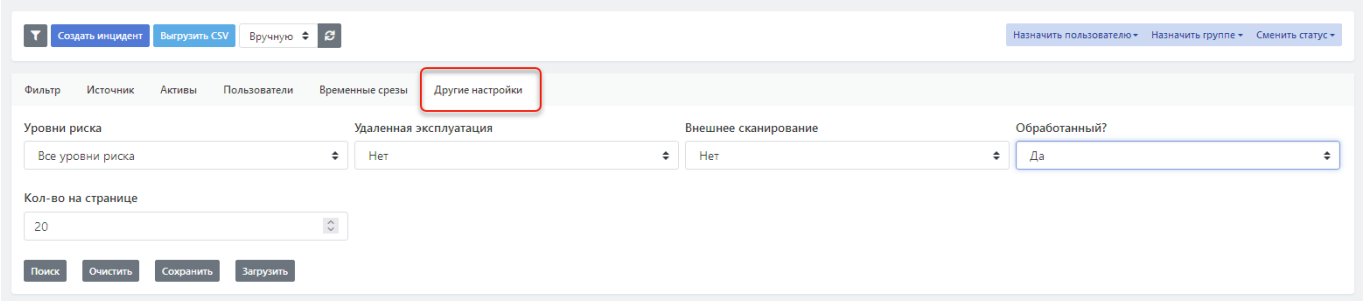



**Рисунок 21 – Вкладка фильтра "Другие настройки" и функция редактирования строк табличного списка инцидентов**

Для фильтрации табличного списка необходимо установить нужные значения фильтров на всех вкладках и нажать на кнопку "**Поиск**" на любой из вкладок (см. рисунок 21). Для сброса всех фильтров - нажать на кнопку "**Очистить**".

Настроенный набор фильтров можно сохранить для последующего использования - кнопка "**Сохранить**".

Для использования ранее созданного и сохраненного набора фильтров - нажать на кнопку "**Загрузить**".

### 5.2.5 Настройка обновления данных

Функция настройки обновления данных состоит из раскрывающегося списка временных интервалов обновления и пиктограммы --  . По умолчанию устанавливается режим ручного обновления. Обновление вручную производится при нажатии на пиктограмму  .

Для автообновления выбрать временной интервал обновления в раскрывающемся списке:

- 5 с.
- 15 с.
- 30 с.
- 60 с.

### 5.2.6 Назначение инцидентов пользователям и группам пользователей

При наличии необходимых прав пользователю предоставляется возможность назначить один или несколько инцидентов для разбора конкретному пользователю, зарегистрированному в **Платформе Радар**, или группе пользователей. Процедура назначения инцидента ответственному пользователю или группе пользователей для расследования подробно описана в разделе «Назначение инцидента ответственным».

### 5.2.7 Смена статуса инцидента

При наличии необходимых прав пользователю предоставляется доступ к функции "**Сменить статус**" для одного или нескольких инцидентов. Процедура смены статуса подробно описана в разделе «Изменение статуса инцидента».

### 5.2.8 Создание инцидента

При наличии необходимых прав пользователю доступна кнопка "Создать инцидент", по нажатию на которую произойдет переход на страницу создания инцидента в Платформе Радар вручную. Подробное описание создания инцидента в Платформе Радар вручную приведено в разделе «Создание инцидента вручную».

## 5.3 Подраздел "Группы инцидентов"

### 5.3.1 Основные элементы подраздела

Подраздел "**Группы инцидентов**" предназначен для управления группами инцидентов. Для инцидентов, объединенных в группы, доступны массовые действия: закрытие, удаление, привязка пользователей и т.д. Подраздел содержит (см. рисунок 22):

- Текущий список групп инцидентов.

- Набор фильтров для просмотра списка групп инцидентов – кнопка  .
- Функция создания новой группы инцидента в системе - кнопка "**Создать**".
- Функция редактирования параметров группы инцидента – кнопка  .

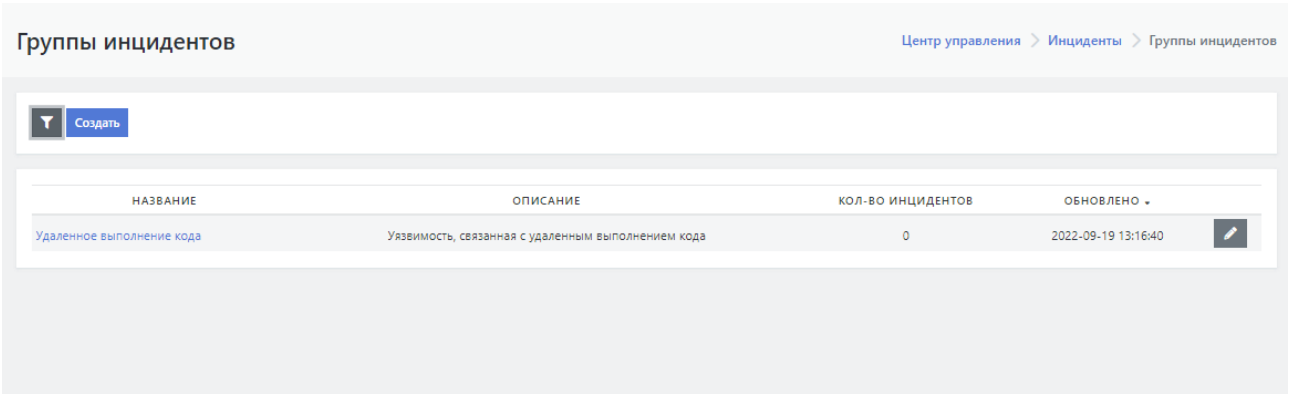



**Рисунок 22 – Рабочая область подраздела «Группы инцидентов»**

## 5.3.2 Список групп инцидентов. Параметры списка

Текущий список групп инцидентов представлен в виде табличного списка со следующими основными параметрами:

- **Название** - содержит название группы инцидентов. Клик по полю откроет окно просмотра всех инцидентов в группе (см. раздел «Управление группой инцидентов»).
- **Описание** - содержит описание группы инцидентов.
- **Кол-во инцидентов** - содержит количество инцидентов, объединенных в группу.
- **Обновлено** - содержит дату и время последнего изменения группы инцидентов.
- Кнопка (  ) – функция редактирования параметров группы инцидента.

## 5.3.3 Настраиваемые фильтры списка групп инцидентов

При нажатии на кнопку  открывается область с настраиваемыми фильтрами для табличного списка групп инцидентов (см. рисунок 23). Фильтр для списка групп инцидентов позволяет провести фильтрацию списка по свободному текстовому вводу.

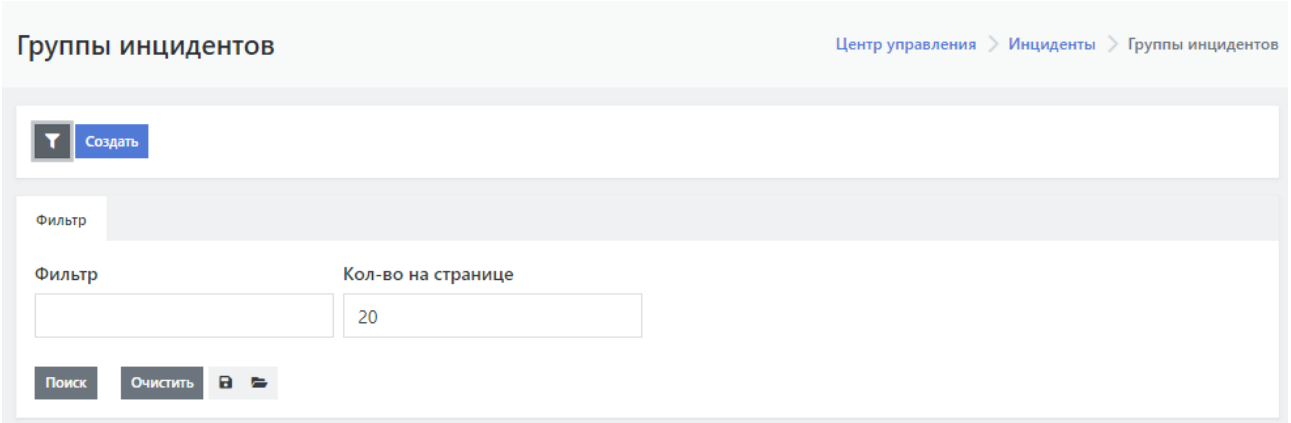



**Рисунок 23 – Фильтры для списка групп инцидентов**

Также в области настройки фильтров расположена функция редактирования количества строк табличного списка на одной экранной странице - "Кол-во на странице".

### 5.3.4 Создание группы инцидентов

При наличии необходимых прав пользователю доступна кнопка "**Создать**", по нажатию на которую произойдет переход на страницу создания новой группы инцидентов. Подробное описание создания новой группы инцидентов в **Платформе Радар** приведено в разделе «Ручное добавление в группу».

### 5.3.5 Управление группой инцидентов

При просмотре перечня инцидентов, объединенных в группу (см. рисунок 24) интерфейс подобен интерфейсу просмотра всех инцидентов, за исключением:

- Отсутствуют элементы управления фильтрами и просмотра панели происшествий.
- Добавление разделы с описанием группы инцидентов, назначенным ответственным за инцидент пользователем (группой пользователей).
- Добавлены кнопки управления инцидентами в группе:
    - **Отвязать выбранные инциденты от группы** - выбранные инциденты исключаются из группы;
    - **Закрыть все инциденты в группе** - все инциденты переводятся в статус "***Закрыт***";
    - **Удалить инциденты группы** - все инциденты в списке удаляются;
    - **Назначить пользователю** - все инциденты группы назначаются пользователю;
    - **Назначить группе** - все инциденты группы назначаются группе пользователей.

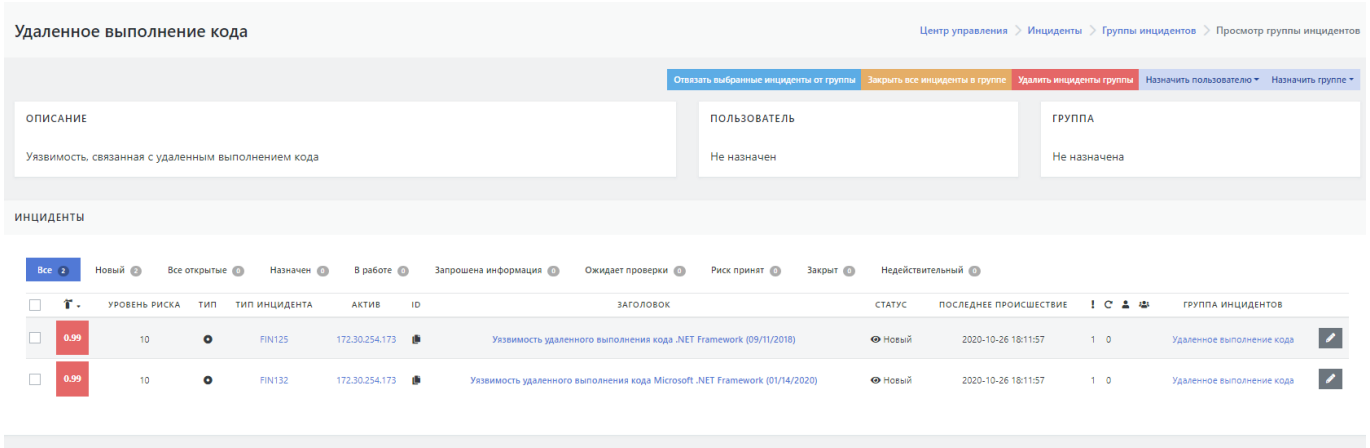



**Рисунок 24 – Просмотр инцидентов в группе.**

## 5.4 Подраздел "Типы инцидентов"

### 5.4.1 Основные элементы подраздела

Подраздел "Типы инцидентов" предназначен для оперирования типами инцидентов.

Подраздел содержит (см. рисунок 25):

- Текущий список типов инцидентов.

- Набор фильтров для просмотра списка типов инцидентов – кнопка ;
- Функция создания нового типа инцидента в системе - кнопка "**Создать**";
- Функция редактирования параметров типа инцидента – кнопка ;
- Функция выгрузки данных по типам инцидентов во внешний файл - кнопка "**CSV**";
- Функция экспорта выбранных типов инцидентов во внешний файл - кнопка "**Экспортировать**";
- Функция импорта выбранных типов инцидентов из внешнего файла - кнопка "**Импортировать**";
- Функция удаления выбранных типов инцидентов - кнопка "**Удалить**";
- Функция экспорта всех типов инцидентов во внешний файл - кнопка "**Экспортировать всё**";
- Функция удаления всех типов инцидентов - кнопка "**Удалить всё**".

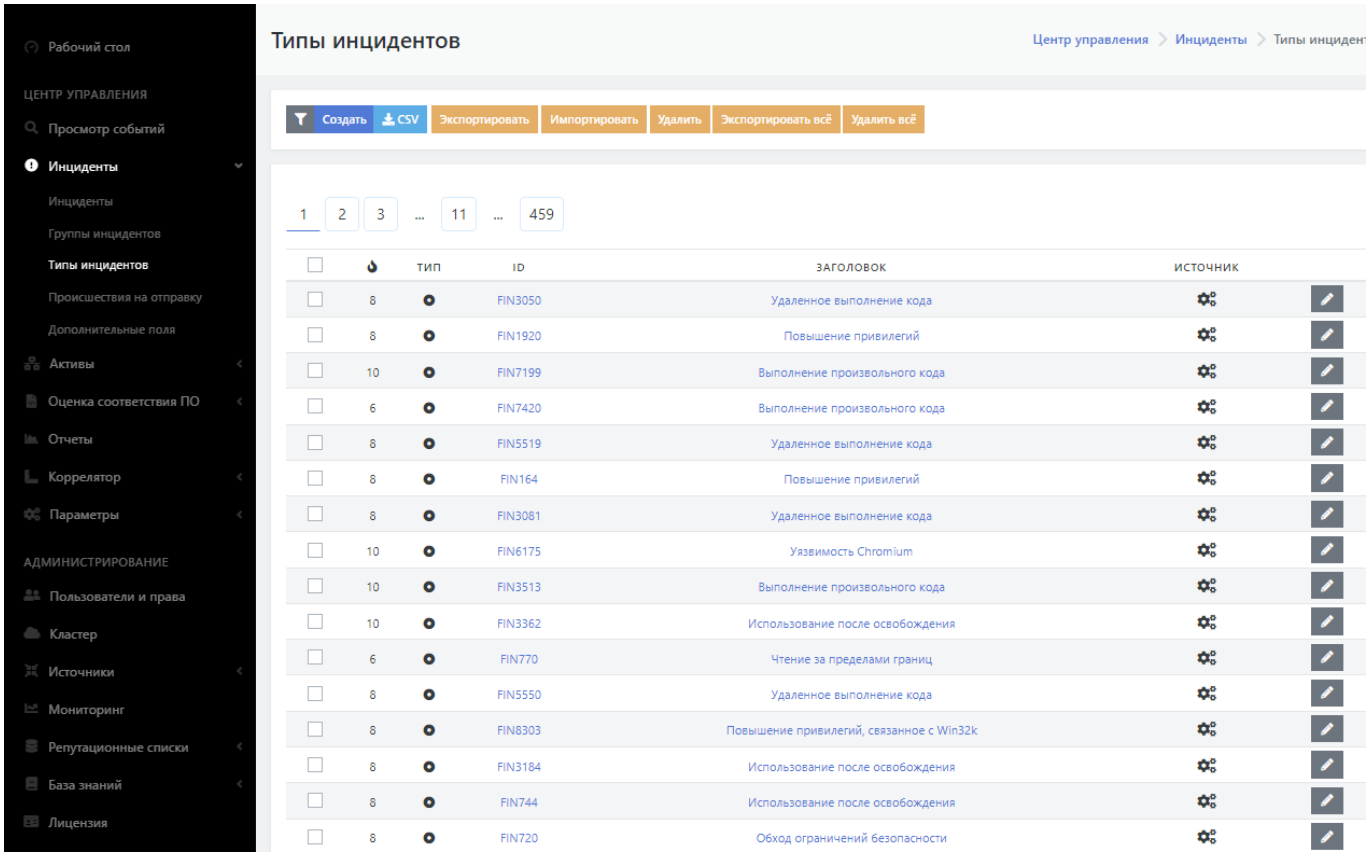



**Рисунок 25 – Рабочая область подраздела «Типы инцидентов»**

## 5.4.2 Список типов инцидентов. Параметры списка

Текущий список типов инцидентов представлен в виде табличного списка со следующими основными параметрами:

- Поле ( / ) - флаговое поле для выбора строк с типами для проведения с ними каких-то действий;

- **Оценка срочности** ( ) - содержит оценку срочности отработки инцидента;
- **Уровень риска** ( ) - содержит численную оценку уровня риска данного типа инцидента;
- **Тип** -- содержит пиктограмму - идентификатор типа;
- Поле ( ) - поле статуса "**Эксплуатируется удаленно**", указывает на возможность удаленной эксплуатации данного типа инцидента;
- **ID** - идентификатор типа инцидента в **Платформе Радар**;
- **Заголовок** - название типа инцидента, под которым он был заведен в **Платформе Радар**;
- **Источник** - содержит пиктограммы, соответствующие тому или иному источнику данных;
- Кнопка ( ) - функция редактирования параметров типа инцидента.

При необходимости разработчиками **Платформы Радар** могут быть введены дополнительные поля списка.

### 5.4.3 Настраиваемые фильтры списка типов инцидентов

При нажатии на кнопку открывается область с настраиваемыми фильтрами для табличного списка типов инцидентов (см. рисунок 26). Фильтр для списка типов инцидентов позволяет провести фильтрацию списка по следующим параметрам:

- Фильтр по заголовку типа инцидента - свободный текстовый ввод;
- Фильтр по статусу - раскрывающийся список с возможными значениями статуса;
- Фильтр по расположению актива - раскрывающийся список предустановленных мест расположения активов (например названия городов, где располагаются сетевые активы);
- Фильтр по наличию удаленной эксплуатации актива - раскрывающийся список "Да/ Нет/ Не важно".

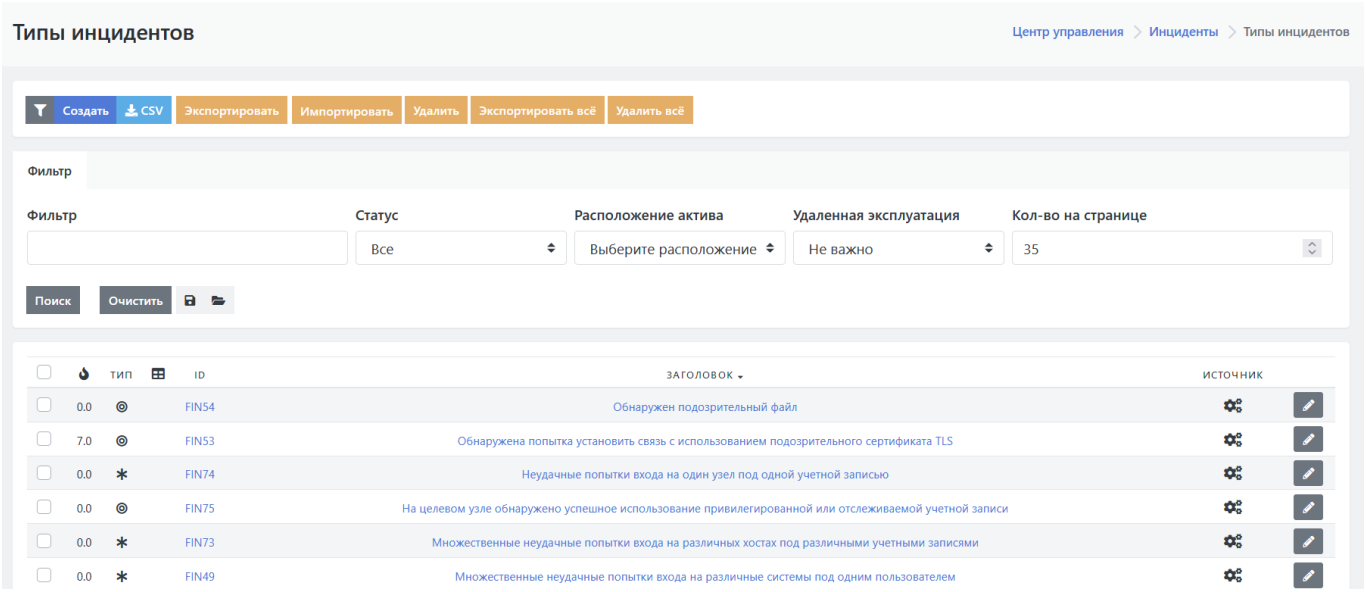



**Рисунок 26 – Фильтры для списка типов инцидентов**

Также в области настройки фильтров расположена функция редактирования количества строк табличного списка на одной экранной странице - "**Кол-во на странице**".

Подробнее работа с фильтрами приведена в разделе «Настраиваемые фильтры списка инцидентов».

### 5.4.4 Создание типа инцидента

При наличии необходимых прав пользователю доступна кнопка "**Создать**", по нажатию на которую произойдет переход на страницу создания нового типа инцидента. Подробное описание создания нового типа инцидента в **Платформе Радар** приведено в разделе «Создание нового типа инцидента вручную».

## 5.5 Подраздел "Дополнительные поля"

### 5.5.1 Основные элементы подраздела

Подраздел "**Дополнительные поля**" предназначен для управления вновь создаваемыми для карточки инцидентов полями. Такие поля можно заполнять в карточке инцидентов вручную, либо настроить автоматическое заполнение полей в правилах корреляции.

Подраздел содержит (см. рисунок 27):

- Текущий список дополнительных полей;
- Набор фильтров для просмотра списка дополнительных полей – кнопка  ;
- Функция создания нового дополнительного поля в системе - кнопка "**Создать**";
- Функция редактирования параметров дополнительного поля – кнопка  .

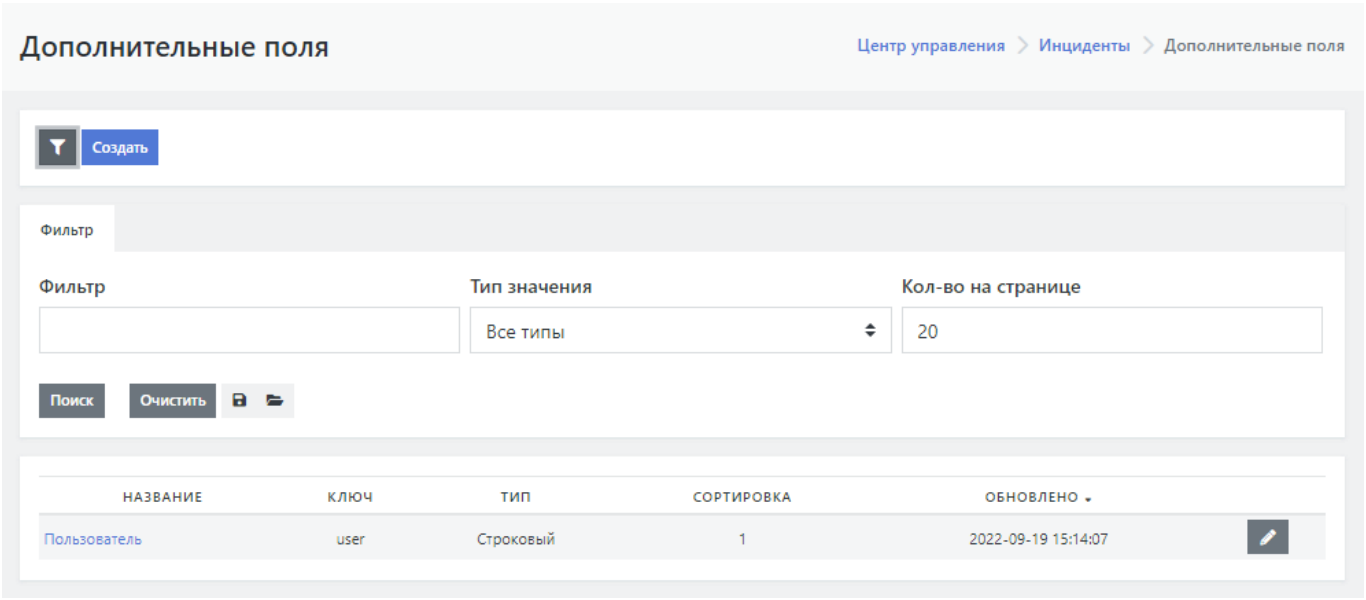



**Рисунок 27 – Рабочая область подраздела «Дополнительные поля»**

### 5.5.2 Список дополнительных полей. Параметры списка

Текущий список дополнительных полей представлен в виде табличного списка со следующими основными параметрами:

- **Название** - содержит название дополнительного поля. Клик по полю откроет окно просмотра всех инцидентов с заполненным дополнительным полем;
- **Ключ** - содержит ключ дополнительного поля;
- **Тип** - содержит тип дополнительного поля;
- **Сортировка** - содержит порядковый номер отображения дополнительного поля в карточке инцидентов;
- **Обновлено** - содержит дату и время последнего изменения дополнительного поля;
- Кнопка ( ) - функция редактирования параметров дополнительного поля.

### 5.5.3 Настраиваемые фильтры списка дополнительных полей

При нажатии на кнопку открывается область с настраиваемыми фильтрами для табличного списка дополнительных полей (см. рисунок 28). Фильтр для списка дополнительных полей позволяет провести фильтрацию списка по следующим параметрам:

- Фильтр по наименованию дополнительного поля - свободный текстовый ввод;
- Фильтр по типу дополнительного поля - выбор из списка:
  - булевый тип;
  - JSON;
  - строка;
  - число;
  - действительное число;
  - дата.

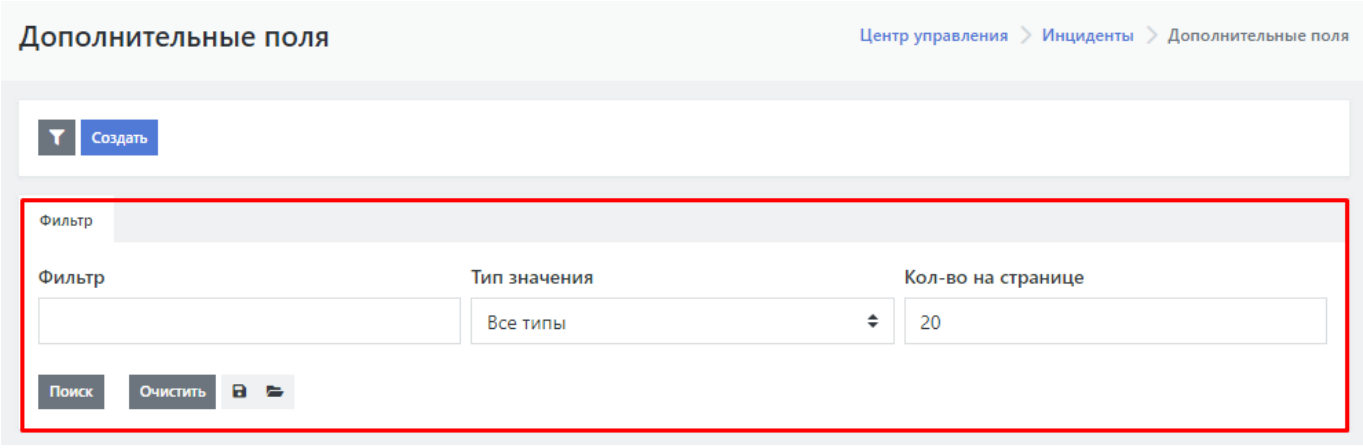



**Рисунок 28 – Фильтры для списка дополнительных полей**

Также в области настройки фильтров расположена функция редактирования количества строк табличного списка на одной экранной странице - "**Кол-во на странице**".

### 5.5.4 Создание дополнительного поля

При наличии необходимых прав пользователю доступна кнопка "**Создать**", по нажатию на которую произойдет переход на страницу создания дополнительного поля. При создании дополнительного поля (см. рисунок 29) заполните обязательные поля:

- **Название** - название дополнительного поля;
- **Ключ** - ключ дополнительного поля, используемый при настройке правил корреляции;
- **Тип** - выбираемый из списка тип дополнительного поля;
- **Сортировка** - порядковый номер отображения дополнительного поля в карточке инцидента, задается числом.

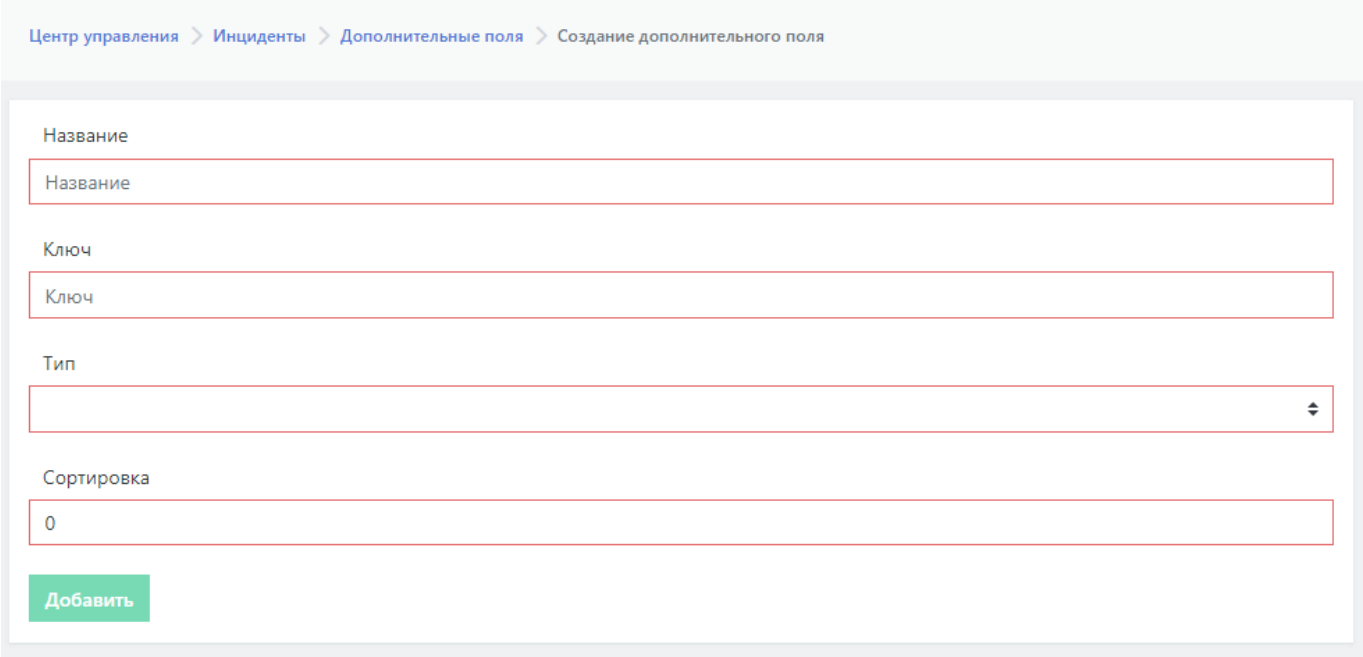



**Рисунок 29 – Создание дополнительного поля**

После заполнения всех полей нажмите кнопку "**Добавить**", после чего дополнительное поле будет добавлено в список и будет готово к использованию.

### 5.5.5 Использование дополнительных полей

Подробно об использовании дополнительных полей в карточке инцидентов описано в разделе «Привязка дополнительных полей».

# 6. Активы

## 6.1 Назначение и состав раздела "Активы"

Раздел "**Активы**" содержит следующие подразделы:

- **Активы** - предназначен для управления активами;
- **Группы активов** - предназначен для создания и работы с группами активов;
- **Настройки идентификации активов** - предназначена для управления стратегиями обнаружения активов;
- **Сетевые интерфейсы** - предназначен для управления сетевыми интерфейсами, обнаруженными у активов;
- **Результаты сканирования** - предназначен для управления импортом результатов сканирования на наличие уязвимостей;
- **Инвентаризация** - предназначен для инвентаризации таких объектов как хосты, сервисы, а также собираемых данных.

## 6.2 Подраздел "Активы"

### 6.2.1 Основные элементы подраздела

Подраздел "**Активы**" предназначен для оперирования активами, зарегистрированными в **Платформе Радар**.

Подраздел содержит следующие элементы (см. рисунок 30):

- Текущий список активов, заявленных в **Платформе Радар**;
- Набор фильтров для просмотра списка активов – кнопка  ;
- Функция создания нового актива в системе вручную - кнопка "**Создать**";
- Функция редактирования параметров актива – кнопка  ;
- Функция выгрузки данных во внешний файл в формате CSV - кнопка "**CSV**";
- Функция настройки временного периода обновления данных - раскрывающийся список "**Вручную**" (где "Вручную" значение по умолчанию);
- Кнопка для запуска обновления данных вручную -  ;
- Набор функций управления активами - раскрывающийся список "**Массовые действия**".

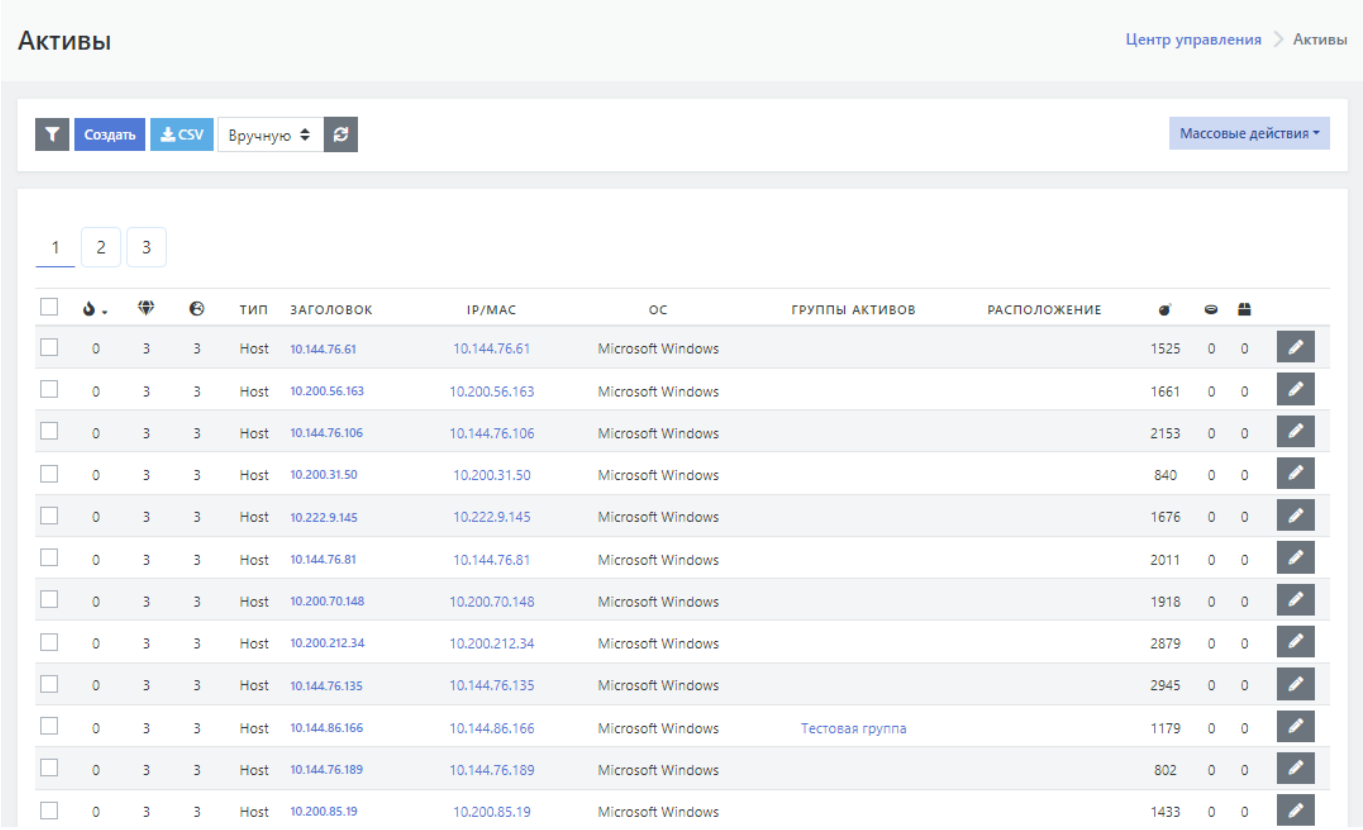



**Рисунок 30 – Рабочая область подраздела "Активы"**

## 6.2.2 Список активов. Параметры списка

Текущий список активов представлен в виде табличного списка со следующими основными параметрами (см. рисунок 31):

- Поле ( / ) - флаговое поле для выбора строк с активами для проведения с ними каких-то действий;
- **Уровень риска** ( ) - содержит численную оценку уровня риска инцидентов произошедших на данном активе;
- **Значимость актива** ( ) - содержит оценку значимости актива, которая в рамках бизнес-процессов оценивается числовыми значениями от 1 до 5;
- **Сетевая видимость** ( ) - оценивается числовыми значениями от 1 до 5;
- **Тип** - содержит тип оборудования актива (например Host, Server);
- **Заголовок** - название актива, под которым он был зафиксирован в **Платформе Радар**;
- **IP/MAC** - IP- или MAC-адрес актива;
- **ОС** - операционная система актива;
- **Группы активов** - название группы активов (или нескольких групп), в которую включен данный актив;
- **Расположение** - территориальное расположение актива, например город (если оно было указано при создании или редактировании записи актива в **Платформе Радар**);

- **Открытые инциденты** ( ) - количество открытых инцидентов на активе;
- **Риск принят** ( ) - количество инцидентов в статусе "риск принят" на активе;
- **Закрытые инциденты** ( ) - количество закрытых инцидентов на активе;
- Кнопка ( ) - функция редактирования параметров актива.

Отображение полей списка настраивается под требования конкретного пользователя. При необходимости разработчиками **Платформы Радар** могут быть введены дополнительные поля списка.

### 6.2.3 Настраиваемые фильтры списка активов

При нажатии на кнопку открывается область с настраиваемыми фильтрами для табличного списка активов (см. рисунок 31). Фильтры позволяют провести поиск в списке активов по следующим параметрам:

- Фильтр "Фильтр" - фильтрация по полю "Заголовок", свободный текстовый ввод;
- Фильтр по группам активов - раскрывающийся список с группами активов;
- Фильтр по расположению актива - раскрывающийся список предустановленных мест расположения активов (например названия городов, где располагаются сетевые активы);
- Фильтр по активности - раскрывающийся список: "Активный/ Неактивный/ Не важно";
- Фильтр по IP/Имя хоста/MAC - фильтрация по полю "IP/MAC", свободный текстовый ввод;
- Фильтр по ОС - фильтрация по полю "ОС", свободный текстовый ввод;
- Быстрый фильтр - раскрывающийся список со следующими значениями:
    - Активы в группах;
    - Активы без групп;
    - Имя похоже на IP адрес;
    - Повторяющееся имя;
    - Активы с пустым полем lookup;
    - Несколько кандидатов ответственных групп пользователей.
- Фильтр по значимости актива - раскрывающийся список со следующими значениями:
    - 1 - ключевой актив;
    - 2 - важный актив;
    - 3 - нормальный актив;
    - 4 - распределенный или некритичный актив;
    - 5 - тестовый актив.
- Фильтр по сетевой видимости актива - раскрывающийся список со следующими значениями:

- 1 - прямое подключение к Интернет;
- 2 - DMZ, частичный доступ из Интернет;
- 3 - штатный доступ в Интернет через Proxy;
- 4 - ограниченный доступ в Интернет;
- 5 - не подключенный к сети.

Также в области настройки фильтров расположена функция редактирования количества строк табличного списка на одной экранной странице - "**Кол-во на странице**".

Для фильтрации табличного списка установите нужные значения фильтров и нажмите на кнопку "**Поиск**" (см. рисунок 31). Для сброса всех фильтров - нажмите на кнопку "**Очистить**".

Настроенный набор фильтров можно сохранить для последующего использования - кнопка "**Сохранить**".

Для использования ранее созданного и сохраненного набора фильтров - нажать на кнопку "**Загрузить**".

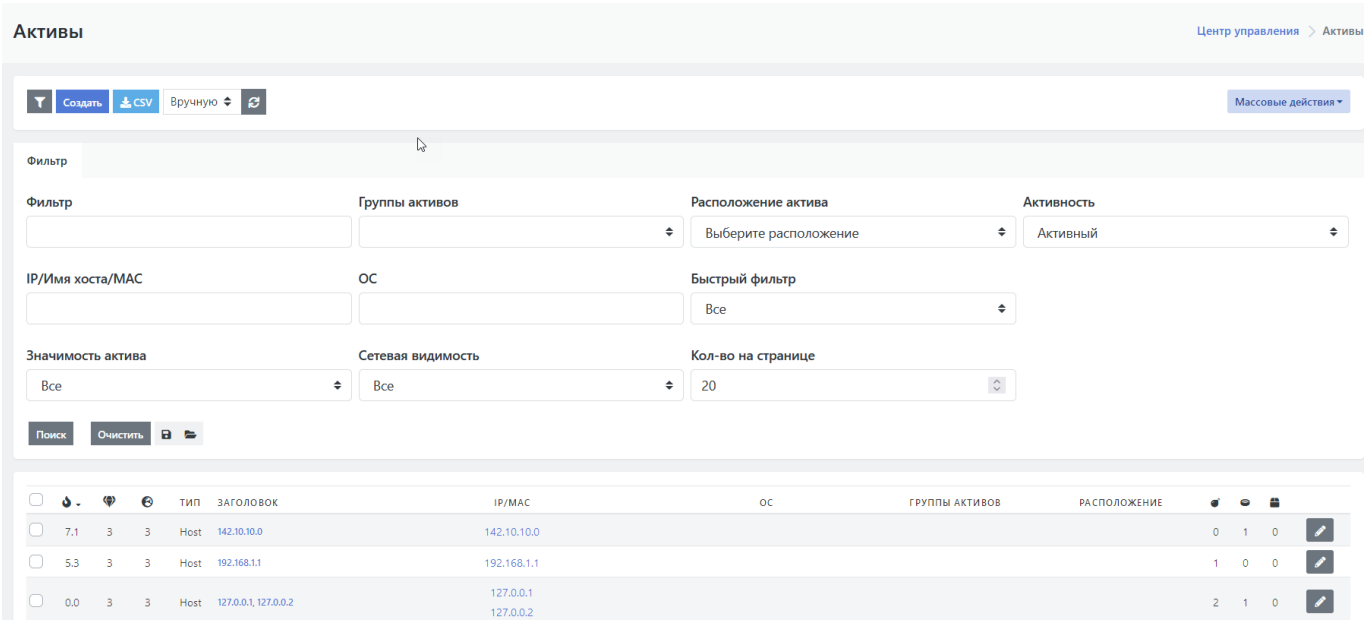



**Рисунок 31 – Фильтры для списка активов**

## 6.2.4 Настройка обновления данных

Функция настройки обновления данных состоит из раскрывающегося списка временных интервалов обновления и пиктограммы --  .

По умолчанию устанавливается режим ручного обновления. Обновление вручную производится при нажатии на пиктограмму  .

Для автообновления выбрать временной интервал обновления в раскрывающемся списке:

- 5 с.
- 15 с.
- 30 с.

- 60 с.

### 6.2.5 Управление активами

При наличии необходимых прав пользователю доступна функция "**Массовые действия**", включая удаление активов с **Платформы Радар**. Подробное описание управления активами приведено в разделе «Работа с активами».

### 6.2.6 Создание актива

При наличии необходимых прав пользователю доступна кнопка "**Создать**", по нажатию на которую произойдет переход на страницу создания актива в **Платформе Радар** вручную. Подробное описание создания актива в **Платформе Радар** вручную приведено в разделе «Создание активов вручную».

### 6.2.7 Редактирование параметров актива

Редактирование параметров актива доступно по нажатию на кнопку  . Подробное описание редактирования параметров группы актива приведено в разделе «Редактирование группы активов».

## 6.3 Подраздел "Группы активов"

### 6.3.1 Основные элементы подраздела

Подраздел "**Группы активов**" предназначен для оперирования группами активов, зарегистрированными в **Платформе Радар**.

Подраздел содержит следующие элементы (см. рисунок 32):

- Текущий список групп активов, созданных в **Платформе Радар**;
- Набор фильтров для просмотра списка групп – кнопка  ;
- Функция создания новой группы активов - кнопка "**Создать**";
- Функция редактирования параметров группы – кнопка  ;
- Функция выгрузки данных во внешний файл в формате CSV - кнопка "**Выгрузить CSV**";
- Функция запуска проверки на соответствие политике установленного ПО на активах группы - кнопка "**Проверка соответствия ПО**".

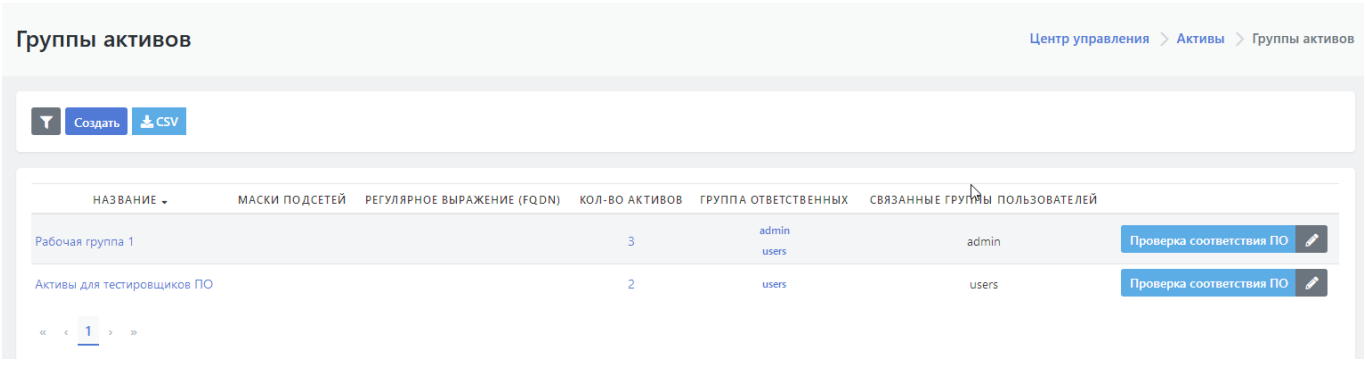



**Рисунок 32 – Рабочая область подраздела "Группы активов"**

### 6.3.2 Список групп активов. Параметры списка

Текущий список групп активов представлен в виде табличного списка со следующими основными параметрами (см. рисунок 32):

- **Название** - название группы активов в **Платформе Радар**;
- **Маски подсетей** - стратегия автоматического добавления активов в группу по заданной маске подсети. Новые активы, попадающие под указанную сетевую маску, будут автоматически включаться в группу;
- **Регулярное выражение (FQDN)** - стратегия автоматического добавления активов в группу по заданному регулярному выражению, применяемому на FQDN активов. Новые активы, чье FQDN отвечает заданному регулярному выражению, будут автоматически включаться в группу;
- **Кол-во активов** - количество активов в группе;
- **Группа ответственных** - группа пользователей, назначенная ответственными за данную группу активов;
- **Связанные группы пользователей** - группы пользователей, связанные с конкретными активами из данной группы;
- Кнопка "**Проверка соответствия ПО** - запуск проверки на соответствие политике установленного ПО на активах группы;
- Кнопка (  ) - функция редактирования параметров инцидента.

### 6.3.3 Настраиваемые фильтры списка групп активов

При нажатии на кнопку  открывается область фильтров для списка групп активов, которая включает в себя фильтр с полем для свободного текстового ввода.

Поиск по введенной текстовой строке осуществляется по полям "**Название**" и "**Кол-во активов**".

Общие правила работы с фильтрами приведены в разделе «Настраиваемые фильтры списка активов».

### 6.3.4 Создание группы активов

При наличии необходимых прав пользователю доступна кнопка "**Создать**", по нажатию на которую произойдет переход на страницу создания группы актива. Подробное описание создания группы активов в **Платформе Радар** вручную приведено в разделе «Создание группы активов».

### 6.3.5 Редактирование параметров группы активов

Редактирование параметров группы активов доступно по нажатию на кнопку  . Подробное описание редактирования параметров группы актива приведено в разделе «Редактирование группы активов».

# 6.4 Подраздел "Настройки идентификации активов"

## 6.4.1 Основные элементы подраздела

Подраздел "**Настройки идентификации активов**" предназначена для управления стратегиями обнаружения активов.

Подраздел содержит следующие элементы (см. рисунок 33):

- Текущий список сегментов с определенным правилом автоматического обнаружения активов;
- Набор фильтров для поиска сегментов в списке – кнопка  ;
- Функция создания нового сегмента - кнопка "**Создать**";
- Функция редактирования параметров сегмента – кнопка  .

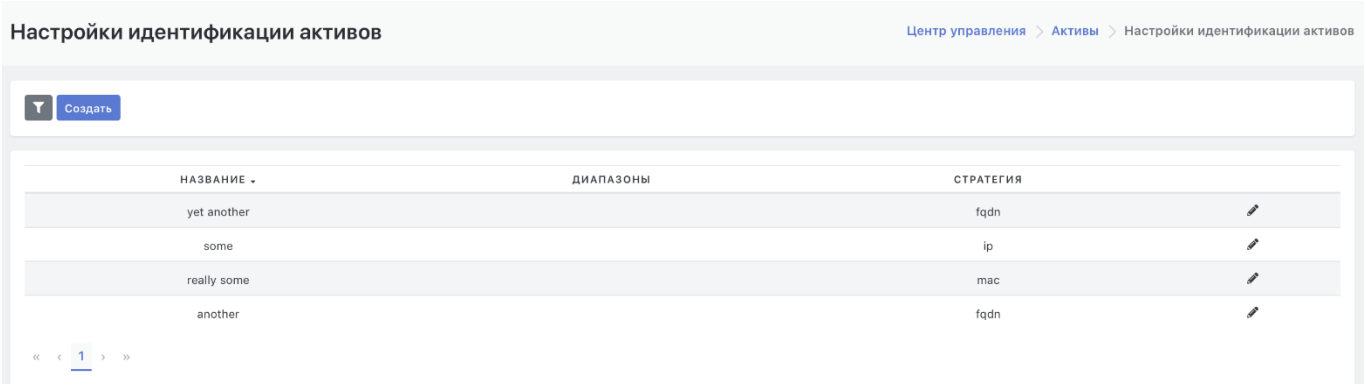



**Рисунок 33 – Рабочая область подраздела "Настройка идентификации активов"**

## 6.4.2 Список настроенных сегментов. Параметры списка

Текущий список настроенных сегментов для идентификации активов представлен в виде табличного списка со следующими основными параметрами (см. рисунок 34):

- Поле "**Название**" - название настроенного сегмента в **Платформе Радар**;
- Поле "**Диапазоны**" - сетевые диапазоны в рамках данного сегмента;
- Поле "**Стратегия**" - выбранная стратегия автоматической идентификации активов в данном сегменте;
- Кнопка (  ) - функция редактирования параметров настройки.

## 6.4.3 Настраиваемые фильтры списка сегментов

При нажатии на кнопку  открывается область с фильтрами для табличного списка настроенных сегментов (см. рисунок 34). Фильтры позволяют провести поиск в списке сегментов по следующим параметрам:

- Фильтр "Фильтр" - фильтрация по полю списка "**Название**", свободный текстовый ввод;
- Фильтр по диапазону сегмента - фильтрация по полю списка "**Диапазон**", свободный текстовый ввод;

- Фильтр по применяемой стратегии в сегменте - раскрывающийся список: "Все/ FQDN/ IP/ MAC".

Стандартные правила работы с фильтрами приведены в разделе «Настраиваемые фильтры списка активов».

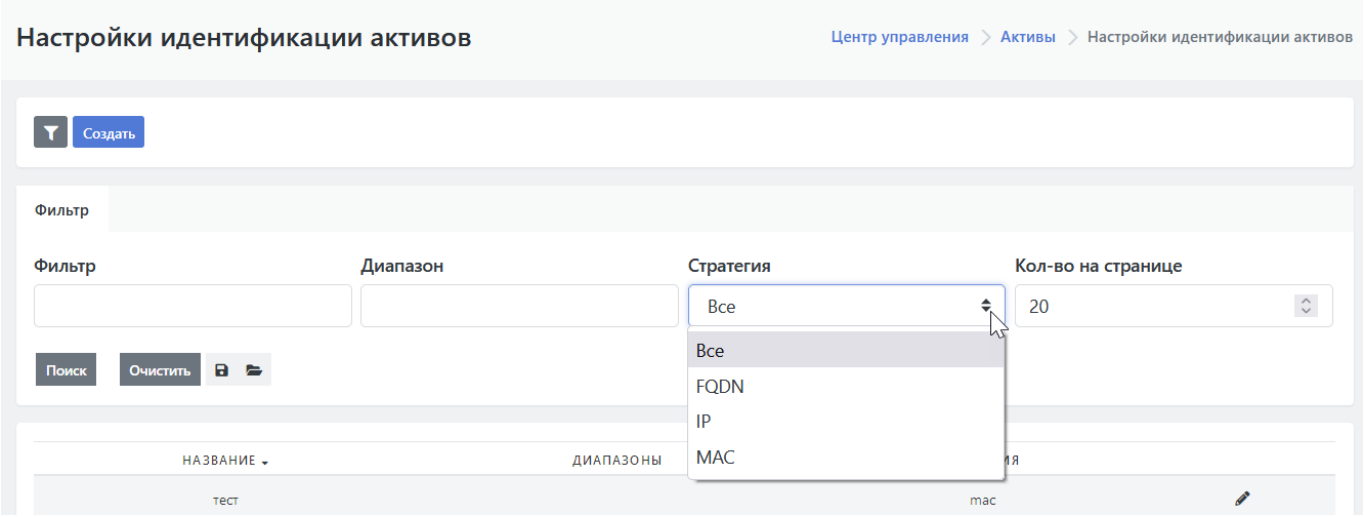



**Рисунок 34 – Фильтры подраздела "Настройка идентификации активов"**

### 6.4.4 Создание нового настроенного сегмента

При наличии необходимых прав пользователю доступна кнопка "**Создать**", по нажатию на которую произойдет переход на страницу создания нового сегмента с определенным правилом автоматического обнаружения активов. Подробное описание создания сегмента в **Платформе Радар** приведено в разделе «Создание новой политики идентификации».

### 6.4.5 Редактирование параметров сегмента

Редактирование параметров настроенного сегмента доступно по нажатию на кнопку  . Подробное описание редактирования параметров сегмента приведено в разделе «Редактирование политики идентификации».

## 6.5 Подраздел "Сетевые интерфейсы"

### 6.5.1 Основные элементы подраздела

Подраздел "**Сетевые интерфейсы**" предназначен для управления сетевыми интерфейсами, обнаруженными у активов.

Подраздел содержит следующие элементы (см. рисунок 35):

- Список обнаруженных на текущих активах сетевых интерфейсов;
- Набор фильтров для поиска сетевого интерфейса в списке – кнопка  ;
- Функция создания нового сетевого интерфейса вручную - кнопка "**Создать**";
- Функция выгрузки данных во внешний файл в формате CSV - кнопка "**Выгрузить CSV**";
- Функция редактирования параметров сегмента – кнопка  ;

- Функция удаления интерфейса – кнопка  .

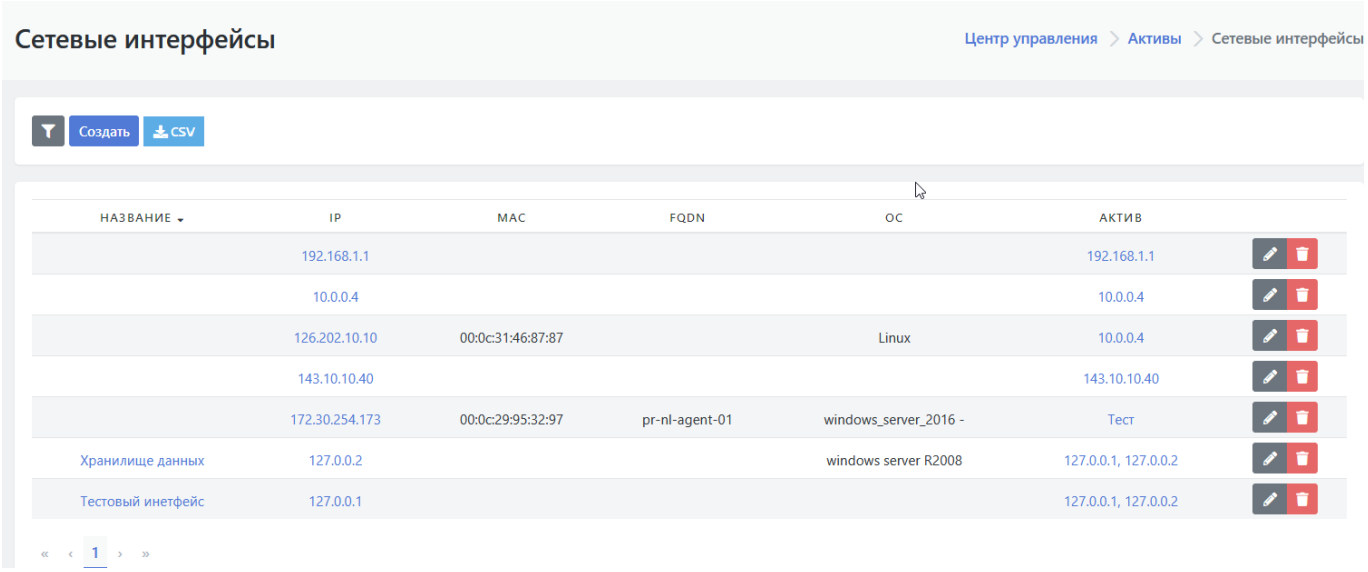



**Рисунок 35 – Рабочая область подраздела "Сетевые интерфейсы"**

## 6.5.2 Список сетевых интерфейсов. Параметры списка

Список сетевых интерфейсов представлен в виде табличного списка со следующими основными параметрами (см. рисунок 35):

- **Название** - имя интерфейса в **Платформе Радар**;
- **IP** - IP-адрес интерфейса;
- **MAC** - MAC-адрес интерфейса;
- **FQDN** -FQDN, определенный по данному IP-адресу;
- **ОС** - операционная система, обнаруженная при сканировании через данный интерфейс;
- **Актив** - название, связанного с интерфейсом актива (активов);
- Кнопка (  ) - функция редактирования параметров интерфейса;
- Кнопка (  ) - функция удаления сетевого интерфейса.

## 6.5.3 Настраиваемые фильтры списка интерфейсов

При нажатии на кнопку  открывается область с настраиваемыми фильтрами для списка интерфейсов (см. рисунок 36). Фильтры позволяют провести поиск по списку интерфейсов по следующим параметрам:

- Фильтр "Имя/ MAC/IP/ FQDN" - фильтрация по полям списка "**Название**", "**MAC**", "**IP**" и "**FQDN**", свободный текстовый ввод;
- Фильтр по ОС - фильтрация по полю "**ОС**", свободный текстовый ввод;
- Фильтр по наличию актива - раскрывающийся список: "Да/ нет/ Не важно";
- Фильтр по связанному активу - раскрывающийся список с текущими активами (см. рисунок 36).

Стандартные правила работы с фильтрами приведены в разделе «Настраиваемые фильтры списка активов».

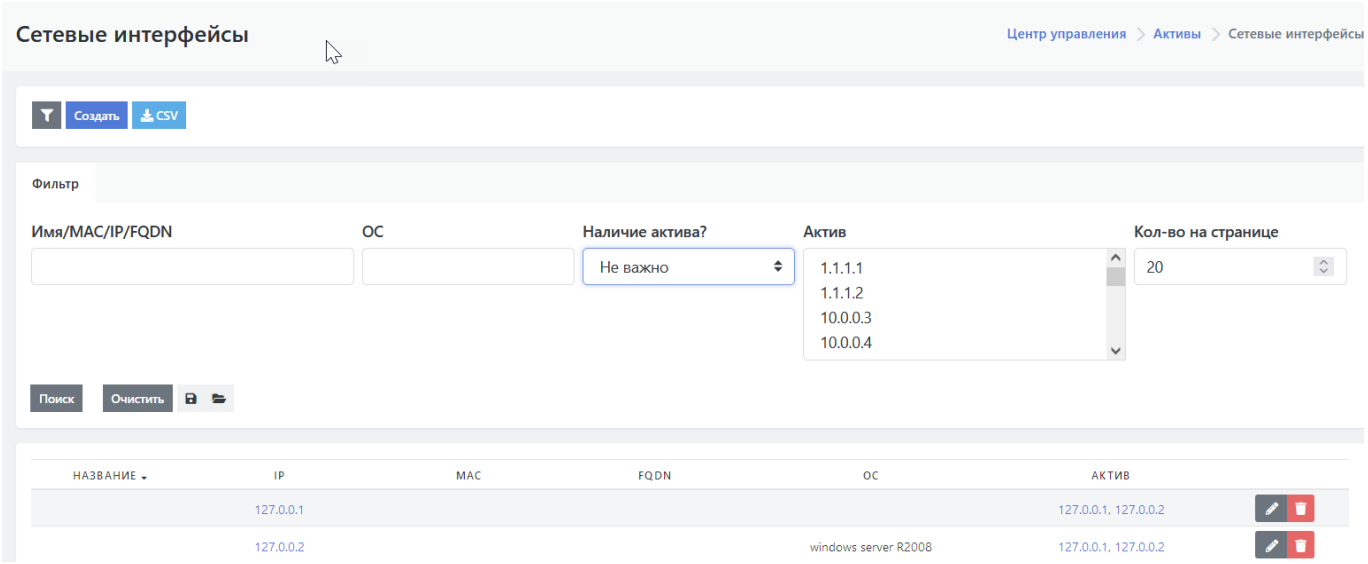



**Рисунок 36 – Фильтр подраздела "Сетевые интерфейсы"**

### 6.5.4 Создание сетевого интерфейса

При наличии необходимых прав пользователю доступна кнопка "**Создать**", по нажатию на которую произойдет переход на страницу создания нового сетевого интерфейса. Подробное описание создания интерфейса в **Платформе Радар** вручную приведено в разделе «Создание сетевых интерфейсов вручную».

### 6.5.5 Редактирование параметров сетевого интерфейса

Редактирование параметров сетевого интерфейса доступно по нажатию на кнопку  . Подробное описание редактирования параметров интерфейса приведено в разделе «Редактирование сетевого интерфейса».

## 6.6 Подраздел "Результаты сканирования"

### 6.6.1 Основные элементы подраздела

Подраздел "**Результаты сканирования**" предназначен для управления импортом результатов сканирования на наличие уязвимостей.

Подраздел содержит следующие элементы (см. рисунок 37):

- Список проведённых сканирований;
- Набор фильтров для поиска сканирования в списке – кнопка  ;
- Функция создания результатов сканирования - кнопка "**Создать**";
- Функция сравнения - кнопка "**Сравнить**".

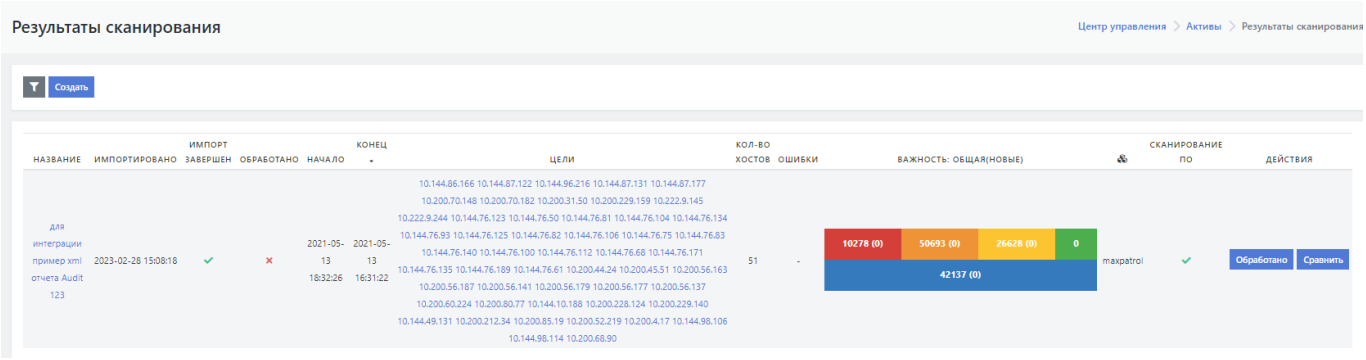



**Рисунок 37 - Рабочая область подраздела "Результаты сканирования"**

## 6.6.2 Список результатов сканирования. Параметры списка

Список результатов сканирования представлен в виде табличного списка со следующими основными параметрами (см. рисунок 37):

- **Название** - уникальное название проведенного сканирования в **Платформе Радар**;
- **Импортировано** - дата и время импорта результатов в **Платформу Радар**;
- **Импорт завершен** - статус успешного завершения импорта: "успешно завершен/не завершен" ( / );
- **Обработано** ( ) - статус обработки результатов сканирования оператором: "обработано/ не обработано" ( / );
- **Начало** - дата и время начала сканирования;
- **Конец** - дата и время завершения сканирования;
- **Цели** - активы (IP-адреса), указанные в задаче сканирования;
- **Кол-во хостов** - количество хостов в результатах сканирования;
- **Ошибки** - наличие ошибок в результатах сканирования;
- **Важность** - отображаются количественные результаты найденных уязвимостей, разделенные на группы важности по цвету согласно оценке CVSS;
- **Тип сканирования** ( ) - содержит тип сканирования: "redcheck / maxpatrol / nessus";
- **Сканирование ПО** - флаг наличия данных о программном обеспечении в результатах сканирования: ( / );
- Действия:
    - Кнопка "**Обработано/Не обработано**" - функция смена статуса обработки результатов сканирования оператором;
    - Кнопка "**Сравнить**" - функция просмотра изменений в составе уязвимостей между результатами сканирования и текущими данными в системе.

### 6.6.3 Настраиваемые фильтры списка результатов сканирования

При нажатии на кнопку  открывается область с настраиваемыми фильтрами для списка результатов сканирования (см. Рисунок 37). Фильтры позволяют провести поиск по списку результатов по следующим параметрам:

- Фильтр "**Фильтр**" - фильтрация по полю списка "**Название**", свободный текстовый ввод;
- Фильтр по флагу "**Внешнее сканирование**" - раскрывающийся список: "Да/ Нет/ Не важно";
- Фильтр по флагу "**Обработано?**" - раскрывающийся список: "Да/ Нет/ Не важно".

Стандартные правила работы с фильтрами приведены в разделе «Настраиваемые фильтры списка активов».

### 6.6.4 Создание новой записи о сканировании

При наличии необходимых прав пользователю доступна кнопка "**Создать**", по нажатию на которую произойдет переход на страницу создания новой записи о результатах сканирования. Подробное описание создания записи о результатах сканирования в **Платформе Радар** вручную приведено в разделе «Загрузка результатов сканирования».

### 6.6.5 Сравнение результатов сканирования

Сравнение между результатами сканирования и текущими данными в системе доступно по нажатию на кнопку "**Сравнить**". Подробное описание сравнения результатов приведено в разделе «Просмотр результатов сканирования».

## 6.7 Подраздел "Инвентаризация"

### 6.7.1 Состав подраздела

Подраздел "**Инвентаризация**" состоит из следующих вкладок:

- **Обнаружение хостов** - вкладка предназначена для запуска сканирование подсети и добавления результатов сканирования в виде новых активов или обновления существующих;
- **Обнаружение сервисов** - вкладка предназначена для запуска сканирования сервисов по добавленным активам в системе;
- **Сбор данных** - вкладка предназначена для запуска сбора информации с актива с авторизацией на активе через выбранные учетные данные.

### 6.7.2 Вкладка "Обнаружение хостов"

#### 6.7.2.1 Основные элементы вкладки

Вкладка "**Обнаружение хостов**" предназначена для запуска сканирование подсети и добавления результатов сканирования в виде новых активов или обновления существующих.

В рабочей области отображаются следующие элементы (см. рисунок 38):

- Список результатов сканирования;

- Настройки сканирования, состоящие из следующих элементов:
    - **IP** - поле ввода IP-адреса сканируемой подсети;
    - **Подсеть** - поле ввода маски для сканируемой подсети.
- Функция запуска сканирования активов указанной подсети - кнопка "**Сканировать**";
- Функция обновления данных активов по результатам сканирования - кнопка "**Обновить**".

### 6.7.2.2 Список результатов сканирования хостов. Параметры списка

Результаты сканирования - табличный список активов, обнаруженных при сканировании заданной подсети, с указанием следующих параметров активов (см. рисунок 38):

- Поле ( / ) - флаговое поле для выбора строк с активами для проведения с ними действий сканирования или обновления;
- **Host** - имя хоста в **Платформе Радар**;
- **IPV4** - IPV4-адрес хоста;
- **IPV6** - IPV6-адрес хоста;
- **MAC** - MAC-адрес хоста.

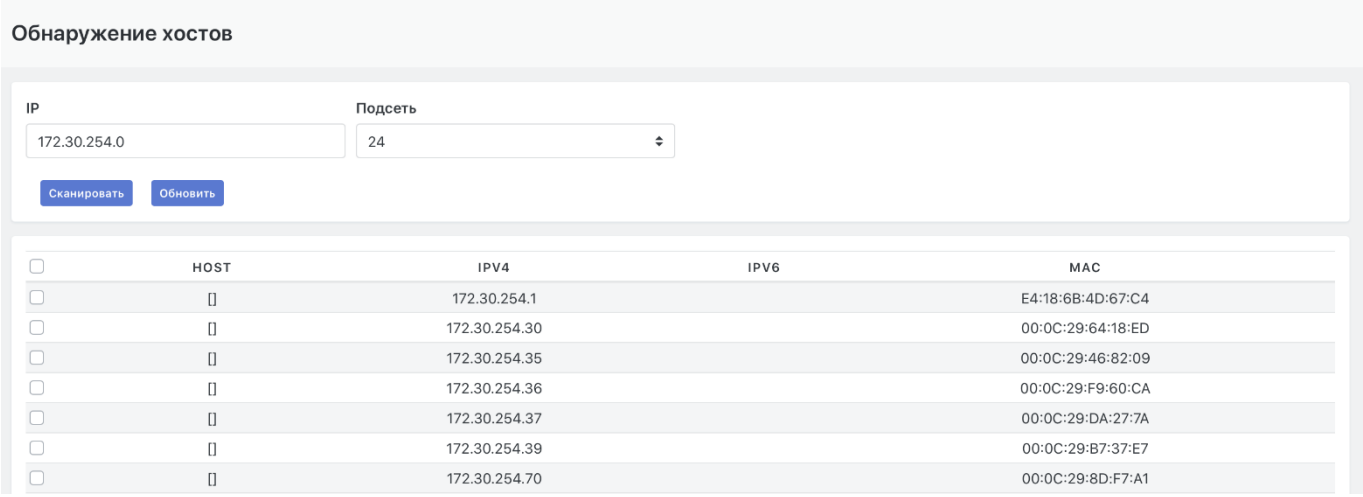



Рисунок 38 – Рабочая область вкладки "Обнаружение хостов"

### 6.7.2.3 Сканирование активов указанной подсети

Для запуска сканирования с целью обнаружения хостов необходимо нажать на кнопку "**Сканирование**". Подробное описание проведения обнаружения хостов приведено в разделе «Поиск активов в компьютерной сети».

### 6.7.2.4 Обновление данных по результатам сканирования

При нажатии на кнопку "**Обновить**" будет произведено повторное сканирование хостов.

## 6.7.3 Вкладка "Обнаружение сервисов"

### 6.7.3.1 Основные элементы подраздела

Вкладка "**Обнаружение сервисов**" предназначена для запуска сканирования сервисов по добавленным активам в системе.

Результатом сканирования является наполнение выбранных активов информацией об открытых портах и диагностике установленного ПО и ОС по открытым данным актива (см. рисунок 39).

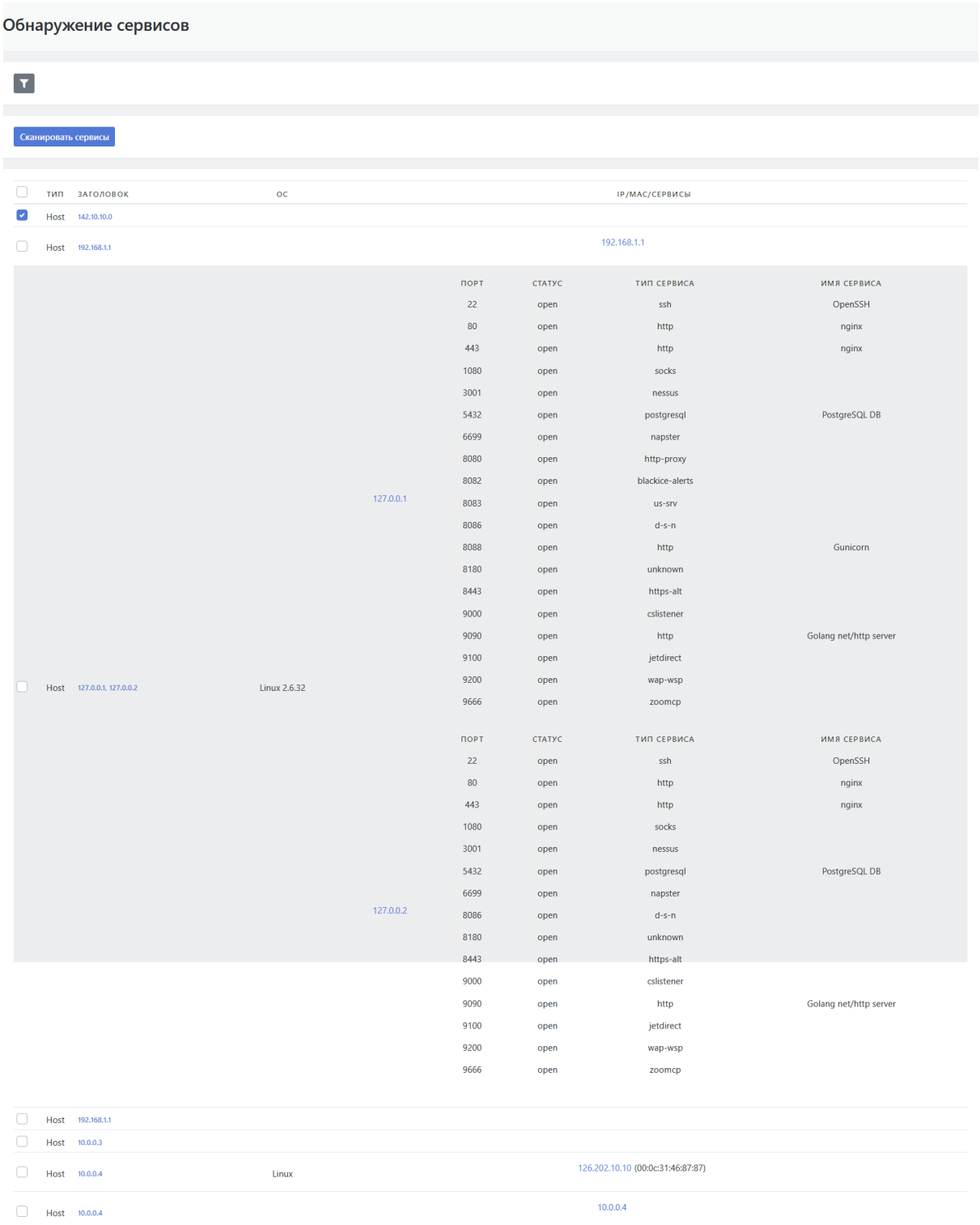



**Рисунок 39 – Рабочая область вкладки "Обнаружение сервисов"**

В рабочей области отображаются следующие элементы (см. рисунок 39):

- Набор фильтров для поиска активов в списке и соответствующих результатов сканирования сервисов – кнопка  ;
- Функция запуска сканирования сервисов - кнопка "**Сканировать сервисы**";
- Список доступных активов в **Платформе Радар** и соответствующих им результатов сканирования сервисов (детализация по сервисам).

### 6.7.3.2 Список активов с результатами сканирования сервисов. Параметры списка

Результаты сканирования - табличный список активов и обнаруженных на них при сканировании сервисов, с указанием следующих параметров активов (см. рисунок 39):

- Поле (  /  ) - флаговое поле для выбора строк с активами для проведения с ними действий сканирования сервисов;
- **Тип** - тип актива;
- **Заголовок** - имя актива в **Платформе Радар** (или IP-адрес);
- **ОС** - операционная система на активе;
- **IP/MAC/Сервисы** - содержит IP/MAC-адрес актива и детализацию по сервисам.

После проведения сканирования поле "**IP/MAC/Сервисы**" содержит детализацию по найденным сервисам, включая следующие данные:

- **Порт** - номер порта, на котором работает обнаруженный при сканировании сервис;
- **Статус** - статус порта (открыт/закрыт);
- **Тип сервиса** - тип обнаруженного при сканировании сервиса;
- **Имя сервиса** - имя обнаруженного при сканировании сервиса.

### 6.7.3.3 Настраиваемые фильтры списка активов

При нажатии на кнопку  открывается область с настраиваемыми фильтрами для списка активов с результатами сканирования сервисов (см. рисунок 40). Фильтры позволяют провести поиск по списку активов по следующим параметрам:

- Фильтр "Фильтр" - фильтрация по полю списка "Заголовок", свободный текстовый ввод;
- Фильтр по группам активов - раскрывающийся список текущих групп активов;
- Фильтр по расположению актива - раскрывающийся список предустановленных мест расположения активов (например названия городов, где располагаются сетевые активы);
- Фильтр по активности - раскрывающийся список: "Активный/ Неактивный/ Не важно";
- Фильтр по IP/MAC/Сервисы - фильтрация по полю "IP/MAC/Сервисы", свободный текстовый ввод;
- Фильтр по ОС - фильтрация по полю "ОС", свободный текстовый ввод;
- Фильтр по значимости актива - раскрывающийся список со следующими значениями:

- 1 - ключевой актив;
- 2 - важный актив;
- 3 - нормальный актив;
- 4 - распределенный или некритичный актив;
- 5 - тестовый актив.

- Фильтр по сетевой видимости актива - раскрывающийся список со следующими значениями:
  - 1 - прямое подключение к Интернет;
  - 2 - DMZ, частичный доступ из Интернет;
  - 3 - штатный доступ в Интернет через Proxy;
  - 4 - ограниченный доступ в Интернет;
  - 5 - не подключенный к сети.

Стандартные правила работы с фильтрами приведены в разделе «Настраиваемые фильтры списка активов».

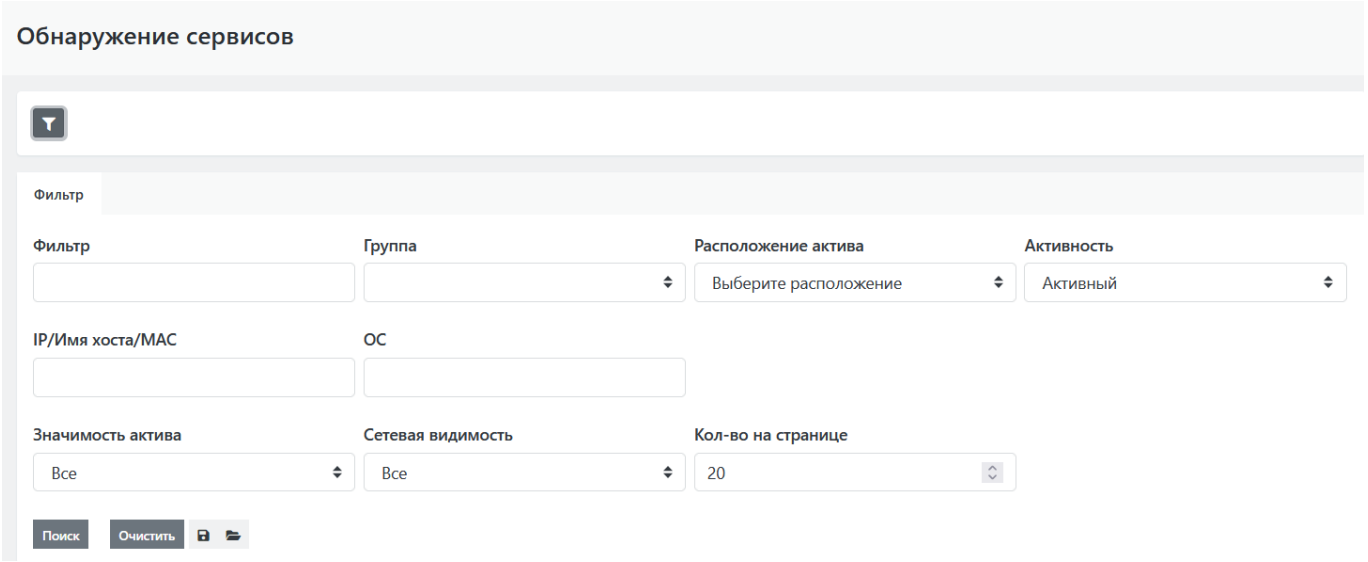



**Рисунок 40 – Фильтры для поиска в списке результатов сканирования сервисов**

### 6.7.3.4 Сканирование сервисов

Для запуска сканирования с целью обнаружения сервисов на активах необходимо нажать на кнопку "**Сканировать сервисы**". Подробное описание проведения сканирования сервисов приведено в разделе «Поиск сетевых сервисов на хосте без авторизации».

## 6.7.4 Вкладка "Сбор данных"

### 6.7.4.1 Основные элементы подраздела

Вкладка "**Сбор данных**" предназначена для запуска сбора информации с актива с авторизацией на активе через выбранные учетные данные.

Результатом работы сбора информации является найденный список установленного программного обеспечения на активе, а также детализация по спецификации устройства.

В рабочей области вкладки отображаются следующие элементы (см. рисунок 41):

- Настройки сбора данных, состоящие из следующих элементов:
  - **Протокол** - выбор протокола для сбора данных, раскрывающийся список протоколов: "SSH/ WMI/ RPS";
  - **Учетная запись** - выбор учетной записи для авторизации на активе, раскрывающийся список доступных учетных записей.;
  - **Данные** - выбор типов данных для сбора:
    - **Аппаратное обеспечение** - режим сбора данных с аппаратного обеспечения;
    - **Программное обеспечение** - режим сбора данных с ПО.
- Функция запуска сбора данных на активах согласно заданным настройкам - кнопка "**Собрать**";
- Список активов с результатами сбора данных на них;
- Набор фильтров для поиска в списке активов и результатов сбора данных – кнопка  .

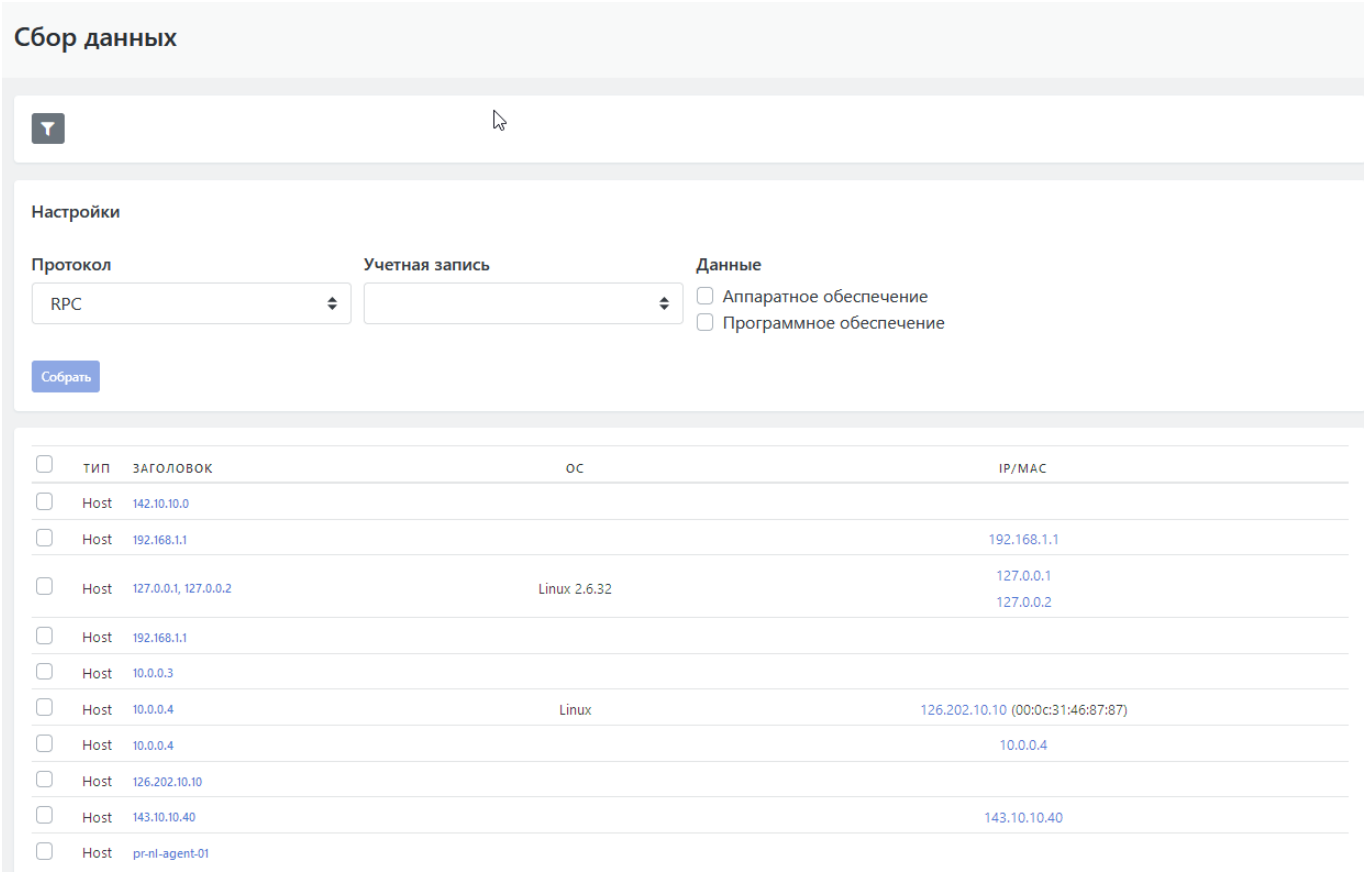



**Рисунок 41 – Рабочая область вкладки "Сбор данных"**

### 6.7.4.2 Список активов с результатами сбора данных. Параметры списка

Результаты сбора данных - табличный список активов и собранных с них данных, с указанием следующих параметров активов (см. рисунок 41):

- Поле (  /  ) - флаговое поле для выбора строк с активами для проведения с ними действий по сбору данных;
- **Тип** - тип актива;
- **Заголовок** - имя актива в **Платформе Радар** (или IP-адрес);
- **ОС** - операционная система на активе;
- **IP/MAC** - содержит IP/MAC-адрес и детализацию по собранным данным.

### 6.7.4.3 Настраиваемые фильтры списка активов

При нажатии на кнопку  открывается область с настраиваемыми фильтрами для списка активов с собранными данными. Для поиска используется набор фильтров идентичный набору фильтров для списка активов с результатами сканирования сервисов. Данный набор фильтров подробно описан в разделе «Настраиваемые фильтры списка активов».

### 6.7.4.4 Сбор данных с актива

Для запуска сбора данных с актива необходимо нажать на кнопку "**Собрать**". Подробное описание проведения сбора данных по разным протоколам приведено в разделе «Обнаружение ПО на хосте с авторизацией».

# 7. Коррелятор

## 7.1 Общее описание раздела "Коррелятор"

Раздел основного меню **Платформы Радар** "**Коррелятор**" включает следующие подразделы:

- **Фильтры потока событий** - подраздел предназначен для управления фильтрами отбора событий, применяемыми в правилах корреляции;
- **Макросы** - подраздел предназначен для управления макросами, применяемыми в правилах корреляции;
- **Правила** - подраздел предназначен для управления правилами корреляции;
- **Шаблоны** - подраздел предназначен для управления шаблонами алертов и шаблонами группировки
- **Табличные списки** - подраздел предназначен для хранения динамических данных, пополняемых пользователем или правилами корреляции;
- **Ретроспективная корреляция** - подраздел предназначен для создания задач анализа исторических данных; подробно описано в разделе «Ретроспективная корреляция».

## 7.2 Подраздел "Фильтры потока событий"

Подраздел "**Фильтры потока событий**" предназначен для управления фильтрами событий, использующимися в правилах корреляции (см. рисунок 42).

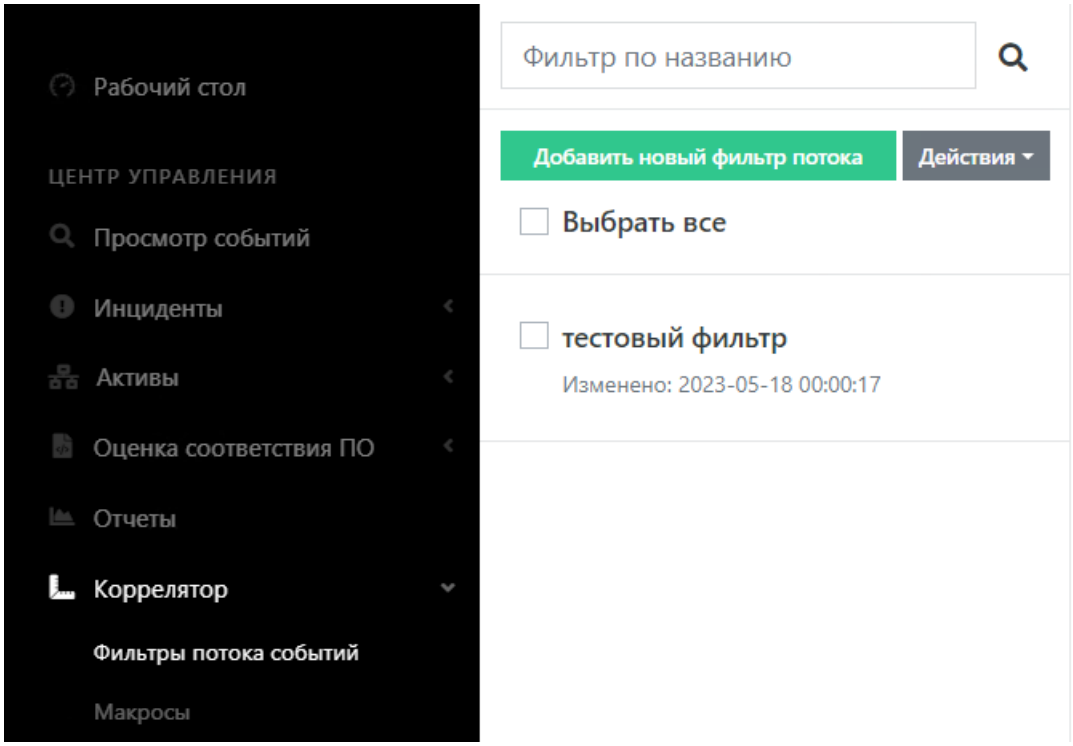



**Рисунок 42 – Рабочая область подраздела "Фильтры потока событий"**

Подраздел содержит:

- текущий список фильтров потока событий;

- функцию поиска фильтров потока событий по наименованию;
- функцию создания нового фильтра потока событий.

Подробно работа с фильтрами потока событий описана в разделе «Управление фильтрами потока событий».

## 7.3 Подраздел "Макросы"

Подраздел "**Макросы**" предназначен для управления макросами, использующимися в правилах корреляции (см. рисунок 43).

Подраздел содержит:

- текущий список макросов;
- функцию поиска макросов по наименованию;
- функцию создания нового макроса.

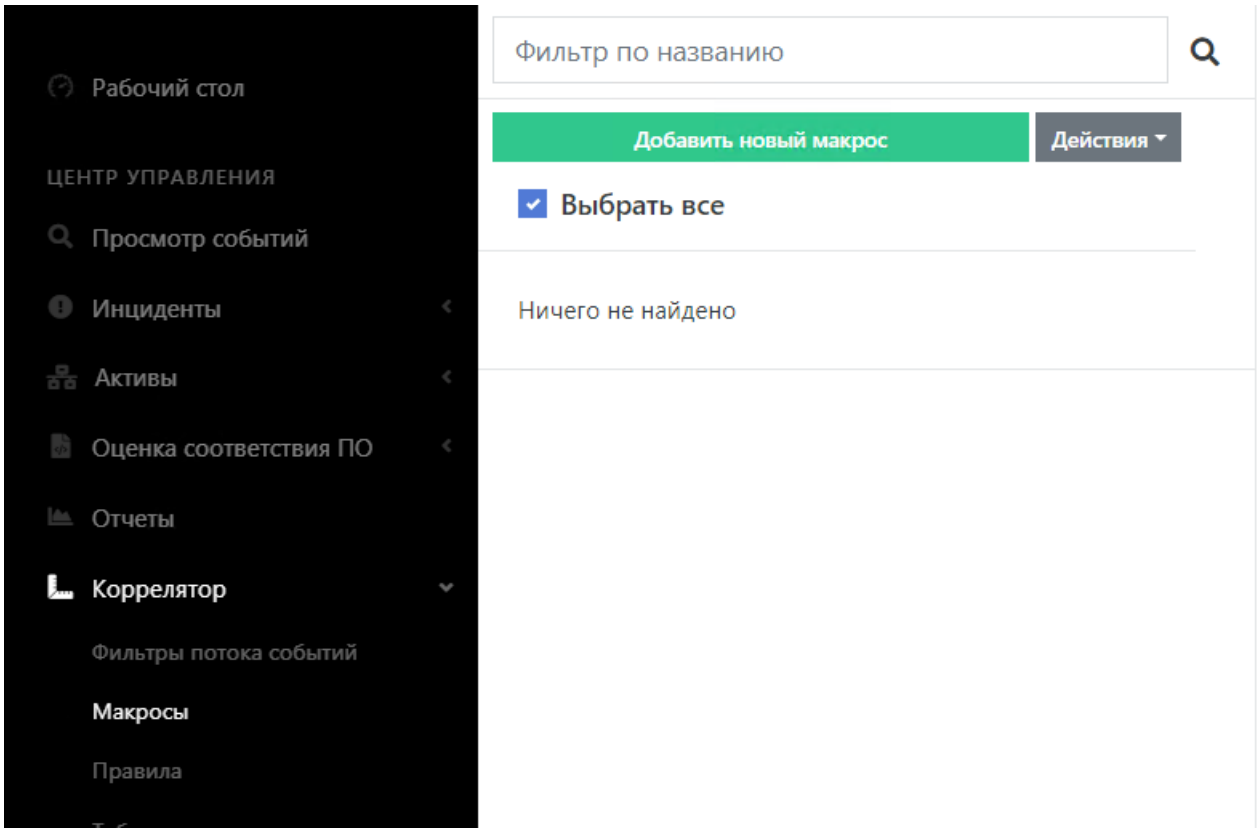



**Рисунок 43 – Рабочая область подраздела "Макросы"**

Подробно работа с макросами описана в разделе «Управление макросами».

## 7.4 Подраздел "Правила"

Подраздел "**Правила**" предназначен для управления правилами корреляции, самим коррелятором и диагностикой работы правил корреляции (см. рисунок 44).

Подраздел содержит:

- текущий список правил корреляции;
- функцию поиска правил корреляции по наименованию;

- функцию создания нового правила корреляции.

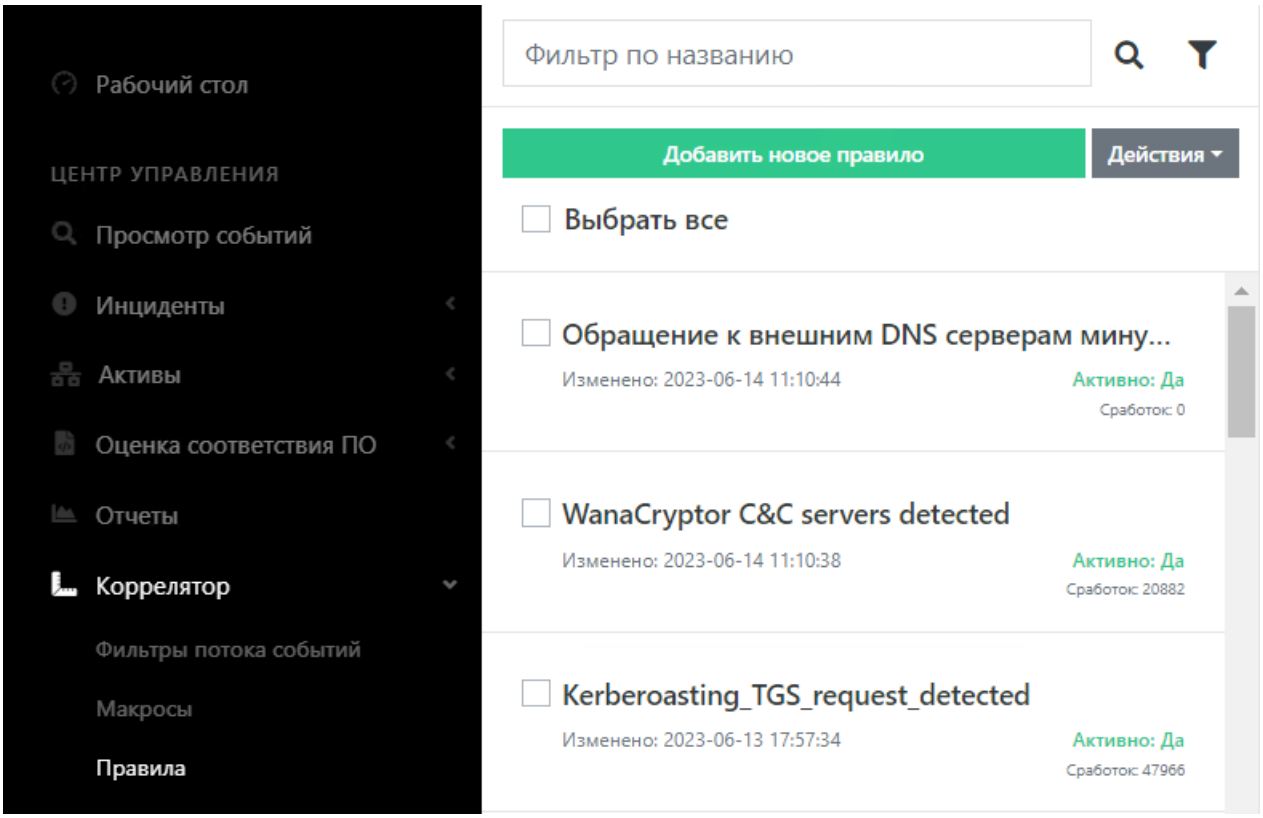



**Рисунок 44 – Рабочая область подраздела "Правила"**

Для каждого правила корреляции доступна информация:

- наименование правила корреляции;
- дата последнего изменения правила корреляции;
- признак активности правила;
- количество срабатываний.

Подробно работа с правилами корреляции описана в разделе «Управление правилами корреляции».

## 7.5 Подраздел "Шаблоны"

Подраздел "**Шаблоны**" предназначен для управления шаблонами алертов и группировки (см. рисунок 45). Шаблоны применяются при разработке правил корреляции (см. раздел «Управление правилами корреляции»).

Подраздел разделен на две части: шаблоны алертов, шаблоны группировки. Каждая из частей содержит:

- текущий список шаблонов;
- функцию поиска шаблона по наименованию;
- функцию создания нового шаблона.

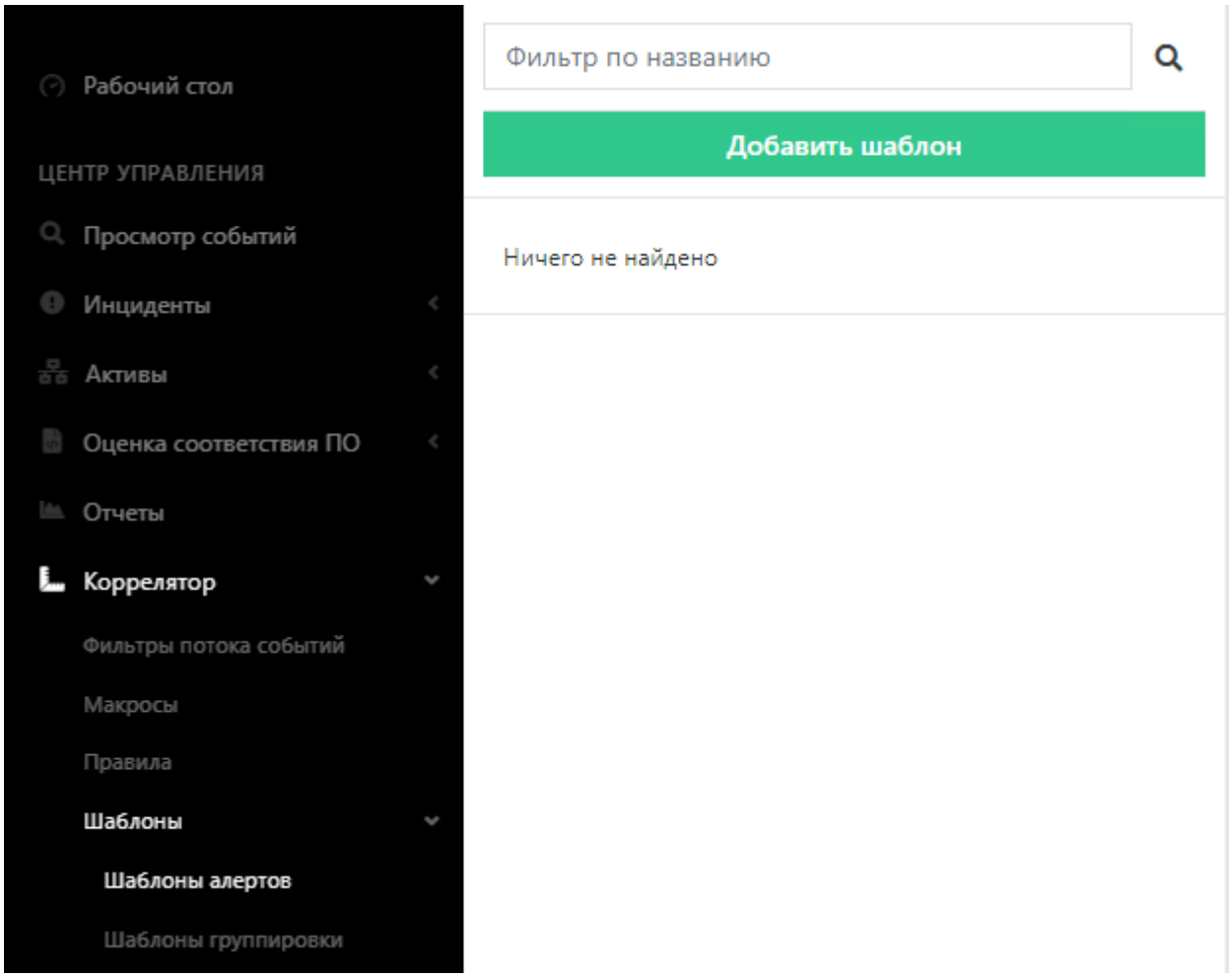



**Рисунок 45 – Рабочая область подраздела "Шаблоны"**

Для каждого шаблона в перечне указывается его наименование.

Подробно работа с шаблонами описана в разделе «Управление шаблонами».

## 7.6 Подраздел "Табличные списки"

Подраздел "**Табличные списки**" предназначен для создания и хранения пользовательских табличных списков, используемых в правилах корреляции (см. рисунок 46).

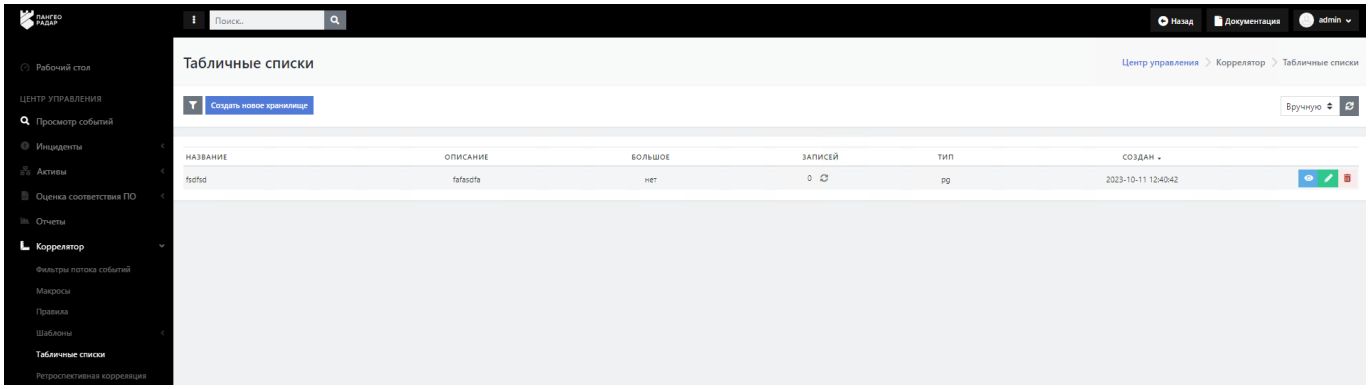



**Рисунок 46 – Рабочая область подраздела «Табличные списки»**

Подраздел содержит:

- текущий список табличных списков;

- функцию создания нового табличного списка.

Текущий список табличных списков представлен в виде таблицы со следующими атрибутами:

- **Название** - название табличного списка;
- **Описание** - описание табличного списка;
- **Большое** - признак большого табличного списка (более миллиона записей);
- **Тип** - тип табличного списка;
- Иконка просмотра табличного списка  ;
- Иконка редактирования табличного списка  ;
- Иконка удаления табличного списка  .

Подробно работа с табличными списками описана в разделе «Управление табличными списками».

# 8. Оценка соответствия ПО

## 8.1 Состав раздела "Оценка соответствия ПО"

Раздел "**Оценка соответствия ПО**" содержит следующие подразделы:

- **Результаты соответствия ПО** - подраздел предназначен для просмотра результатов проверки соответствия группы активов политикам контроля списков установленного программного обеспечения;
- **Список ПО** - подраздел предназначен для редактирования перечня обнаруженного программного обеспечения и создания групп программного обеспечения;
- **Наборы правил** - подраздел предназначен для создания политик, на соответствие которым будут в дальнейшем проводиться проверки программного обеспечения активов;
- **Правила** - подраздел предназначен для создания и редактирования правил контроля, из которых составляются политики для проверки соответствия программного обеспечения, установленного на активах.

## 8.2 Подраздел "Результаты соответствия ПО"

### 8.2.1 Основные элементы подраздела

Подраздел "**Результаты соответствия ПО**" предназначен для просмотра результатов проверки соответствия группы активов политикам контроля списков установленного программного обеспечения.

В рабочей области отображаются следующие элементы (см. рисунок 47):

- Результаты проверки соответствия ПО в виде табличного списка текущих результатов;
- Набор фильтров для поиска результата(-ов) в списке – кнопка  .

Запуск процесса проверки соответствия ПО производится из раздела "Активы". Подробное описание функции запуска приведено в разделе «Запуск процесса проверки соответствия».

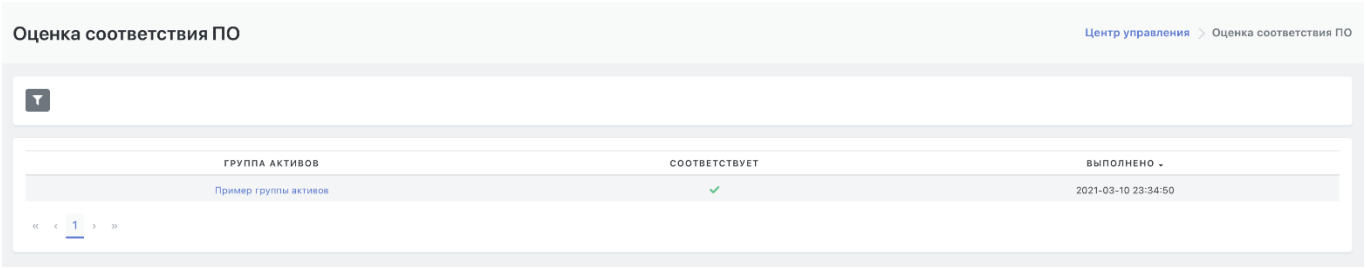



**Рисунок 47 – Рабочая область подраздела "Результаты соответствия ПО"**

### 8.2.2 Список результатов проверки ПО. Параметры списка

Текущий список результатов проверки соответствия ПО представлен в виде табличного списка со следующими параметрами:

- **Группа активов** - название группы активов, на которых проводилась данная проверка, активная ссылка на детализацию результатов проверки соответствия ПО;

- **Соответствует** - статус соответствия ПО для группы активов по результату проверки;
- **Выполнено** - дата и время время, в которое запускалась проверка соответствия ПО на указанном активе.

### 8.2.3 Настраиваемые фильтры списка результатов проверки ПО

При нажатии на кнопку  открывается область фильтров для списка результатов проверки ПО, которая включает в себя фильтр с полем для свободного текстового ввода.

Поиск по введенной текстовой строке осуществляется по полю "**Группа активов**".

### 8.2.4 Просмотр детализации результатов контроля соответствия ПО

Детализация результатов проверки ПО доступна по клику на название группы активов в строке проверки. Данная функция подробно приведена в разделе «Анализ результатов проверок соответствия ПО».

## 8.3 Подраздел "Список ПО"

### 8.3.1 Основные элементы подраздела

Подраздел "Список ПО" предназначен для редактирования перечня ПО, обнаруженного сканерами уязвимостей при сканировании активов, и для создания групп ПО.

В рабочей области отображаются следующие элементы (см. рисунок 48):

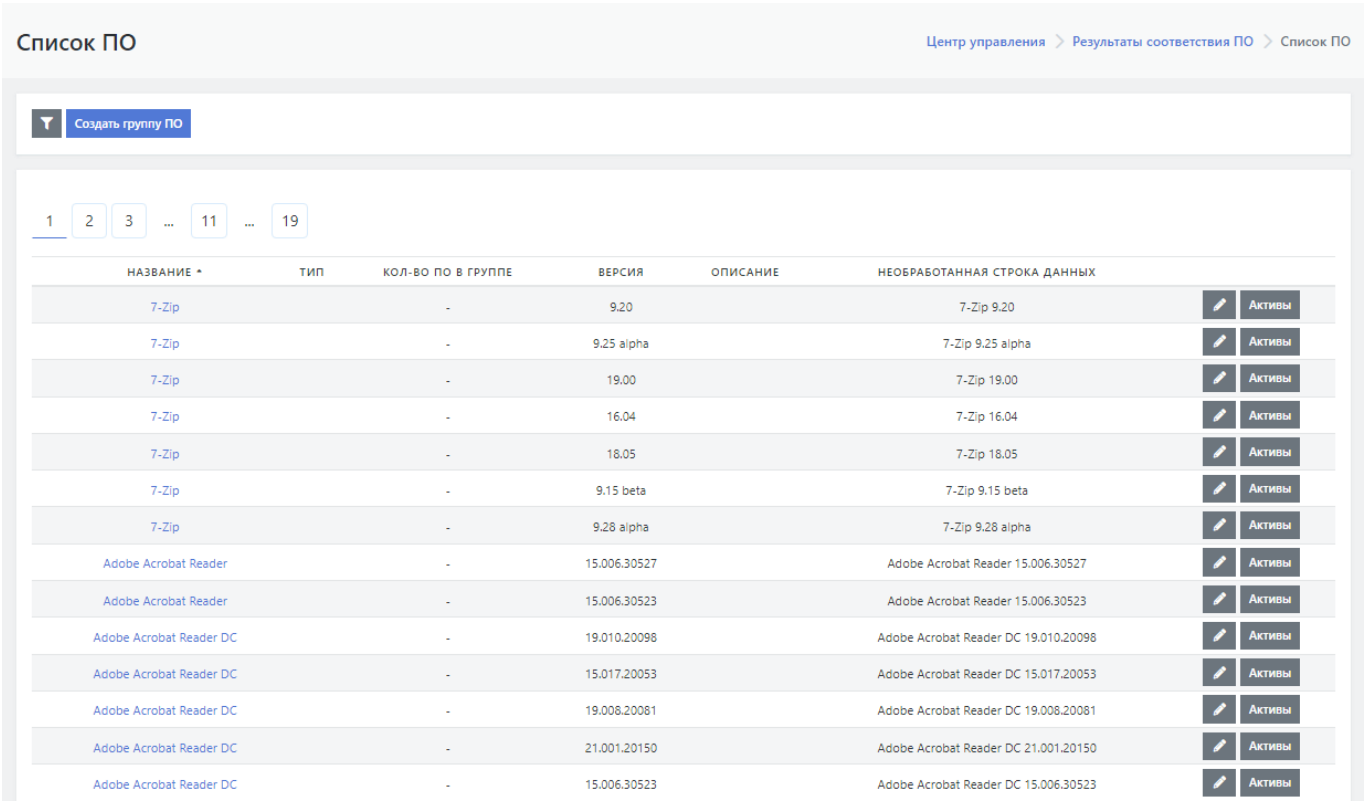



**Рисунок 48 – Рабочая область подраздела "Список ПО"**

- Табличный список программного обеспечения, обнаруженного сканерами уязвимостей при сканировании активов;
- Набор фильтров для поиска ПО в списке – кнопка  ;
- Функция создания группы ПО - кнопка "**Создать группу ПО**";
- Функция редактирования параметров групп ПО – кнопка  ;
- Функция просмотра информации по активам, на которых найдено данное ПО - кнопка "**Активы**".

### 8.3.2 Список ПО. Параметры списка

Текущий список ПО, обнаруженного сканерами уязвимостей при сканировании активов, представлен в виде табличного списка со следующими параметрами:

- **Название** - название ПО или группы ПО, активная ссылка на краткое описание ПО;
- **Тип**;
- **Кол-во ПО в группе** - количество ПО в составе группы;
- **Версия** - текущая версия ПО;
- **Описание** - описание ПО, заданное пользователем **Платформы Радар**;
- **Необработанная строка данных** - данные, полученные от сканера уязвимостей;
- Кнопка (  ) - функция редактирования данных о ПО;
- Кнопка "**Активы**" - функция просмотра информации по активам, на которых установлено данное ПО.

### 8.3.3 Настраиваемые фильтры списка ПО

При нажатии на кнопку  открывается область фильтров для списка ПО, которая включает в себя следующие фильтры:

- Фильтр с полем для свободного текстового ввода. Поиск по введенной текстовой строке осуществляется по полю "**Название**".
- Фильтр по состоянию ПО - раскрывающийся список, возможные значения "**Установленное**" / "**Все**".

### 8.3.4 Просмотр информации о ПО

Для просмотра деталей по записи о программном обеспечении нужно щёлкнуть по названию ПО в поле "**Название**". Откроется форма просмотра деталей записи о программном обеспечении.

Для просмотра перечня активов, на которых установлено программное обеспечение необходимо нажать кнопку "**Активы**" в строке интересующего ПО. На экране откроется перечень активов, на которых найдено данное ПО.

Более подробное описание просмотра детализации приведено в разделе «Анализ программного обеспечения на активах».

### 8.3.5 Создание группы ПО

При наличии необходимых прав пользователю доступна кнопка "**Создать группу ПО**", по нажатию на которую произойдет переход на страницу создания группы. Подробное описание функции создания группы ПО приведено в разделе «Анализ программного обеспечения на активах».

### 8.3.6 Редактирование данных ПО

Для редактирования данных о ПО необходимо нажать на кнопку  , после чего произойдет переход на страницу редактирования данных. Подробное описание функции редактирования приведено в разделе «Анализ программного обеспечения на активах»

## 8.4 Подраздел "Наборы правил"

### 8.4.1 Основные элементы подраздела

Подраздел "**Наборы правил**" предназначен для создания политик, (набор правил), на соответствие которым будут в дальнейшем проводиться проверки программного обеспечения активов.

В рабочей области отображаются следующие элементы (см. рисунок 49):

- Табличный список политик, созданных на текущий момент в **Платформе Радар**.
- Набор фильтров для поиска политик в списке – кнопка  .
- Функция создания новой политики - кнопка "**Создать**".
- Функция редактирования политики – кнопка  .

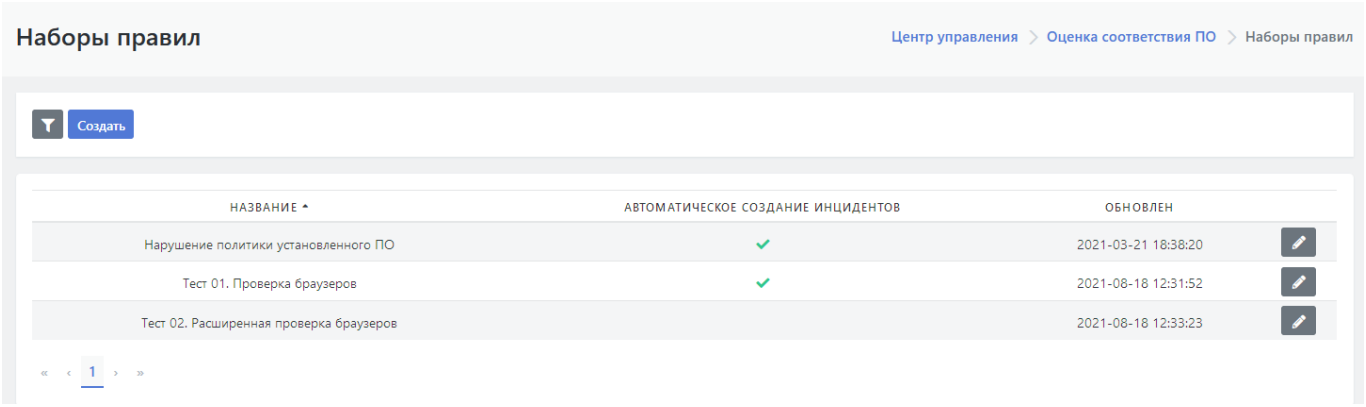



**Рисунок 49 – Рабочая область подраздела "Наборы правил"**

### 8.4.2 Список политик. Параметры списка

Текущий список политик представлен в виде табличного списка со следующими параметрами:

- **Название** - название политики (группы правил).
- **Автоматическое создание инцидентов** - включена/выключена функция автоматического создания инцидентов при выявлении нарушения политики.
- **Обновлен** - дата и время создания или последнего редактирования политики.

- Кнопка ( ) - функция редактирования параметров политики.

### 8.4.3 Настраиваемые фильтры списка политик

При нажатии на кнопку открывается область фильтров для списка политик, которая включает в себя фильтр с полем для свободного текстового ввода.

Поиск по введенной текстовой строке осуществляется по полю "**Название**".

### 8.4.4 Создание, редактирование, удаление политик

При нажатии на кнопку "**Создать**" открывается форма создания политики.

При нажатии на кнопку открывается форма редактирования указанной политики, включая функцию "**Удалить**".

Подробное описание создания, редактирования и удаления политик приведено в отдельном разделе «Настройка контроля установленного программного обеспечения. Управление политиками проверки соответствия ПО».

## 8.5 Подраздел "Правила"

### 8.5.1 Основные элементы подраздела

Подраздел "**Правила**" предназначен для создания и редактирования правил контроля, из которых составляются политики для проверки соответствия программного обеспечения, установленного на активах.

В рабочей области отображаются следующие элементы (см. рисунок 50):

- Табличный список правил, созданных на текущий момент в **Платформе Радар**.
- Набор фильтров для поиска правил в списке – кнопка .
- Функция создания нового правила - кнопка "**Создать**".
- Функция редактирования правила – кнопка .

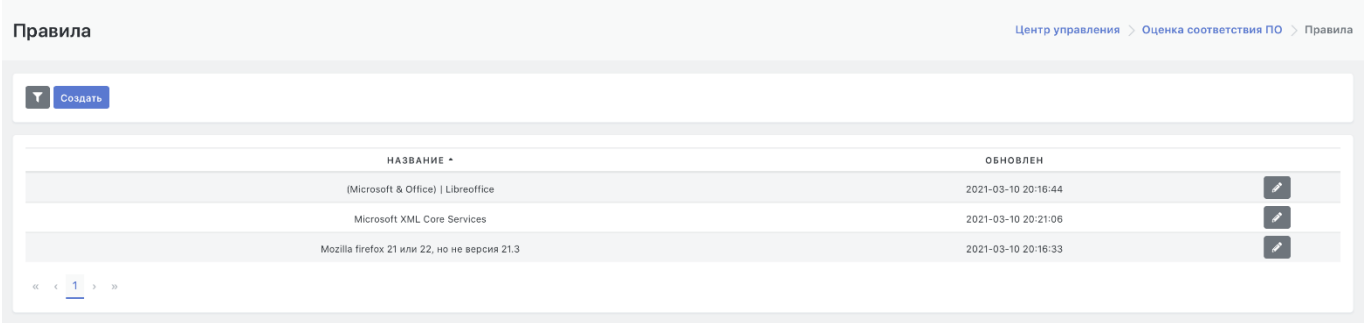



**Рисунок 50 – Рабочая область подраздела "Правила"**

### 8.5.2 Список правил. Параметры списка

Текущий список правил, представлен в виде табличного списка со следующими параметрами:

- **Название** - название правила.

- **Обновлен** - дата и время создания или последнего редактирования правила.
- Кнопка (  ) - функция редактирования параметров правила.

### 8.5.3 Настраиваемые фильтры списка политик

При нажатии на кнопку  открывается область фильтров для списка правил, которая включает в себя фильтр с полем для свободного текстового ввода.

Поиск по введенной текстовой строке осуществляется по полю "**Название**".

### 8.5.4 Создание, редактирование, удаление правила

При нажатии на кнопку "**Создать**" открывается форма создания правила.

При нажатии на кнопку  открывается форма редактирования указанного правила, включая функцию "**Удалить**".

Подробное описание создания, редактирования и удаления правила приведено в отдельном разделе «Настройка контроля установленного программного обеспечения. Управление правилами».

# 9. Параметры

## 9.1 Состав раздела "Параметры"

Раздел "**Параметры"** состоит из следующих подразделов:

- **Параметры** - подраздел предназначен для настройки общих параметров **Платформы Радар**.
- **Сопоставление данных** - подраздел предназначен для настройки интеграции полей данных **Платформы Радар** с системой ГосСОПКА (подробнее см. в разделе «Работа с НКЦКИ»).
- **API конструктор** - подраздел предназначен для общей настройки интеграции **Платформы Радар** с системой ГосСОПКА (подробнее см. в разделе «Работа с НКЦКИ»).
- **Черный список ID плагинов** - подраздел предназначен для создания списка ID плагинов сканера Nessus, игнорируемых в процессе работы.
- **Оповещения по задержкам в обработке** - подраздел предназначен для настройки автоматических оповещений по задержкам в обработке инцидентов, формируемых **Платформой Радар**.

## 9.2 Подраздел «Параметры»

### 9.2.1 Состав и назначение вкладок

Подраздел "**Параметры**" предназначен для обновления общих параметров панели управления, обновления параметров сканера уязвимости и обновления идентификатора.

Подраздел включает следующие вкладки:

- **Общие** - вкладка предназначена для обновления общих параметров **Платформы Радар**, включая значения по умолчанию (см. рисунок 51);
- **Обработка уязвимостей** - вкладка предназначена для настройки параметров автоматической обработки уязвимостей;
- **Синхронизация с Базой Знаний** - вкладка предназначена для проведения синхронизации с Базой знаний.

### 9.2.2 Вкладка "Общие". Обновление общих параметров

Рабочее поле вкладки "**Общие**" содержит поля для редактирования следующих общих параметров (см. рисунок 51):

- **Название клиента** - текстовое поле ввода, в котором указывается наименование организации в которой установлена **Платформа Радар**;
- **Риск принят** - текстовое поле ввода, в котором необходимо указать количество дней. При принятии риска инцидента указанное количество дней будет устанавливаться **Платформой Радар** в качестве срока по умолчанию в параметре "Принять до". Чтобы оставить значение параметра "Принять до" пустым, укажите в поле "0".

- **Расположение** - текстовое поле ввода, предназначенное для редактирования списка территориального расположения активов для соответствующих фильтров.
- **Группа пользователей по-умолчанию** - выбор из списка группы пользователей, которая будет назначаться по-умолчанию для инцидентов, связанных с активами без определенного "ответственного пользователя".
- **Стратегия идентификации активов по-умолчанию** - выбор из списка глобальной стратегии идентификации, которая будет назначаться по-умолчанию, если актив не попал ни под одну политику идентификации. Доступны следующие стратегии идентификации:
    - IP;
    - FQDN;
    - MAC.

Для сохранения внесенных обновлений нажмите на кнопку "**Сохранить**".

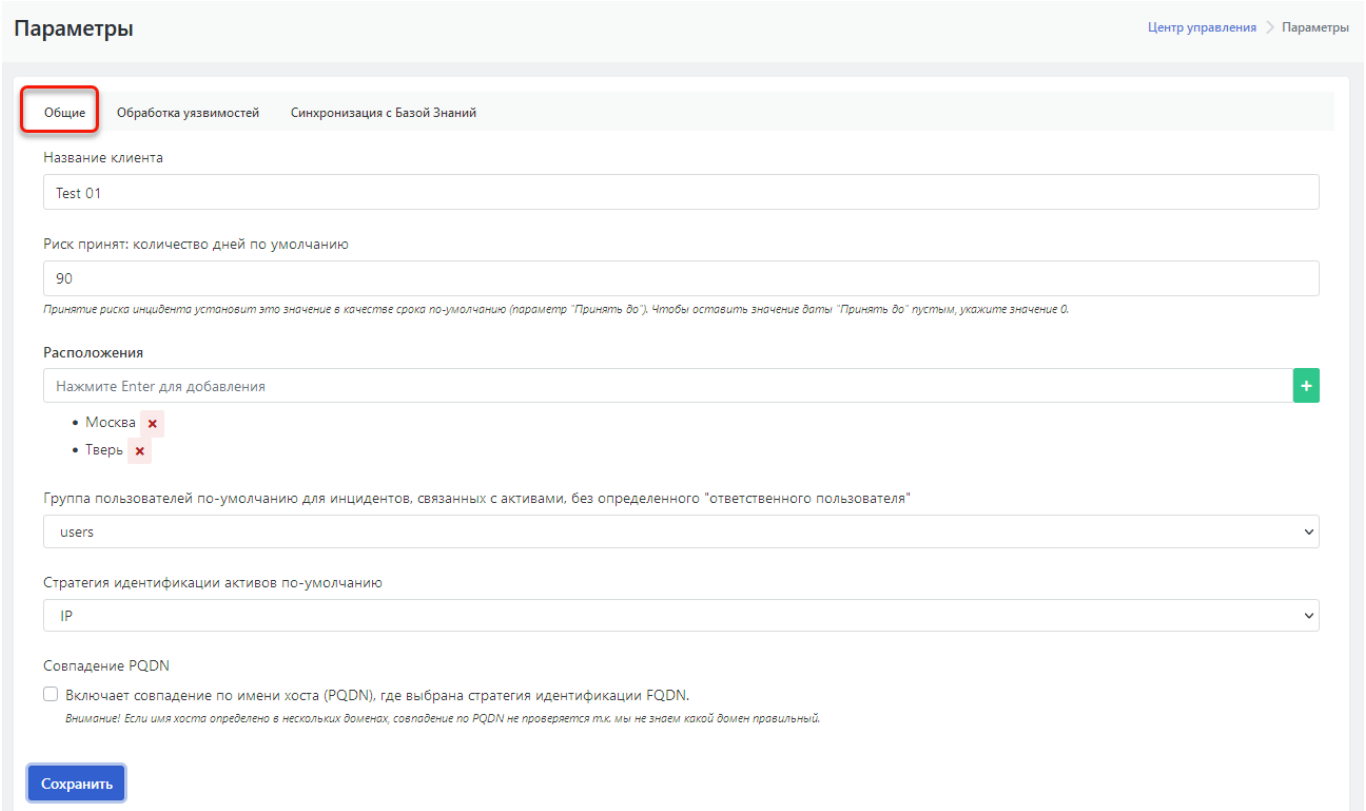



**Рисунок 51 - Подраздел Параметры – Общие**

## 9.2.3 Вкладка "Обработка уязвимостей"

Рабочее поле вкладки "**Обработка уязвимостей**" содержит поля для редактирования параметров автоматического создания и автоматического переоткрытия инцидентов (см. рисунок 52):

- **Автоматически создавать инциденты при импорте результатов сканирования** - включение/ отключение режима автоматического создания инцидентов;
- **Минимальный уровень важности для открытия инцидента** - выбор важности (от 0 до 4) для автоматически созданных инцидентов;

- **Создавать новый инцидент для повторных происшествий, если инцидент закрыт** - выбор правила поведения **Платформы Радар** при повторных происшествиях:
    - **Создавать новый инцидент** - создается новый инцидент;
    - **Переоткрывать инцидент** - существующий инцидент открывается заново;
- **Минимальный уровень риска для повторного открытия инцидентов** - риски ниже указанного уровня не переоткрываются автоматически; параметр задается, только если выбрано переоткрытие инцидента;
- **Статус повторно открытых инцидентов** - переоткрываемые автоматически инциденты будут переводиться в указанный статус; параметр задается, только если выбрано переоткрытие инцидента.

Для сохранения внесенных обновлений нажмите на кнопку "**Сохранить**".

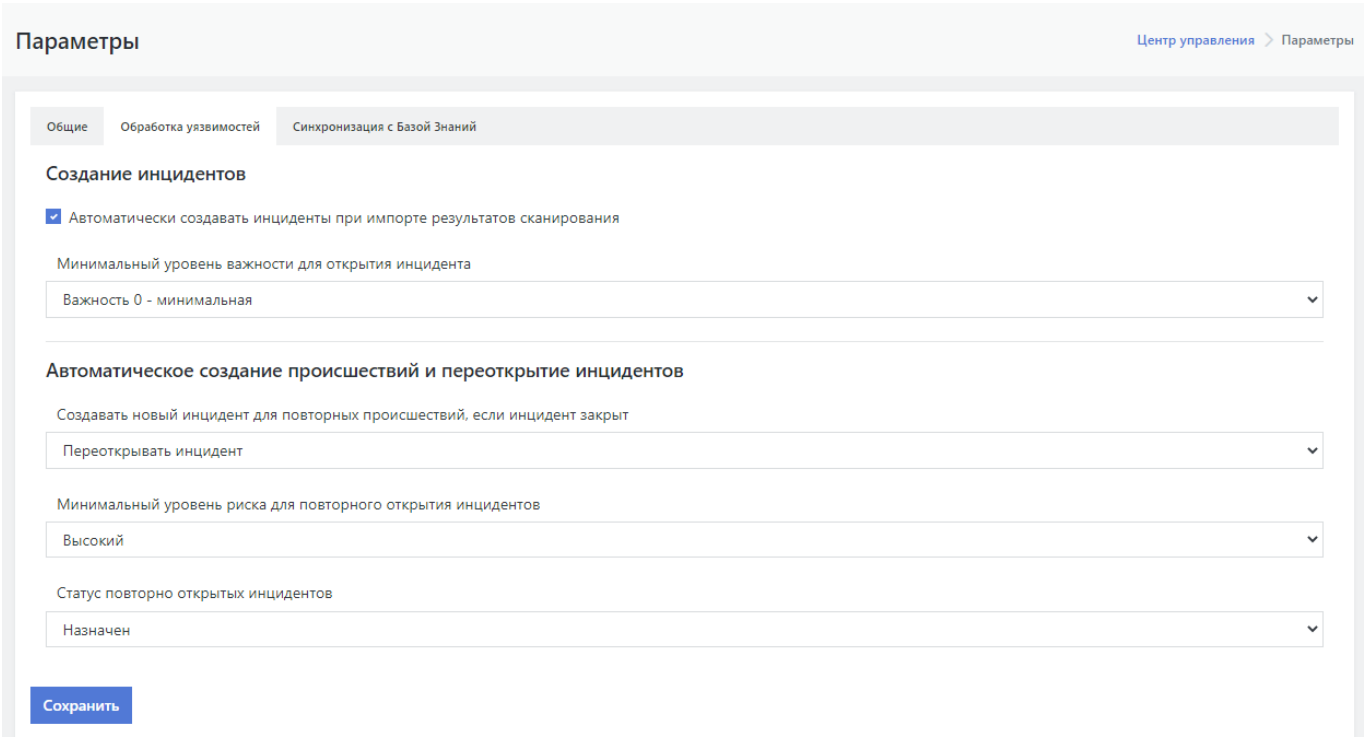



**Рисунок 52 – Подраздел Параметры - Обработка уязвимостей**

## 9.2.4 Вкладка "Синхронизация с Базой Знаний"

Рабочее поле вкладки "**Синхронизация с Базой Знаний**" содержит два функциональных элемента (см. рисунок 53):

- Кнопка "**Синхронизация типов инцидентов**" - предназначена для разового проведения синхронизации типов инцидентов с Базой знаний.
- Кнопка "**Синхронизация коррелятора**" - предназначена для разового проведения синхронизации коррелятора с Базой знаний.

Процесс синхронизации начинается по нажатию на соответствующую кнопку, при этом справа от кнопки появится флажок - ✔ (см. рисунок 53).

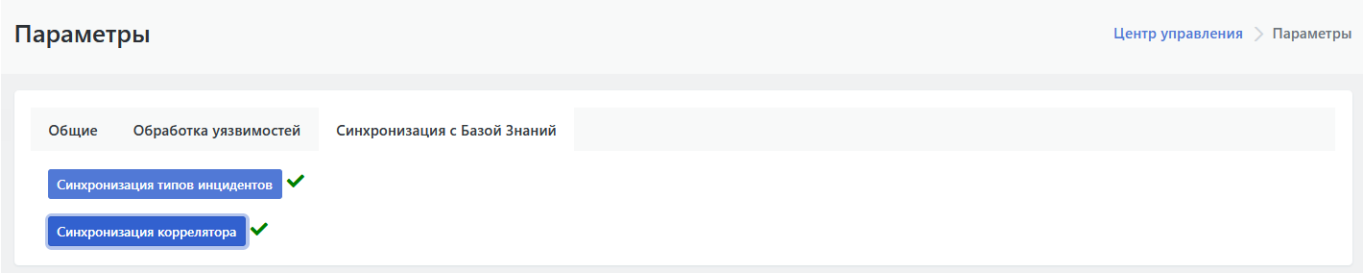



**Рисунок 53 – Подраздел *Параметры - Синхронизация с Базой Знаний***

# 9.3 Подраздел «Черный список ID плагинов»

## 9.3.1 Основные элементы подраздела

Подраздел "**Черный список ID плагинов**" предназначен для создания черного списка ID плагинов сканера Nessus, игнорируемых в процессе работы.

В рабочей области отображаются следующие элементы (см. рисунок 54):

- Табличный список плагинов Nessus, которые необходимо игнорировать в процессе работы ("черный список").
- Набор фильтров для поиска плагина (-ов) в списке – кнопка  .
- Функция добавления нового плагина в список игнорируемых - кнопка "**Создание**".
- Функция редактирования параметров плагина, в том числе удаление плагина из списка – кнопка  .

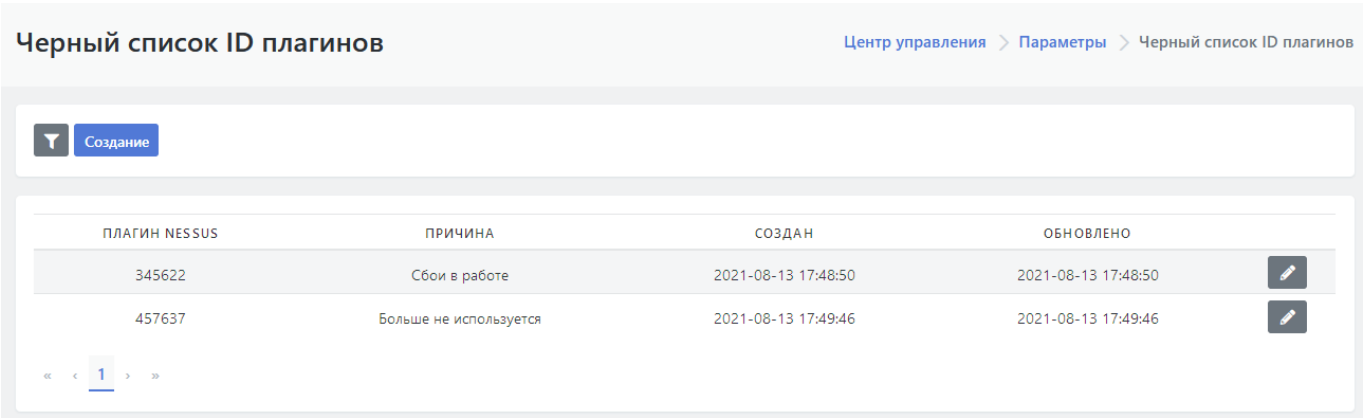



**Рисунок 54 – Рабочая область подраздела "Черный список ID плагинов"**

## 9.3.2 Список плагинов. Параметры списка

Текущий список игнорируемых плагинов Nessus представлен в виде табличного списка со следующими основными параметрами:

- Поле "**Плагин Nessus**" - ID плагина Nessus;
- Поле "**Причина**" - причина, по которой данный плагин был занесен в черный список;
- Поле "**Создан**" - дата и время занесения плагина в черный список;
- Поле "**Обновлено**" - дата и время обновления нахождения плагина в черном списке;

- Кнопка ( ) - функция редактирования параметров плагина, а также удаления плагина из списка.

### 9.3.3 Настраиваемые фильтры списка плагинов

При нажатии на кнопку открывается область фильтров для списка плагинов, которая включает в себя фильтр с полем для свободного текстового ввода.

Поиск по введенной текстовой строке осуществляется по полям "**Плагин Nessus**" и "**Причина**".

### 9.3.4 Включение нового плагина в список, удаление плагина из списка

Для включения в черный список нового плагина необходимо (см. рисунок 55):

1. Нажать кнопку "**Создать**".
2. В открывшейся форме ввести:
    - ID плагина сканера Nessus, который необходимо игнорировать в процессе работы в дальнейшем;
    - причину, по которой плагин занесен в черный список.
3. Для сохранения введённых данных нажать на кнопку "**Сохранить**".

Откроется обновленный черный список плагинов.

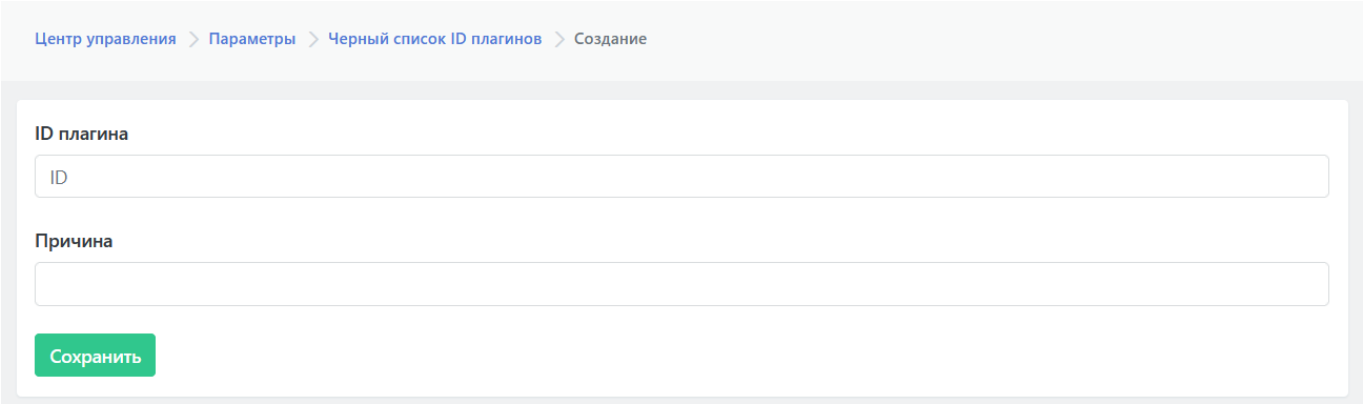



**Рисунок 55 – Включение нового плагина в "Черный список ID плагинов"**

### 9.3.5 Редактирование, удаление плагина из списка

Для редактирования параметров плагина или исключения плагина из черного списка необходимо:

1. Нажать кнопку редактирования в строке интересующего плагина - .
2. В открывшейся форме с параметрам выбранного плагина провести необходимые изменения параметров (см. рисунок 56).
3. Для сохранения изменений нажать на кнопку "**Сохранить**". Для удаления плагина из черного списка нажать на кнопку "**Удалить**".

Откроется обновленный черный список плагинов.

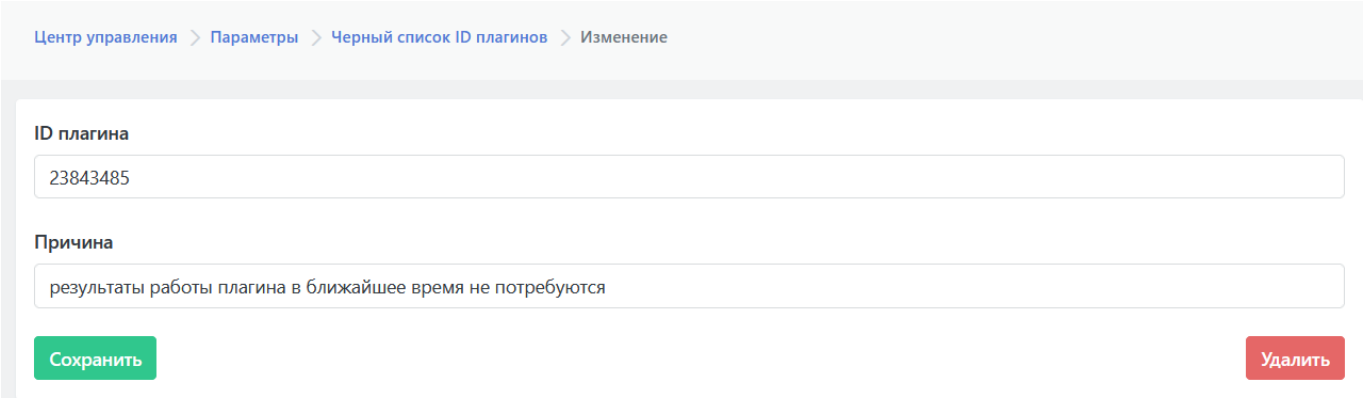



**Рисунок 56 – Форма редактирования параметров плагина из черного списка**

# 9.4 Подраздел "Оповещения по задержкам в обработке"

## 9.4.1 Основные элементы подраздела

В системе предусмотрена возможность отсылки оповещений при наступлении различных условий, связанных с разбором инцидентов.

Подраздел "**Оповещения по задержкам в обработке**" предназначен для настройки автоматических оповещений по задержкам в обработке инцидентов, формируемых **Платформой Радар**.

Рабочее поле подраздела "Оповещения по задержкам в обработке" состоит из трех блоков:

1. Блок настроек временных отсечек для оповещений;
2. Блок настройки режимов отправки оповещений;
3. Блок настройки текстов для оповещений.

## 9.4.2 Настройка временных отсечек для оповещений

В **Платформе Радар** возможно настроить 3 контрольных отсечки по времени разбора инцидента (см. рисунок 57):

- **Нормально** – время, в пределах которого разбор инцидентов считается штатным (в днях);
- **Небольшая задержка** – время, в пределах которого разбор считается выполненным с небольшой задержкой (в днях);
- **Задержка** – время, в пределах которого разбор инцидентов считается выполненным с задержкой (в днях);

При превышении последнего порога указанного в поле "**Задержка**", время разбора инцидентов считается недопустимым.

Времена отсечки конфигурируются отдельно для каждого уровня риска инцидентов:

- высокий риск;
- низкий риск;
- средний риск;

- риск отсутствует.

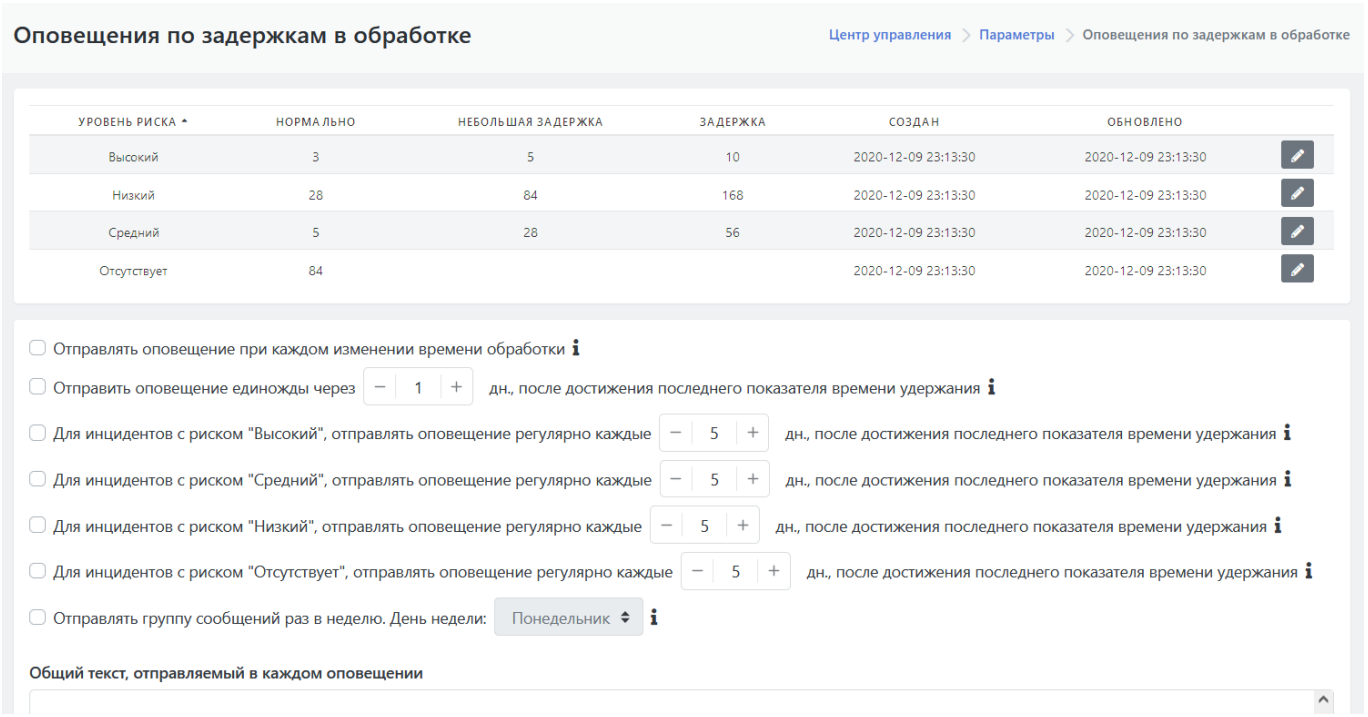



**Рисунок 57 – Подраздел "Оповещения по задержкам в обработке"**

Для обновления времени контрольных отсечек необходимо:

1. Нажать на кнопку  в строке интересующего уровня риска;
2. В открывшейся форме изменить значения временных отсечек (см. рисунок 58);
3. Нажать на кнопку "**Сохранить**".

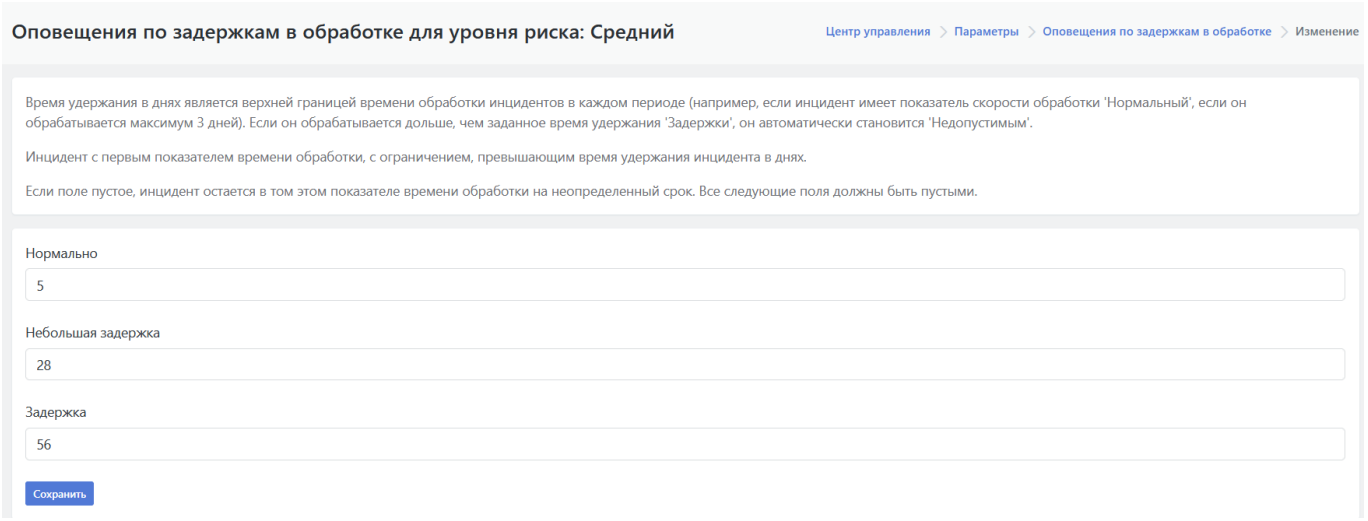



**Рисунок 58 – Редактирование времени контрольных отсечек для среднего уровня риска**

## 9.4.3 Настройка режима отправки оповещений

В **Платформе Радар** возможно настроить следующие режимы отправки оповещений (см. рисунок 59):

- **Отправлять оповещения при каждом изменении времени обработки** - при активации опции оповещение будет отправляться при прохождении каждой временной отсечки, указанной для разбора инцидента.
- **Отправлять оповещение единожды через <...> дн., после достижения последнего показателя времени удержания** - при активации опции оповещение будет отправляться после прохождения последней сконфигурированной временной отсечки.
- **Для инцидентов с риском "Высокий" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания** - при активации опции оповещение для инцидентов с высоким риском будет отправляться после прохождения последней сконфигурированной временной отсечки.
- **Для инцидентов с риском "Средний" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания** - при активации опции оповещение для инцидентов со средним риском будет отправляться после прохождения последней сконфигурированной временной отсечки.
- **Для инцидентов с риском "Низкий" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания** - при активации опции оповещение для инцидентов с низким риском будет отправляться после прохождения последней сконфигурированной временной отсечки.
- **Для инцидентов с риском "Отсутствует" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания** - при активации опции оповещение для инцидентов с отсутствующим риском будет отправляться после прохождения последней сконфигурированной временной отсечки.
- **Отправлять группу сообщений раз в неделю. День недели <...>** - при активации опции все накопившиеся оповещения будут отправляться единожды в указанный день.

Для сохранения настроек режима отправки оповещений нажмите на кнопку **"Сохранить"**, расположенную внизу страницы под всеми блоками настроек.

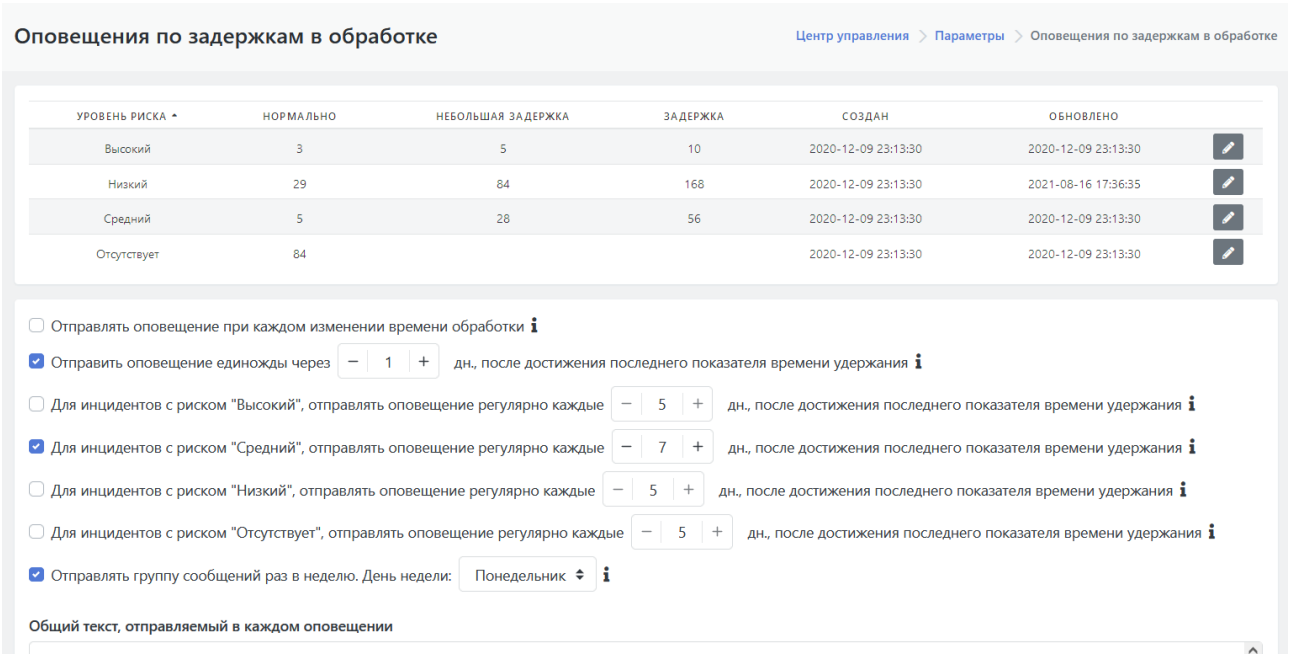



**Рисунок 59 – Настройка режимов отправки оповещений**

### 9.4.4 Настройка текстов для оповещений

Для оповещений по задержкам в обработке можно настроить следующий текст (см. рисунок 60):

- **Общий текст, отправляемый в каждом оповещении**;
- **Текст сообщения об изменении времени удержания инцидента от "Задержки" до "Недопустимого"** ;
- **Текст сообщения об изменении времени удержания инцидента от "Небольшой задержки" до "Задержки"** ;
- **Текст сообщения об изменении времени удержания инцидента от "Нормального" до "Небольшой задержки"**.

Для сохранения настроек текста оповещений нажмите на кнопку "**Сохранить**", расположенную внизу страницы под всеми блоками настроек (см. рисунок 60).

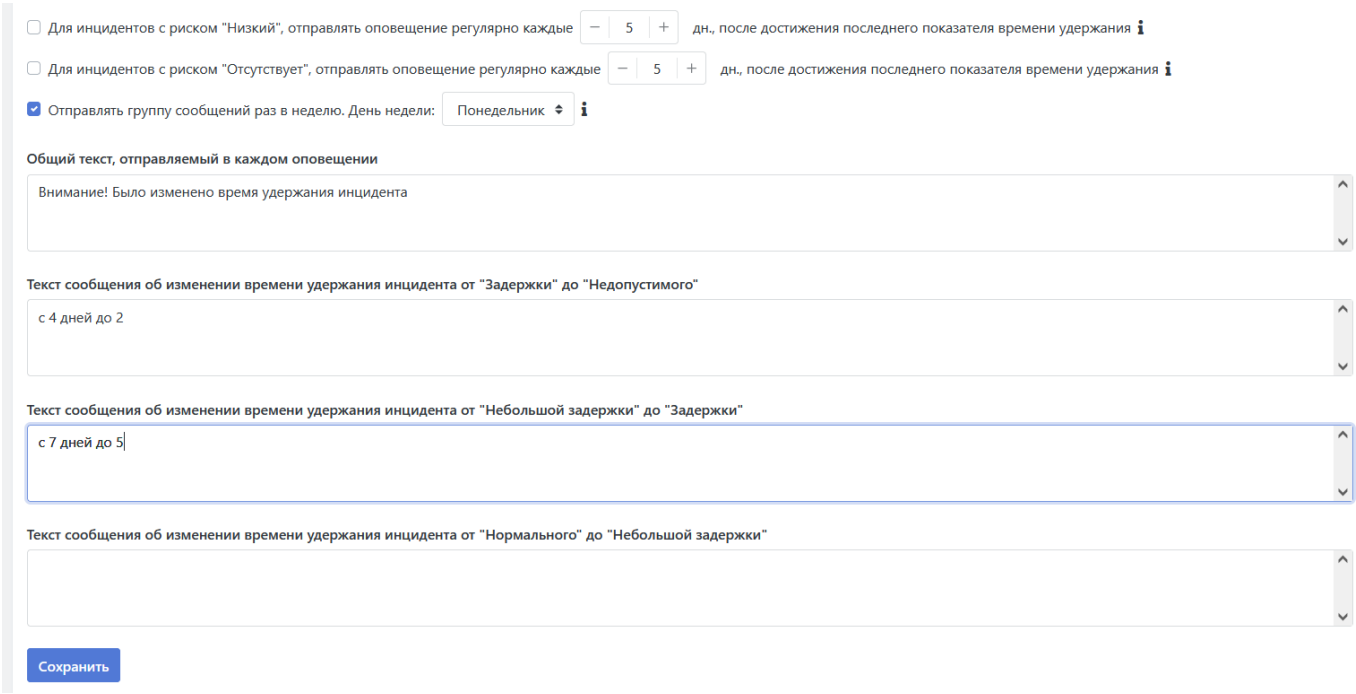



**Рисунок 60 – Настройка текстов оповещений**

# 10. Сообщения

Сообщения -- механизм обмена информацией между пользователями системы, аналогично электронной почте.

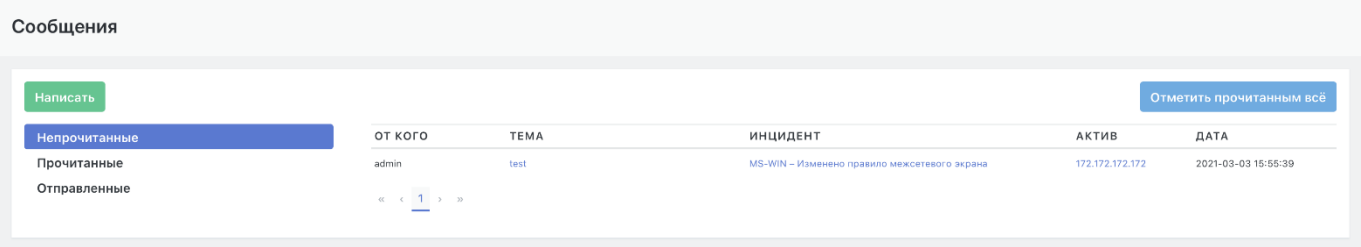



**Рисунок 61 – Рабочая область раздела «Сообщения»**

В рабочей области отображаются следующие виды сообщений (см. рисунок 61):

- Непрочитанные;
- Прочитанные;
- Отправленные;

Список сообщений, содержит следующие поля:

- От кого;
- Тема;
- Тип инцидента и Инцидент;
- Актив;
- Дата

Для создания нового сообщения необходимо нажмите кнопку "**Написать**".

В появившемся окне "**Новое сообщение**" заполните поля "**Получатель**" и "**Заголовок**", введите новое сообщение и нажмите кнопку "**Отправить**" (см. рисунок 62).

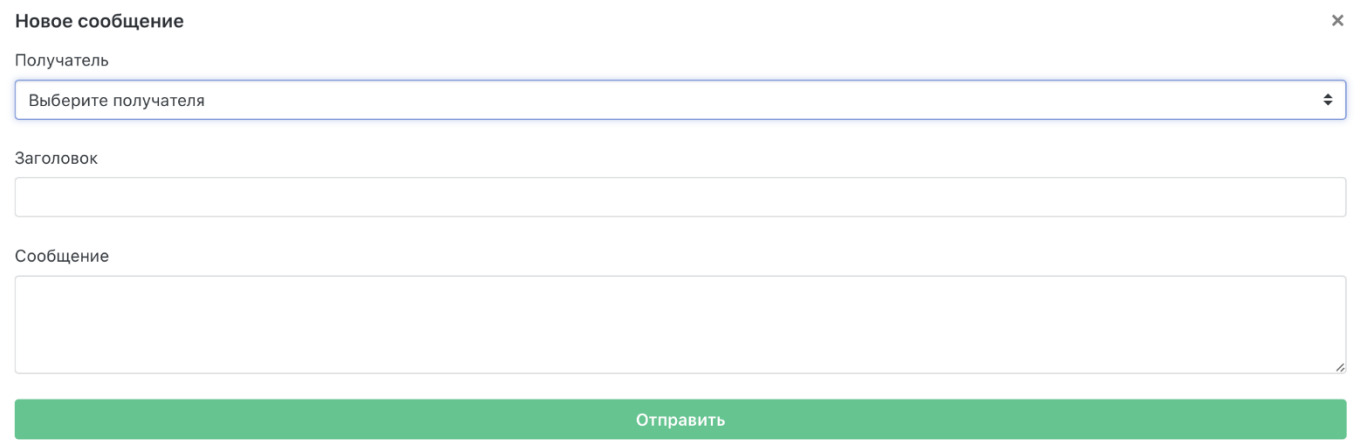



**Рисунок 62 – Окно «Новое сообщение»**

# 11. Отчеты

## 11.1 Основные элементы раздела

Раздел "**Отчеты**" предназначен для создания и управления отчетами типа "дашборд".

Раздел состоит из следующих элементов (см. рисунок 63):

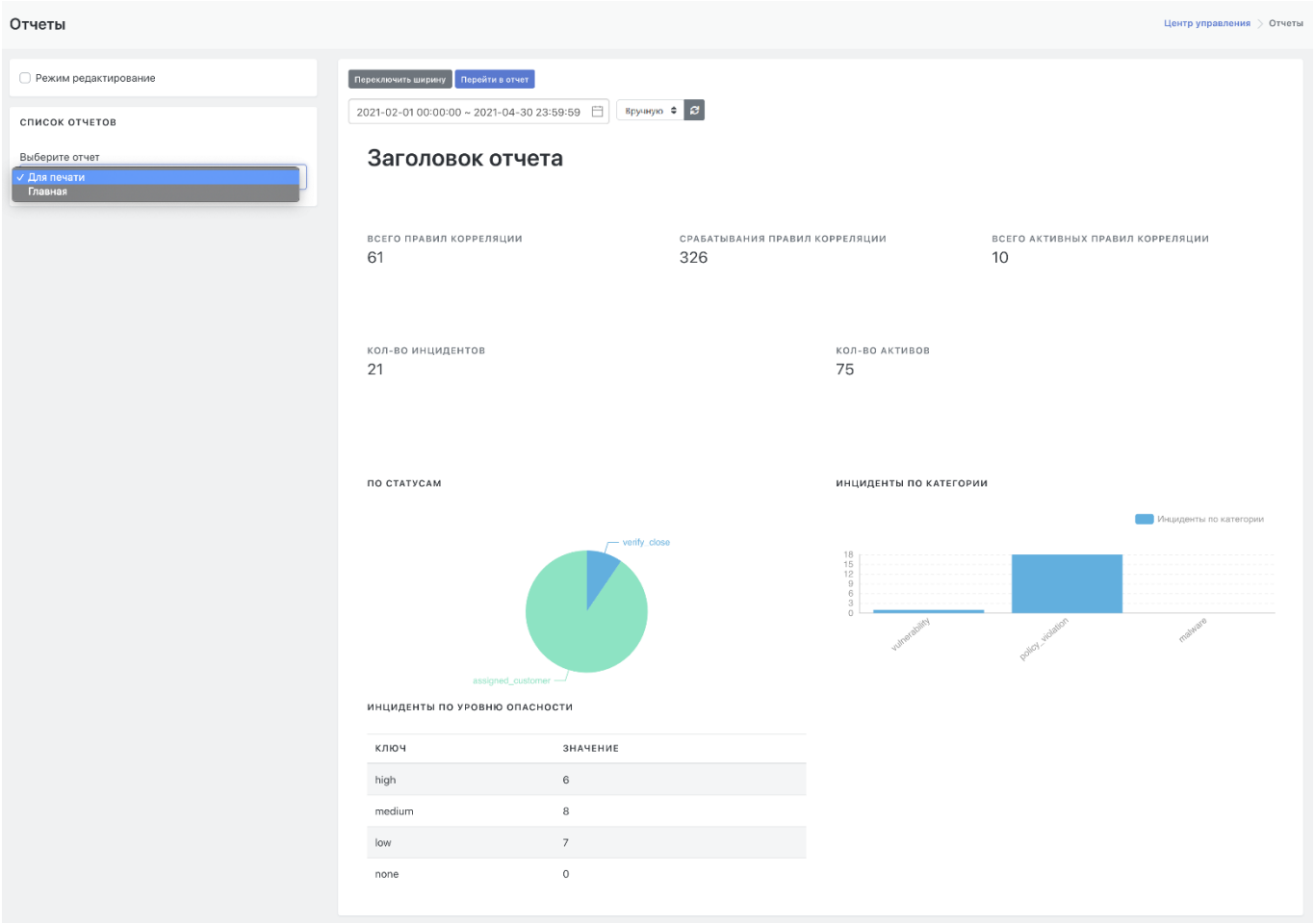



**Рисунок 63 – Рабочая область раздела "Отчеты"**

- Рабочая область раздела: либо пустая, либо отображает отчет, заданный "по умолчанию";
- Над рабочей областью располагаются функции настройки отображения отчета:
  - поле выбора нового временного интервала отчета;
  - функция подстройки ширины отчета под формат А4 - кнопка "**Переключить ширину**";
  - функция предварительного просмотра печатной версии отчета - кнопка "**Перейти в отчет**";
  - функция настройки временного периода обновления данных - раскрывающийся список "**Вручную**" (где "Вручную" - значение по умолчанию);

- кнопка для запуска обновления данных -  .

- Слева расположено меню раздела, которое содержит:
  - текущий список отчетов - раскрывающийся список "**Выберите отчет**";
  - функцию перевода в режим редактирования - флаговое поле "**Режим редактирования**".

## 11.2 Основные элементы раздела в режиме редактирования

При наличии у пользователя необходимых прав ему доступны функции управления отчетами в режиме редактирования.

Если установить флаг в поле "**Режим редактирования",** то на экране появятся новые дополнительные функции (см. рисунок 64):

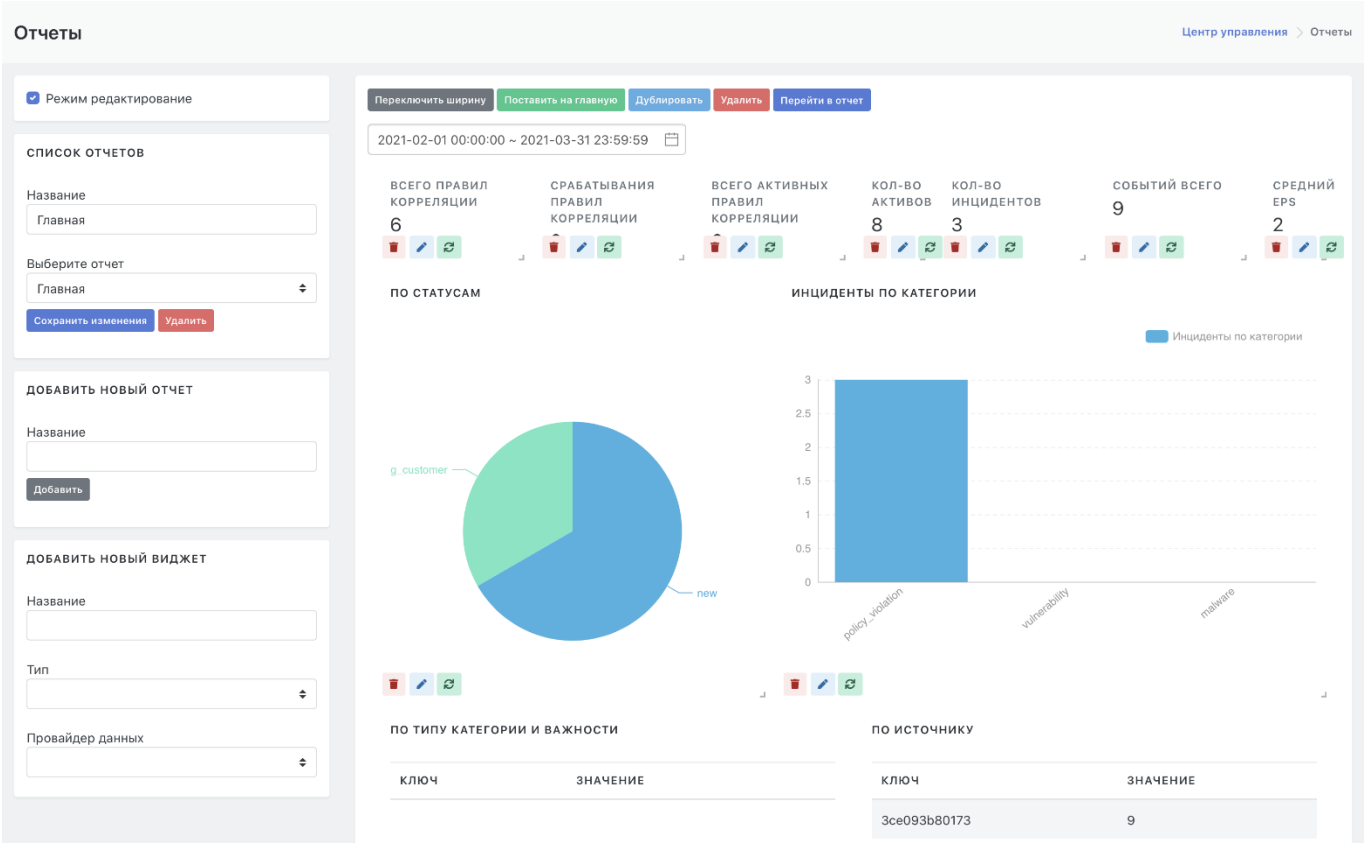



**Рисунок 64 – Рабочая область раздела "Отчеты" в режиме редактирования**

- Рабочая область раздела: для виджетов отчета будут установлены функции управления виджетами:
  - удаление виджета из отчета – кнопка  ;
  - редактирование виджета – кнопка  ;
  - обновление виджета из отчета – кнопка  .
- Над рабочей областью добавятся следующие функции работы с отчетом:

    - функция установки отчета "по умолчанию" - кнопка "**Поставить на главную**":
    - функция дублирования отчета - кнопка "**Дублировать**";
    - Функция удаления отчета - кнопка "**Удалить**".
- В меню раздела (расположенном слева) добавятся следующие функции управления отчетами:
    - создание нового отчета - блок "**Добавить новый отчет**";
    - удаление существующего отчета - кнопка "**Удалить**";
    - сохранение внесенных изменений в существующий отчет - кнопка "**Сохранить изменения**";
    - добавление нового виджета в отчет - блок "**Добавить новый виджет**".

## 11.3 Управление отчетами

С помощью функционала раздела с отчетами можно выполнить следующие действия:

- Посмотреть данные в отчете за указанный диапазон времени;
- Распечатать отчет;
- Установить для отчета статус "по умолчанию";
- Создать новый по составу данных отчет, отвечающий текущим задачам;
- Изменить список виджетов в существующем отчете;
- Изменить расположения и размер виджетов в существующем или новом отчете;
- Скопировать существующий отчет для безопасного внесения изменений.

Подробное описание действий с отчетами приведено в разделе «Работа с отчетами».

## 11.4 Состав виджетов отчета

Состав блоков информации в отчете (виджетов) зависит от назначения отчета.

Информация в отчетах может предоставляться в следующих видах:

- численное значение;
- круговая диаграмма;
- столбчатая диаграмма;
- таблица;
- заголовок.

# 12. Работа с инцидентами

## 12.1 Общие данные об инцидентах

**Платформа Радар** предназначена для автоматизации деятельности специалистов SOC. Обработка инцидентов ИБ является одним из ключевых процессов деятельности центра мониторинга.

**Инцидент информационной безопасности (инцидент ИБ)** - появление одного или нескольких нежелательных/неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операции и создания угрозы ИБ [ГОСТ Р ИСО/МЭК ТО 18044-2007].

**Платформа Радар** обрабатывает инциденты следующих категорий:

- Уязвимость (при интеграции со сканером уязвимостей) - дефект в исходном коде программного обеспечения или его конфигурации;
- Нарушение политики - действия, выявленные системой, идущие в разрез с политикой безопасности;
- Сетевая аномалия - сетевая активность, имеющая отклонения от нормы.

В рамках **Платформы Радар** инцидент всегда имеет определенный тип инцидента и привязку к активу, на котором он выявлен.

## 12.2 Выявление инцидентов (автоматическое создание инцидентов)

### 12.2.1 Механизмы выявления инцидентов

В рамках **Платформы Радар** реализованы следующие механизмы выявления инцидентов:

- Правила корреляции -- подробное описание в разделе «Работа с правилами корреляции»;
- Данные об уязвимостях -- подробное описание в разделе «Работа с сетевым сканером и инвентаризацией»;
- Создание инцидента вручную;
- Контроль списка программного обеспечения -- подробное описание в «Руководстве администратора» → «Настройка контроля установленного программного обеспечения»;

### 12.2.2 Присвоение статуса новым инцидентам

Новые инциденты могут быть созданы в следующих статусах:

- **Новый** - инциденты видны во всех интерфейсах системы, используется для создания инцидентов в рамках штатной работы системы;
- **ПГ Новый** - инцидент в данном статусе виден только в интерфейсе администратора, используется для создания инцидентов, требующих дополнительную проверку со стороны высококвалифицированного аналитика.

### 12.2.3 Происшествия

В **Платформе Радар** реализован механизм создания происшествий в рамках существующего инцидента без порождения нового, что значительно повышает эффективность работы специалистов по расследованию инцидентов.

Инцидент, у которого следующие атрибуты:

- тип инцидента;
- IP-адрес актива, на котором он обнаружен;
- TCP-порт (опционально);
- идентификатор, передаваемый из корреляции (опционально),

совпадают с соответствующими атрибутами существующего инцидента, регистрируется не как отдельный инцидент, а как происшествие в рамках существующего инцидента.

В случае, если происшествие добавляется в инцидент в статусе «Закрыт», то, в зависимости от настройки переоткрытия инцидента, инцидент будет переоткрыт или будет создан новый инцидент.

## 12.3 Создание инцидента вручную

### 12.3.1 Общие положения

Создание инцидента вручную может потребоваться в следующих случаях:

- инцидент выявлен аналитиком по результатам анализа данных актива, событий или иных источников информации;
- инцидент выявлен вне **Платформы Радар** и передан аналитику по внешнему каналу (электронная почта, телефон).

### 12.3.2 Доступ к функции создания нового инцидента вручную

Функция создания вручную нового инцидента доступна:

- на экране со списком инцидентов: ***Инциденты - Инциденты***;
- на карточке типа инцидента: ***Инциденты - Типы инцидентов - /щелкнуть по заголовку интересующего типа в списке/***.

### 12.3.3 Создание нового инцидента со страницы списка инцидентов

Для создания инцидента со страницы со списком инцидентов необходимо:

1. Перейти в раздел ***Инциденты - Инциденты***;
2. Нажать на кнопку "**Создать инцидент**";
3. В открывшемся окне указать тип создаваемого инцидента, выбрав его из раскрывающегося списка "**Тип инцидента**" (см. рисунок 65);

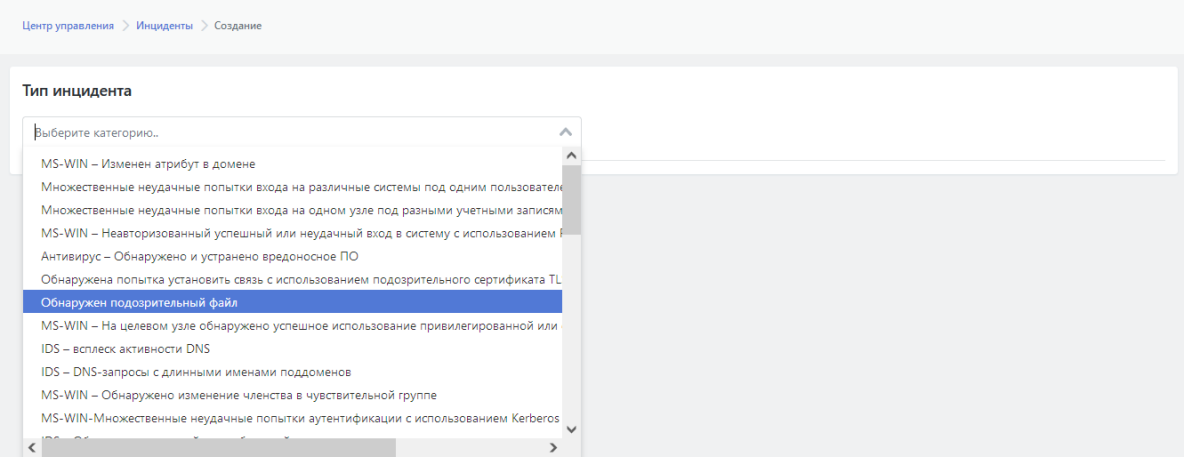



**Рисунок 65 – Выбор типа для создаваемого вручную инцидента**

4. После выбора типа открывается форма со стандартными параметрами указанного типа инцидента (см. рисунок 66). Отредактировать стандартные значения полей, если это необходимо. Полное описание параметров типа инцидента приведено в разделе «Просмотр детализации типа инцидента»;

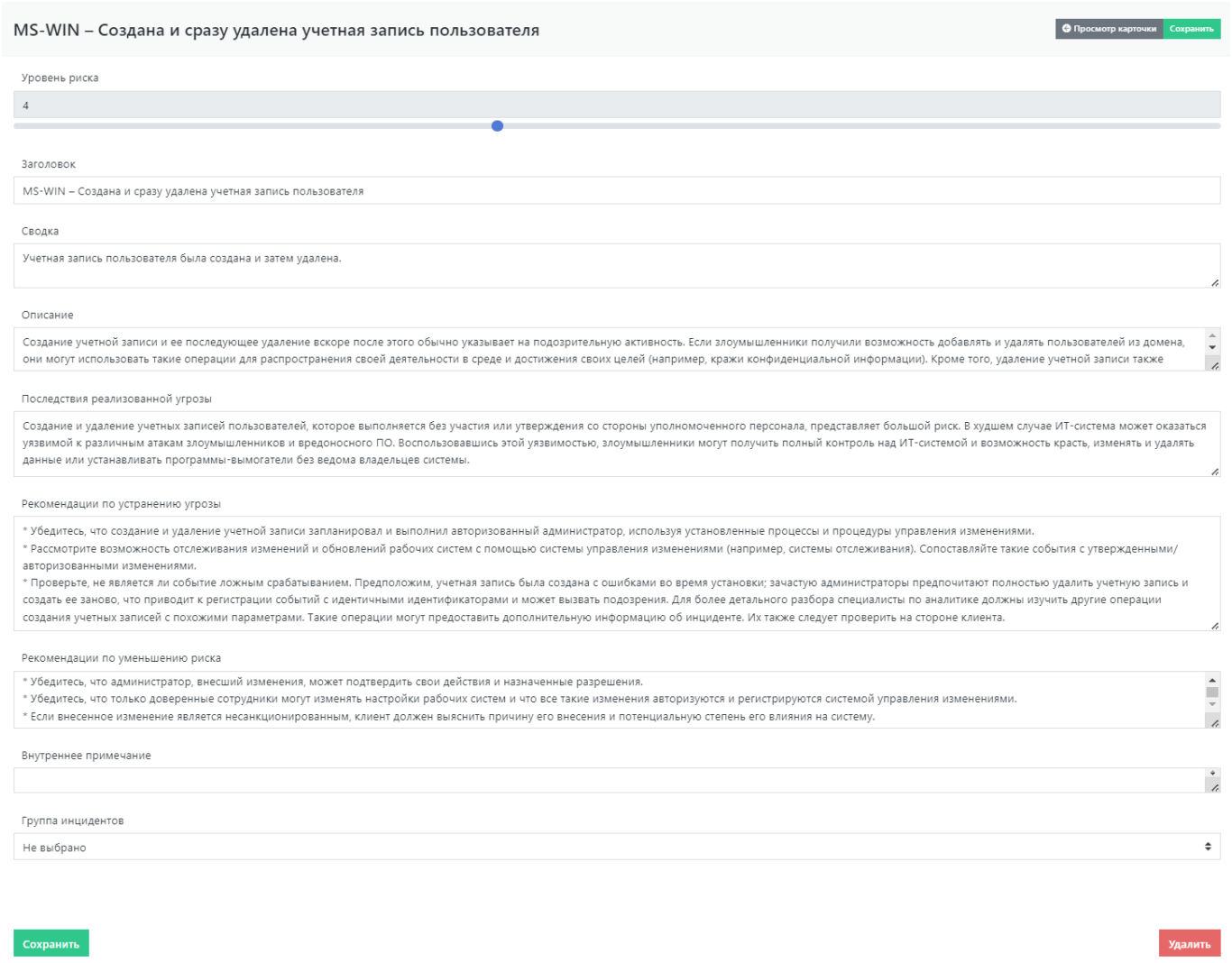



**Рисунок 66 - Настройка параметров типа при создании нового инцидента**

5. В области "**Актив**" указать IP-адрес актива на котором произошел инцидент и нажать кнопку "**Поиск активов**". Произойдет привязка создаваемого инцидента к активу. Если

указанный актив уже существует, то появится область "**Добавление к существующему активу**" и кнопка "**Сохранить**" (см. рисунок 67). При отсутствии регистрации актива в **Платформе Радар** будет предложено создать актив. Алгоритм создания нового актива в **Платформе Радар** приведен ниже;

6. Для завершения создания инцидента в **Платформе Радар** нажать на кнопку "**Сохранить**".

Произойдет возврат к обновленному списку инцидентов на странице ***Инциденты - Инциденты***.

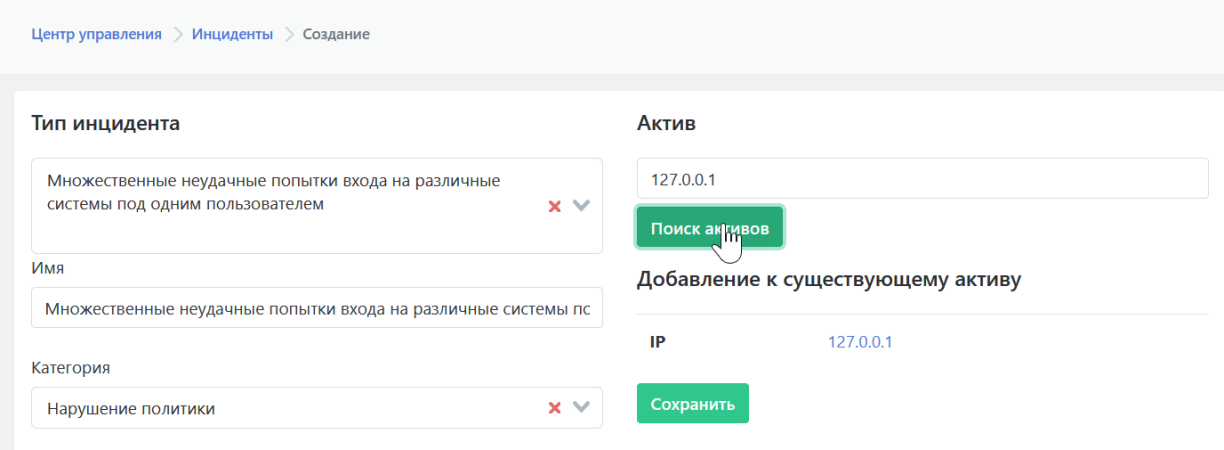



**Рисунок 67 – Привязка нового инцидента к активу и сохранение созданного инцидента**

При отсутствии в **Платформе Радар** данных об активе, будет предложено создать новый актив (см. рисунок 68).

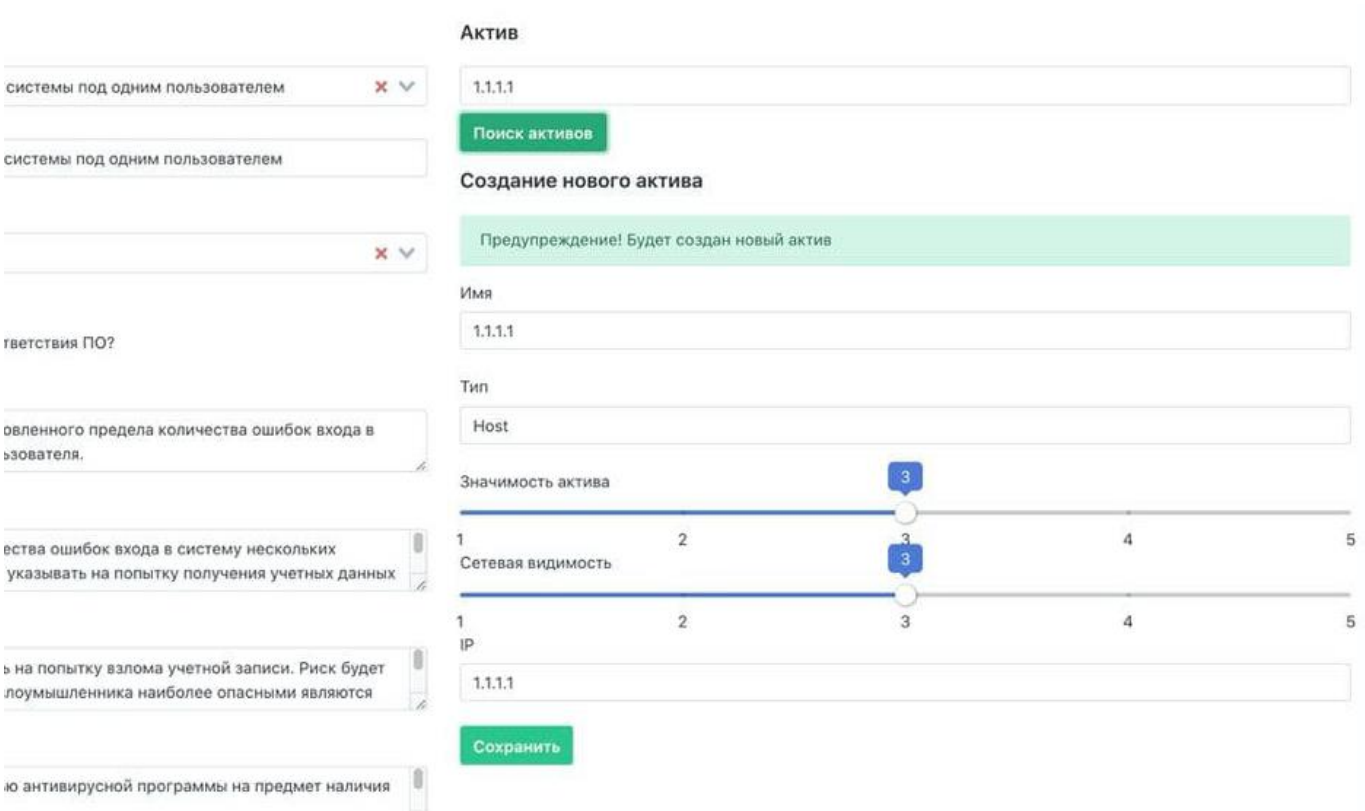



**Рисунок 68 - Область с формой создания актива (при создании инцидента)**

На экране откроется область "**Создание нового актива**". Для нового актива необходимо указать:

- Поле "**Имя**" - указать имя актива в **Платформе Радар**;

- Поле "**Тип**" - тип или роль оборудования, к которому принадлежит актив;
- Функция "**Значимость актива**" - установка числового значения значимости актива (1-5);
- Функция "**Сетевая видимость**" - установка числового значения сетевой видимости актива (1-5);
- Поле "**IP**" - ввести IP-адрес актива.

Более подробное описание создания актива приведено в разделе «Работа с активами».

### 12.3.4 Создание нового инцидента с карточки типа инцидента

Для создания инцидента с карточки типа инцидента необходимо:

1. Перейти в раздел ***Инциденты - Типы инцидентов - /щелкнуть по заголовку интересующего типа в списке/***.
2. В открывшейся карточке типа в блоке со списком инцидентов данного типа нажать на кнопку "**Создать инцидент**".

На экране сразу откроется форма со стандартными параметрами того типа инцидента, с карточки которого была активирована функция создания инцидента. Дальнейшие шаги по созданию инцидента аналогичны шагам создания инцидента со страницы списка инцидента - см. предыдущий раздел.

### 12.3.5 Привязка дополнительных событий вручную

При необходимости можно привязать к существующему инциденту дополнительные события, изначально не относящиеся к данному инциденту. Привязка осуществляется вручную. Цель привязки дополнительных событий к инциденту - обеспечить более точный анализ инцидента.

Для привязки события к инциденту необходимо выполнить следующие действия:

1. В веб-интерфейсе **Платформы Радар** перейти в раздел ***Просмотр событий***;
2. Открыть интересующее событие, щелкнув по значку ▶ (см. рисунок 69).


**Рисунок 69 – Открытие "сырых" данных события**

3. Нажать кнопку "**Найти инцидент**" (см. рисунок 70);

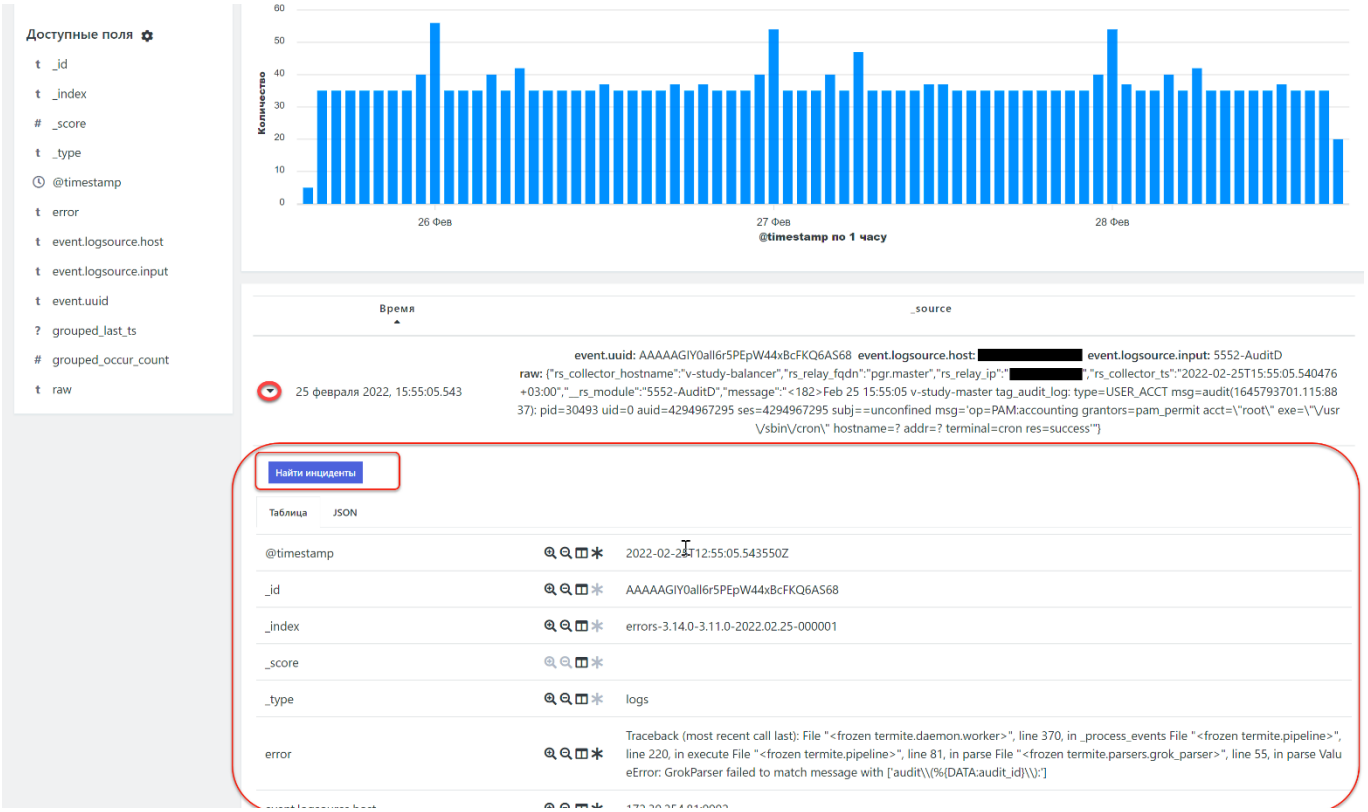



**Рисунок 70 - Функция поиска инцидента, которому может принадлежать данное событие**

4. Если для данного события связанный с ним инцидент не будет найден, то **Платформа Радар** предложит (см. рисунок 71) либо вручную создать инцидент на основе данного события (кнопка "**Создать инцидент**"), либо добавить событие к существующему инциденту (кнопка "**Добавить к существующему**");

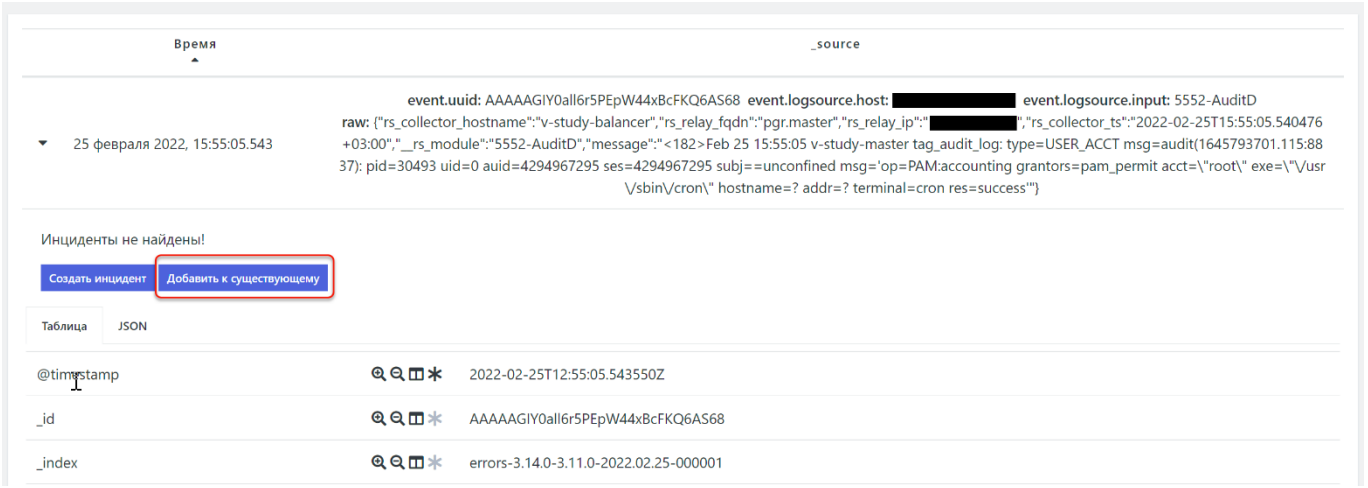



**Рисунок 71 – Результат работы функции "Найти инциденты"**

5. Нажать кнопку "**Добавить к существующему**";
6. В открывшемся окне (см. рисунок 72):
   - выбрать подходящее правило корреляции для данного события;
   - найти инцидент, к которому необходимо привязать данное событие, по ссылке или ID или выбрать нужный инцидент из предложенного списка.

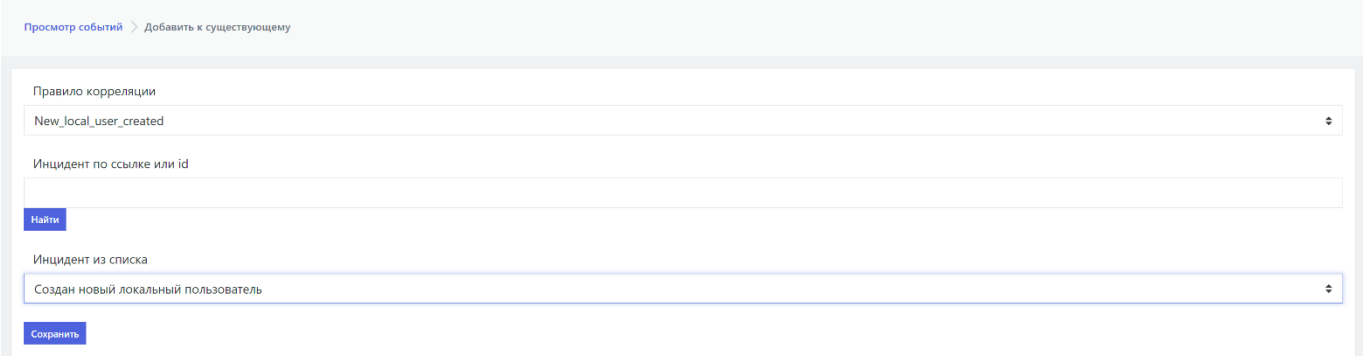



**Рисунок 72 – Привязка события к инциденту**

7. Для привязки события к инциденту нажать кнопку "**Сохранить**".

Для того, чтобы проверить, что привязка события к инциденту произошла, нужно повторить шаги 1-3 приведенного выше алгоритма. По нажатию кнопки "**Найти инциденты**" откроется имя инцидента, к которому было привязано вручную событие (см. рисунок 73). По имени инцидента можно перейти на карточку инцидента для просмотра детализации. Описание карточки инцидента приведено в разделе документа «Просмотр карточки инцидента».

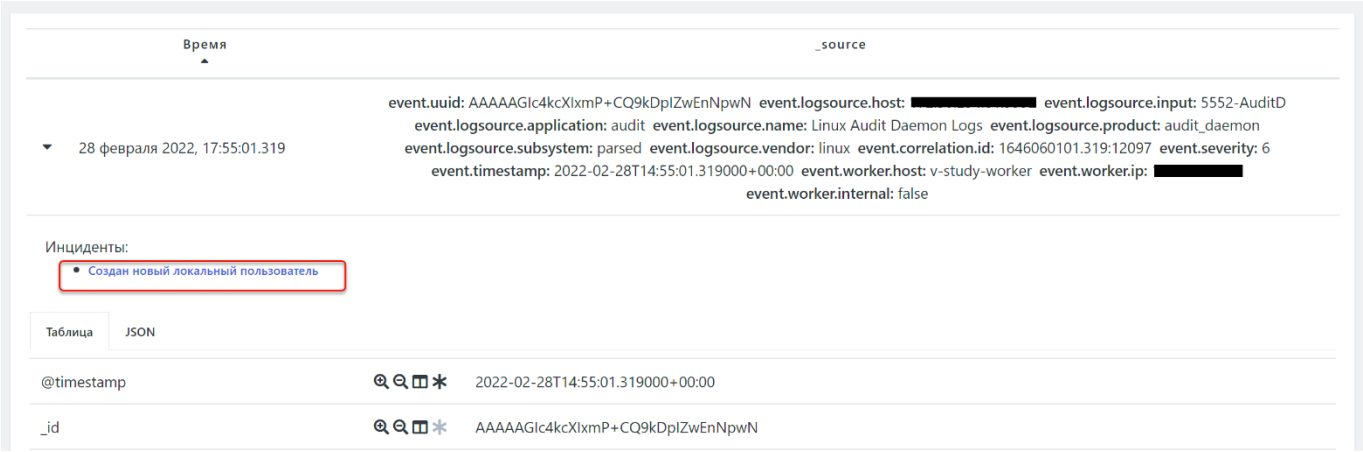



**Рисунок 73 – Просмотр списков инцидентов, к которым привязано событие**

## 12.3.6 Привязка дополнительных полей

К любому инциденту можно добавить дополнительные поля вручную в карточке инцидента. Перечень дополнительных полей определяется в разделе «Подраздел "Дополнительные поля"».

Для добавления дополнительного поля выберите инцидент и перейдите к его редактированию. В блоке "**Дополнительные поля**" (см. рисунок 74) выберите доступные дополнительные поля и задайте их значение.

После добавления дополнительных полей и задания их значений нажмите кнопку "**Сохранить**". Для удаления дополнительного поля из карточки инцидентов нажмите кнопку "**Удалить поле**". Для удаления всех дополнительных полей из карточки инцидентов нажмите кнопку "**Удалить**".

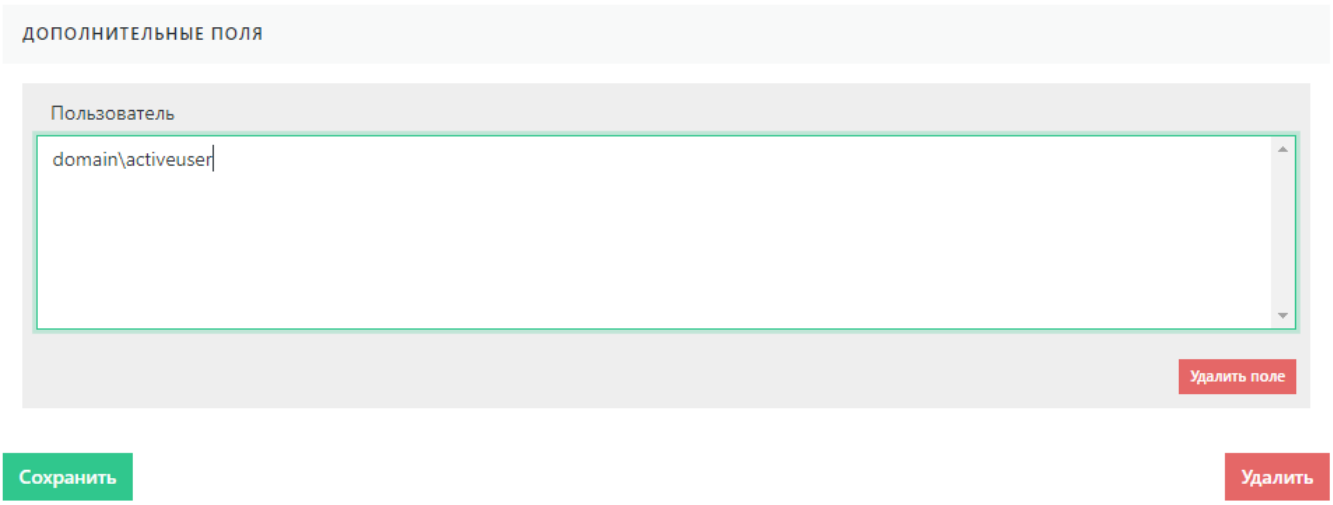



**Рисунок 74 – Добавление дополнительных полей**

# 12.4 Анализ инцидента

## 12.4.1 Просмотр списка инцидентов

Основная цель этапа анализа - оценить степень риска для данного инцидента и необходимость проведения дальнейших действий по расследованию.

Полный табличный список инцидентов расположен в разделе: ***Инциденты - Инциденты*** (см. рисунок 75).

Так же на карточке актива доступен список инцидентов, произошедших на данном активе: ***Активы - Активы - /щелкнуть по названию интересующего актива в списке/***.


**Рисунок 75 – Список инцидентов в разделе *Инциденты - Инциденты***

Гиперссылки в строке инцидента обеспечивают просмотр следующей детальной информации:

- **Тип инцидента** - содержит идентификатор типа произошедшего инцидента. Гиперссылка ведет на карточку типа инцидента с детальной информацией по данному типу. Описание карточки типа инцидента приведено в разделе «Просмотр карточки инцидента».
- **Актив** - содержит название актива, на котором произошел инцидент . Гиперссылка ведет на карточку актива с детальной информацией по данному активу. Описание карточки актива приведено в разделе «Работа с активами».
- **Заголовок** - содержит название инцидента. Гиперссылка ведет на карточку инцидента с детальной информацией по данному инциденту. Описание карточки инцидента приведено в разделе документа «Просмотр карточки инцидента».

- **Пользователь** ( ) - содержит имя пользователя **Платформы Радар**, которому назначен данный инцидент для расследования. Гиперссылка ведет на страницу с краткой информацией по данному пользователю.
- **Группа** ( ) - содержит имя группы пользователей **Платформы Радар**, которой назначен данный инцидент для расследования. Гиперссылка ведет на страницу с краткой информацией о данной группе.
- Кнопка редактирования ( ) - переводит на страницу редактирования параметров инцидента. Описание страницы редактирования приведено в разделе документа «Редактирование параметров инцидента».

## 12.4.2 Просмотр карточки инцидента

### 12.4.2.1 Общее описание карточки инцидента

Для просмотра детализации по интересующему инциденту необходимо:

1. Перейти в раздел ***Инциденты - Инциденты***;
2. В списке инцидентов щелкнуть по названию интересующего инцидента в поле "**Заголовок**".

На экране откроется карточка инцидента, содержащая полный набор данных по инциденту (см. рисунок 76).

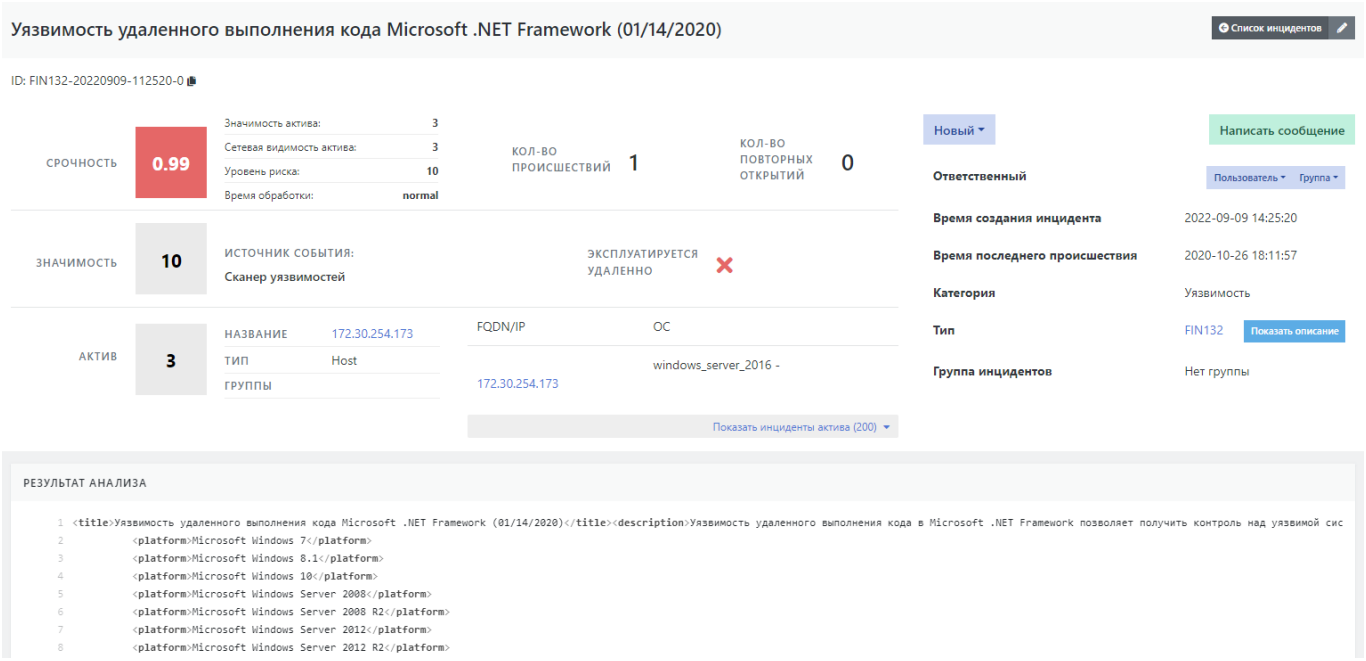



**Рисунок 76 – Карточка инцидента с детальной информацией**

Карточка инцидента состоит из следующих информационных блоков:

- Сводная информация по инциденту - верхняя часть экрана;
- Блок "**Происшествия**" - содержит информацию по происшествиям, зафиксированным в рамках одного инцидента;
- Блок "**История**" - история действий с инцидентом.

### 12.4.2.2 Блок сводной информации по инциденту

Блок сводной информации содержит следующие данные по инциденту:

- **ID** - сквозной идентификатор инцидента;
- **Количество происшествий** - количество происшествий, зафиксированных на текущий момент в рамках инцидента;
- **Количество повторных открытий** - количество повторных открытий инцидента;
- **Источник события** - указывается тип источника инцидента, например "Введен вручную";
- Данные актива на котором произошел инцидент:
    - **Название**- уникальное название актива в **Платформе Радар**. Реализовано в виде гиперссылки, которая ведет на карточку актива. Описание карточки актива приведено в разделе документа «Просмотр карточки инцидента»;
    - **Тип** - тип актива;
    - **Группы** - указываются одна или несколько групп, которым принадлежит данный актива;
    - **FQDN / IP** - IP- адрес или FQDN актива. Реализован в виде гиперссылки, которая ведет на список сетевых интерфейсов актива;
    - **ОС** - операционная система, установленная на активе.
- Текущий статус инцидента - представляет собой функцию смены статуса в виде раскрывающегося список статусов (см. рисунок 77). Список содержит возможные варианты смены текущего статуса и позволяет поменять статус инцидента непосредственно на карточке инцидента;

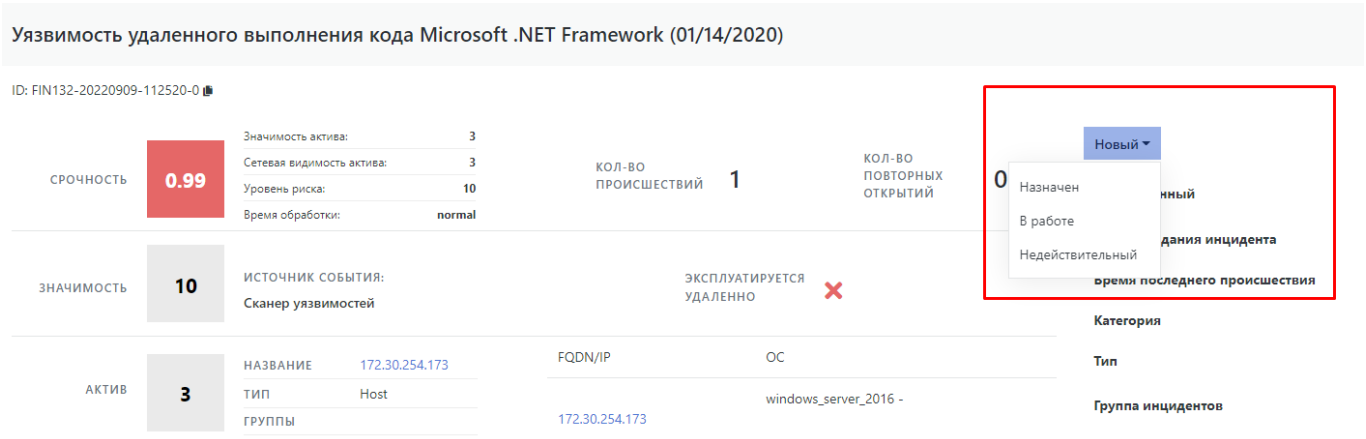



**Рисунок 77 – Функция смены статуса на карточке инцидента**

- **Время происшествия** - время создания инцидента;
- **Ответственный** - представляет собой два раскрывающихся списка: список пользователей и список групп пользователей (см. рисунок 78). По умолчанию указывается текущий назначенный пользователь и/или группа пользователей, которым назначен данный инцидент для расследования. Списки в поле "Ответственный" позволяют переназначить

инцидент другому пользователю или другой группе пользователей непосредственно на карточке инцидента;

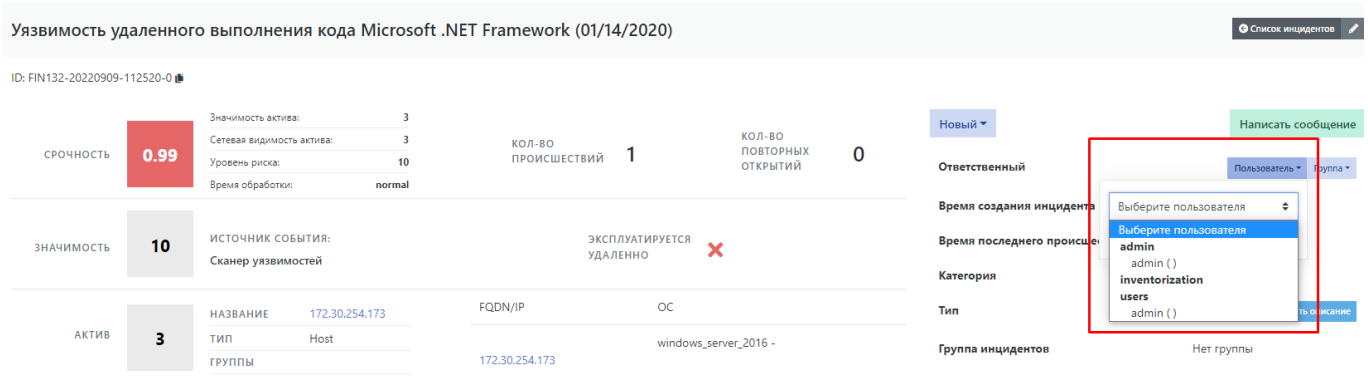



**Рисунок 78 – Функция переназначения инцидента другому ответственному пользователю или группе пользователей**

- **Категория** - категория инцидента. Возможно одно из следующих значений: "Уязвимость", "Нарушение политики" или "Сетевая аномалия";
- **Тип инцидента** - указывается идентификатор типа, к которому относится данный инцидент. Реализовано в виде гиперссылки, которая ведет на карточку типа инцидента. Описание карточки типа инцидента приведено в разделе документа «Просмотр карточки инцидента»;
- В блоке сводной информации присутствует три типа оценок. Подробное описание работы с оценками приведено в разделе «Детализация оценок инцидента».

Помимо перечисленных параметров в блоке сводной информации присутствуют следующие функции:

- **Редактировать** - при нажатии на кнопку открывается страница редактирования параметров инцидента. Подробное описание редактирования приведено в разделе «Редактирование параметров инцидента»;
- **Написать сообщение** - при нажатии на кнопку открывается стандартное окно **Платформы Радар** для создания и отправки сообщения. Подробное описание отправки сообщений с карточки инцидента приведено в разделе документа «Создание и отправка сообщения со ссылкой на инцидент»;
- **Показать описание** - при нажатии на кнопку отрывается информационное окно, содержащее описание инцидента (см. рисунок 79). Описание содержит следующую информацию:
    - **Сводка** - описание действия, вызвавшего инцидент;
    - **Описание угрозы**;
    - **Последствия реализованной угрозы**;
    - **Рекомендации по устранению угрозы**;
    - **Рекомендации по уменьшению риска**.

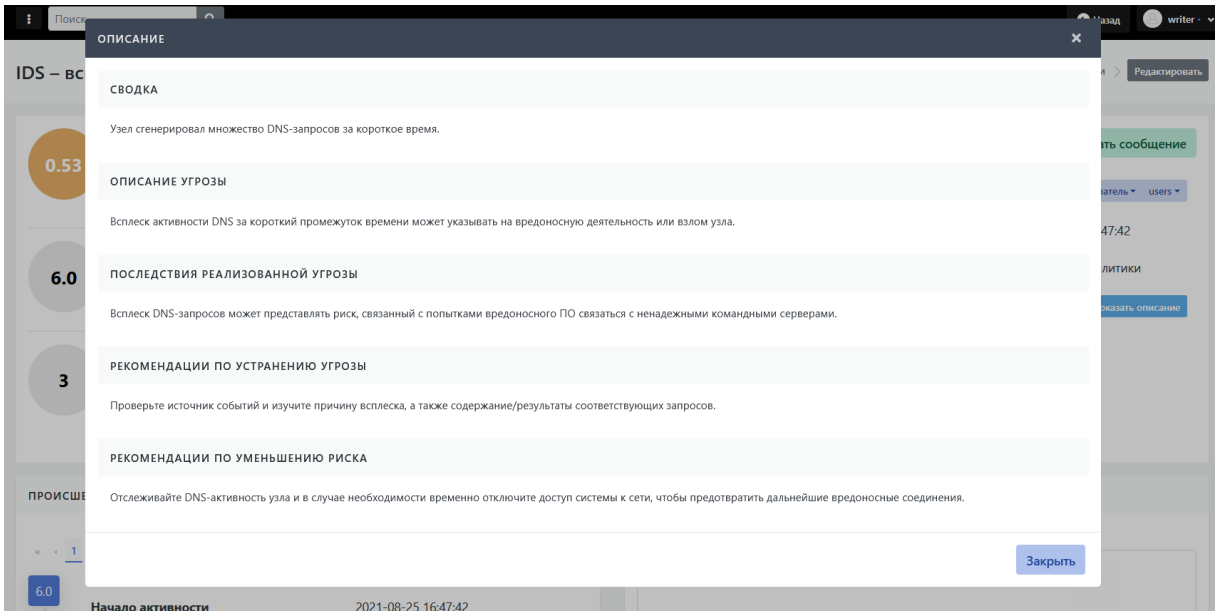



**Рисунок 79 – Описание инцидента**

### 12.4.2.3 Детализация оценок инцидента

На карточке инцидента указаны три типа оценок:

- Оценка срочности;
- Уровень риска (уровень значимости инцидента) инцидента;
- Уровень значимости актива.

**Оценка срочности** - параметр, определяющий степень срочности необходимых мер по устранению инцидента. Параметр вычисляется автоматически на базе уровня риска указанного типа инцидента и значимости активов, на которых он обнаружен. При наведении курсора мыши открывается список параметров, формирующих оценку срочности (см. рисунок 80).

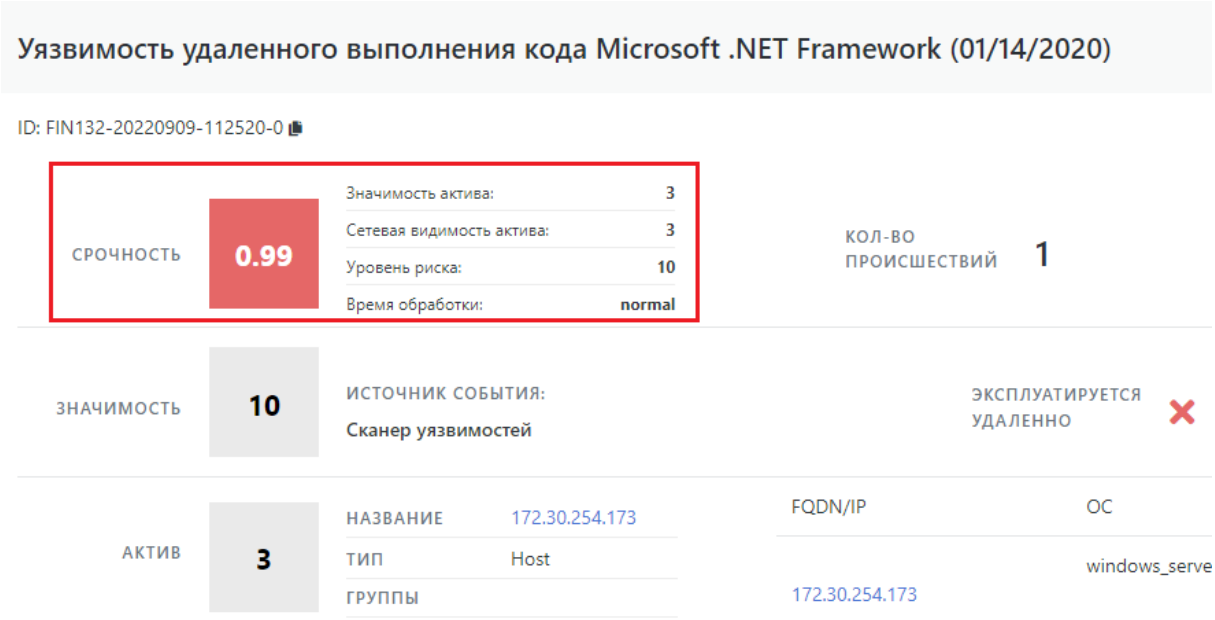



**Рисунок 80 – Просмотр параметров, формирующих оценку срочности**

**Уровень риска** (уровень значимости инцидента) - определяет степень опасности данного типа инцидента для инфраструктуры (см. рисунок 81). Значение уровня риска задается при создании типа инцидента в **Платформе Радар**. Оценивается по шкале от 0 до 10.

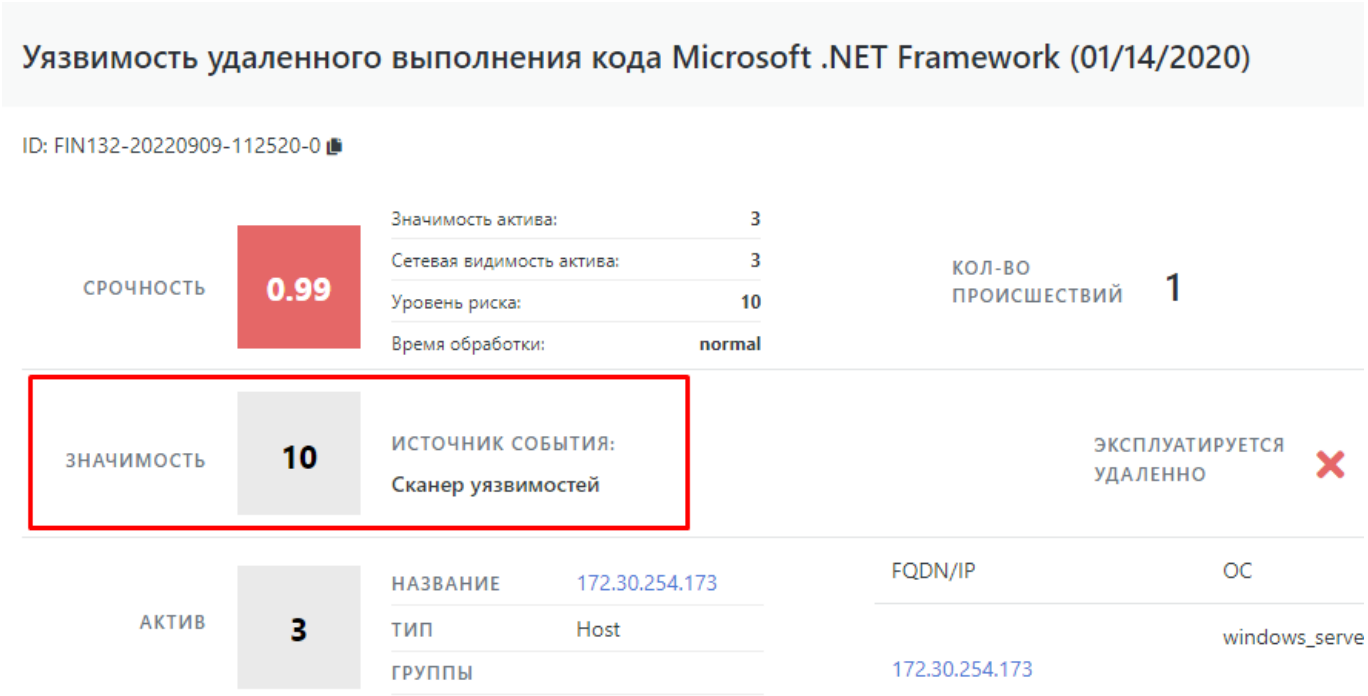



**Рисунок 81 – Уровень риска для инцидента**

**Уровень значимости актива** - значимость актива, на котором произошел инцидент (см. рисунок 82). Оценивается числовыми значениями от 1 до 5.

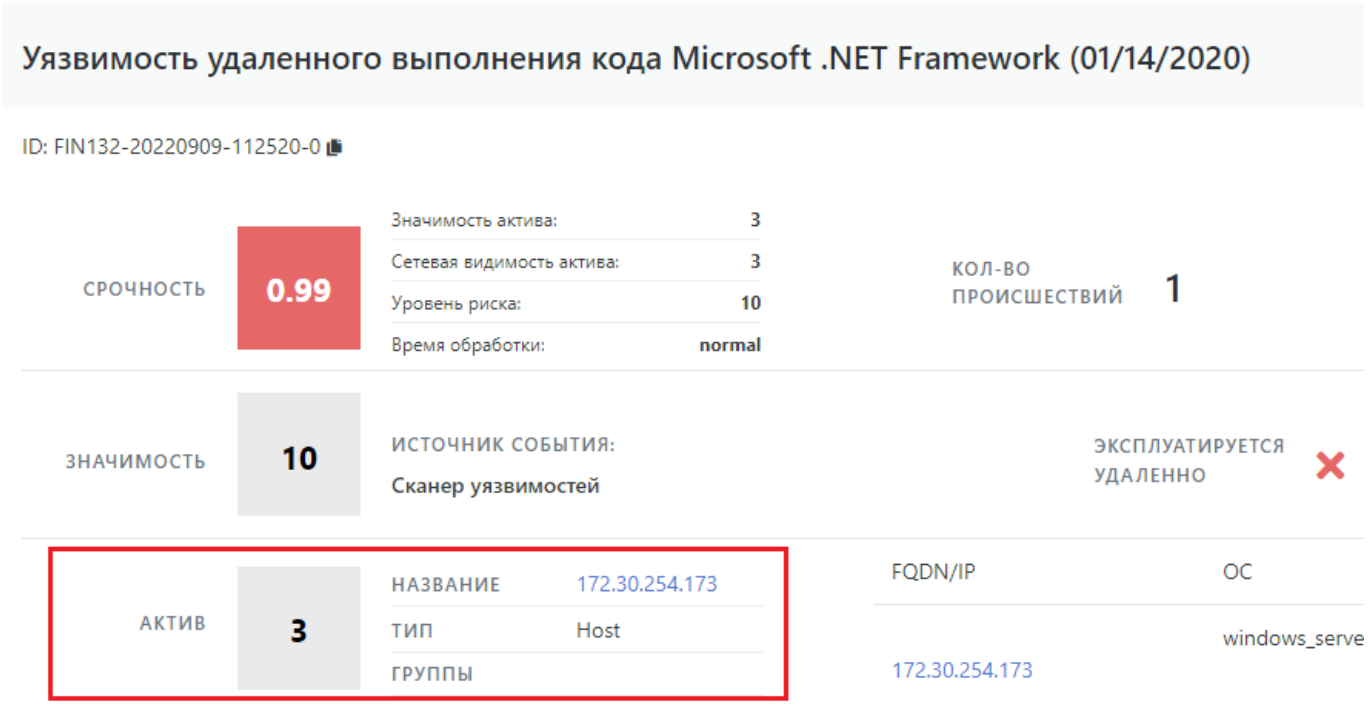



**Рисунок 82 – Уровень значимости актива, на котором произошел инцидент**

### 12.4.2.4 Блок информации "Происшествия". Общая информация

В данном блоке отображается текущий перечень происшествий, произошедших в рамках данного инцидента (см. рисунок 83). Для каждого происшествия отображаются следующие параметры:

- "**Начало активности**" - дата и время начала процессов происшествия;
- "**Конец активности**" - дата и время окончания процессов происшествия;
- "**Отправлено в НКЦКИ**" - статус отправки данных о происшествии в НКЦКИ (национальный координационный центр по компьютерным инцидентам) - отправлено / не отправлено.

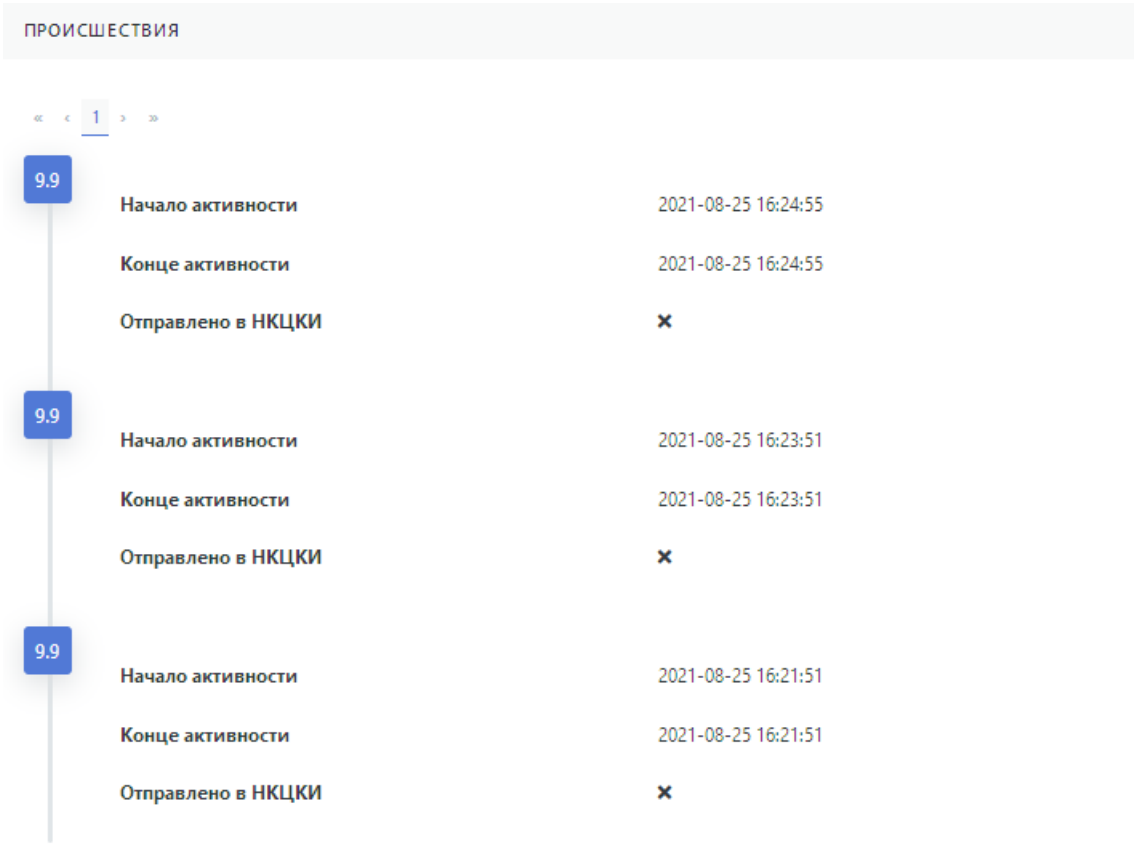



**Рисунок 83 – Информация о происшествиях на карточке инцидента**

### 12.4.2.5 Просмотр происшествий, обнаруженных правилами корреляции

Для происшествий, **обнаруженных правилами корреляции**, дополнительно выводится следующая информация:

- результаты анализа - данные, формируемые правилом корреляции как результат работы;
- событие - данные о событиях, вызвавших срабатывание правила корреляции (по кнопке "**Показать детали**", см. рисунок 84);
- уровень риска;
- правило корреляции, породившее инцидент (чтобы перейти к правилу корреляции, необходимо нажать на его название (см. рисунок 84));
- идентификатор, передаваемый из правила корреляции.

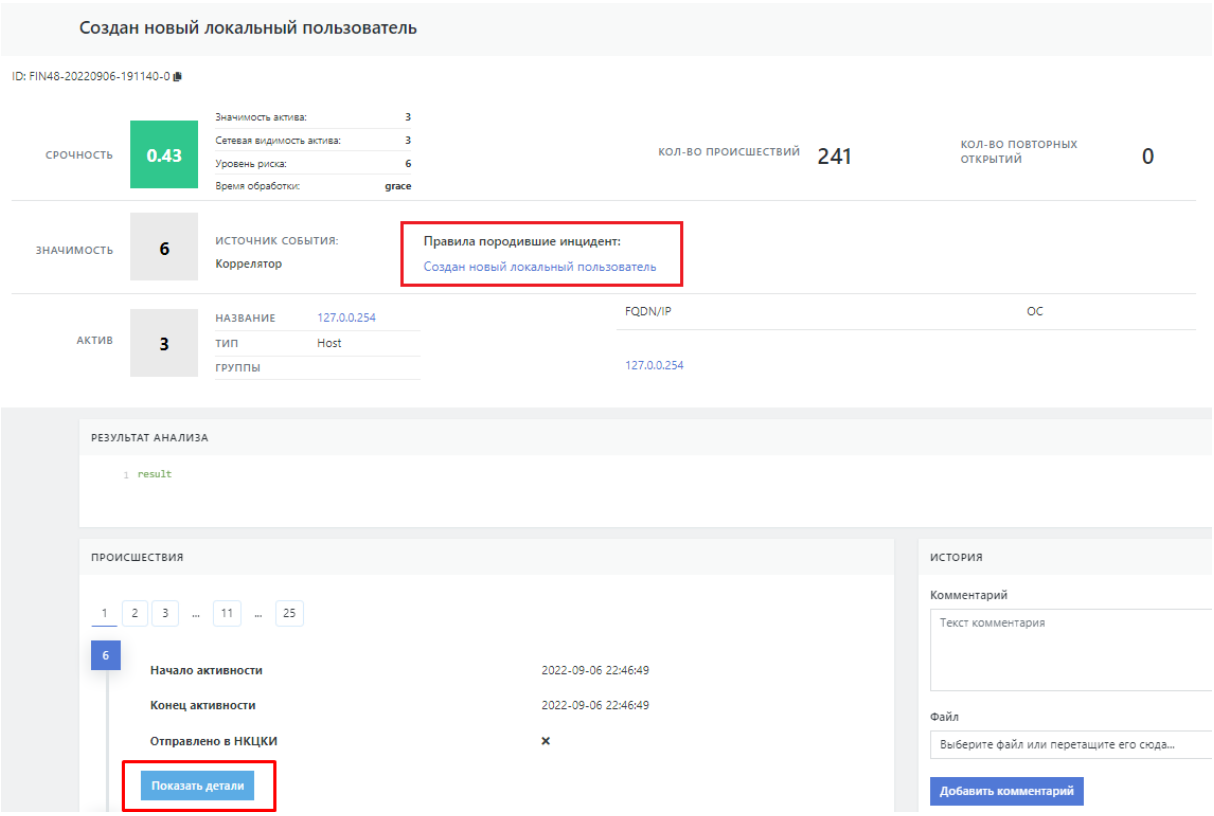



**Рисунок 84 – Информация о происшествиях на карточке инцидента, обнаруженного правилами корреляции**

Так же для подобных происшествий доступен просмотр деталей события. При нажатии кнопки "**Показать детали**" откроется просмотр "сырого" события в котором можно уточнить детали происшествия (см. рисунок 85).

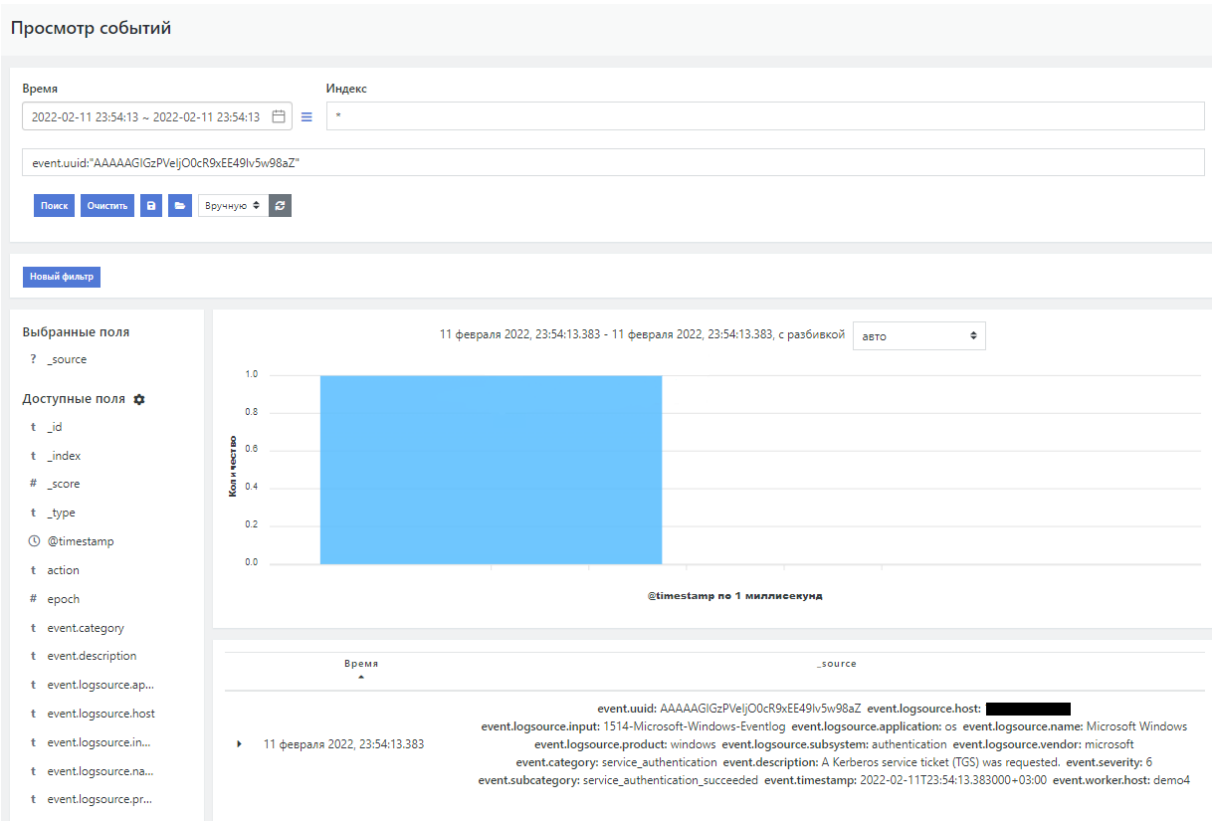



**Рисунок 85 – Просмотр сырого события**

### 12.4.2.6 Просмотра происшествий, обнаруженных сканером уязвимостей

Для происшествий, **обнаруженных по результатам анализа данных сканера уязвимостей**, дополнительно выводится информация о плагине сканера уязвимостей, обнаружившего уязвимость:

- ID плагина;
- название плагина;
- порт;
- протокол;
- внешнее сканирование
- вектор CVSS;
- CVSS Temporal Vector;
- CVSS Base Score;
- CVSS Temporal Score;
- фактор риска;
- дата изменения плагина;
- дата публикации.

### 12.4.2.7 Блок информации "История"

В данном блоке отображается история изменения статуса данного инцидента. Для каждой смены статуса отображается (см. рисунок 86):

- на какой статус изменен;
- дата и время изменения;
- пользователь, изменивший статус.

Помимо уведомлений о смене статуса в истории отображаются комментарии пользователя к смене того или иного статуса.

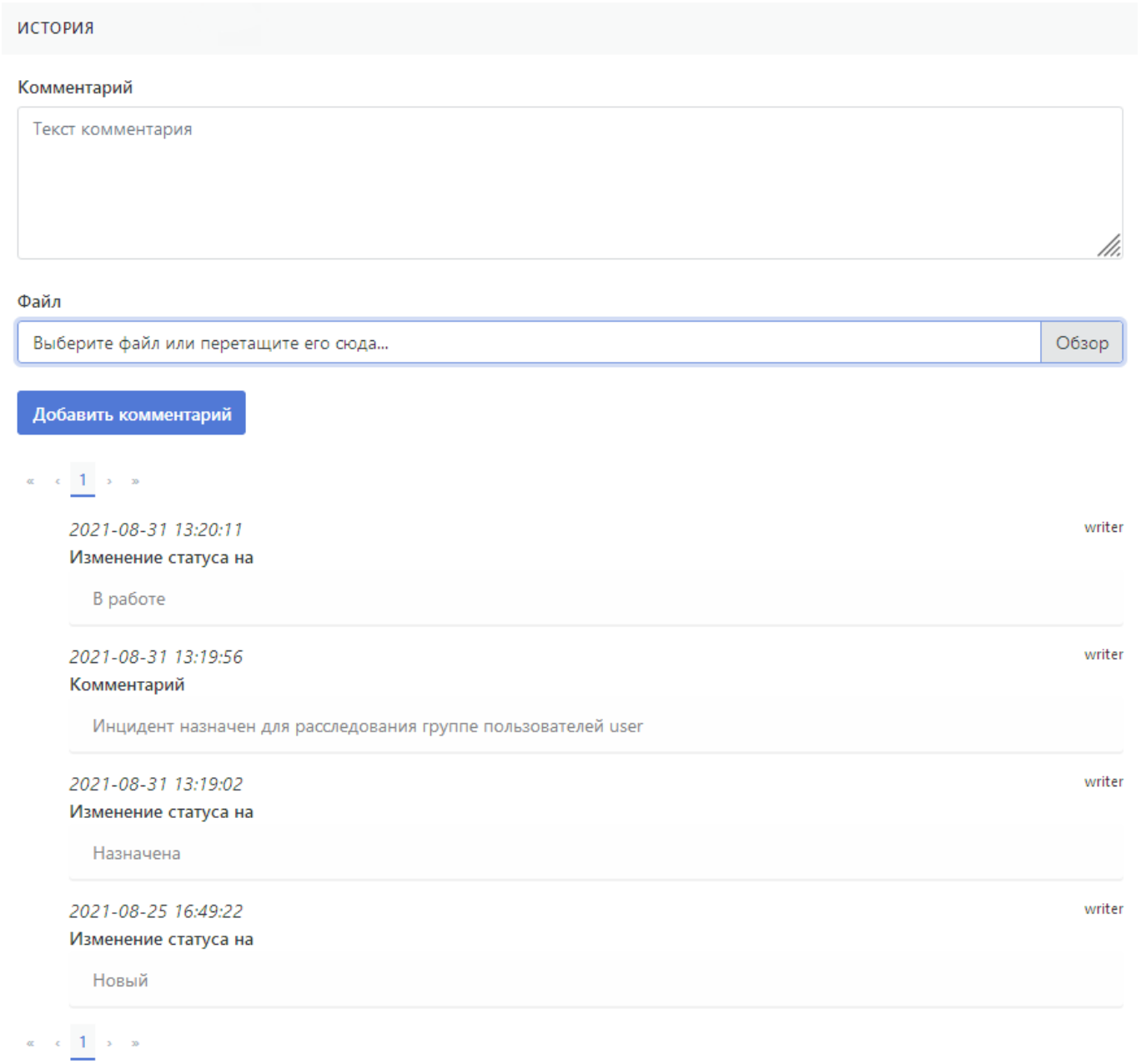



**Рисунок 86 – История изменений статуса инцидента**

Для добавления комментария при смене статуса необходимо:

1. Ввести комментарий в поле "**Текст комментария**";
2. При необходимости приложить к комментарию файл с данными, например график или текстовый файл. Для выбора добавляемого файла используется стандартная функция "**Обзор**";
3. Нажать на кнопку "**Добавить комментарий**".

Введенный текст отобразится в истории с указанием действия "**Комментарий**" (см. рисунок 87). Если к комментарию был добавлен файл, то в комментарии перед текстом комментария отобразится гиперссылка с именем файла.

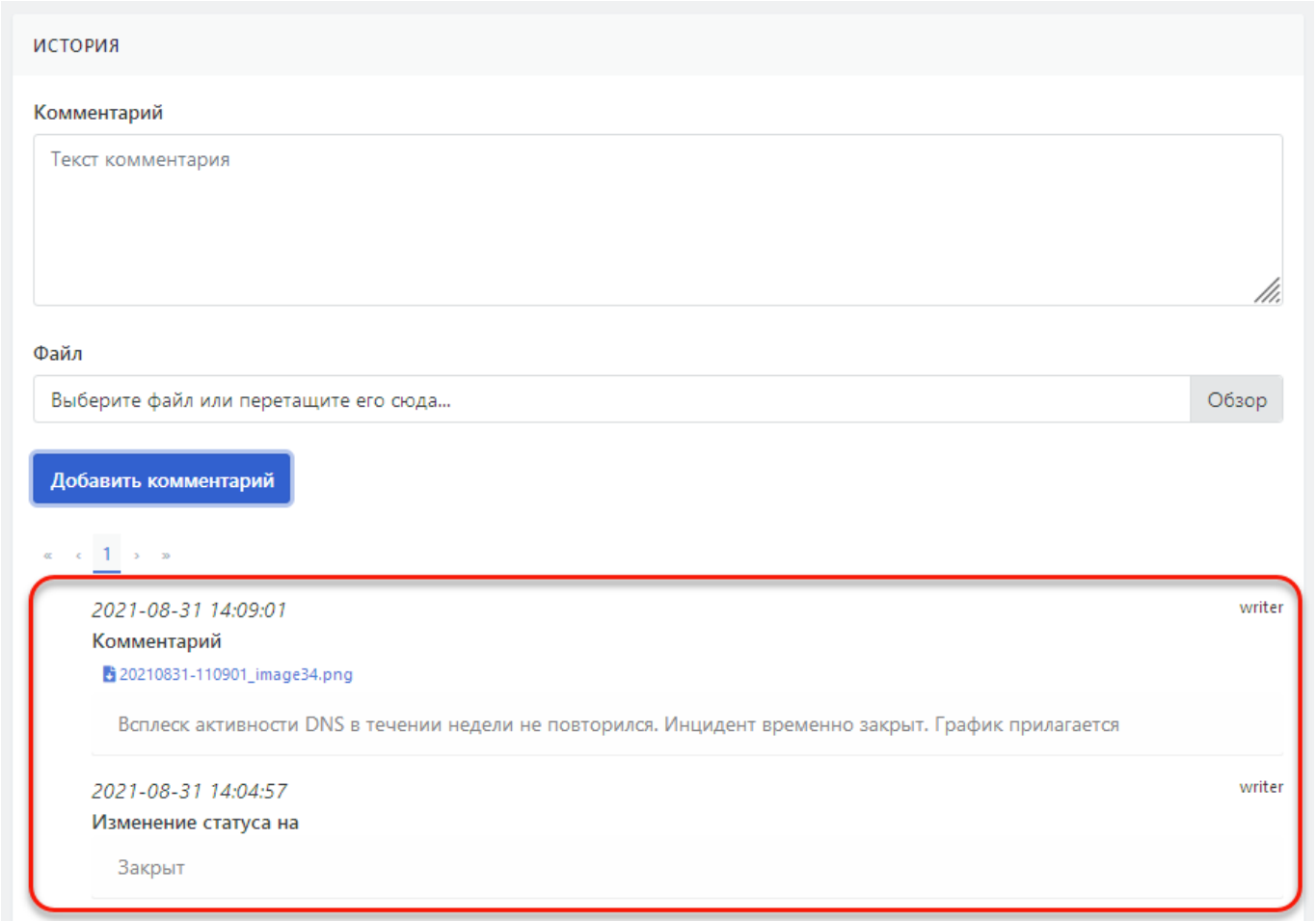



**Рисунок 87 – Комментарий с добавленным файлом**

# 12.5 Расследование инцидента

## 12.5.1 Алгоритм смены статусов при расследовании инцидента

В ходе расследования инцидент проходит ряд статусов (см. рисунок 88), имеющих следующую смысловую нагрузку:

- **ПР Новый** - статус используется вне основного рабочего процесса, например для тестирования. (Deprecated);
- **Новый** -инцидент находится в открытом состоянии в очереди на разбор;
- **В работе** - по инциденту ведутся работы;
- **Запрошена информация** - обработка инцидента приостановлена, была запрошена дополнительная информация;
- **Ожидает проверки** - для исправления инцидента применены контрмеры, требуется проверка со стороны компетентного лица;
- **Риск принят** - со стороны компетентного лица было принято решения отказаться от дальнейшего расследования инцидента;
- **Закрыт** - работы по расследованию инцидента завершены;
- **Недействительный** - инцидент был создан по ошибке, закрыт без разбора.

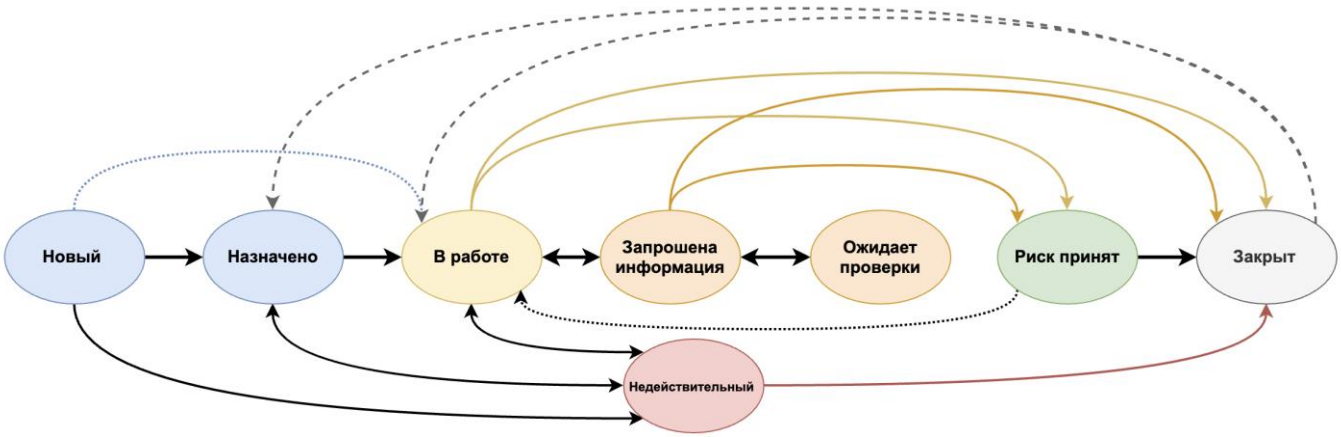



**Рисунок 88 – Алгоритм смены статусов при расследовании инцидентов**

В ходе расследования инцидентов пользователь **Платформы Радар** выполняет следующие действия:

- изменение статуса инцидента;
- назначение ответственных;
- редактирование параметров инцидента, включая удаление инцидента при необходимости;
- создание сообщений в контексте инцидента.

## 12.5.2 Изменение статуса инцидента

### 12.5.2.1 Доступ к функции смены статуса

Изменение статуса производится при завершении определенной стадии работы над инцидентом. Функция смены статуса находится:

- на экране со списком инцидентов: ***Инциденты - Инциденты***;
- на карточке инцидента: ***Инциденты - Инциденты - /щелкнуть по заголовку интересующего инцидента в списке/***.

### 12.5.2.2 Изменение статуса инцидента/инцидентов в списке инцидентов

**Внимание!** Функция смены статуса на данной станице доступна пользователю только при наличии необходимых прав.

Для изменения статуса инцидента или группы инцидентов требуется:

1. Открыть список инцидентов: ***Инциденты - Инциденты***;
2. Выделить флажками одну или несколько строк инцидентов, чей статус необходимо изменить (см. рисунок 89);
3. Раскрыть список статусов и выбрать в нем новый статус (см. рисунок 89).

При выборе нового статуса происходит запуск автоматического обновления страницы списка. По завершению обновления выбранные инциденты должны отобразится с новым статусом.

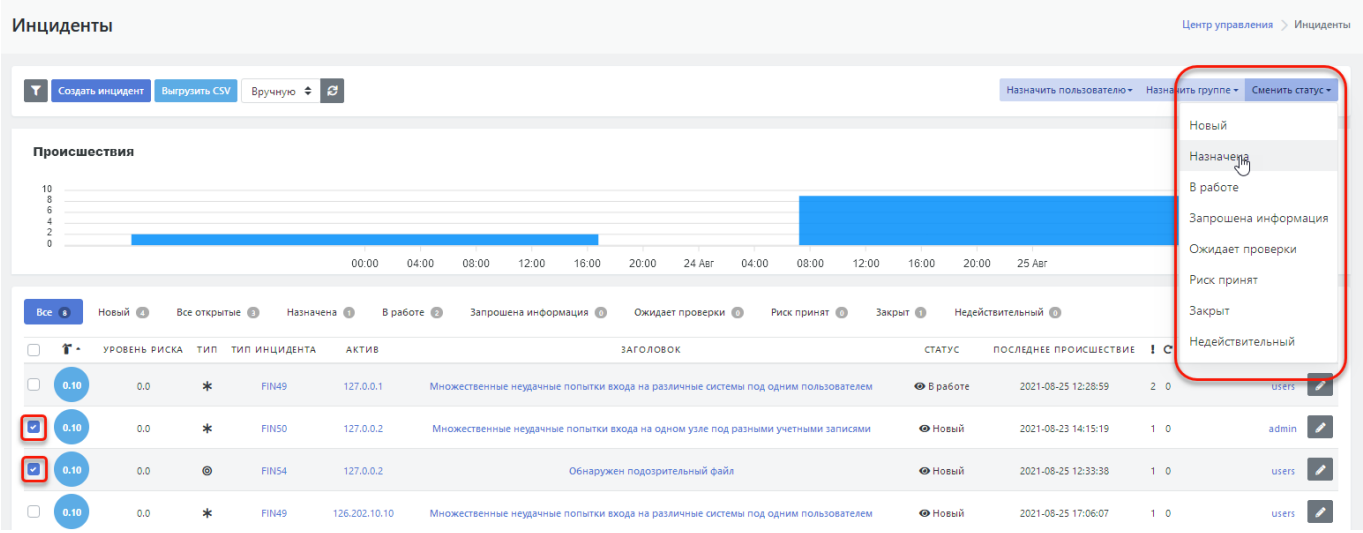



**Рисунок 89 – Смена статуса инцидентов на странице списка инцидентов**

### 12.5.2.3 Изменение статуса инцидента на карточке инцидента

Для изменения статуса инцидента через карточку инцидента требуется:

1. Открыть карточку инцидента: ***Инциденты - Инциденты - /щелкнуть по заголовку интересующего инцидента в списке/***;
2. Раскрыть список статусов и выбрать в нем новый статус (см. рисунок 90). Список будет содержать только перечень статусов, доступных для смены текущего статуса согласно алгоритму смены статусов - см. раздел «Алгоритм смены статусов при расследовании инцидента».

При выборе нового статуса происходит запуск автоматического обновления статуса. Изменение статуса будет отображено в блоке информации "**История**". Описание работы с данным блоком приведено в разделе «Просмотр карточки инцидента».

При необходимости в блоке "**История**" пользователь может:

- Добавить текстовый комментарий к проведенной смене статуса. Например, указать причину смены статуса.
- В качестве комментариев добавить данные из внешних источников в виде прикрепленного файла. Например, добавить изображение с графиком или таблицу с данными, которые повлияли на смену статуса.

Подробное описание работы с комментариями к смене статуса приведено в разделе «Просмотр карточки инцидента».

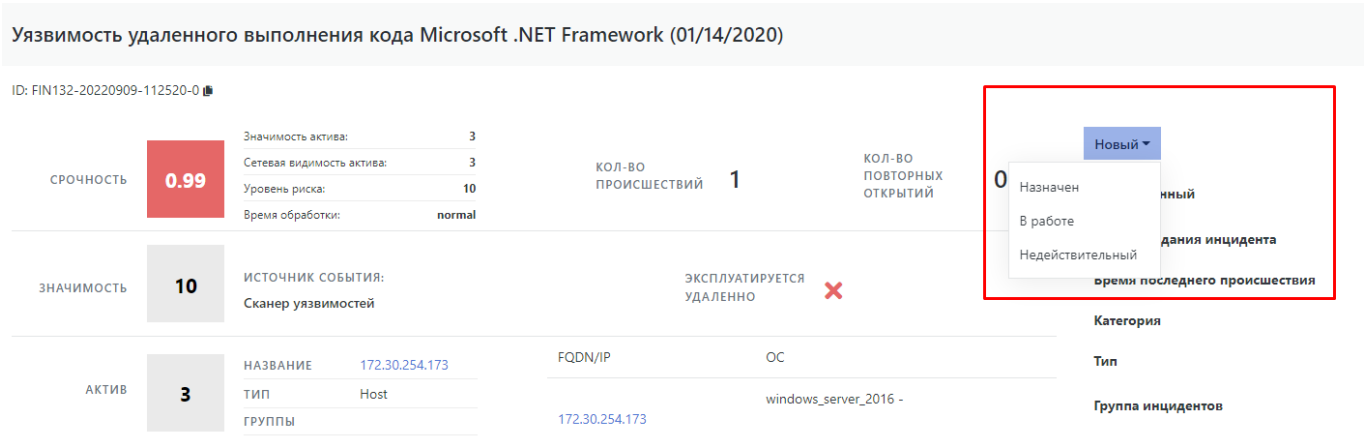



**Рисунок 90 – Смена статуса на карточке инцидента**

## 12.5.3 Назначение инцидента ответственным

### 12.5.3.1 Доступ к функции выбора ответственных пользователей

Инцидент может быть назначен как отдельному пользователю, так и группе пользователей.

Изменение ответственного (группы ответственных) за инцидент производится пользователем при необходимости передать полномочия по ведению данного инцидента другому пользователю или группе пользователей.

Функции назначения ответственных находятся:

- на экране со списком инцидентов: ***Инциденты - Инциденты***;
- на карточке инцидента: ***Инциденты - Инциденты - /щелкнуть по заголовку интересующего инцидента в списке/***.

### 12.5.3.2 Назначение инцидента ответственным в списке инцидентов

**Внимание!** *Функции назначения инцидента ответственным на данной станице доступна пользователю только при наличии необходимых прав.*

Для назначения инцидента новому пользователю, ответственному за расследование, требуется:

1. Открыть список инцидентов: ***Инциденты - Инциденты***;
2. Выделить флажками одну или несколько строк инцидентов, для которых необходимо сменить ответственного (см. рисунок 91);
3. Для назначения инцидента новому ответственному выбрать на экране функцию "**Назначить пользователю**" - станет доступным раскрывающийся список пользователей и кнопка "**Назначить**" (см. рисунок 91);
4. Выбрать в списке нового пользователя и нажать кнопку "**Назначить**".

Произойдёт обновление списка и для выбранных инцидентов будет указан новый ответственный пользователь в поле "**Пользователь**" ( ).

Назначение одного или нескольких инцидентов группе пользователей проводится аналогично назначению отдельного пользователя. При этом выбирается функция "**Назначить группе**". Раскрывающийся список будет содержать текущий список групп. По нажатию на кнопку

"**Назначить** "произойдёт обновление списка и для выбранных инцидентов будет указана новая ответственная группа пользователей в поле "**Группа**" ( ).

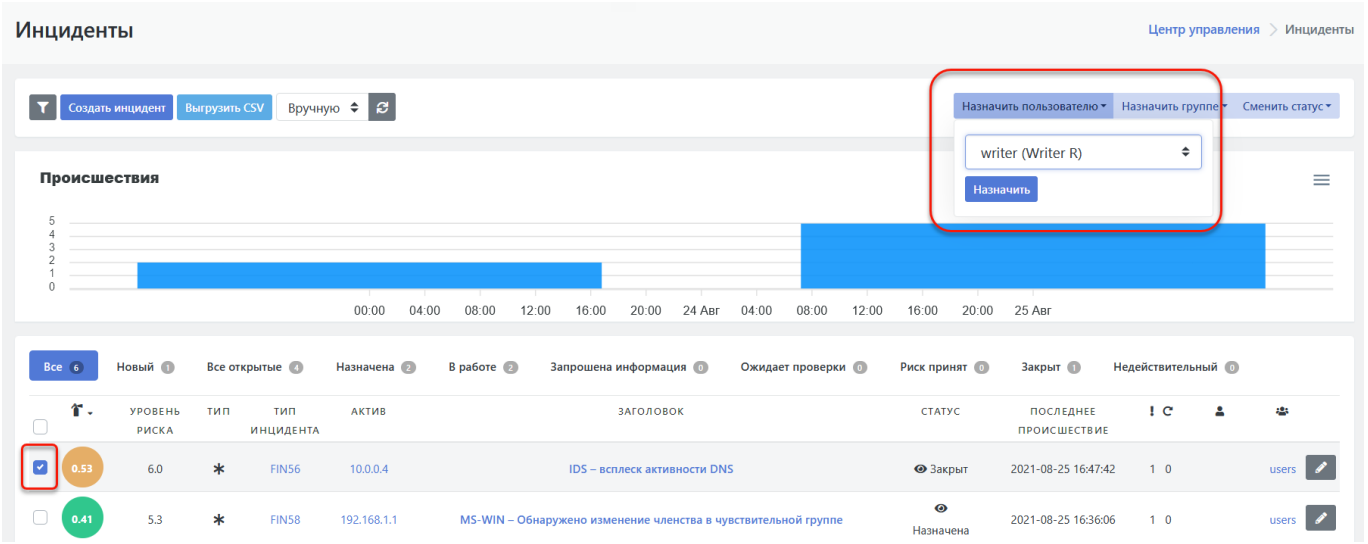



**Рисунок 91 - Выбор пользователя, ответственного за инцидент**

### 12.5.3.3 Назначение ответственных на карточке инцидента

Для назначения инцидента новым ответственным через карточку инцидента требуется:

1. Открыть карточку инцидента: ***Инциденты - Инциденты - /щелкнуть по заголовку интересующего инцидента в списке/***.

   На карточке для параметра "**Ответственный**" указаны в виде функциональных элементов:

   - текущий ответственный пользователь (функция слева) -- имя пользователя;
   - текущая ответственная группа (функция справа) -- имя группы.

   Если ни пользователь, ни группа еще не назначены, то функциональные элементы будут иметь соответствующие подписи "Пользователь" и "Группа" (см. рисунок 92).

2. Для назначения инцидента новому пользователю выбрать функцию (слева) с именем текущего ответственного пользователя -- станет доступным раскрывающийся список пользователей и кнопка "**Назначить**" (см. рисунок 92).

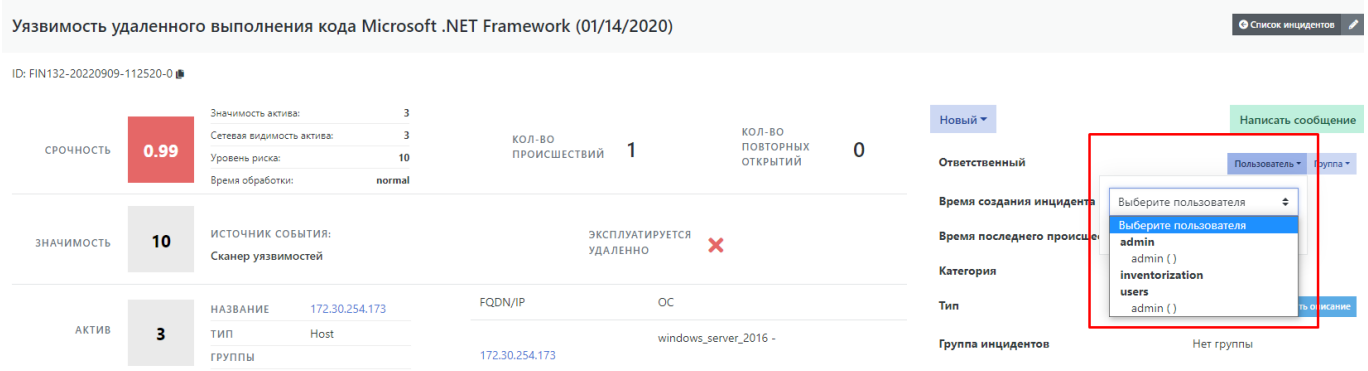



**Рисунок 92 – Назначение ответственного или группы ответственных на карточке инцидента**

3. Выбрать в списке нового пользователя и нажать на кнопку "**Назначить**".

Для параметра "**Ответственный**" будет указано имя нового ответственного за инцидент пользователя (на соответствующем функциональном элементе).

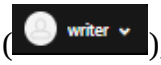
Назначение инцидента новой группе ответственных пользователей проводится аналогично назначению отдельного пользователя. Выбирается функция с названием текущей ответственной группы. Раскрывающийся список будет содержать текущий список групп.

## 12.5.4 Создание и отправка сообщения со ссылкой на инцидент

При проведении расследования инцидента пользователь может отправить текстовое сообщение другому пользователю **Платформы Радар**. Для этого необходимо:

1. Открыть карточку инцидента: ***Инциденты - Инциденты - /щелкнуть по заголовку интересующего инцидента в списке/***;
2. Нажать на кнопку "**Написать сообщение**";
3. В открывшейся форме сообщения заполнить следующие поля:
    - **Получатель** - выбрать адресата из раскрывающегося списка пользователей **Платформы Радар**;
    - **Заголовок** - ввести заголовок сообщения;
    - **Сообщение** - ввести текст сообщения.
4. Нажать на кнопку "**Отправить**".

При отправке к сообщению будет автоматически прикреплена ссылка на данную карточку инцидента.

Отправленное из карточки инцидента сообщение отобразится в списке отправленных сообщений пользователя. Список отправленных сообщений пользователя расположен в профиле пользователя ( 

), в разделе ***Сообщения***.

Подробное описание работы пользователя с сообщениями приведено в разделе «Работа с сообщениями».

## 12.5.5 Редактирование параметров инцидента

### 12.5.5.1 Доступ к функции редактирования

**Внимание**! *Функция редактирования доступна пользователю только при наличии необходимых прав доступа.*

Функция редактирования параметров инцидента доступна:

- на экране со списком инцидентов: ***Инциденты - Инциденты***;
- на карточке инцидента: ***Инциденты - Инциденты - /щелкнуть по заголовку интересующего инцидента в списке/***.

### 12.5.5.2 Перечень редактируемых параметров

В случае необходимости можно отредактировать следующие параметры инцидента (см. рисунок 93):

- значение уровня риска (уровень значимости) инцидента;
- имя инцидента в **Платформе Радар**;
- параметры описания инцидента, такие как:
    - **Сводка** - описание действия, вызвавшего инцидент;
    - **Описание угрозы**;
    - **Последствия реализованной угрозы**;
    - **Рекомендации по устранению угрозы**;
    - **Рекомендации по уменьшению риска**;
    - **Внутреннее примечание**.

### 12.5.5.3 Редактирование параметров инцидента

Редактирование параметров инцидента необходимо в случае, если в описании инцидента есть неточности, выявленные аналитиком или у аналитика есть дополнительные сведения, требующие фиксации в контексте инцидента (см. рисунок 93).

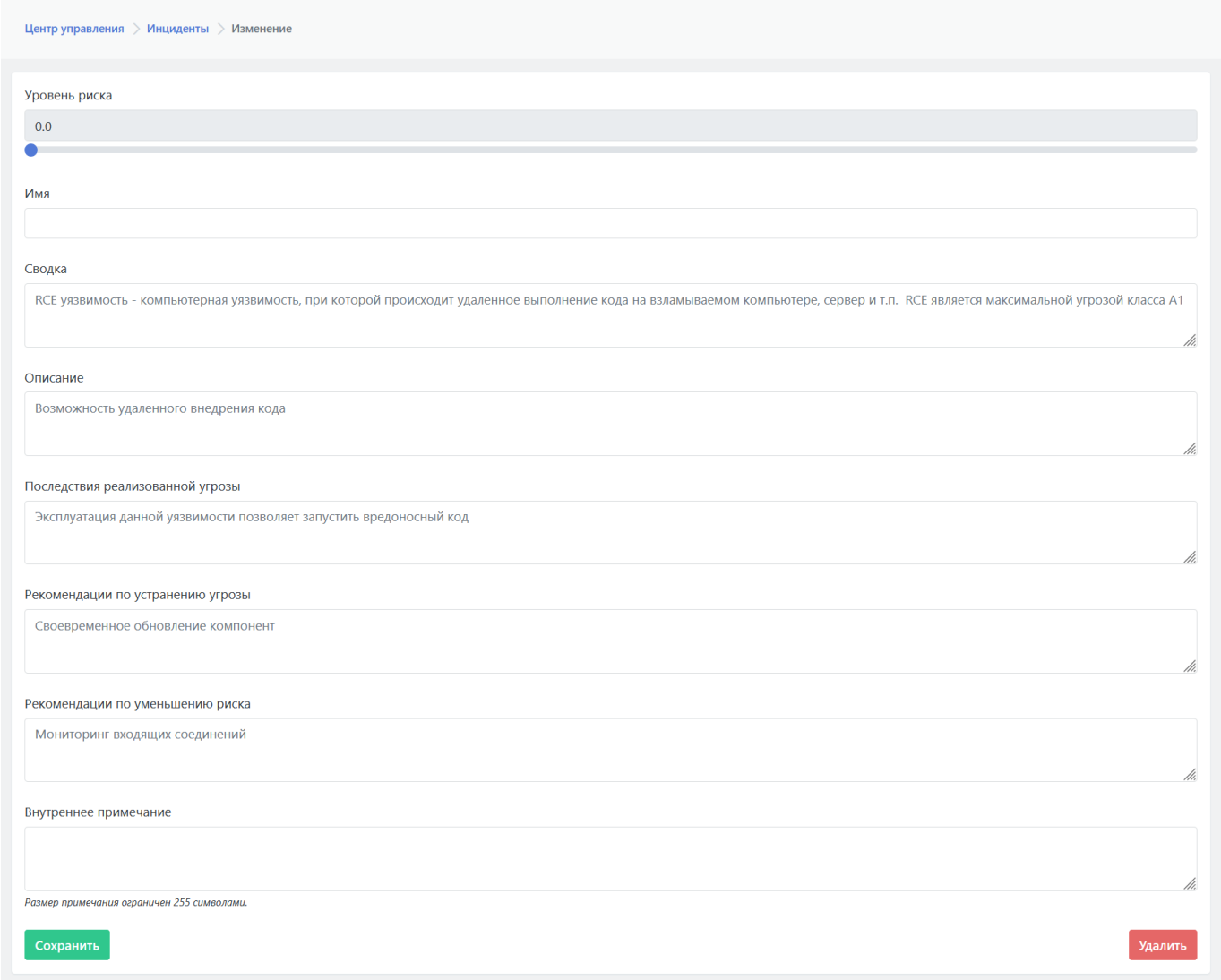



**Рисунок 93 – Окно редактирования параметров**

Для проведения редактирования необходимо:

1. Открыть окно редактирования одним из следующих способов:
    - Открыть список инцидентов ***Инциденты - Инциденты***, и нажать в строке интересующего инцидента на кнопку  ;
    - Открыть карточку инцидента ***Инциденты - Инциденты - /щелкнуть по заголовку интересующего инцидента в списке/***, и нажать на кнопку "**Редактировать**", расположенную в блоке сводной информации карточки;
2. Для сохранения изменений нажать на кнопку "**Сохранить**";

## 12.5.6 Удаление инцидента

**Внимание**! Функция удаления доступна пользователю только при наличии необходимых прав доступа. Инцидент должен быть назначен данному пользователю рассмотрения.

Функция удаления доступна через окно редактирования параметров инцидента.

Для удаления инцидента с **Платформы Радар** необходимо:

1. Открыть окно редактирования одним из следующих способов:
    - Открыть список инцидентов ***Инциденты - Инциденты***, и нажать в строке интересующего инцидента на кнопку  ;
    - Открыть карточку инцидента ***Инциденты - Инциденты - /щелкнуть по заголовку интересующего инцидента в списке/***, и нажать на кнопку "**Редактировать**", расположенную в блоке сводной информации карточки.
2. В открывшейся форме редактирования параметров инцидента нажать на кнопку "**Удалить**" (см. рисунок 93);
3. В открывшемся окне подтверждения удаления нажать на кнопку "**Да**".

Произойдет автоматический переход к обновленному списку инцидентов.

## 12.5.7 Группировка инцидента

При формировании инцидента **Платформа Радар** позволяет поместить инцидент в группу. При этом система позволяет

- Поместить инцидент в уже имеющуюся группу инцидентов;
- Создать новую группу, из правила корреляции;
- Поместить инцидент в группу вручную.

### 12.5.7.1 Группировка с использованием корреляций

Объединение инцидентов в группы можно с помощью правил корреляции с использованием скриптового языка Lua.

Группа инцидентов указывается с использованием параметра incident_group при формировании инцидента (alert).

```
########################################################################
rule_settings = {
      "risk_score": 6,
      "create_incident": True,
      "assign_to_customer": False,
      "template_name": 'template'
}

########################################################################
print(rule_settings)


@log_connection.fetch("#.web_server.#")
def handle_logline(logline):
      #tab
      useragent=logline.get("initiator.http.user-agent.full")
      if 'openvas' in useragent.lower():
            alert(rule_settings["template_name"],
                        logline,
                        rule_settings["risk_score"],
                        {"ip": logline.target.host.ip[0]},
                        create_incident=rule_settings["create_incident"],
                        assign_to_customer=rule_settings["assign_to_customer"],
                        incident_identifier=logline.initiator.host.ip[0],
                        incident_group="test-group-1")
```

В качестве группы можно передавать как статическое значение, так и и значение поля из logline.

```
########################################################################
rule_settings = {
      "risk_score": 6,
      "create_incident": True,
      "assign_to_customer": False,
      "template_name": 'template'
}

########################################################################
print(rule_settings)


@log_connection.fetch("#.web_server.#")
def handle_logline(logline):
      #tab
      useragent=logline.get("initiator.http.user-agent.full")
      if 'openvas' in useragent.lower():
            alert(rule_settings["template_name"],
                        logline,
                        rule_settings["risk_score"],
                        {"ip": logline.target.host.ip[0]},
                        create_incident=rule_settings["create_incident"],
                        assign_to_customer=rule_settings["assign_to_customer"],
                        incident_identifier=logline.initiator.host.ip[0],
                        incident_group=logline.target.host.ip[0])
```

**Платформа Радар** позволяет помещать в одну группу события от разных источников и типов.

```
########################################################################
rule_settings = {
      "risk_score": 6,
      "create_incident": True,
      "assign_to_customer": False,
      "template_name": 'template_brut'
}

########################################################################
print(rule_settings)

@log_connection.fetch("#.windows.os.#")
def handle_logline(logline):
         if logline.observer.event.id == "4776" and logline.observer.event.type ==
"security":
             print( logline.target.user.name )
             if logline.outcome.name == "failure":
                 alert(rule_settings["template_name"],
                 logline,
                 rule_settings["risk_score"],
                 {"fqdn": logline.observer.host.fqdn[0], "ip":
logline.event.worker.ip},
                 create_incident=rule_settings["create_incident"],
                 assign_to_customer=rule_settings["assign_to_customer"],
                 incident_identifier=logline.observer.host.fqdn[0],
                 incident_group="test-group-1")
```

### 12.5.7.2 Ручное добавление в группу

**Платформа Радар** позволяет помещать инциденты как уже в созданные группы, так и в новые.

Для создания группы инцидентов перейдите в раздел ***Инциденты - Группы инцидентов*** и нажимаем кнопку "**Создать**" (см. рисунок 94).

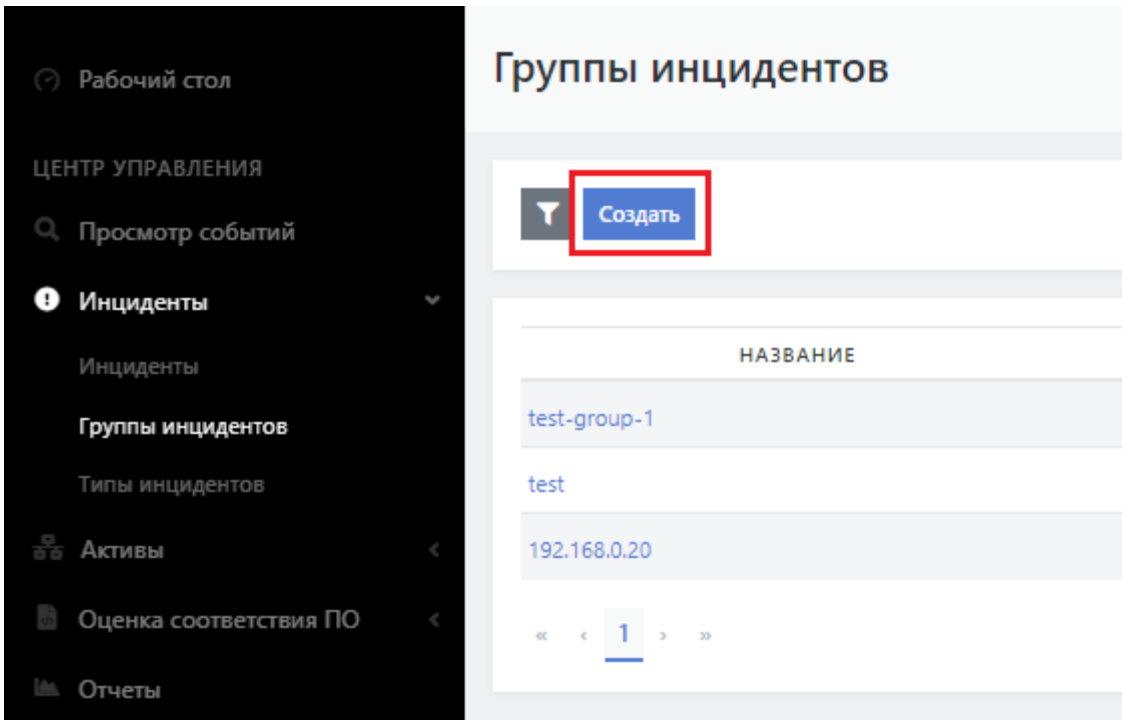



**Рисунок 94 – Создание группы инцидентов**

В появившейся форме указывается **Название** группы, а также, если необходимо, **Описание**, **Пользователя по умолчанию** и/или **Группу пользователей по умолчанию** (см. рисунок 95).

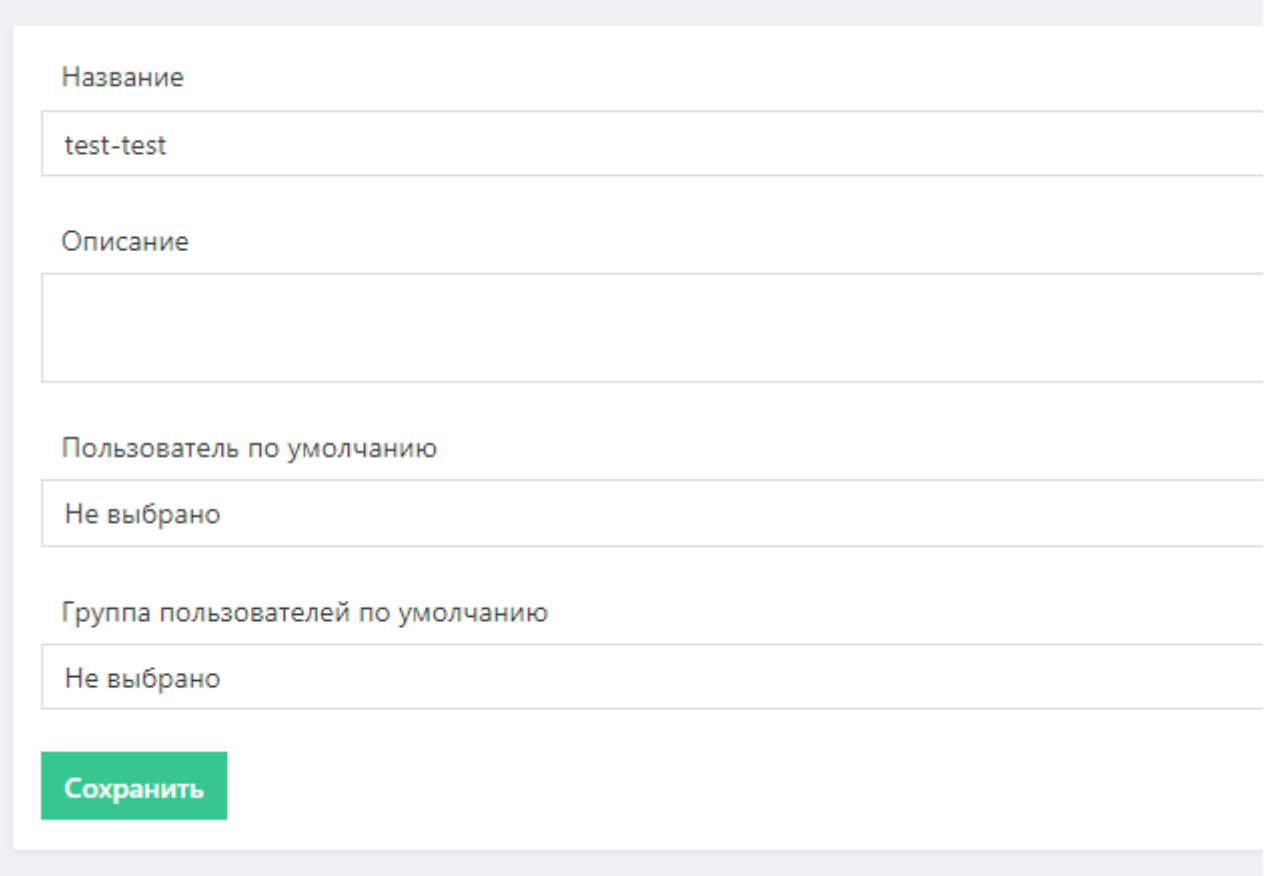



**Рисунок 95 – Параметры группы инцидентов**

Для добавления инцидентов в группу, нужно перейти в раздел ***Инциденты - Инциденты***:

- Устанавить чек-бокс напротив инцидентов, которые необходимо объединить в группу;
- В правом верхнем угру нажать на кнопку "**Объединить в группу**";
- В выпадающем списке выбирать необходимую группу;
- Нажать кнопку "**Назначить группу**" (см. рисунок 96).

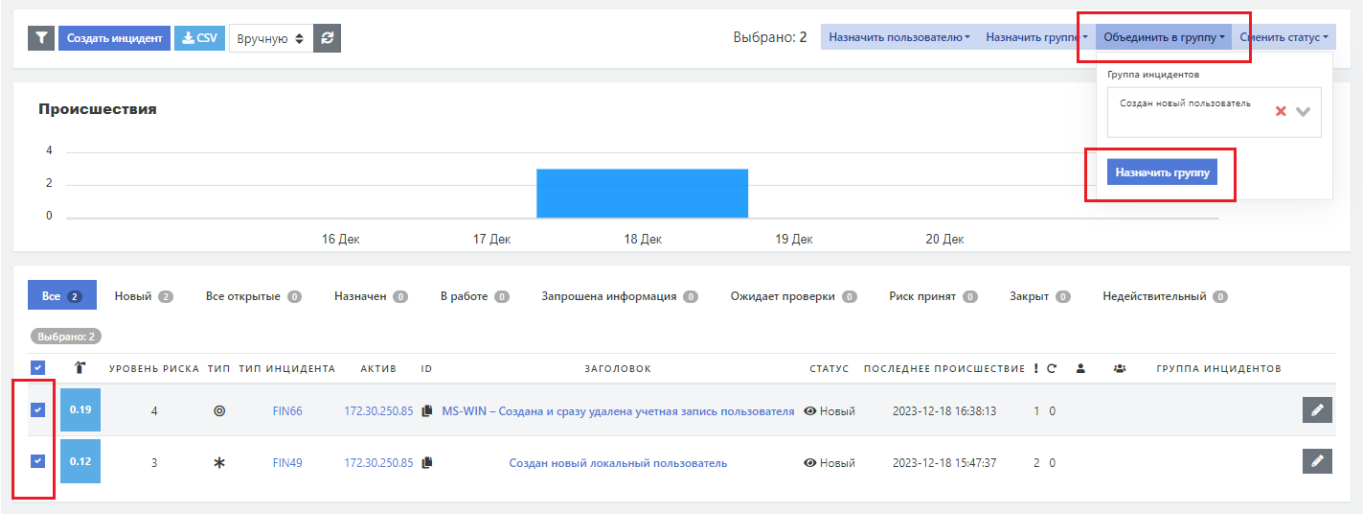



**Рисунок 96 – Назначение нескольких инцидентов в группу**

Для добавления инцидента в группу из карточки инцидента открыть инцидент на редактирование (см. рисунок 97).

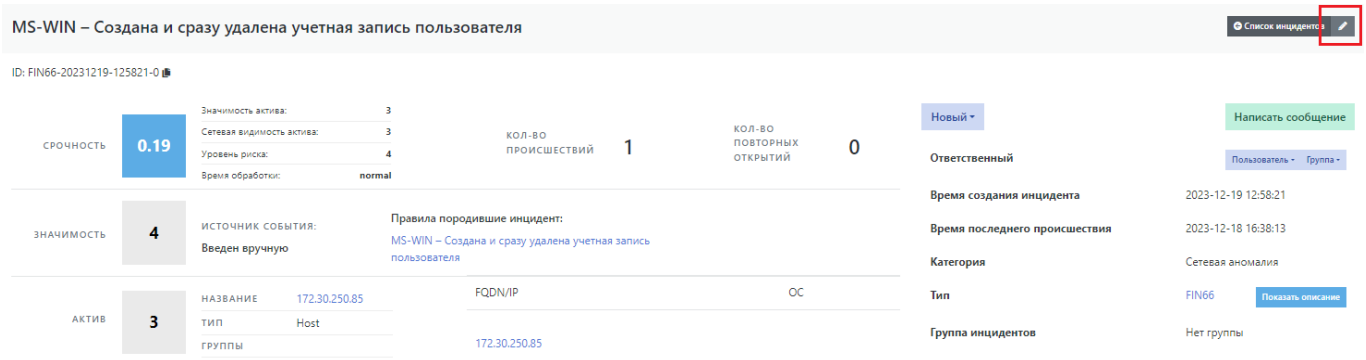



**Рисунок 97 – Добавление инцидента в группу инцидентов**

В разделе группа инцидентов выбрать необходимую группу из списков нажать кнопку "**Сохранить**" (см. рисунок 98).

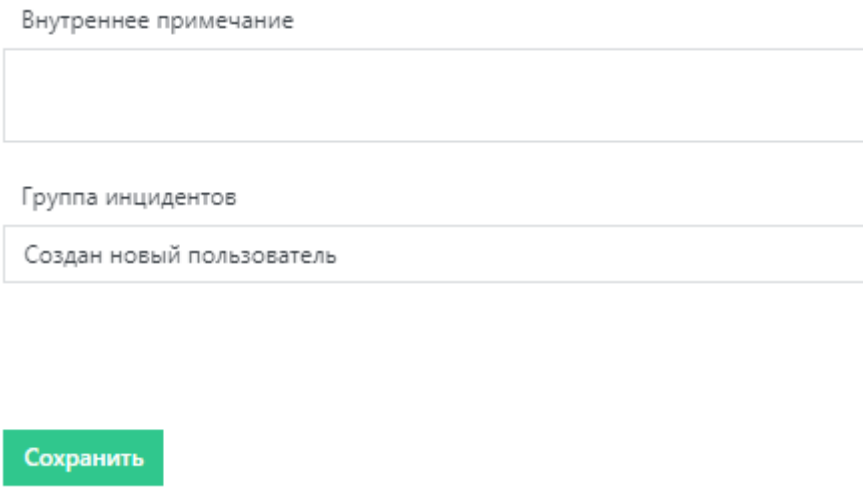



**Рисунок 98 – Сохранение инцидента в группу инцидентов**

# 13. Работа с базой знаний типов инцидентов

## 13.1 Общие данные о типах инцидентов

В рамках **Платформы Радар** каждый инцидент всегда принадлежит к определенному предустановленному типу инцидентов.

Раздел интерфейса "**Типы инцидентов**" предназначен для управления базой знаний по типам обрабатываемых инцидентов. Актуализация базы знаний является одной из приоритетных задач SOC.

## 13.2 Анализ типов инцидентов

### 13.2.1 Просмотр списка типов инцидентов

Полный табличный список типов инцидентов расположен в разделе: ***Инциденты - Типы инцидентов*** (см. рисунок 99).

Подробное описание табличного списка типов инцидентов и возможностей фильтрации списка приведены в разделе «Подраздел "Типы инцидентов"».

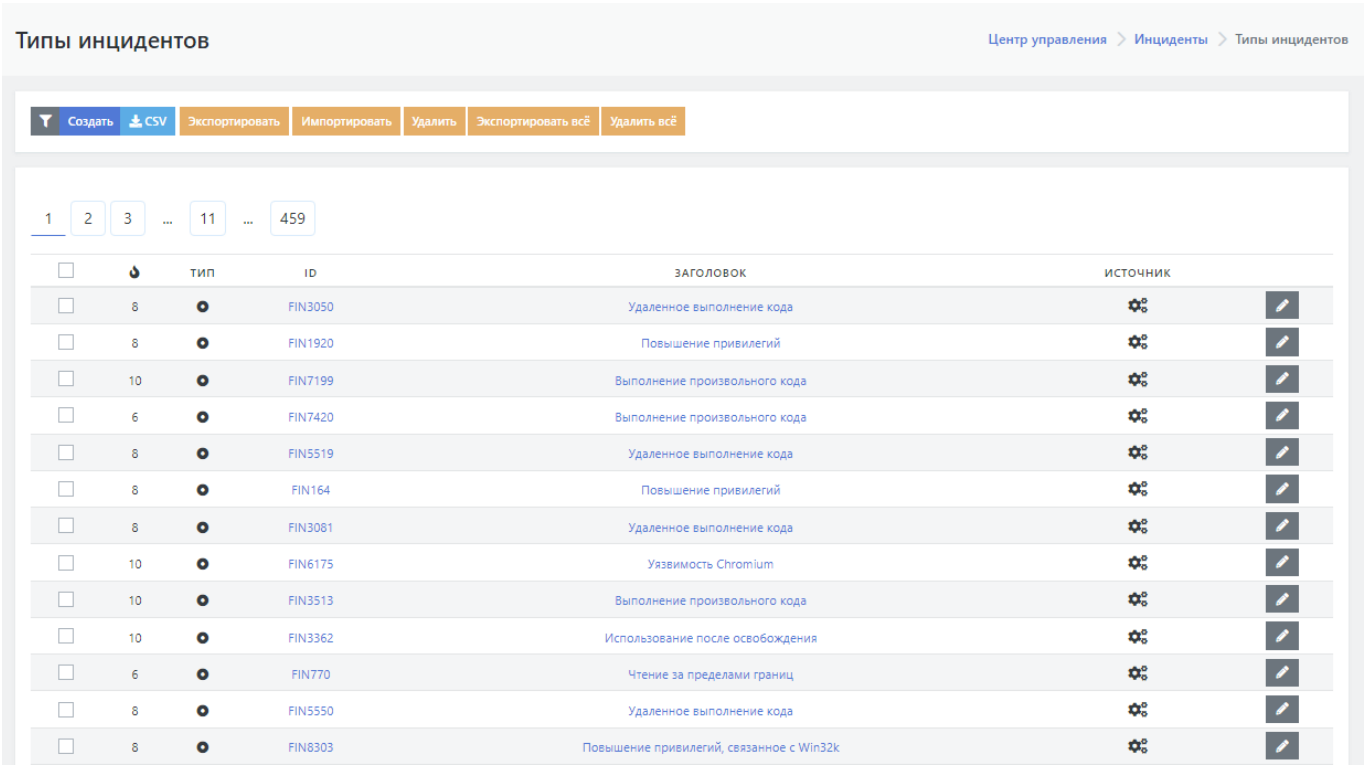



**Рисунок 99 – Список типов инцидентов в разделе *Инциденты - Типы инцидентов***

Гиперссылки в строке типа обеспечивают просмотр следующей детальной информации:

- **ID** - содержит идентификатор типа произошедшего инцидента. Гиперссылка ведет на карточку типа инцидента с детальной информацией. Описание карточки типа инцидента приведено в разделе документа «Просмотр детализации типа инцидента»;

- **Заголовок** - содержит название типа инцидента. Гиперссылка ведет на карточку типа инцидента с детальной информацией . Описание карточки актива приведено в разделе документа «Просмотр детализации типа инцидента».
- Кнопка редактирования ( ) - переводит на страницу редактирования параметров инцидента;
- **Источник**" - содержит пиктограммы, соответствующие тому или иному источнику данных.

  Если в поле установлена пиктограмма коррелятора ( ), то при наведении на нее курсора откроется всплывающее окно "**Связанные правила Logmule**" с гиперссылкой на страницу с описанием правил коррелятора (см. рисунок 100). Переход на страницу с описанием правил корреляции возможен только при наличии у пользователя соответствующих прав.

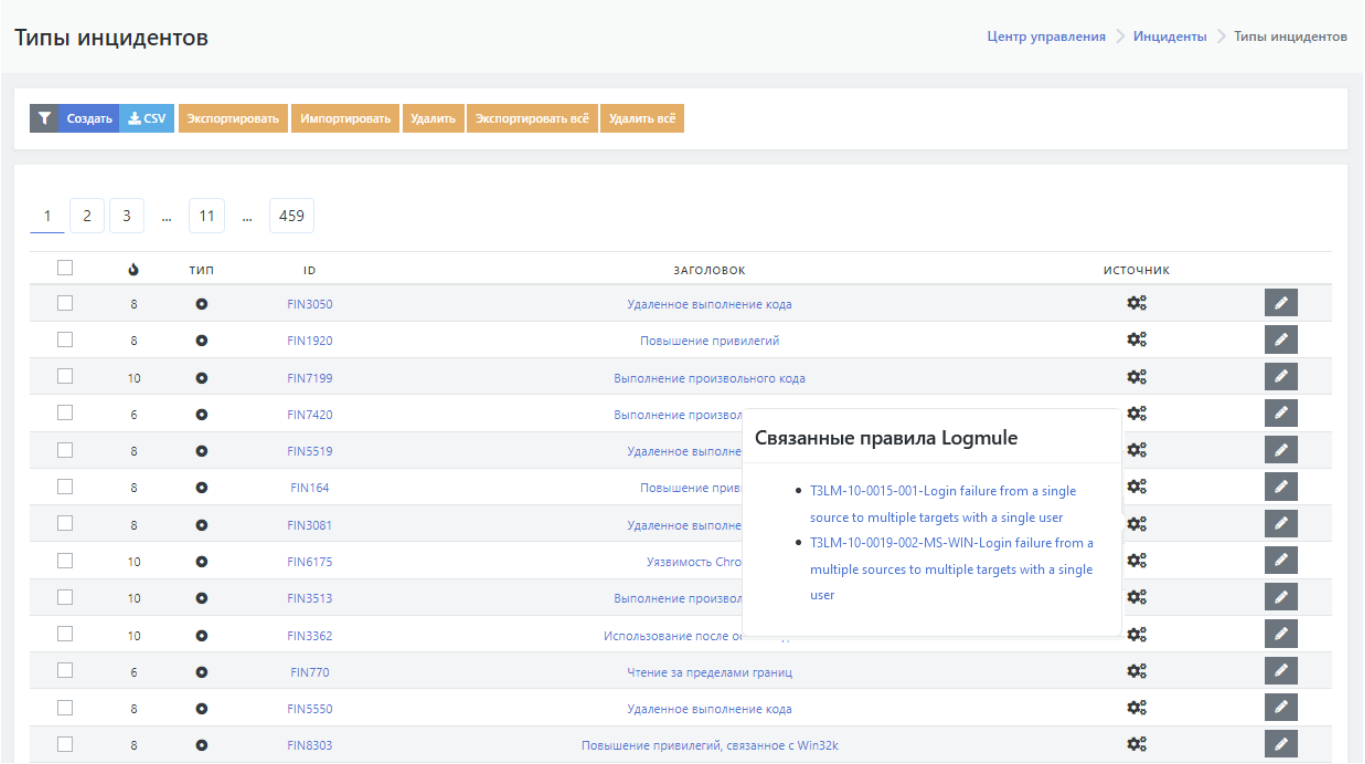



**Рисунок 100 – Просмотр правил корреляции, связанных с типом иницдента**

## 13.2.2 Просмотр детализации типа инцидента

### 13.2.2.1 Общее описание карточки типа инцидента

Для просмотра детализации по интересующему типу инцидента необходимо:

1. Перейти в раздел ***Инциденты - Типы инцидентов***;
2. В списке типов инцидентов щелкнуть по названию интересующего типа в поле "**Заголовок**" или "**ID**".

На экране откроется карточка типа инцидента, содержащая полный набор данных по выбранному типу (см. рисунок 101).

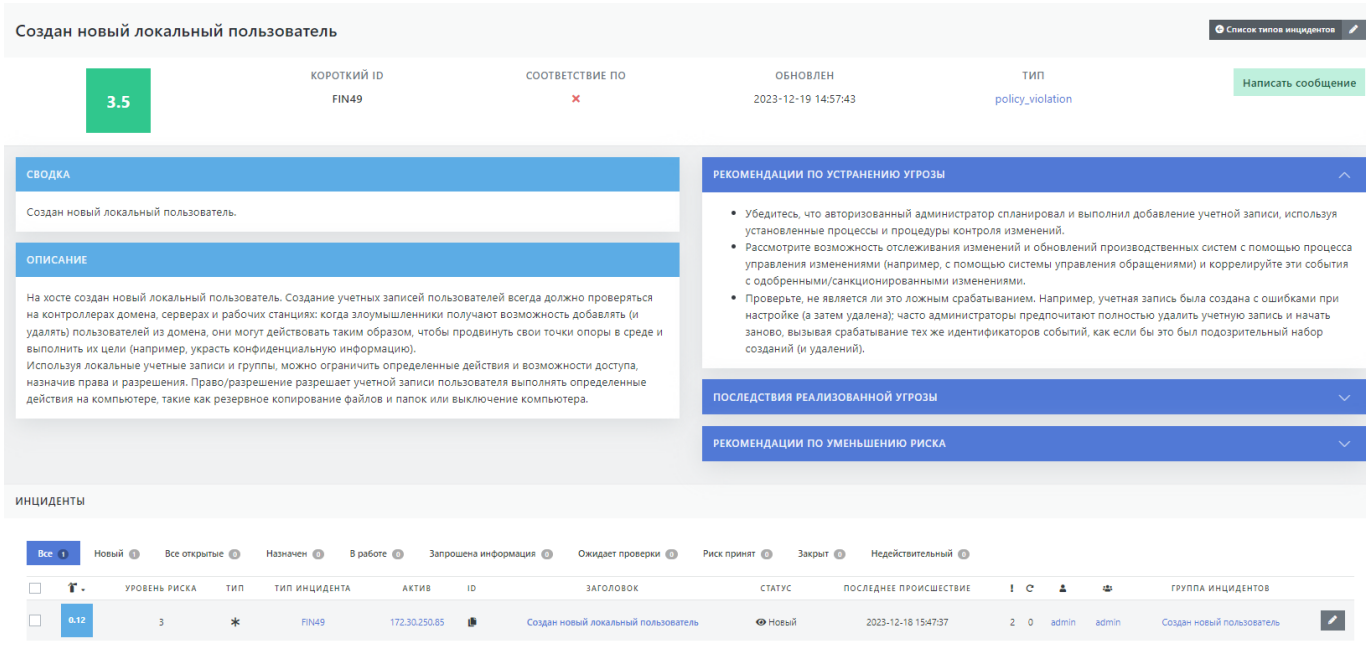



**Рисунок 101 – Детали по выбранному типу инцидентов**

Карточка типа инцидента состоит из следующих информационных блоков:

- Сводная информация по типу - верхняя часть экрана;
- Блок описания - содержит информацию по происшествиям, зафиксированным в рамках одного инцидента;
- Блок рекомендаций - содержит различные рекомендации по данному типу угроз;
- Блок "**Инциденты**" - содержит текущий список инцидентов данного типа.

### 13.2.2.2 Блок сводной информации по типу инцидента

Блок сводной информации содержит следующие данные по типу инцидента (см. рисунок 101):

- Полное название инцидента в **Платформе Радар** - верхняя строка карточки;
- Оценка риска - оценка риска по умолчанию для инцидентов данного типа. Предлагается при создании инцидента и может быть изменена пользователем для отдельных инцидентов;
- **Короткий ID** - короткий идентификатор типа инцидента, устанавливаемый **Платформой Радар**;
- **Соответствие ПО** - флаг использовать/не_использовать тип для создания инцидентов при оценке соответствия ПО; .
- **Обновлен** - дата и время последнего обновления (создания) типа инцидента;
- **Категория** - категория типа инцидента. Возможно одно из следующих значений:
    - Нарушение политики - гиперссылка *"policy_violation"*, открывает список инцидентов, относящихся к данной категории;
    - Сетевая аномалия - гиперссылка "*network_anomaly*", открывает список инцидентов, относящихся к данной категории;

- Уязвимость - гиперссылка *"policy_violation"*, открывает список инцидентов, относящихся к данной категории.

Помимо перечисленных параметров в блоке сводной информации присутствуют следующие функции:

- **Редактировать** - при нажатии на кнопку открывается страница редактирования параметров типа инцидента. Подробное описание редактирования приведено в разделе «Редактирование параметров типа инцидента»;
- **Написать сообщение** - при нажатии на кнопку открывается стандартное окно **Платформы Радар** для создания и отправки сообщения. Подробное описание отправки сообщений приведено в разделе документа «Отправка сообщений со ссылкой на тип инцидента».

### 13.2.2.3 Блок описания

Блок описания - это информационный блок, который содержит следующие поля (см. рисунок 102):

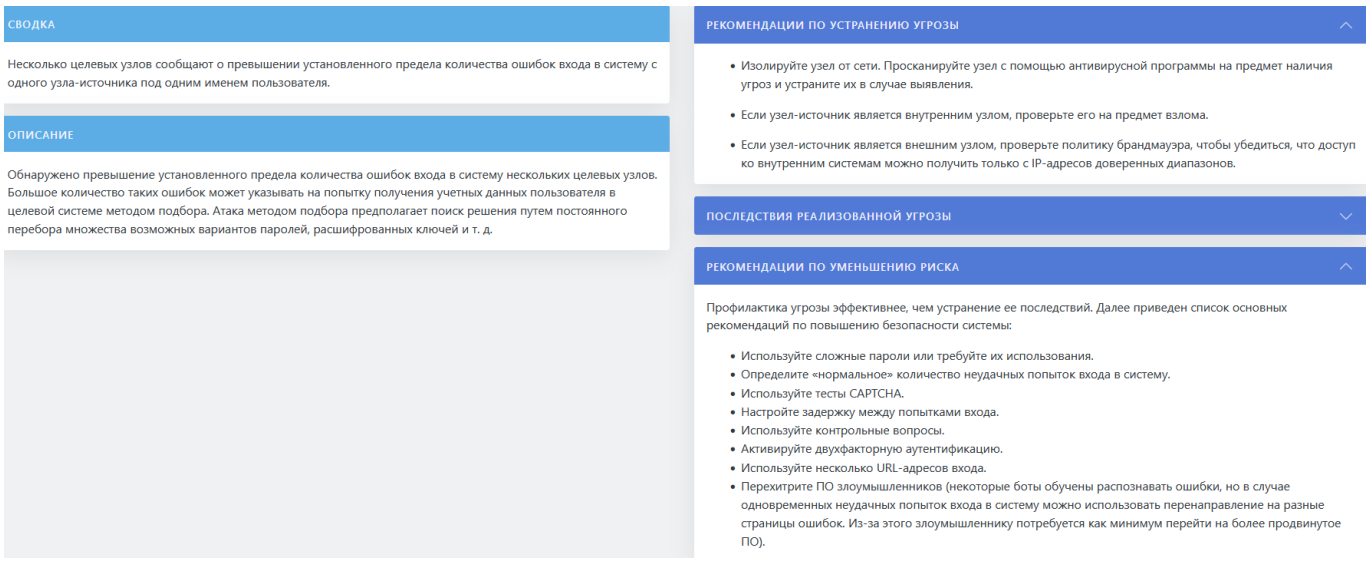



**Рисунок 102 – Описание угрозы и рекомендации по ее устранению на карточке типа инцидента**

- **Сводка** - краткое описание действий, спровоцировавших инцидент;
- **Описание** - описание причины, по которой данные действия были причислены к разряду инцидентов.

### 13.2.2.4 Блок рекомендаций

Блок рекомендаций - это информационный блок, который содержит следующие поля (см. рисунок 102):

- **Рекомендации по устранению угрозы** - блок содержит набор рекомендаций по устранению угрозы.
- **Последствия реализованной угрозы** - блок содержит перечень последствий реализации угрозы.
- **Рекомендации по уменьшению риска** - блок содержит набор рекомендаций по уменьшению риска возникновения угрозы данного типа.

Текст в каждом из полей блока рекомендаций можно при необходимости скрыть или развернуть используя функцию ( ) в заголовке поля.

#### 13.2.2.5 Блок "Инциденты"

Блок "**Инциденты**" содержит стандартный табличный инцидентов, состоящий только из инцидентов данного типа.

Полное описание табличного списка инцидентов приведено в разделе «Инциденты».

Подробное описание работы со списком инцидентов приведена в разделе «Работа с инцидентами.

# 13.3 Управление базой знаний типов инцидентов

## 13.3.1 Создание нового типа инцидента вручную

База знаний центра реагирования должна постоянно расширяться. Помимо получения постоянных обновлений со стороны разработчиков **Платформы Радар** существует возможность самостоятельного расширения базы знаний вручную.

Для создания нового типа инцидента необходимо:

1. Перейти в раздел ***Инциденты - Типы инцидентов***;
2. Нажать на кнопку "**Создать**";
3. В открывшейся форме с параметрами типа инцидента заполнить соответствующие поля (см. рисунок 103):

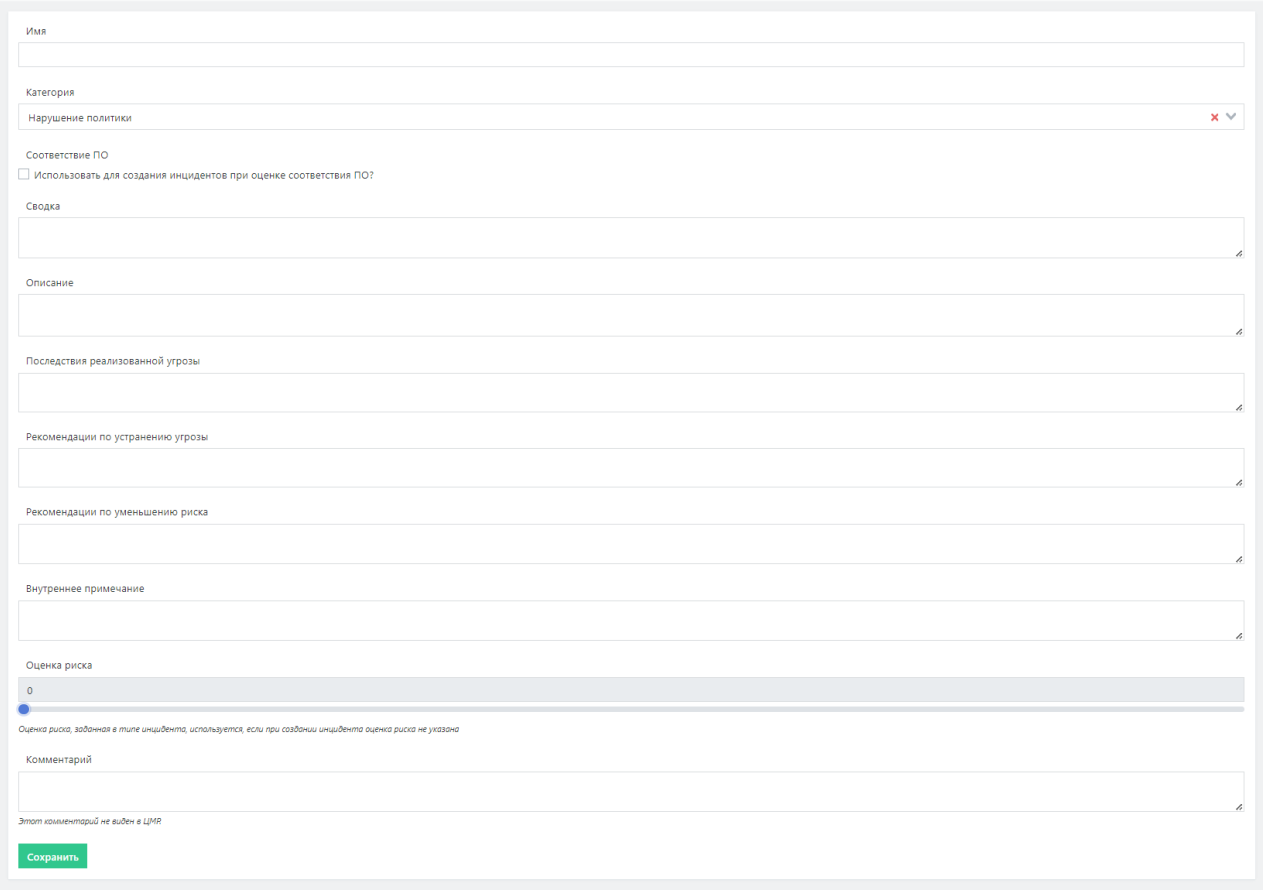



**Рисунок 103 – Форма для создания нового объекта "Тип инцидента"**

Подробное описание используемых при создании типа полей приведено в разделе «Просмотр детализации типа инцидента».

4. Нажать на кнопку "**Сохранить**".

На экране откроется обновленный табличный список типов.

## 13.3.2 Редактирование параметров типа инцидента

### 13.3.2.1 Доступ к функции редактирования

**Внимание**! *Функция редактирования доступна пользователю только при наличии необходимых прав доступа*.

Функция редактирования параметров типа инцидента доступна:

- на экране со списком типов : ***Инциденты - Типы инцидентов***;
- на карточке инцидента: ***Инциденты - Типы инцидентов - /щелкнуть по заголовку интересующего типа инцидента в списке/***.

### 13.3.2.2 Перечень редактируемых параметров

В случае необходимости можно отредактировать такие параметры типа инцидента как:

- значение уровня риска (**Оценка риска**) по умолчанию для типа инцидента;
- **Имя** типа инцидента в **Платформе Радар**;
- поменять **Категорию** угрозы для данного типа инцидента;
- поменять статус "**Использовать тип для создания инцидентов при оценке соответствия ПО?**";
- параметры описания типа инцидента, такие как:
    - **Сводка** - краткое описание действий, спровоцировавших инцидент;
    - **Описание угрозы** - описание причины, по которой данные действия были причислены к разряду инцидентов;
    - **Рекомендации по устранению угрозы** - набор рекомендаций по устранению угрозы;
    - **Последствия реализованной угрозы** - перечень последствий реализации угрозы;
    - **Рекомендации по уменьшению риска** - набор рекомендаций по уменьшению риска возникновения угрозы данного типа;
    - **Внутреннее примечание**;
    - **Комментарий**.

### 13.3.2.3 Проведение редактирования

Редактирование параметров типа инцидента необходимо в случае, если в описании типа есть неточности, выявленные аналитиком или у аналитика есть дополнительные сведения, требующие фиксации в контексте типа инцидента.

Для проведения редактирования необходимо:

1. Открыть окно редактирования одним из следующих способов:
    - Открыть список инцидентов ***Инциденты - Типы инцидентов***, и нажать в строке типа, требующего модификации, на кнопку  ;
    - Открыть карточку типа инцидента, требующего модификации ***Инциденты - Типы инцидентов -> /щелкнуть по заголовку интересующего типа в списке/***, и нажать на кнопку "**Редактировать**", расположенную в блоке сводной информации карточки.
2. В открывшейся форме редактирования параметров типа инцидента внести необходимые изменения (см. рисунок 104);
3. Для сохранения изменений нажать на кнопку "**Сохранить**".

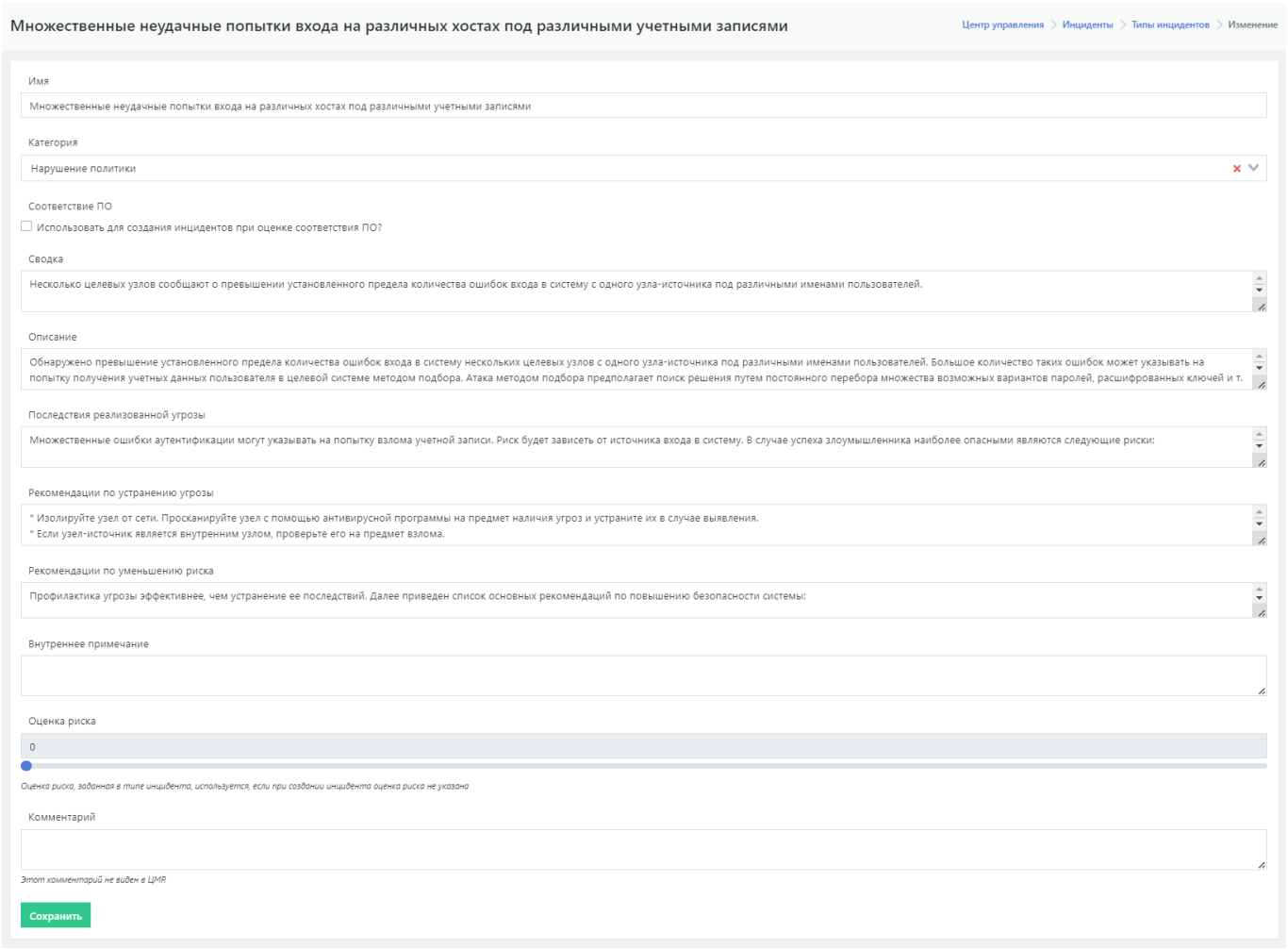



**Рисунок 104 – Окно редактирования выбранного типа инцидента**

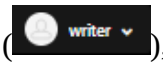
## 13.3.3 Отправка сообщений со ссылкой на тип инцидента

При работе с базой знаний пользователь может отправить текстовое сообщение другому пользователю **Платформы Радар**. Для этого необходимо:

1. Открыть карточку типа инцидента: ***Инциденты - Типы инцидентов -> /щелкнуть по заголовку интересующего типа в списке/***;

2. Нажать на кнопку "**Написать сообщение**";
3. В открывшейся форме сообщения заполнить следующие поля:
    - **Получатель** - выбрать адресата из раскрывающегося списка пользователей **Платформы Радар**;
    - **Заголовок** - ввести заголовок сообщения;
    - **Сообщение** - ввести текст сообщения.
4. Нажать на кнопку "**Отправить**".

При отправке к сообщению будет автоматически прикреплена ссылка на данную карточку типа инцидента.

Отправленное из карточки типа сообщение отобразится в списке отправленных сообщений пользователя. Список отправленных сообщений пользователя расположен в профиле пользователя ( 

), в разделе "**Сообщения**".

Подробное описание работы пользователя с сообщениями приведено в разделе документации «Работа с сообщениями».

### 13.3.4 Создание вручную инцидента указанного типа

На карточке типа под списком инцидентов данного типа расположена функция создания инцидента - кнопка "**Создать инцидент**" (см. раздел «Просмотр детализации типа инцидента»). Данная функция позволяет создать вручную инцидент того типа, с карточки которого была активирована функция создания инцидента.

Полное описание создания приведено в разделе «Создание нового инцидента с карточки типа инцидента».

# 14. Работа с событиями

## 14.1 Общие данные

**Внимание!** *Раздел "**Просмотр событий**" доступен только пользователям с соответствующими правами на просмотр событий.*

Раздел "**Просмотр событий**" предназначен для поиска, просмотра и анализа зафиксированных событий, вызвавших инцидент, включая сырые данные событий.

## 14.2 Первичная настройка вывода событий на экран

### 14.2.1 Проведение настройки

Для начала работы с событиями необходимо выполнить следующие действия:

1. В поле "**Время**" указать временной диапазон поиска. Подробное описание вариантов выбора временного интервала приведено в разделе «Особенности выбора временного интервала»;
2. В поле "**Индекс**" указать:
   - искомый индекс, например ElasticSearch, для поиска;
   - оставить «*» для поиска по всему кластеру данных.
3. Написать поисковый запрос или оставить поле пустым для просмотра всех событий;
4. Нажать на кнопку "**Поиск**".

На экране отобразятся в виде диаграммы данные по событиям, произошедшим за указанный временной период и отвечающие заданным фильтрам (см. рисунок 105). Также на экране отобразится список описаний по каждому найденному событию.

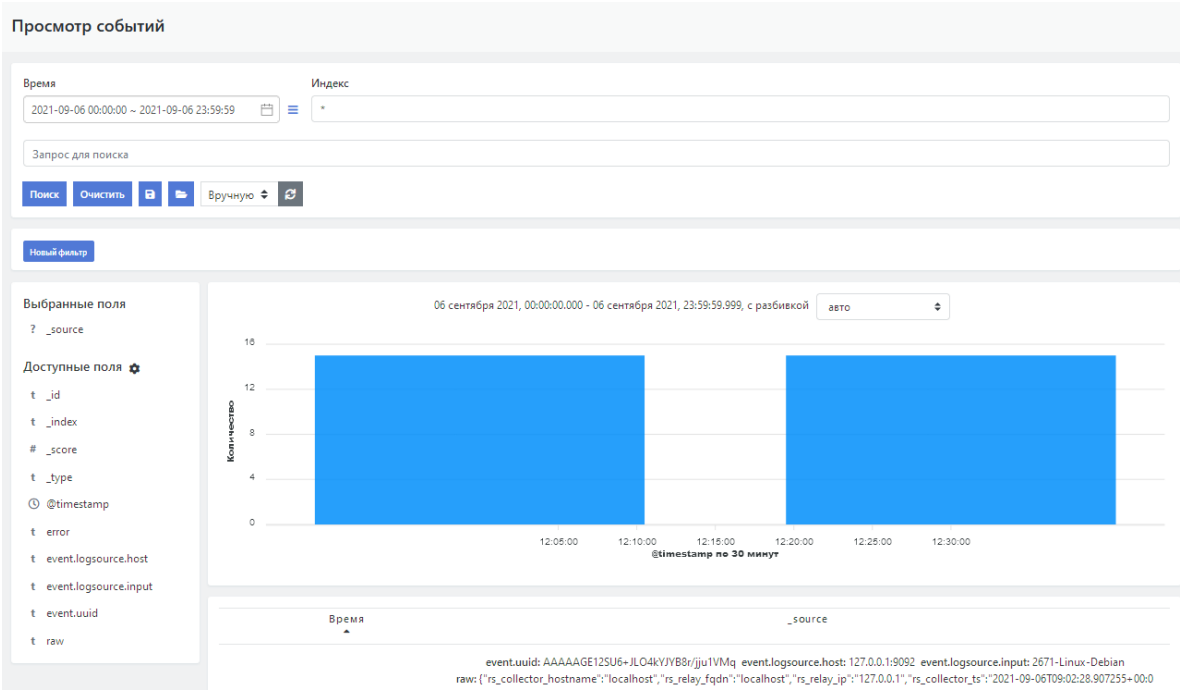



**Рисунок 105 – Результат поиска событий по заданным параметрам**

## 14.2.2 Управление фильтрами настройки просмотрщика

Для сброса всех фильтров настройки просмотрщика - нажать на кнопку "**Очистить**".

Настроенный набор фильтров можно сохранить для последующего использования - кнопка "**Сохранить**".

Для использования ранее созданного и сохраненного набора фильтров - нажать на кнопку "**Загрузить**".

## 14.2.3 Настройка обновления данных

В поле фильтров расположена функция настройки обновления данных - поле с пиктограммой (  ). По умолчанию устанавливается режим ручного обновления. Обновление вручную производится при нажатии на пиктограмму.

Для автообновления выбрать временной интервал обновления в раскрывающемся списке (см. рисунок 106).

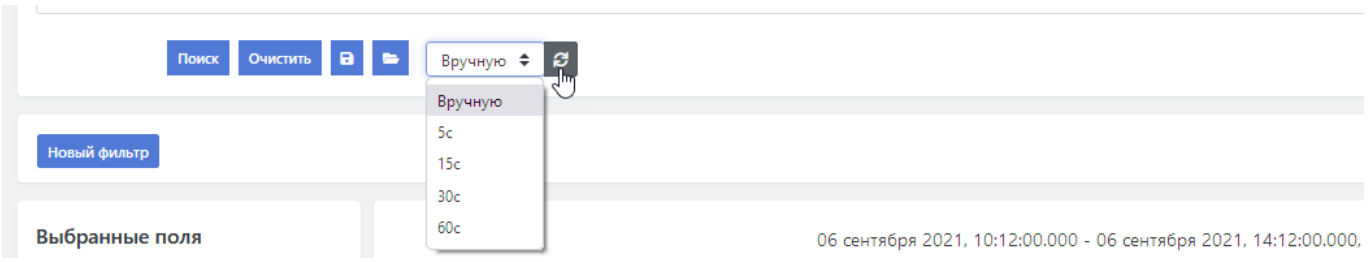



**Рисунок 106 – Настройка обновления данных**

## 14.2.4 Особенности выбора временного интервала

### 14.2.4.1 Быстрый выбор дат

"**Просмотр событий**" позволяет установить время по предустановленным временным интервалам (быстрый выбор дат).

Для настройки времени по предустановленному временному интервалу необходимо нажать на пиктограмму (  ) слева от поля "**Время**".

Откроется двухуровневый список "**Быстрый выбор дат**", включающий следующие предустановленные временные интервалы (см. рисунок 107):

- **Текущие**:
  - Текущая минута;
  - Текущий час;
  - Текущий день;
  - Текущая неделя;
  - Текущий месяц;
  - Текущий год.
- **Последние** - перечень последних используемых в сеансе точных временных интервалов (см. раздел "Точная настройка временного интервала").

- **Минуты**:
    - Прошлая минута;
    - Прошлые 3 минуты;
    - Прошлые 5 минут;
    - Прошлые 10 минут;
    - Прошлые 15 минут;
    - Прошлые 30 минут.
- **Часы**:
    - Прошлый час;
    - Прошлые 2 часа;
    - Прошлые 3 часа;
    - Прошлые 6 часов;
    - Прошлые 12 часов.
- **Дни**:
    - Прошлый день;
    - Прошлые 2 дня;
    - Прошлые 3 дня;
    - Прошлые 5 дней;
    - Прошлые 7 дней;
    - Прошлые 12 дней.
- **Месяцы**:
    - Прошлый месяц;
    - Прошлые 2 месяца;
    - Прошлые 3 месяца;
    - Прошлые 6 месяцев.
- **Года**:
    - Прошлый год;
    - Прошлые 2 года;
    - Прошлые 3 года.

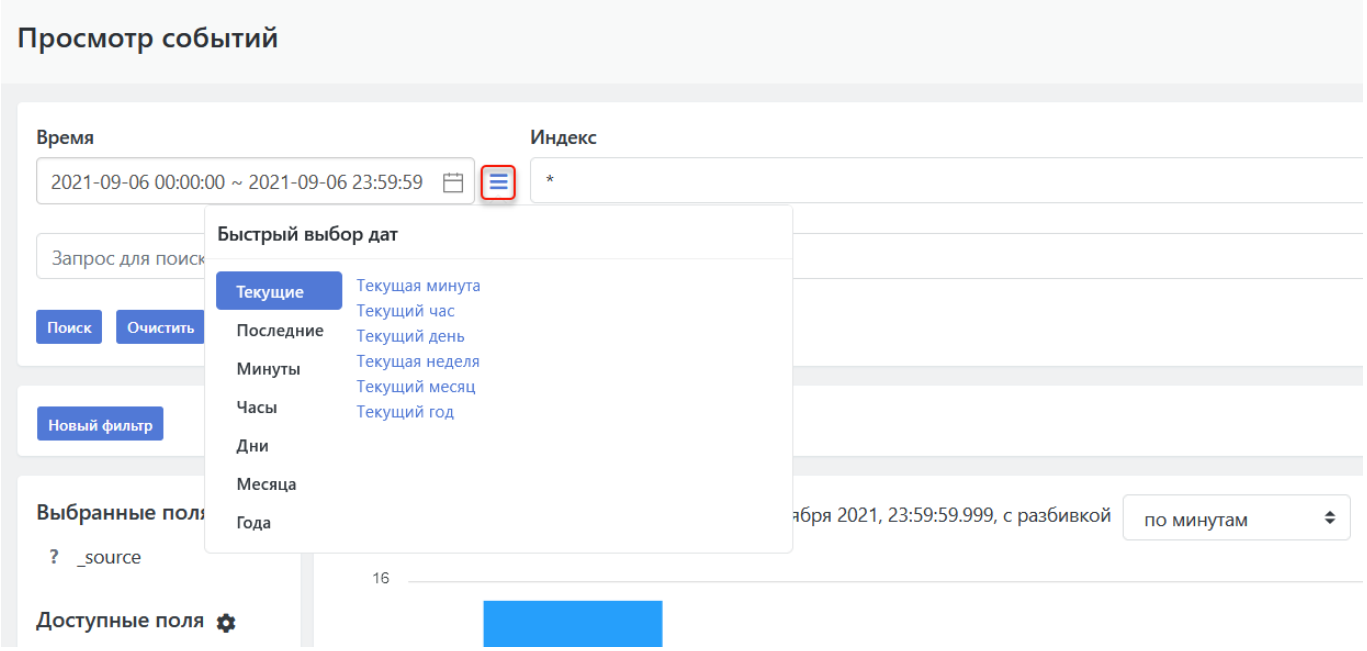



**Рисунок 107 – Выбор предустановленного временного интервала для поиска событий**

### 14.2.4.2 Точная настройка временного интервала

При необходимости можно настроить точный временной интервал для вывода событий. Для этого необходимо:

1. Щёлкнуть по полю "**Время**";
2. В открывшемся календаре выбрать дату начала и дату конца временного диапазона (см. рисунок 108). Если необходимо указать один день, то два раза щелкнуть по нужному дню;

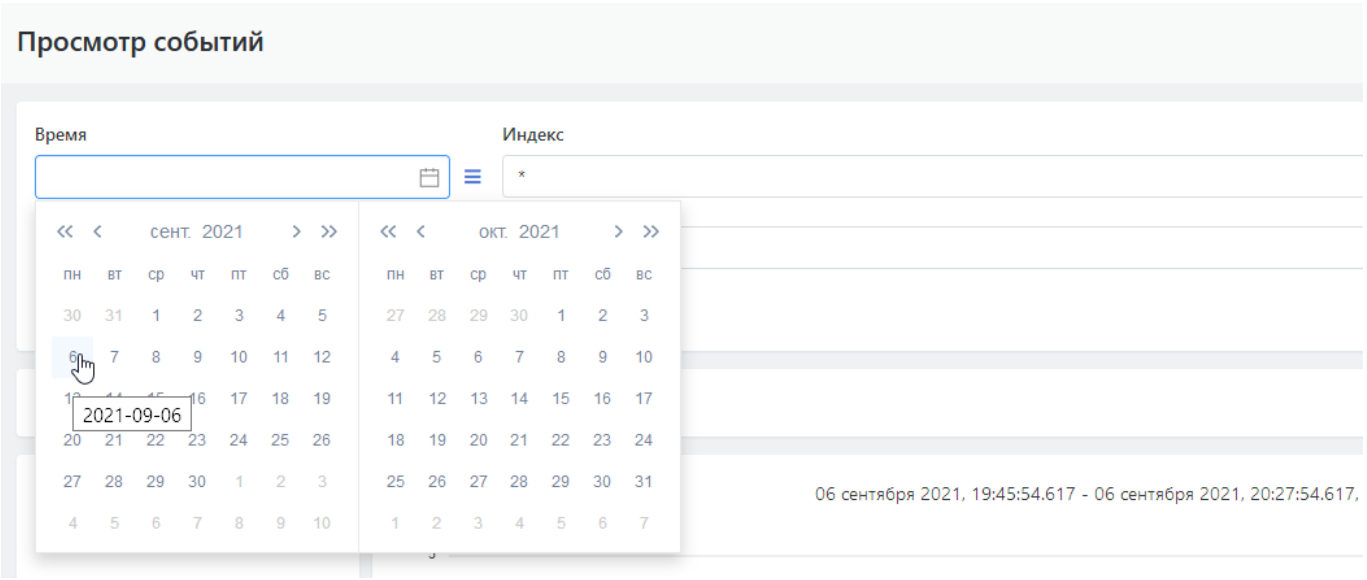



**Рисунок 108 – Установка дат начала и конца временного интервала для поиска событий**

3. После установки дат откроется панель выбора времени в формате ЧЧ.ММ.СС для даты начала и конца временного интервала. Установить время для дат начала и конца временного интервала (см. рисунок 109);

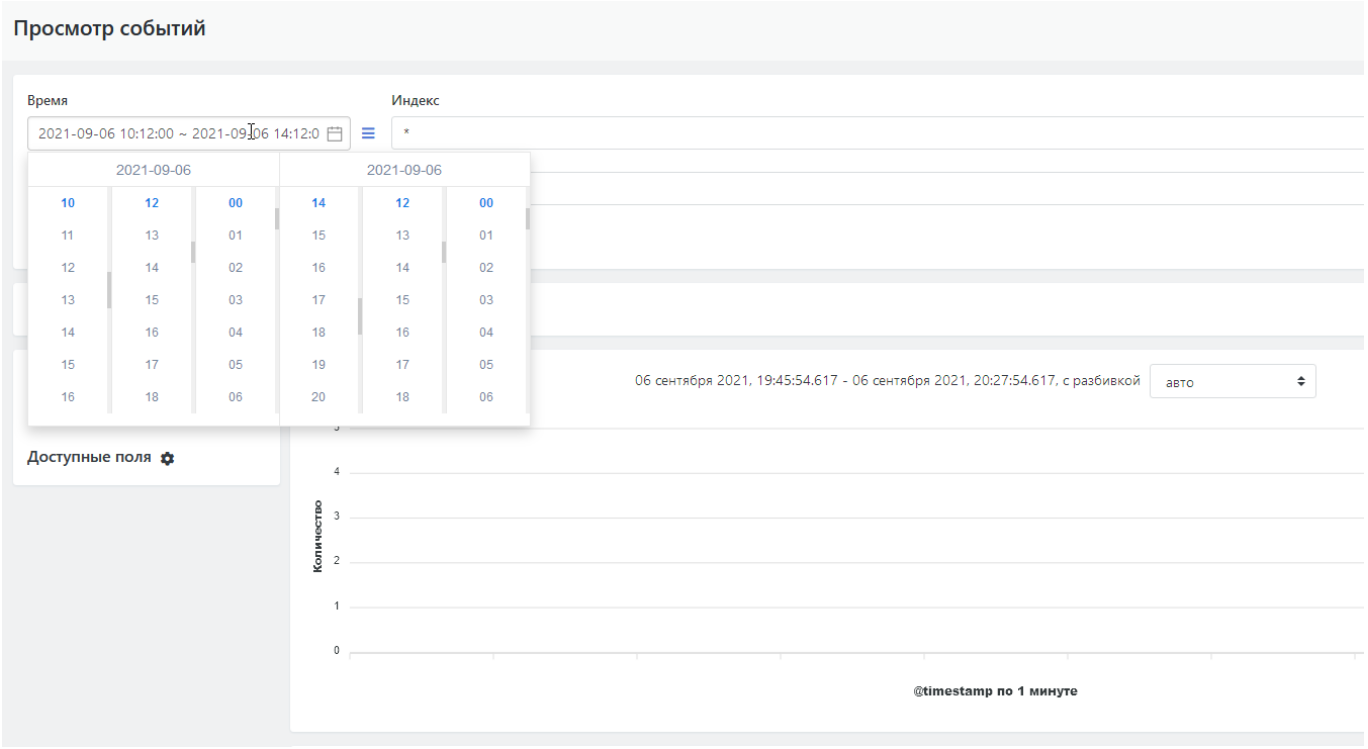



**Рисунок 109 – Установка времени для дат начала и конца временного интервала для поиска событий**

# 14.3 Анализ событий

## 14.3.1 Настройка просмотра временной диаграммы событий

На диаграмме отображается количество событий, зафиксированных за указанный временной интервал. События на диаграмме сгруппированы по заданным временным интервалам. Например: при выборе временного интервала группировки событий "**по часам**" в списке, расположенном в заголовке диаграммы, столбик диаграммы будет отображать события, зафиксированные в течение 1 часа (см. рисунок 110).

Если в списке выбрать значение "**по минутам**", то те же события будут отображаться на диаграмме в виде столбиков, в которых события сгруппированы по минутным интервалам (см. рисунок 111).

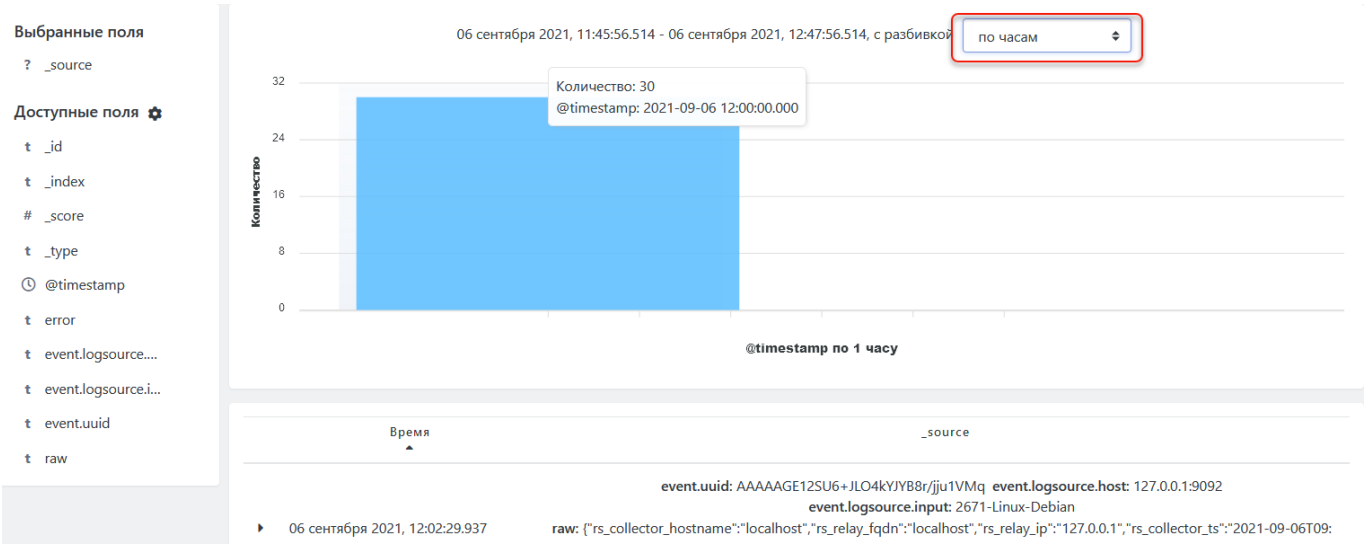



**Рисунок 110 – Пример вывода данных о событиях с разбивкой по часам**

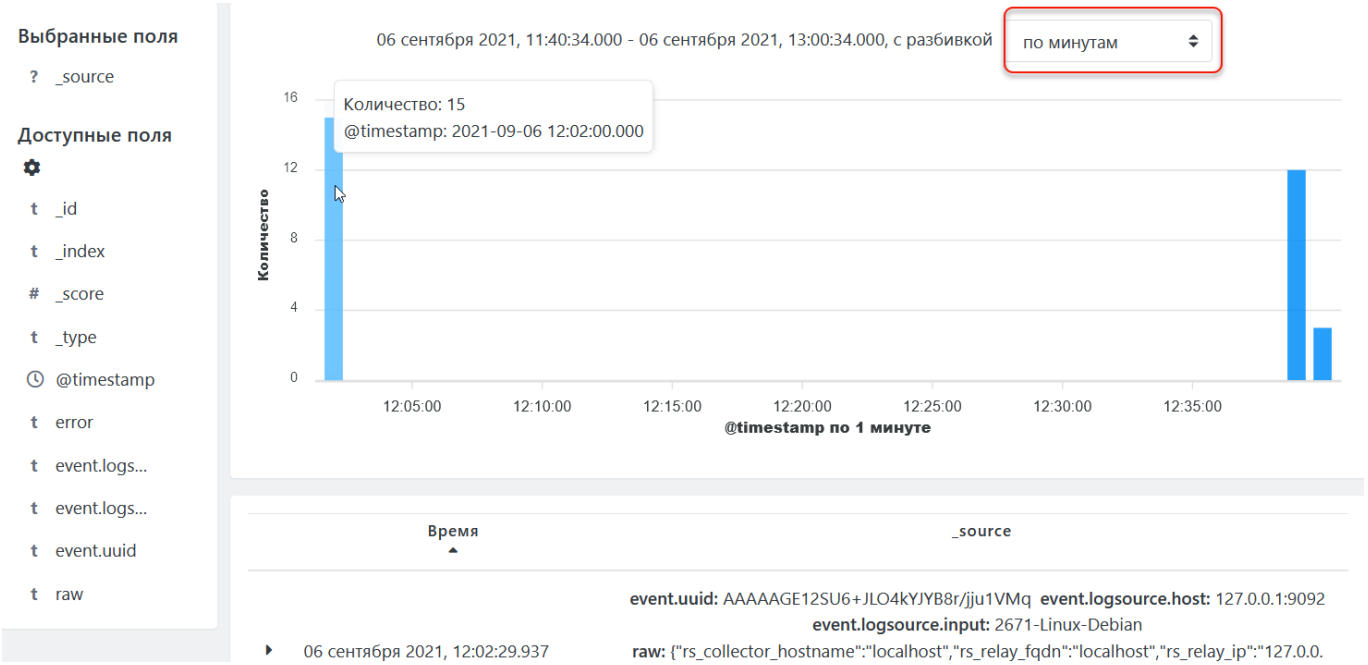



**Рисунок 111 – Пример вывода данных о событиях с разбивкой по минутам**

В списке выбора временных интервалов для группировки событий можно выбрать следующие типы разбивки:

- авто (система сама подбирает временной интервал группировка для событий в заданном диапазоне);
- по миллисекундам;
- по секундам;
- по минутам;
- по часам;
- по дням;
- по неделям;
- по месяцам;
- по годам.

При наведении курсора мыши на столбик диаграммы всплывет окно с параметрами (см. рисунки 110 и 111):

- количество событий, произошедших за заданный интервал времени для группировки событий;
- начальное значение установленной временной отсечки.

## 14.3.2 Настройка полей табличного списка событий

### 14.3.2.1 Список событий по умолчанию

Под диаграммой расположен табличный список событий, произошедших в заданном диапазоне времени.

По умолчанию данный список содержит следующие поля:

- Поле "**Время**" - дата и время когда произошло событие;
- Поле "**_source**" - содержит набор параметров.

Для табличного списка событий можно настроить набор полей (параметров), выводимых на экран. Список доступных для вывода на экран параметров отображен слева от диаграммы в области "**Доступные поля**" (см. рисунок 112).

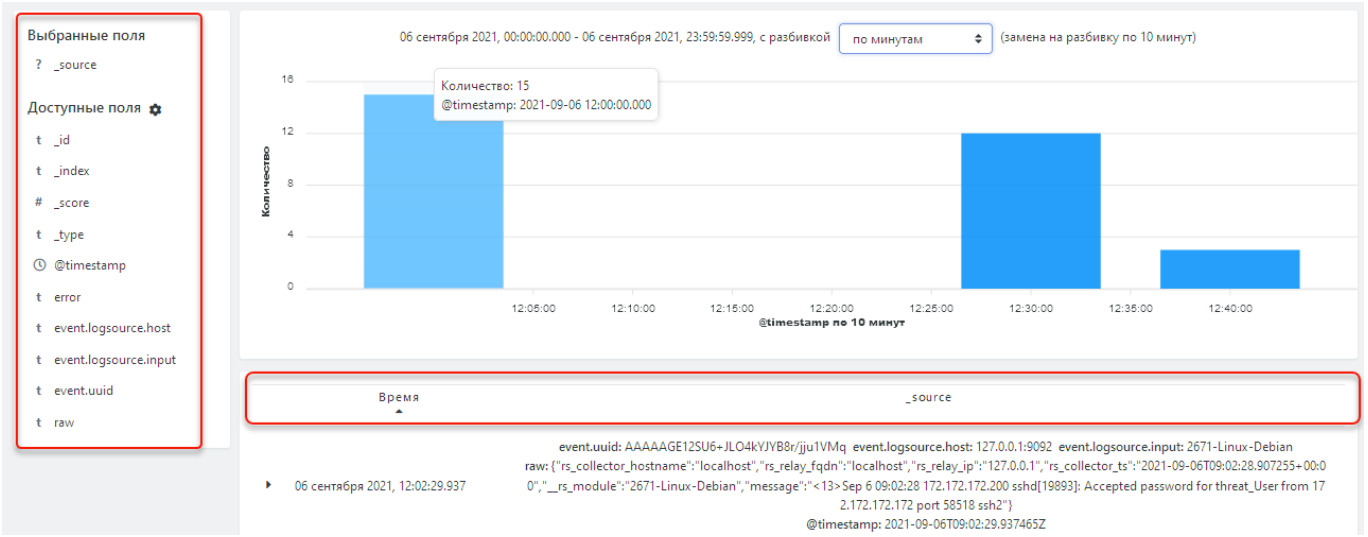



**Рисунок 112 – Список событий по умолчанию**

### 14.3.2.2 Добавление нового поля (параметра) в табличный список событий

Для включения параметра в список событий необходимо:

1. В блоке "**Доступные поля**" навести курсор на интересующий параметр;
2. Нажать на кнопку (+), появившуюся при наведении курсора справа от названия параметра (см. рисунок 113).

Выбранный параметр будет добавлен в виде поля к табличному списку событий.

Также данный параметр отобразится слева от диаграммы в области "**Выбранные поля**" (см. рисунок 113).

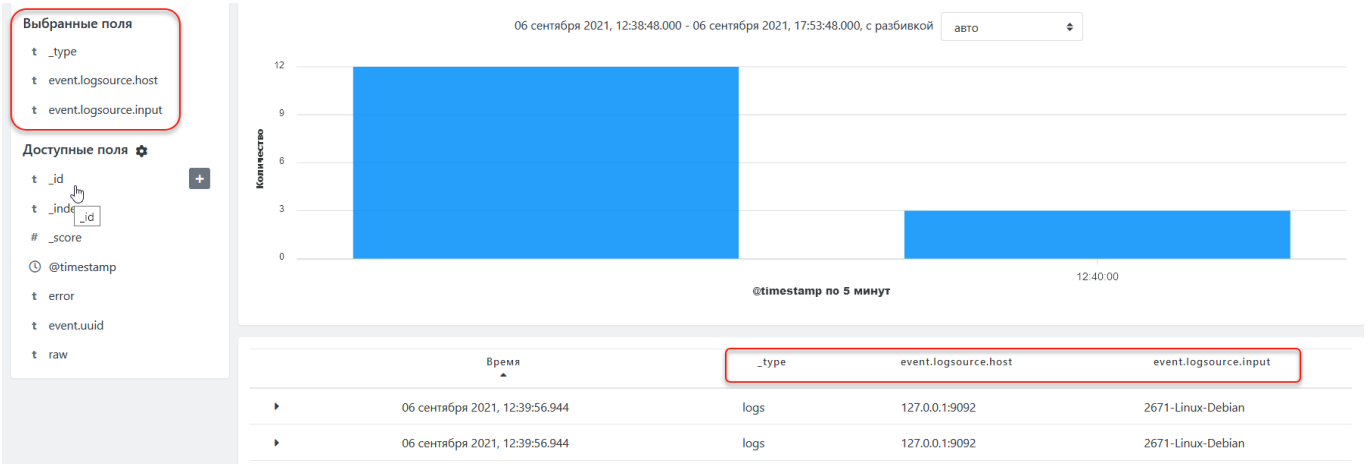



**Рисунок 113 – Настройка полей табличного списка событий**

#### 14.3.2.3 Удаление поля (параметра) из табличного списка событий

Для исключения параметра из списка событий необходимо:

1. В блоке "**Выбранные поля**" навести курсор на интересующий параметр;
2. Нажать на кнопку ( ), появившуюся при наведении курсора справа от названия параметра.

Поле с данным параметром будет удалено из табличного списка событий.

Также данный параметр отобразится слева от диаграммы в области "**Доступные поля**".

Исключить параметр из списка можно непосредственно в самом списке:

1. Навести курсор на название поля в списке, которое необходимо удалить;
2. Нажать на появившийся значок удаления ( ) (см. рисунок 114).

Выбранное поле будет удалено из списка. Соответствующий ему параметр буде перенесён из области "**Выбранные поля**" в область "**Доступные поля**".


**Рисунок 114 – Удаление поля из списка событий**

### 14.3.3 Фильтрация списка событий

#### 14.3.3.1 Условия фильтрации, применяемые для списка событий

Для фильтрации списка событий могут применяться следующие условия:

- "**равен**" - фильтрация по указанному значению параметра. Формируется список событий, у которых данный параметр содержит такое же значение.
- "**не равен**" - фильтрация по указанному значению параметра. Формируется список событий, у которых данный параметр содержит значения отличные, от указанного.
- "**один из**" - фильтрация по набору значений параметра. Формируется список событий, у которых данный параметр содержит значение из заданного набора.
- "**не один из**" - фильтрация по набору значений параметра. Формируется список событий, у которых данный параметр содержит значения, не совпадающие с указанным набором.
- "**существует**" - фильтрация по наличию у события указанного параметра. Формируется список событий, у которых данный параметр используется .
- "**не существует**" - фильтрация по отсутствию у события указанного параметра. Формируется список событий, у которых данный параметр не используется.

#### 14.3.3.2 Настройка фильтрации событий в списке по значению поля

Табличный список событий содержит встроенные средства фильтрации списка.

В строке сообщения при наведении курсора на значение любого поля справа появятся пиктограммы создания фильтра (см. рисунок 115):

- – вывести на экран только те сообщения, у которых значение в данном поле совпадает с указанным ("равен"). Например вывести на экран только события произошедшие "06 сентября 2021, 12:39:56:944" (см. рисунок 115);
- – вывести на экран только те сообщения, у которых значение в данном поле не совпадает с указанным ("не равен").

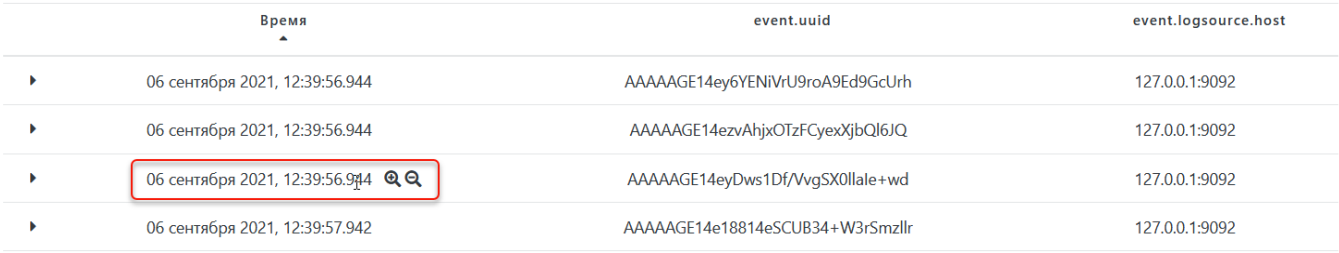



**Рисунок 115 – Встроенные средства фильтрации табличного списка по значению поля**

При необходимости, фильтрацию можно проводить последовательно по нескольким параметрам. Произведённые фильтрации отображаются в поле фильтра, расположенном над диаграммой, виде записей на каждую проведенную фильтрацию (см. рисунок 116).

В записи фильтра указываются название и значение параметра (либо название фильтра, если оно было задано), по которому провидится фильтрация, а так же цветовая градация:

- синий цвет записи - фильтрация по совпадению заданных в фильтре значений;
- красный цвет записи - фильтрация по несовпадению заданных в фильтре значений.

Результаты фильтрации так же отображаются на диаграмме (см. рисунок 116).

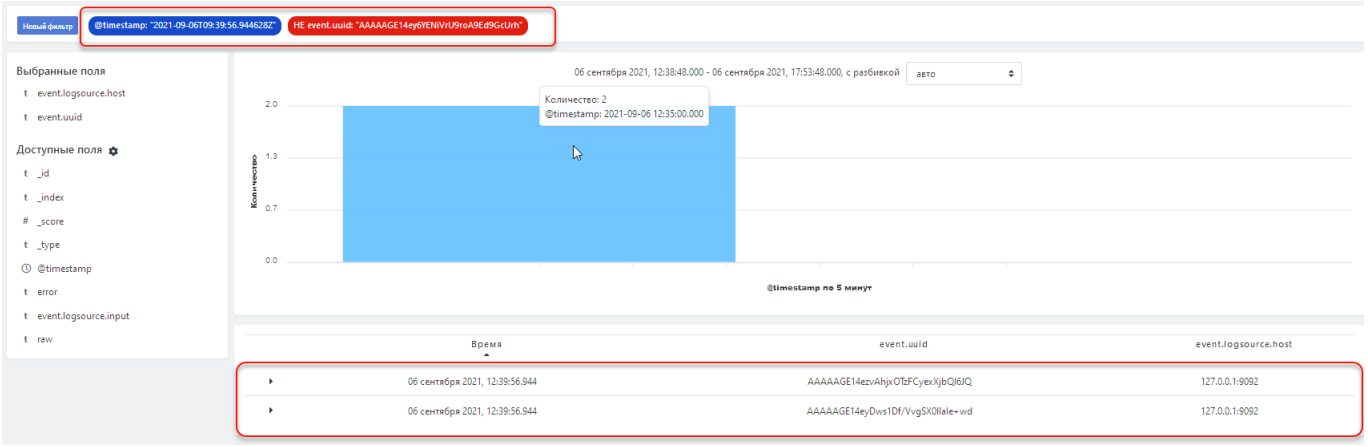



**Рисунок 116 – Пример отфильтрованного по двум условиям списка сообщений**

### 14.3.3.3 Снятие фильтра

Для снятия фильтра необходимо (см. рисунок 117):

1. Навести курсор на нужную запись в поле фильтров - на записи фильтра отобразится панель управления данным фильтром;
2. Нажать на пиктограмму "Удалить фильтр" - .

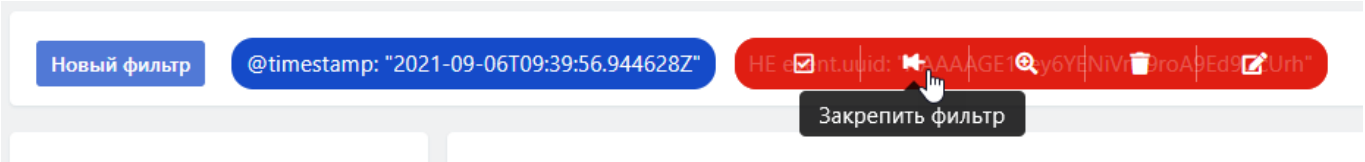



**Рисунок 117 – Управление фильтром**

### 14.3.3.4 Панель управления фильтром

Панель управления фильтром содержит следующие функции (см. рисунок 117):

- **Выключить (включить) фильтр** ( / ) - отключить действие данного фильтра на список. Сам фильтр остается доступен в поле фильтров и может быть задействован обратно;
- **Закрепить (открепить) фильтр** ( / ) - закрепить (открепить) запись фильтра в области фильтров;
- **Включить (исключить) совпадения** ( / ) - изменить действие фильтра на противоположное. Если фильтр работал по несовпадению, то после использования данной функции фильтр будет работать по совпадению значений поля;
- **Удалить фильтр** ( ) - отключить действие данного фильтра на список и удалить запись из поля фильтров;
- **Отредактировать фильтр** ( ) - открывает форму редактирования параметров фильтра. Может быть использована для создания нового фильтра на базе существующего.

### 14.3.3.5 Создание фильтра

Создать фильтр по списку сообщений можно вручную. Для этого необходимо:

1. Нажать на кнопку "**Новый фильтр**" в поле фильтров;
2. В открывшейся форме ввести следующие параметры (см. рисунок 118):
    - в строке "**Поле**" ввести название поля, по которому будет вестись фильтрация;
    - в раскрывающемся списке "**Вид фильтрации**" выбрать какой вид фильтрации будет применен (описание видов приведено в разделе «Условия фильтрации, применяемые для списка событий»);
    - указать значение поля по которому будет вестись отбор;
    - в строке "**Заголовок**" при необходимости укать название фильтра, под которым строка фильтра будет отображаться в области фильтрации.
3. Для сохранения и запуска фильтрации нажать на кнопку "**Добавить**".

В область фильтров добавляется запись о новом фильтре. Список событий фильтруется по новому условию.

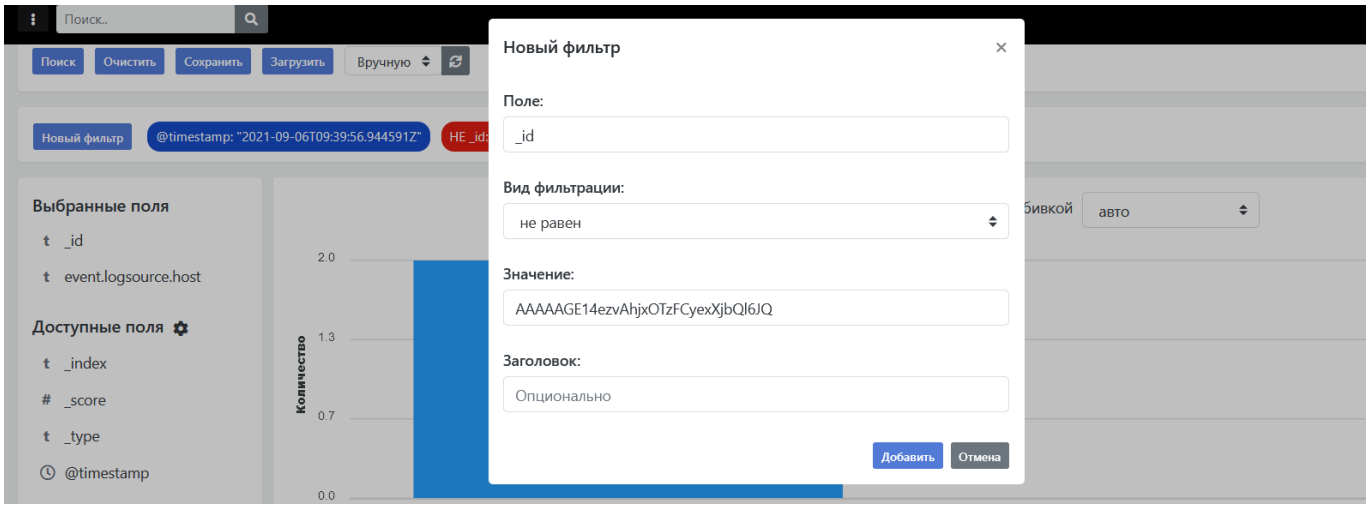



**Рисунок 118 – Создание нового фильтра вручную, редактирование фильтра**

### 14.3.3.6 Редактирование фильтра

Если нужно отредактировать параметры использующегося фильтра, необходимо:

1. Навести курсор на строку фильтра;
2. В появившейся панели управления фильтром выбрать функцию редактирования - . Откроется окно редактирования с параметрами фильтра по составу идентичное окну создания фильтра (см. рисунок 118);
3. Внести необходимые изменения в параметры фильтра;
4. Для сохранения изменений нажать на кнопку "**Добавить**".

## 14.3.4 Просмотр детализации события

### 14.3.4.1 Доступ к детализации события

По каждому событию из списка можно просмотреть детализацию, включая "сырые" данные.

Для просмотра детализации необходимо нажать на пиктограмму , расположенную в начале строки интересующего события.

Область детализации раскрывается непосредственно в списке под указанным событием (см. рисунок 119) и состоит из двух вкладок: "**Таблица**" (по умолчанию) и "**JSON**". Также в детализации доступна функция "**Найти инциденты**" .

### 14.3.4.2 Детализация события на вкладке "Таблица"

Вкладка "**Таблица**" содержит (см. рисунок 119):

- перечень всех параметров события;
- значения данных параметров;
- встроенные средства настройки и фильтрации табличного списка событий.

Встроенные средства фильтрации включают следующие функции:

- - создать новый фильтр по данному параметру и его значению, вид фильтрации "равно". Формируется список из событий, у которых данный параметр содержит такое же значение;
- - создать новый фильтр по данному параметру и его значению, вид фильтрации "не равно". Формируется список из событий, у которых данный параметр содержит значения отличные, от указанного;
- - создать новый фильтр по данному полю, вид фильтрации "существует". Формируется список из событий, у которых данный параметр.
- - добавить колонку с данным параметром в табличный список событий.

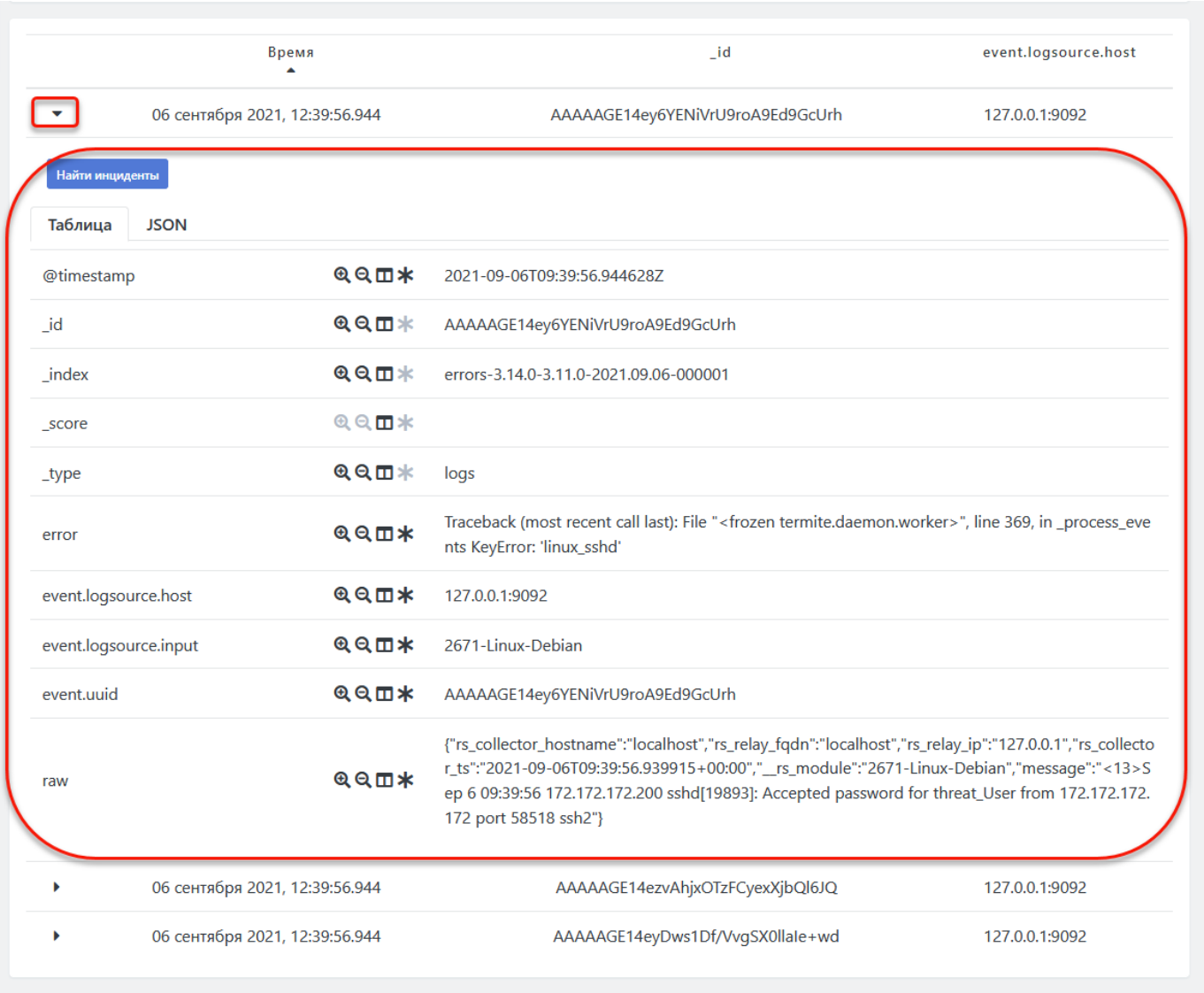



**Рисунок 119 – Область детализации события, вкладка "Таблица"**

### 14.3.4.3 Детализация события на вкладке "JSON"

Вкладка "**JSON**" содержит "сырые" данные события в формате JSON (см. рисунок 120).

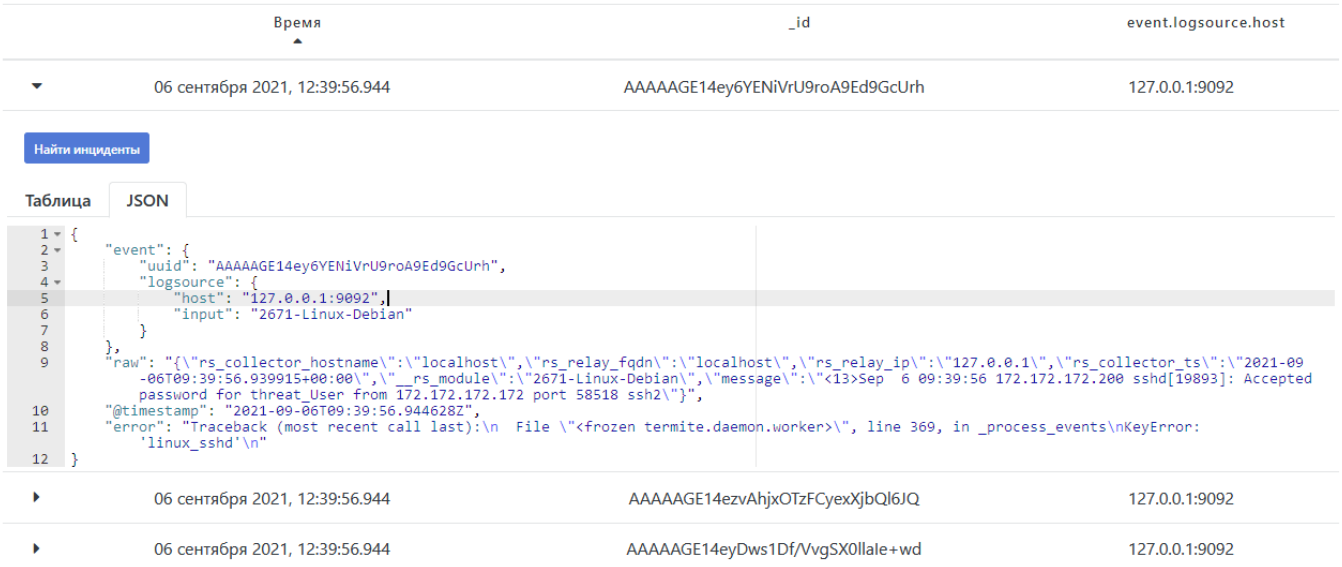



**Рисунок 120 – Просмотр данных события в формате JSON**

## 14.3.5 Создание инцидента из события

Для создания инцидента из событий необходимо выполнить следующие действия:

1. На любой из вкладок детализации ("**Таблица**" или "**JSON**") нажать на кнопку "**Найти инциденты**";
2. При нажатии на кнопку "**Найти инциденты**" будет произведен поиск событий среди созданных инцидентов и по результатам поиска предложены варианты (см. рисунок 121):
   - Перейти к просмотру инцидента;
   - Создание нового инцидента.

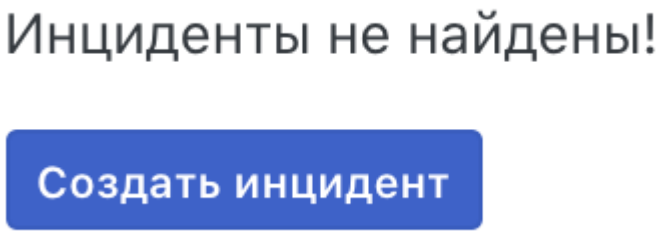



**Рисунок 121 – Создание инцидента из результатов поиска события**

3. Нажать на кнопку "**Создать инцидент**" (см. рисунок 121). Откроется форма создания инцидента (см. рисунок 122);
4. В открывшейся форме необходимо минимум заполнить следующие данные:
   - тип инцидента;
   - дополнительные поля, если есть необходимость переопределить поля по умолчанию в типе инцидента;
   - оценку риска.
5. Для создания инцидента нажать на кнопку "**Сохранить**".

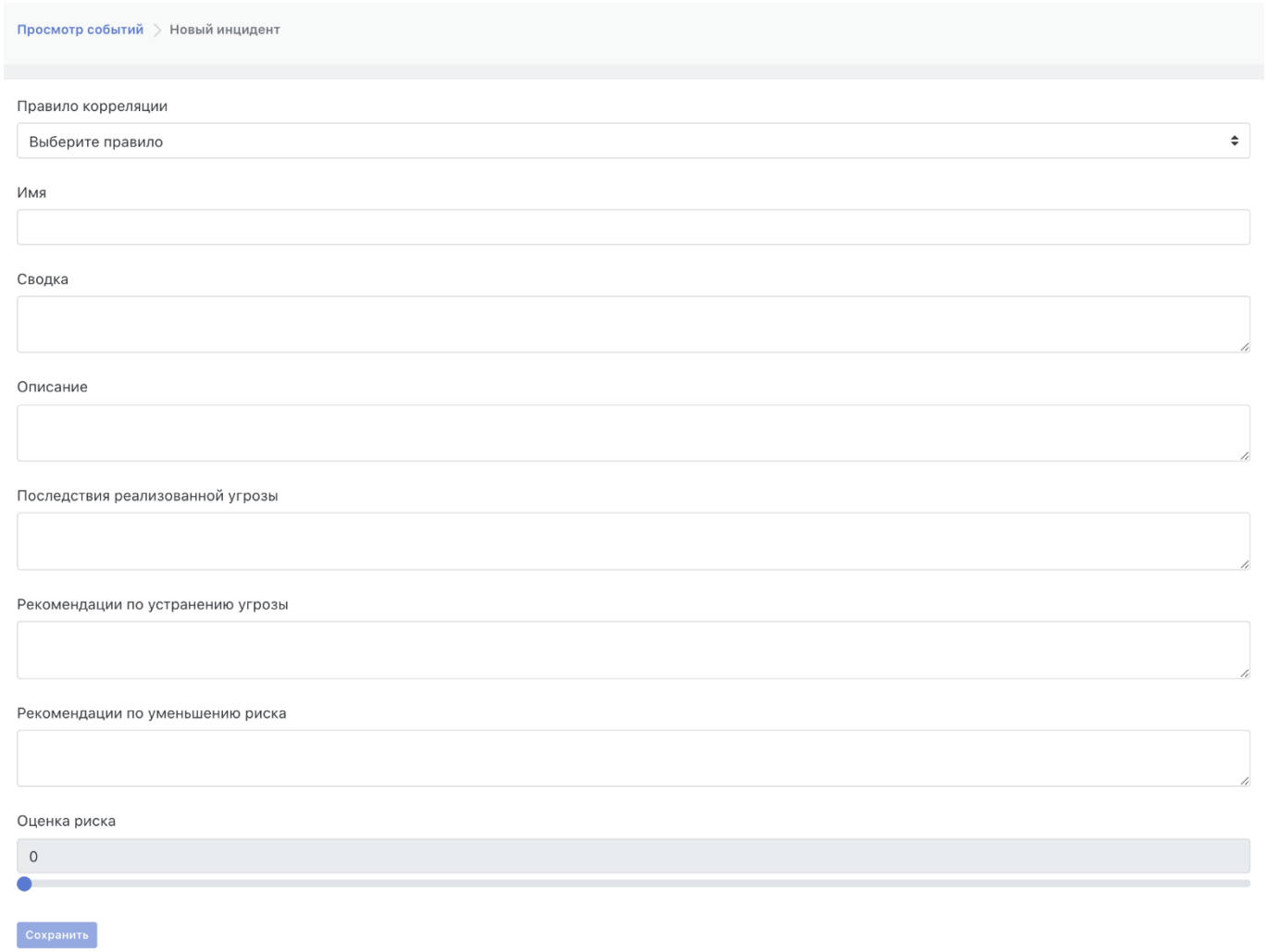



**Рисунок 122 – Форма создания инцидента из результатов поиска события**

# 15. Работа с активами

**Активом**, в рамках системы, называется сетевой хост (рабочая станция, сервер, сетевое устройство и т.д.). Активы идентифицируются по FQDN, IP-адресу или MAC-адресу (в зависимости от настроек).

Атрибуты актива:

- Имя актива - произвольная текстовая строка;
- Значимость актива - числовое значение 1 - 5:
    - 1 - ключевой актив. Актив в составе системы, обеспечивающей функционирование бизнеса;
    - 2 - важный актив. Актив в составе системы, требуемой для штатной работы компании;
    - 3 - нормальный актив. Значение по умолчанию;
    - 4 - распределенный или не критичный актив. Актив в составе распределенной системы или системы, не задействованной в ключевых бизнес-процессах;
    - 5 - тестовый актив. Актив, расположенный в тестовой среде. Недоступность данного актива не влияет на ключевые бизнес-процессы.
- Сетевая видимость - числовое значение 1 - 5:
    - 1 - прямое подключение к Интернет (межсетевой экран, сетевой балансировщик, VPN-сервер);
    - 2 - DMZ, частичный доступ из Интернет для некоторых сервисов (Web-сервер, Proxy);
    - 3 - штатный доступ в Интернет через Proxy (рабочие станции, внутренние сервера) - значение по умолчанию;
    - 4 - ограниченный доступ в Интернет, доступ к ограниченному набору Интернет-сервисов (тонкие клиенты, POS-терминалы, удаленные офисы);
    - 5 - актив, не подключенный к сети.
- Тип - текстовый идентификатор типа системы;
- Внутреннее примечание - примечание, отображаемое только в интерфейсе администратора;
- Описание - произвольное текстовое описание.

К активу может быть привязано несколько сетевых интерфейсов.

Для актива может быть задана группа ответственных, в этом случае при автоматическом создании инцидентов они будут назначаться данной группе ответственных.

Для удобства управления активы могут добавляться в группы активов.

## 15.1 Обнаружение активов

Существует несколько способов появления активов в системе:

- обработка результатов сканера уязвимостей;
- обработка результатов сетевого сканера;
- создание активов вручную;
- создание из результатов работы правил корреляции;

### 15.1.1 Создание активов из результатов сканера уязвимостей

Регулярная актуализация перечня активов по результатам работы сканера уязвимостей является основным методом создания новых активов в системе.

Подробнее описывается в разделе «Интеграция со сканерами уязвимостей».

### 15.1.2 Создание активов из результатов сетевого сканера

Регулярная актуализация перечня активов по результатам работы сетевого сканера является одним из основных методов создания новых активов в системе и их обновления.

Подробнее описывается в разделе «Работа с сетевым сканером и инвентаризацией».

### 15.1.3 Создание активов вручную

Создание актива вручную может потребоваться, если система не интегрирована со сканерами уязвимостей или актив не попадает в область сканирования, или сканирование сети невозможно по каким-то причинам.

Для создания нового актива необходимо:

- Перейти в раздел ***Активы - Активы***;
- Нажать кнопку "**Создать**";
- Заполнить поля карточки актива (см. рисунок 123):
    - **Имя актива**;
    - **Значимость актива** - числовое значение 1 - 5:
        - 1 - ключевой актив. Актив в составе системы, обеспечивающей функционирование бизнеса;
        - 2 - важный актив. Актив в составе системы, требуемой для штатной работы компании;
        - 3 - нормальный актив. Значение по умолчанию;
        - 4 - распределенный или не критичный актив. Актив в составе распределенной системы или системы не задействованной в ключевых бизнес-процессах;
        - 5 - тестовый актив. Актив, расположенный в тестовой среде. Недоступность данного актива не влияет на ключевые бизнес-процессы.
    - **Сетевая видимость** - числовое значение 1 - 5:

        - 1 - прямое подключение к Интернет (межсетевой экран, сетевой балансировщик, VPN-сервер);
        - 2 - DMZ, частичный доступ из Интернет для некоторых сервисов (Web-сервер, Proxy);
        - 3 - штатный доступ в Интернет через Proxy (рабочие станции, внутренние сервера) - значение по умолчанию;
        - 4 - ограниченный доступ в Интернет, доступ к ограниченному набору Интернет-сервисов (тонкие клиенты, POS-терминалы, удаленные офисы);
        - 5 - актив, не подключенный к сети.
    - **Тип** - текстовый идентификатор типа системы;
    - **Ответственное лицо**;
    - **Технические специалист**;
    - **Расположение**;
    - **Описание** - произвольное текстовое описание актива;
    - **Сетевые интерфейсы** из списка в системе. Если сетевой интерфейс актива отсутствует в списке его необходимо добавить;
- Нажать кнопку "**Сохранить**".

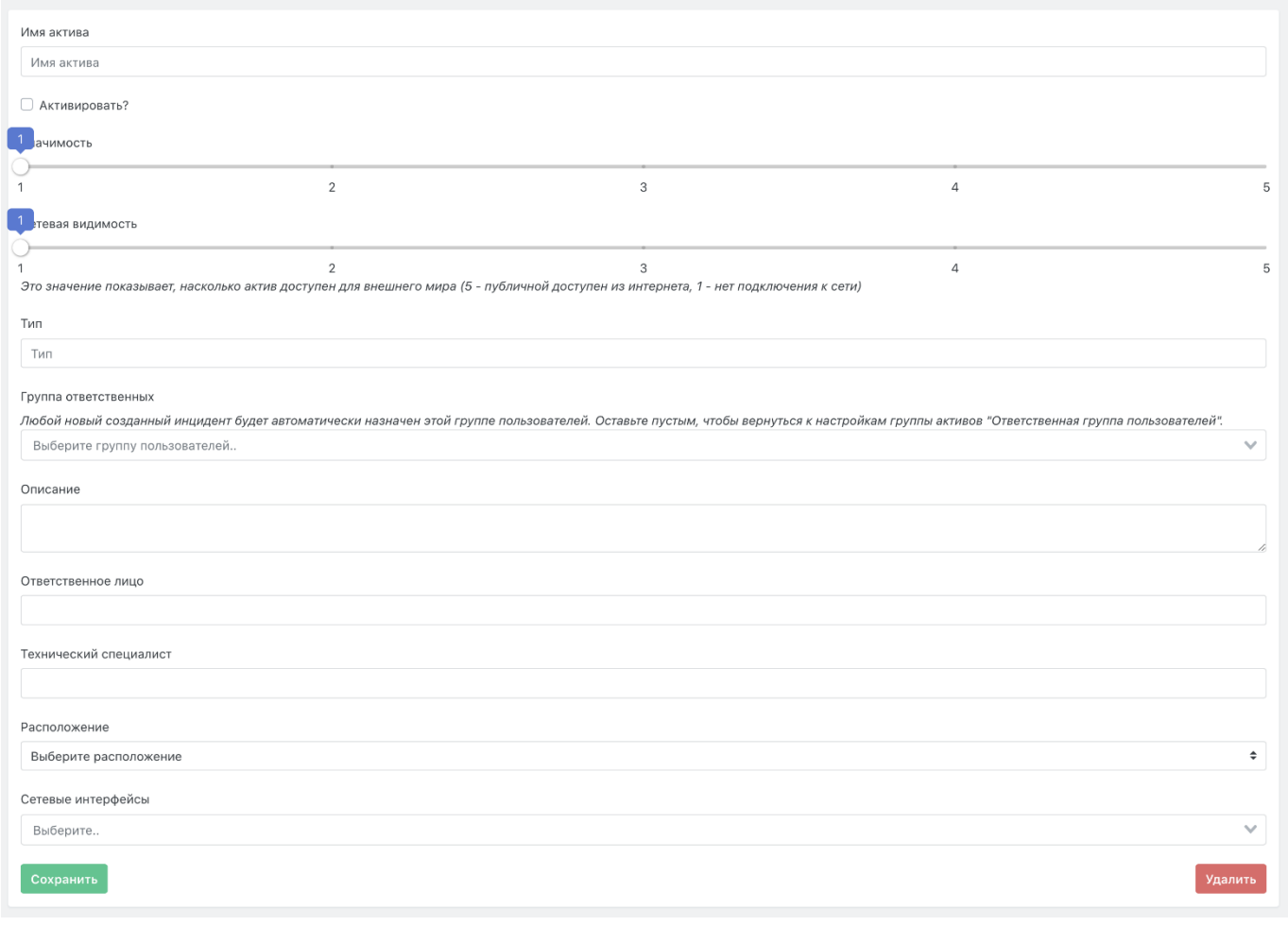



**Рисунок 123 – Окно создания актива**

### 15.1.4 Создание активов из результатов работы правил корреляции

В системе реализовано автоматическое создание активов по результатам работы правил корреляции.

Если правило корреляции создает инцидент на активе, идентификатор которого отсутствует в списке активов, система добавляет новый актив в список в состоянии "**Неактивен**".

### 15.1.5 Конфигурирование стратегий идентификации активов

Идентификация активов требуется системе для понимания, к какому активу отнести новые инциденты - к существующему или требуется создать новый актив.

В качестве идентификаторов актива могут выступать: FQDN, IP-адрес и MAC-адрес. В системе можно сконфигурировать различные политики идентификации для различных сетевых сегментов. Помимо этого, в системе задается глобальная политика идентификации, которая применяется если актив не попадает под действие ни одной политики, сконфигурированной для подсетей

#### 15.1.5.1 Создание новой политики идентификации

Для создания новой политики идентификации необходимо:

- Перейти в раздел ***Активы - Настройка идентификации активов***;
- Нажать кнопку "**Создать**";
- Заполнить атрибуты политики идентификации (см. рисунок 124):
    - **Имя** - название политики;
    - **Диапазоны** - область действия политики. Адреса подсетей в CIDR-нотации, для который будет применяться выбранная стратегия идентификации;
    - **Стратегия** - стратегия идентификации. Атрибут, который будет использоваться для идентификации актива (FQDN, IP-адрес или MAC-адрес).
- Нажать кнопку "**Сохранить**".

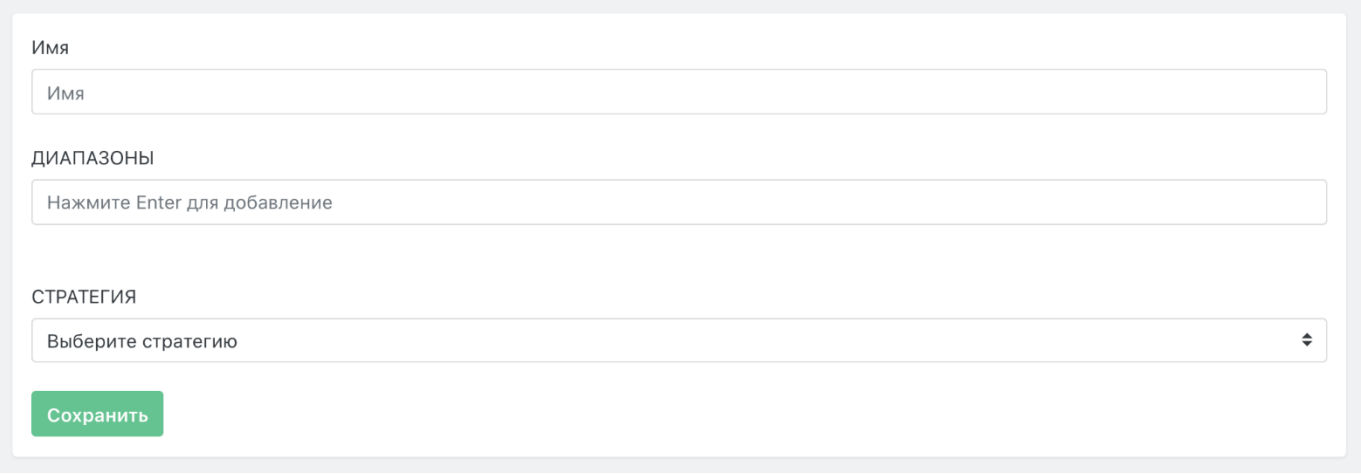



**Рисунок 124 – Окно создания новой политики идентификации**

### 15.1.5.2 Редактирование политики идентификации

Для редактирования политики идентификации необходимо:

- Перейти в раздел ***Активы - Настройка идентификации активов***;
- Нажать кнопку **Изменить** напротив политики, в которую необходимо внести изменения;
- Внести изменения в атрибуты политики идентификации (см. рисунок 125):
    - **Имя** - название политики;
    - **Диапазоны** - область действия политики. Адреса подсетей в CIDR-нотации, для который будет применяться выбранная стратегия идентификации;
    - **Стратегия** - стратегия идентификации. Атрибут, который будет использоваться для идентификации актива (FQDN, IP-адрес или MAC-адрес).
- Нажать кнопку "**Сохранить**".

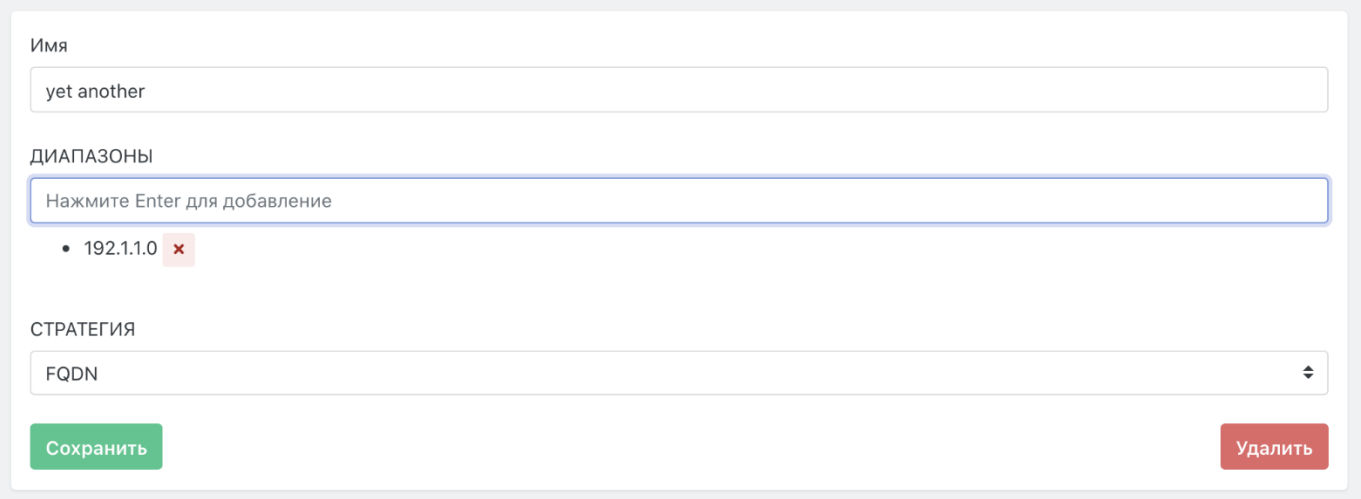



**Рисунок 125 – Окно редактирования настройки обнаружения активов**

### 15.1.5.3 Удаление политики идентификации

Для удаления политики идентификации необходимо:

- Перейти в раздел ***Активы - Настройка идентификации активов***;
- Перейти в необходимую политику идентификации;
- Нажать кнопку "**Удалить**".

## 15.2 Аналитика по активам

Для оценки риска в разрезе активов доступны следующие инструменты работы с активами:

- Фильтрация активов;
- Просмотр данных по активу;
- Соответствие ПО.

### 15.2.1 Фильтрация активов

Для применения фильтра необходимо перейти в раздел ***Активы - Активы***, после чего (см. рисунок 126):

- для активации фильтра необходимо задать значения фильтруемых атрибутов и нажать кнопку "**Поиск**";
- для сброса условий фильтрации необходимо нажать кнопку "**Очистить**";
- для сохранения условий фильтра нажать кнопку "**Сохранить**";
- для управления фильтрами нажать кнопку "**Загрузить**".

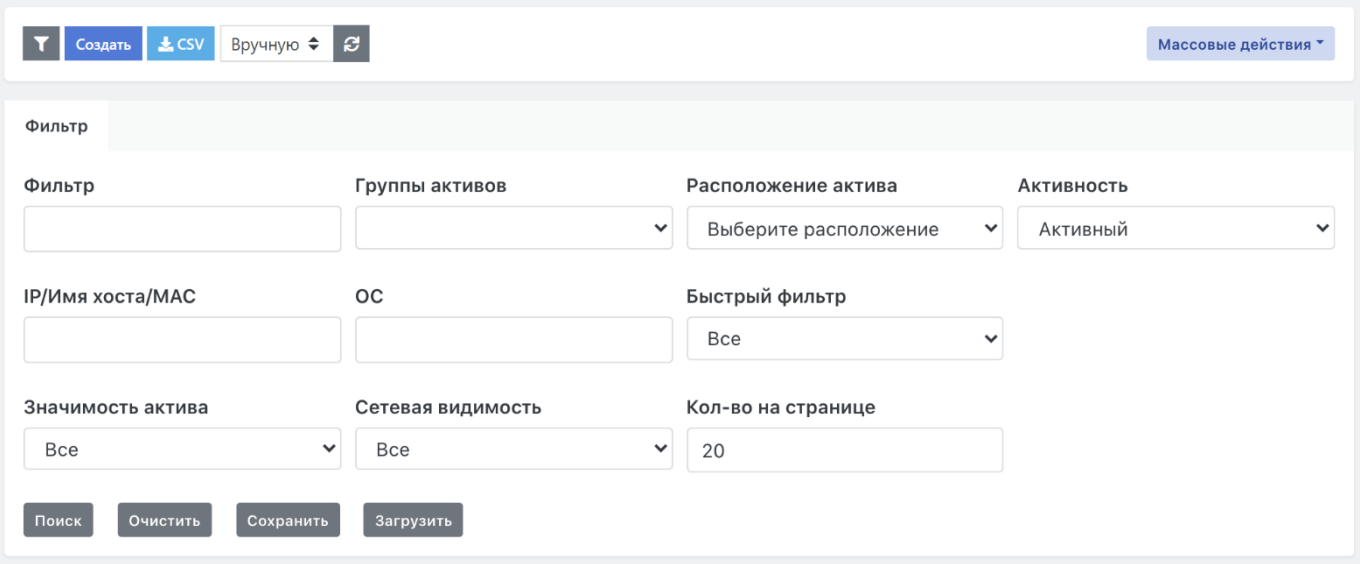



**Рисунок 126 – Фильтр активов**

Более подробную информацию об использовании фильтра можно узнать в разделе «Настраиваемые фильтры списка активов».

### 15.2.2 Просмотр данных по активу

Для того, чтобы посмотреть данные по активу, необходимо перейти в раздел ***Активы - Активы - /щелкнуть на название заголовка нужного актива/***

В сводной информации по активу отображаются (см. рисунок 127):

- Заголовок актива;
- **Тип**;
- **Расположение** - где территориально находится актив;
- **Описание**;
- **Ответственная группа пользователей** за данный актив. По клику возможен переход в интерфейс просмотра группы пользователей;
- Перечень сетевых интерфейсов: **Имя**, **FQDN**, **IP**, **MAC**, **ОС**, **Сервисы**, которые представляют результат работы поиска сетевых сервисов;
- **Список программного обеспечения** - описание поиска ПО в разделе «Подраздел "Список ПО"»;

- **Список аппаратного обеспечения** - результат работы обнаружения аппаратного обеспечения;
- **Сетевая видимость** актива:
    - 1 - прямое подключение к Интернет (межсетевой экран, сетевой балансировщик, VPN-сервер);
    - 2 - DMZ, частичный доступ из Интернет для некоторых сервисов (Web-сервер, Proxy);
    - 3 - штатный доступ в Интернет через Proxy (рабочие станции, внутренние сервера) - значение по умолчанию;
    - 4 - ограниченный доступ в Интернет, доступ к ограниченному набору Интернет-сервисов (тонкие клиенты, POS-терминалы, удаленные офисы);
    - 5 - актив, не подключенный к сети.
- **Сканирование** - дата последнего сканирования (при интеграции со сканером уязвимостей);
- **Группы**, в которых состоит актив. По клику возможен переход в интерфейс просмотра группы активов;
- **Инциденты**, связанные с активом. Работа с инцидентами описана в разделе «Работа с инцидентами».

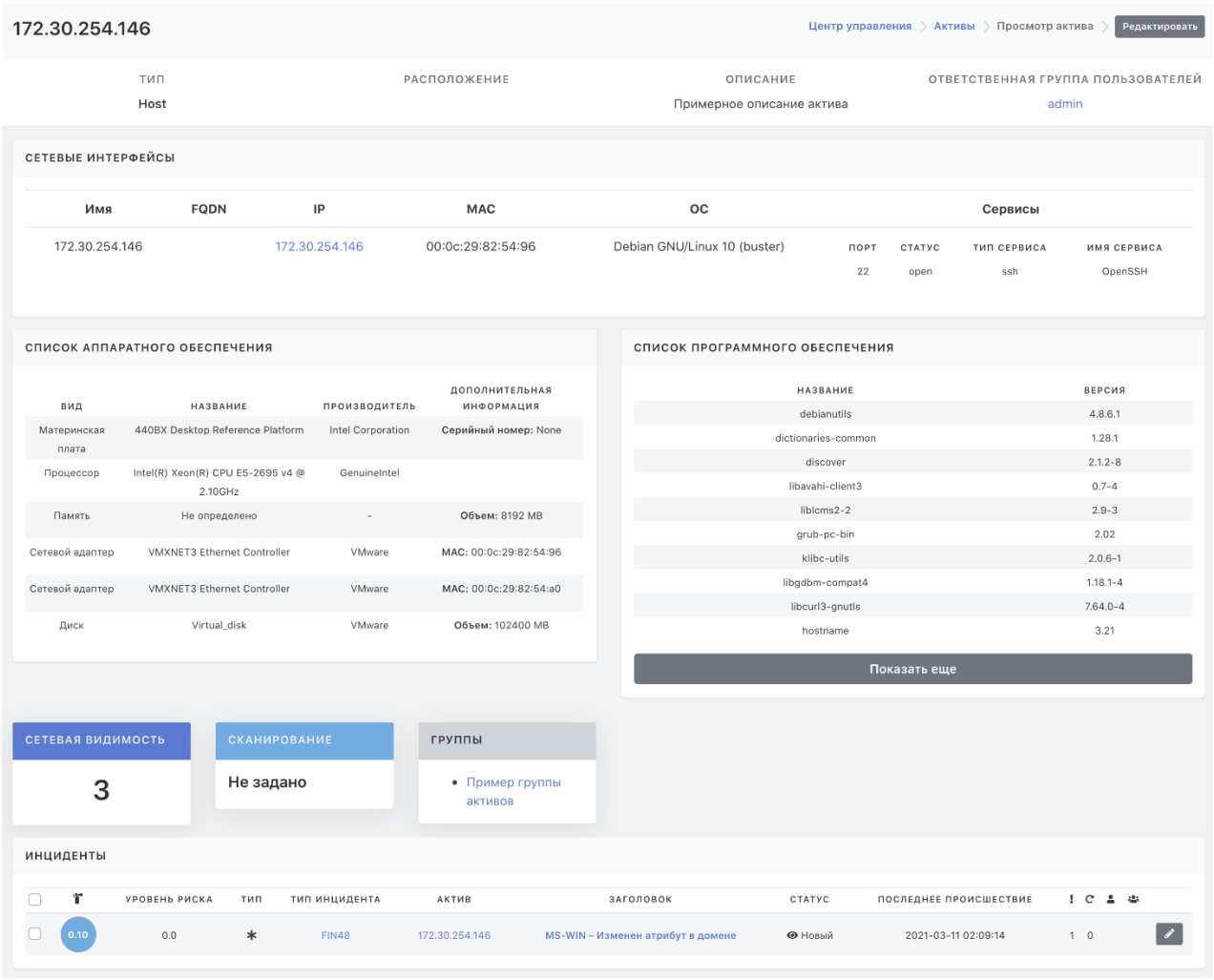



**Рисунок 127 – Окно отображения сводной информации по активу**

### 15.2.3 Соответствие ПО

В разделе ***Оценка соответствия ПО - Результаты соответствия ПО*** отображаются детали по проверке соответствия программного обеспечения политикам контроля.

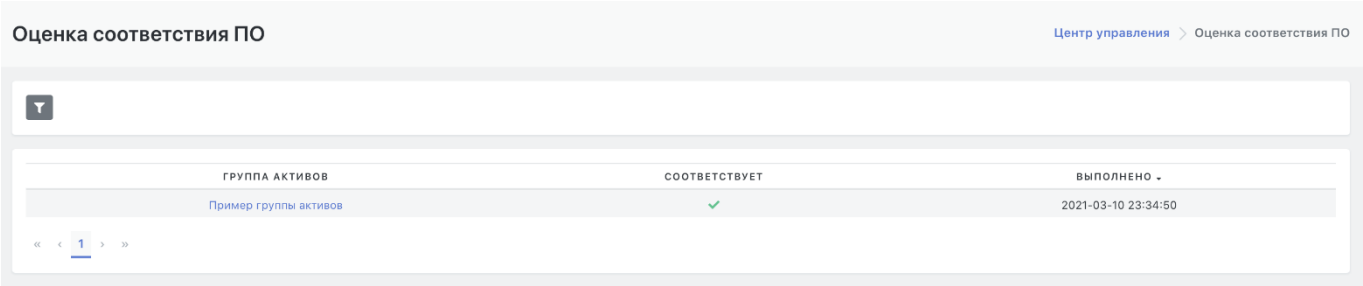



**Рисунок 128 – Вкладка *Оценка соответствия ПО - Результаты соответствия ПО***

В таблице отображаются следующие колонки (см. рисунок 128):

- Группа активов - группа активов, в рамках которой выполнялась оценка соответствия;
- Состояние - статус проверки соответствия для правила контроля;
- Дата выполнения.

Более подробную информацию можно узнать в разделе «Анализ результатов проверок соответствия ПО».

## 15.3 Работа с группами активов

Группы активов упрощают процесс управления активами.

### 15.3.1 Создание группы активов

Для создания группы активов необходимо:

- Перейти в раздел ***Активы - Группы активов***;
- Нажать кнопку "**Создать**";
- Заполнить атрибуты группы активов (см. рисунок 129).
    - **Название** - название группы активов;
    - **Маски подсетей в CIDR-нотации** - если данный атрибут заполнен, новые активы, попадающие под указанную сетевую маску, будут автоматически включаться в группу;
    - **Регулярное выражение для FQDN**;
    - **Группа ответственных** - группы пользователей, ответственных за данную группу активов;
    - **Связанные группы пользователей** - группы пользователей, которые также ответственны за данную группу активов;
    - **ИД объекта**, **ИД субъекта**, **ИД системы** - идентификаты, указанные в протоколе интеграции с ГосСОПКОЙ (при необходимости);

- Чек-бокс **КИИ?** - является ли актив объектом критической информационной инфраструктуры;
- **Ответственное лицо**;
- **Технический специалист**;
- **Актив** - выбрать актив из выпадающего списка;
- **Набор правил** - указать наборы правил контроля соответствия установленного программного обеспечения.

- Нажать кнопку "**Сохранить**".

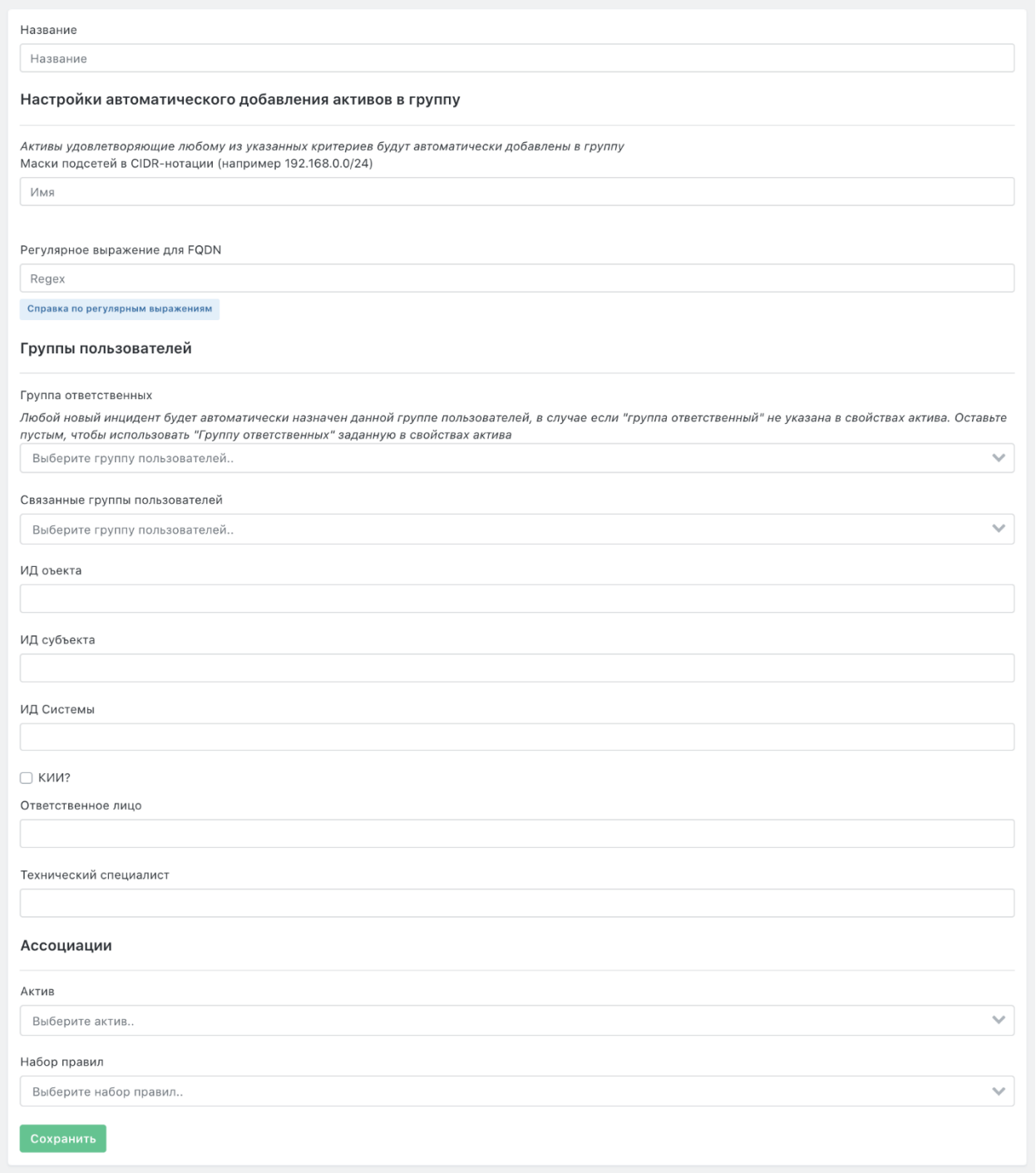



**Рисунок 129 – Окно создания группы активов**

## 15.3.2 Просмотр информации по группе активов

Для просмотра информации по группе активов необходимо:

- Перейти в раздел ***Активы - Группы активов***;
- Кликнуть на название группы, по которой требуется просмотреть информацию.

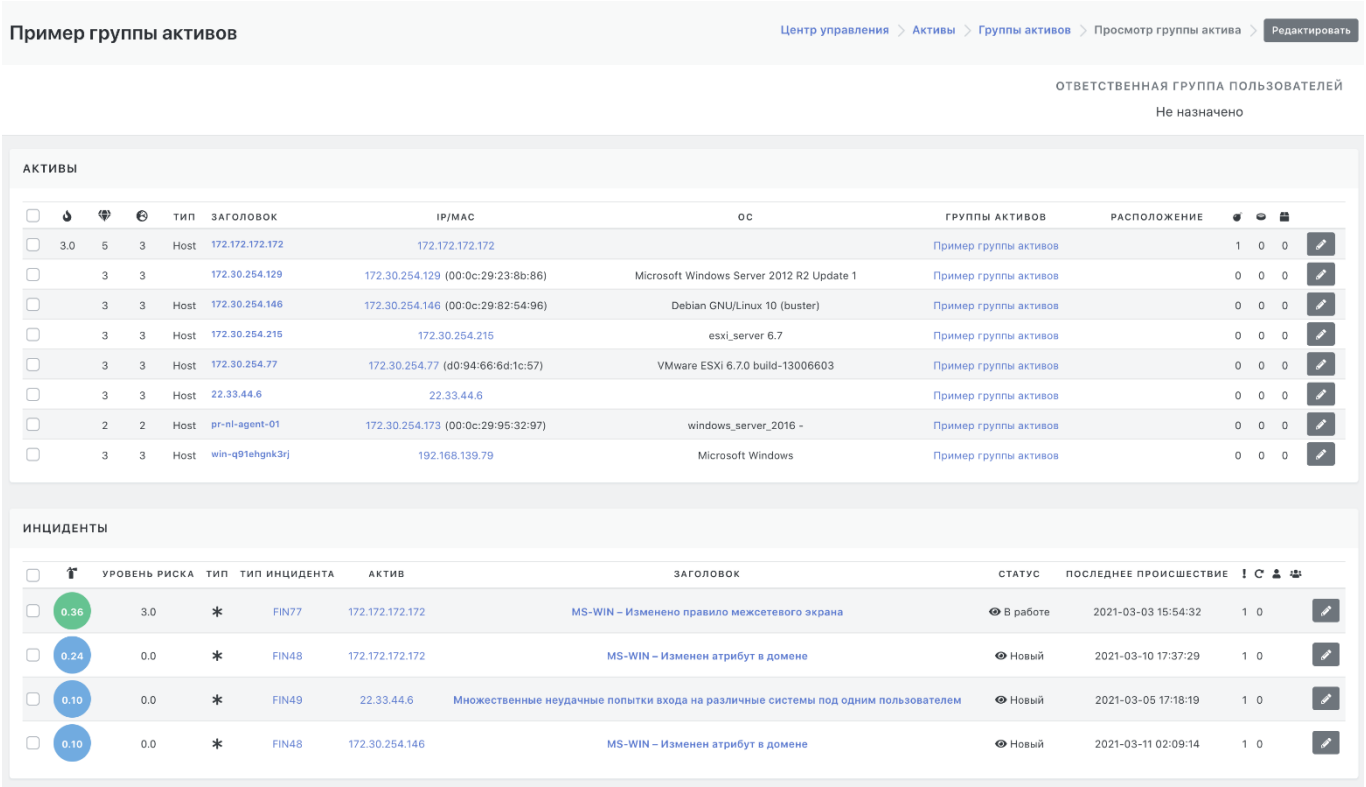



**Рисунок 130 – Информация по группе активов**

В форме просмотра отображаются (см. рисунок 130):

- Название группы;
- **Ответственная группа пользователей** - перечень групп пользователей, ответственных за данную группу активов;
- Список активов, который содержит в себе поля:
    - Поле ( / ) - флаговое поле для выбора строк с активами для проведения с ними каких-то действий;
    - Поле **Уровень риска** ( ) - содержит численную оценку уровня риска инцидентов, произошедших на данном активе;
    - Поле **Значимость актива** ( ) - содержит оценку значимости актива, которая в рамках бизнес-процессов оценивается числовыми значениями от 1 до 5;
    - Поле **Сетевая видимость** ( ) - оценивается числовыми значениями от 1 до 5;
    - Поле **Тип** - содержит тип оборудования актива (например Host, Server);

- Поле **Заголовок** - название актива, под которым он был зафиксирован в **Платформе Радар**;
- Поле **IP/MAC** - IP- или MAC-адрес актива;
- Поле **ОС** - операционная система актива;
- Поле **Группы активов** - название группы активов (или нескольких групп), в которую включен данный актив;
- Поле **Расположение** - территориальное расположение актива, например город (если оно было указано при создании или редактировании записи актива в **Платформе Радар**);
- Поле **Открытые инциденты** ( ) - количество открытых инцидентов на активе;
- Поле **Риск принят** ( ) - количество инцидентов в статусе "риск принят" на активе;
- Поле **Закрытые инциденты** ( ) - количество закрытых инцидентов на активе;
- Кнопка ( ) - функция редактирования параметров актива.

- Перечень связанных инцидентов.

Кнопка "**Редактировать**" открывает форму редактирования атрибутов группы.

### 15.3.3 Редактирование группы активов

Для редактирования группы активов необходимо (см. рисунок 131):

- Перейти в раздел ***Активы - Группы активов***;
- Нажать кнопку "**Редактировать**";
- Отредактировать необходимые атрибуты группы активов (см. раздел «Создание группы активов»);
- Нажать кнопку "**Сохранить**".

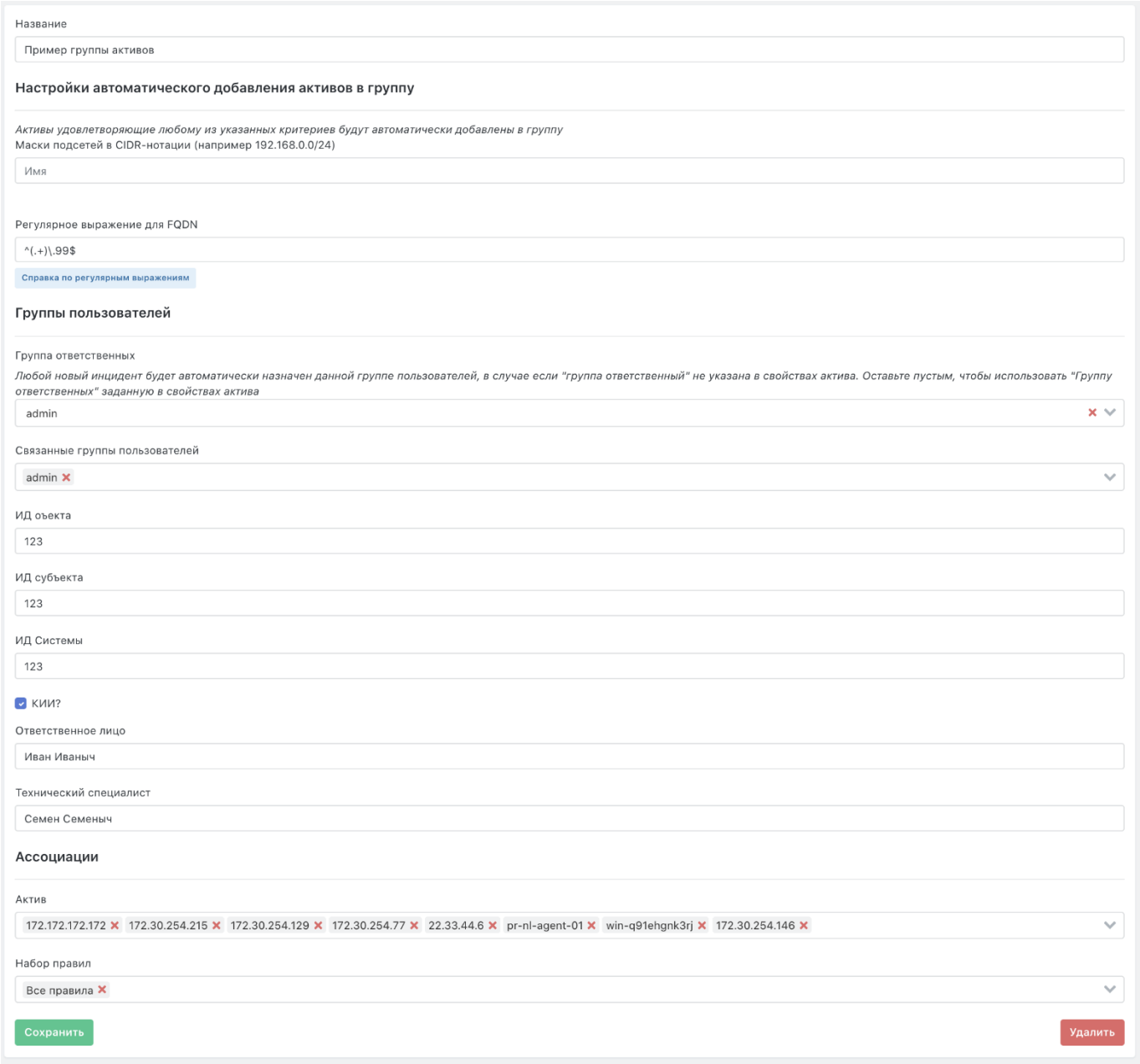



**Рисунок 131 – Окно редактирования группы активов**

## 15.3.4 Включение активов в группу активов

Включение активов в группу производится в форме редактирования атрибутов активов (см. рисунок 132).


**Рисунок 132 – Форма включения активов в группу**

Для удобства связывания список доступных интерфейсов можно отфильтровать по имени и IP-адресу - для этого нужно начать вводить в поле имя или начало IP-адреса.

Для включения активов в группу необходимо выбрать один или несколько активов в списке.

После проделанных манипуляций необходимо сохранить изменения в группе активов. Данная операция также доступна из контекста списка активов.

### 15.3.5 Исключение активов из группы

Исключение активов из группы производится в форме редактирования атрибутов активов (см. рисунок 133).


**Рисунок 133 – Форма исключения активов из группы**

Исключить актив из группы возможно нажатием на кнопку  рядом с именем актива.

После проделанных манипуляций необходимо сохранить изменения в группе активов. Данная операция также доступна из контекста списка активов.

## 15.4 Актуализация данных об активах

В ходе эксплуатации системы может потребоваться внести дополнительную информацию или коррективы в данные по активу.

### 15.4.1 Редактирование данных по активу

Для редактирования информации необходимо:

- Перейти в раздел ***Активы - Активы***;
- Кликнуть по заголовку актива, в который необходимо внести изменения.
- Нажать кнопку редактирования  ;
- Внести коррективы в данные об активе;
- Нажать кнопку "**Сохранить**".

### 15.4.2 Классификация новых активов

Для поиска активов, которые некорректно классифицировались автоматически, предусмотрены специализированные фильтры активов, которое можно увидеть, нажав на кнопку  в разделе ***Активы - Активы***, где откроется область с настраиваемыми фильтрами для табличного списка активов:

- Активы без группы - перечень активов, не привязанный ни к одной группе;
- Имя похоже на IP адрес - системе не удалось определить имя узла автоматически;
- Повторяющееся имя - активы с повторяющимся значением имени актива.

### 15.4.3 Объединение активов

В системе доступен интерфейс, позволяющий объединить данные из нескольких активов в один. Это может потребоваться в случаях:

- Данные по одному и тому же активу появились в системе из разных источников;

- Актив был просканирован сканером уязвимостей через различные сетевые интерфейсы.

Для объединения данных по активу необходимо:

- Перейти в раздел ***Активы - Активы***;
- Выбрать несколько активов с помощью чек-боксов;
- Нажать кнопку "**Объединить активы**".

После выполнения данной операции будет создан новый актив, в котором будут присутствовать следующие данные из объединенных активов:

- Сетевые интерфейсы;
- Привязка к группам активов;
- Инциденты.

# 15.5 Работа с сетевыми интерфейсами

Манипуляции с сетевыми интерфейсами могут потребоваться в случае, если от сканера уязвимостей поступили неточные данные о сетевых интерфейсах или сетевая конфигурация изменилась в ходе эксплуатации

## 15.5.1 Связывание интерфейса с активом

Форма связывания актива с сетевыми интерфейсами доступна при создании актива вручную и при редактировании актива (см. рисунок 134).


**Рисунок 134 – Форма связывания интерфейса с активом**

Для удобства связывания список доступных интерфейсов можно отфильтровать по имени интерфейса, IP-адресу или MAC-адресу - для применения фильтра необходимо начать писать искомое значение в форму "**Связанные интерфейсы**".

Для связывания сетевых интерфейсов с активом необходимо выбрать один или несколько активов в списке.

Для отвязывания сетевых интерфейсов от актива необходимо нажать на кнопку  рядом с именем интерфейса.

После указанных изменений необходимо сохранить изменения в активе.

## 15.5.2 Создание сетевых интерфейсов вручную

Для создания нового сетевого интерфейса вручную необходимо:

- Перейти в раздел ***Активы - Сетевые интерфейсы***;

- Нажать кнопку "**Создать**";
- Заполнить атрибуты сетевого интерфейса (см. рисунок 135):
    - **Имя** - имя интерфейса для удобства поиска;
    - **MAC** - MAC-адрес, заданный на интерфейсе;
    - **IP** - IP-адрес, заданный на интерфейсе;
    - **FQDN** - доменное имя для IP-адреса заданного на интерфейсе;
    - **ОС** - операционная система, определяемая через данный интерфейс;
    - Выбрать актив, с которым требуется связать новый интерфейс.
- Нажать кнопку "**Сохранить**".

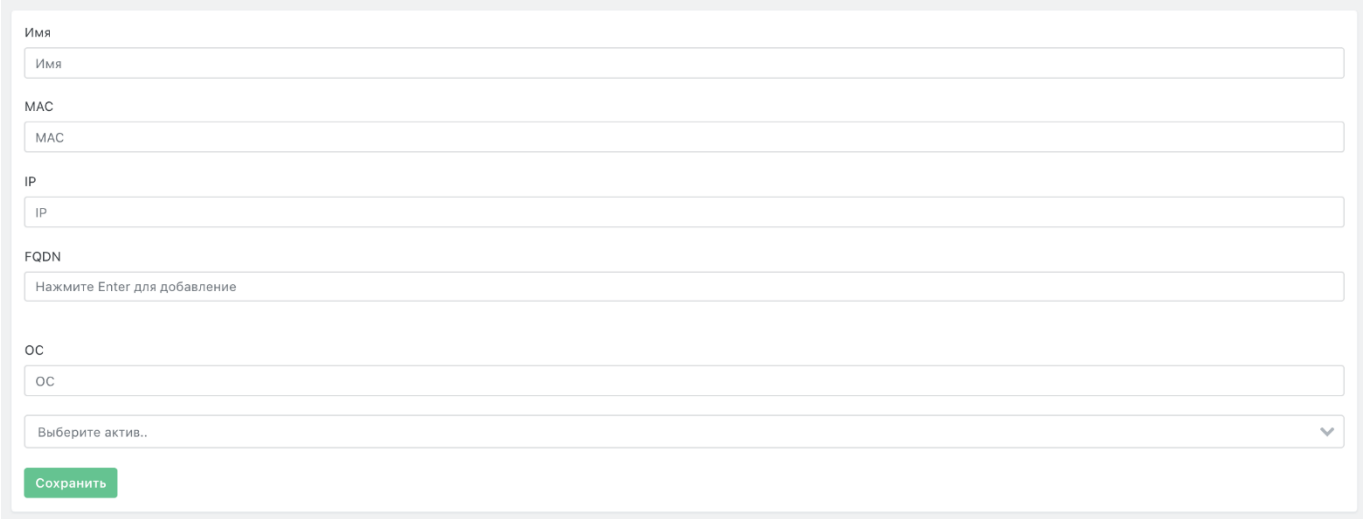



**Рисунок 135 – Создание сетевых интерфейсов вручную**

## 15.5.3 Редактирование сетевого интерфейса

Для редактирования сетевого интерфейса необходимо:

- Перейти в раздел ***Активы - Сетевые интерфейсы***;
- Нажать кнопку  рядом с именем интерфейса, который необходимо отредактировать;
- Внести изменения в атрибуты сетевого интерфейса (см. рисунок 136):
    - **Имя** - имя интерфейса для удобства поиска;
    - **MAC** - MAC-адрес, заданный на интерфейсе;
    - **IP** - IP-адрес, заданный на интерфейсе;
    - **FQDN** - доменное имя для IP-адреса заданного на интерфейсе;
    - **ОС** - операционная система, определяемая через данный интерфейс;
    - Выбрать актив, с которым требуется связать новый интерфейс.
- Нажать кнопку "**Сохранить**".

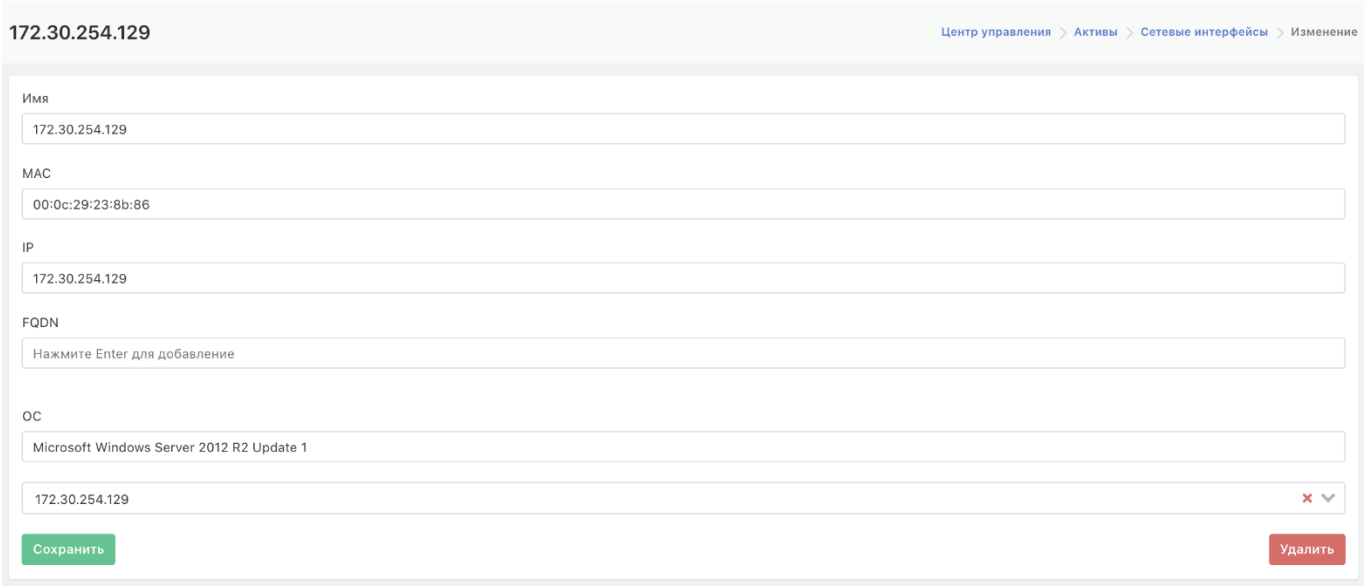



**Рисунок 136 – Окно редактирования сетевого интерфейса**

## 15.5.4 Удаление сетевого интерфейса

Для удаления сетевого интерфейса необходимо:

- Перейти в раздел ***Активы - Сетевые интерфейсы***;
- Перейти в режим редактирования необходимого сетевого интерфейса
- Нажать кнопку "**Удалить**".

# 16. Работа с сетевым сканером и инвентаризацией

Сетевой сканер - это специализированное программное обеспечение, предназначенное для поиска хостов в компьютерной сети и определение сетевых сервисов и программного обеспечения на обнаруженном хосте.

Поддерживаемые системы:

- ОС Семейства MS Windows с использованием RPC/WMI;
- ОС семейства Linux с использованием SSH.

## 16.1 Поиск активов в компьютерной сети

Для обнаружения новых активов и актуализации старых необходимо:

- Перейти в раздел ***Активы - Инвентаризация - Обнаружение хостов***;
- Далее указать в поле IP-адрес подсети которую необходимо просканировать;
- В поле подсеть выбрать глубину сканирования сети (по умолчанию выбрана 24-ая подсеть), доступны варианты:
    - 0 (весь интернет)
    - 1 (128 классов A)
    - 2 (64 класса A)
    - 3 (32 класса A)
    - 4 (16 классов A)
    - 5 (8 классов A)
    - 6 (4 класса A)
    - 7 (2 класса A)
    - 8 (1 класс A)
    - 9 (128 классов B)
    - 10 (64 класса B)
    - 11 (32 класса B)
    - 12 (16 классов B)
    - 13 (8 классов B)
    - 14 (4 класса B)
    - 15 (2 класса B)
    - 16 (1 класс B)
    - 17 (128 классов C)

    - 18 (64 класса C)
    - 19 (32 класса C)
    - 20 (16 классов C)
    - 21 (8 классов C)
    - 22 (4 класса C)
    - 23 (2 классов C)
    - **24 (1 класс C - 254 хоста)**
    - 25 (128 хостов)
    - 26 (64 хоста)
    - 27 (32 хоста)
    - 28 (16 хостов)
    - 29 (8 хостов)
    - 30 (4 хоста)
    - 31 (2 хоста)
    - 32 (1 хост)
- Нажать кнопку "**Сканировать**"

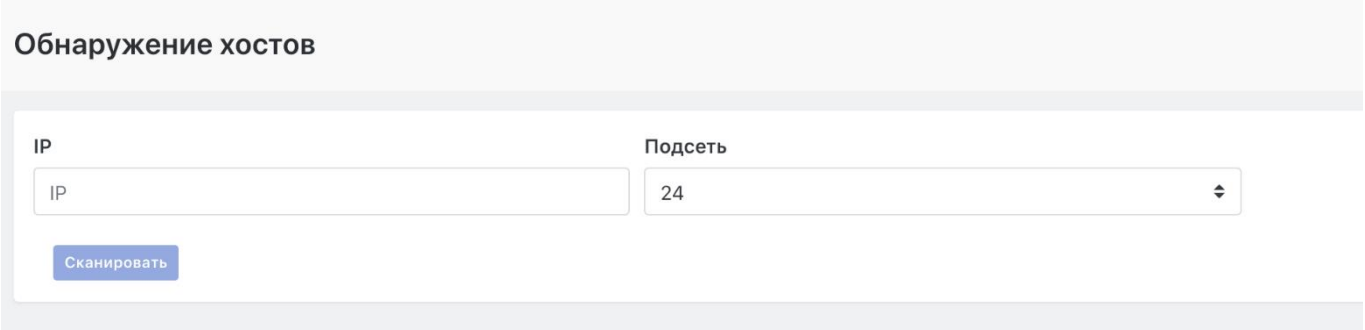



**Рисунок 137 - Форма обнаружения хостов**

После запуска сканирования появится индикатор процесса сканирования


**Рисунок 138 – Процесс сканирования**

И после завершения сканирования будут доступен результат сканирования в виде таблицы с аттрибутами (см. рисунок 139):

- Имена хоста (если удалось определить);
- IPV4 и IPV6 адреса хоста;
- MAC адрес хоста.

| HOST | IPV4 | IPV6 | MAC |
|---|---|---|---|
| [] | 172.30.254.1 | | E4:18:6B:4D:67:C4 |
| [] | 172.30.254.30 | | 00:0C:29:64:18:ED |
| [] | 172.30.254.35 | | 00:0C:29:46:82:09 |
| [] | 172.30.254.36 | | 00:0C:29:F9:60:CA |
| [] | 172.30.254.37 | | 00:0C:29:DA:27:7A |
| [] | 172.30.254.39 | | 00:0C:29:B7:37:E7 |
| [] | 172.30.254.70 | | 00:0C:29:8D:F7:A1 |
| [] | 172.30.254.71 | | 00:0C:29:B5:A6:2B |
| [] | 172.30.254.73 | | 00:0C:29:92:7F:D6 |

**Рисунок 139 – Результаты сканирования сети**

Для добавления или обновления активов из результатов сканирования сети необходимо:

- выделить с помощью чекбоксов нужные хосты;
- нажать на кнопку "**Обновить**" появившуюся в форме обнаружения хоста после завершения результатов сканирования (см. рисунок 140).

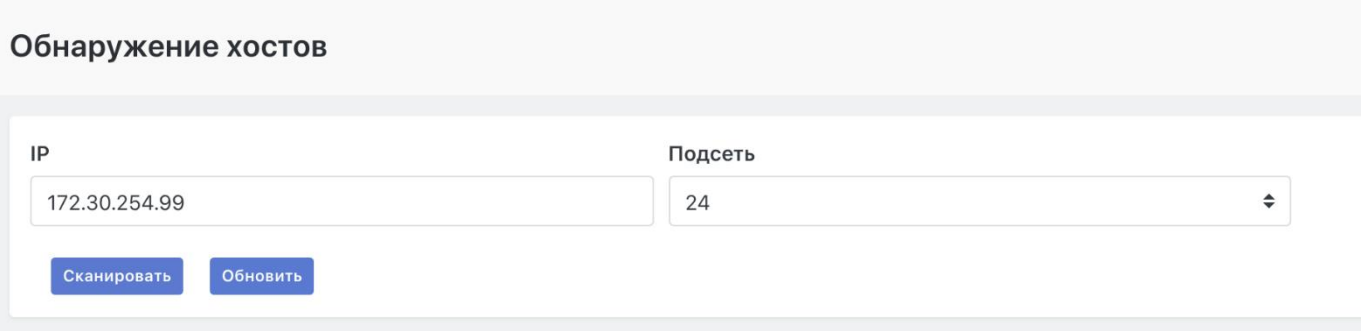



**Рисунок 140 - Форма обнаружения хостов после завершения сканирования**

После запуска процедуры обновления появится индикатор прогресса обновления активов. Как только он дойдет до конца и исчезнет с экрана - процедура обновления или добавления активов завершена. Результаты доступны в разделе ***Активы - Активы***.

## 16.2 Поиск сетевых сервисов на хосте без авторизации

Для запуска сканирования сетевых сервисов необходимо:

- Перейти на вкладку ***Активы - Инвентаризация - Обнаружение сервисов***;
- Отметить чек-боксами нужные для сканирования активы (при необходимости воспользоваться поиском и фильтрацией);
- Нажать на кнопку "**Сканировать сервисы**".

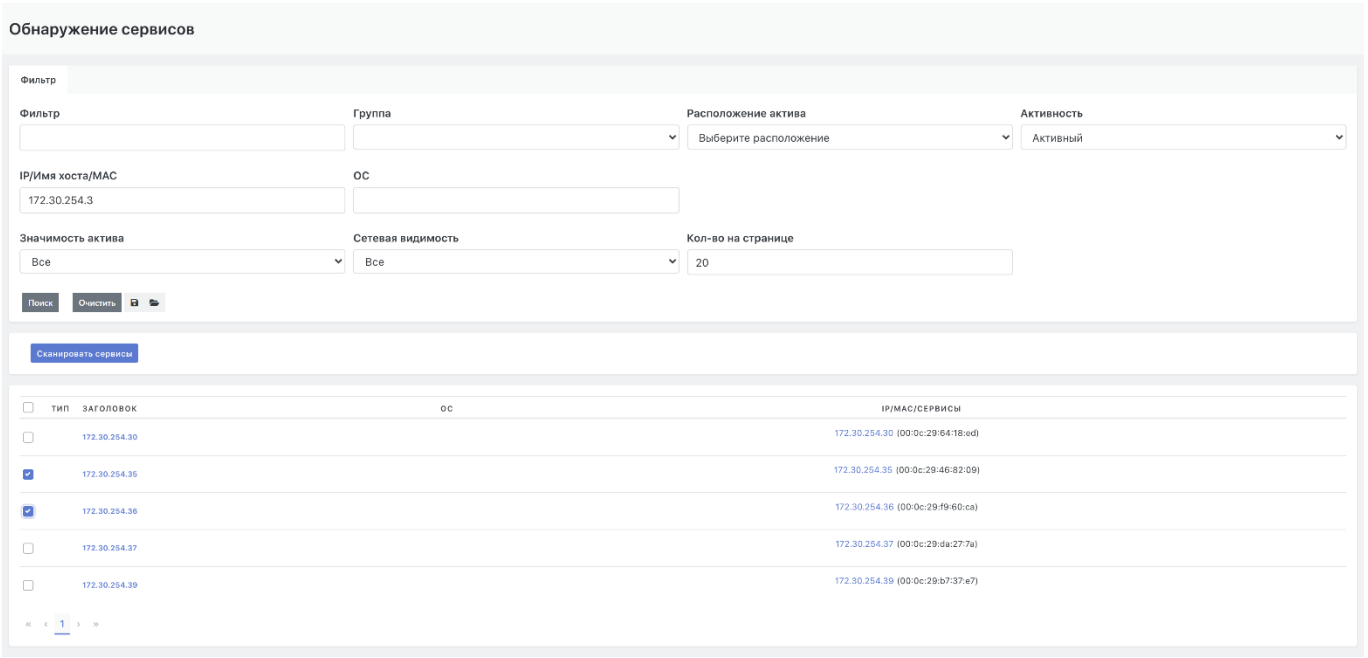



**Рисунок 141 – Экран сканирования сетевых сервисов**

После нажатия на кнопку "**Сканировать сервисы**" появится индикатор прогресса сканирования.

Процедура занимает длительное время, в процессе её выполнения данные на странице будут обновляться (см. рисунок 142).

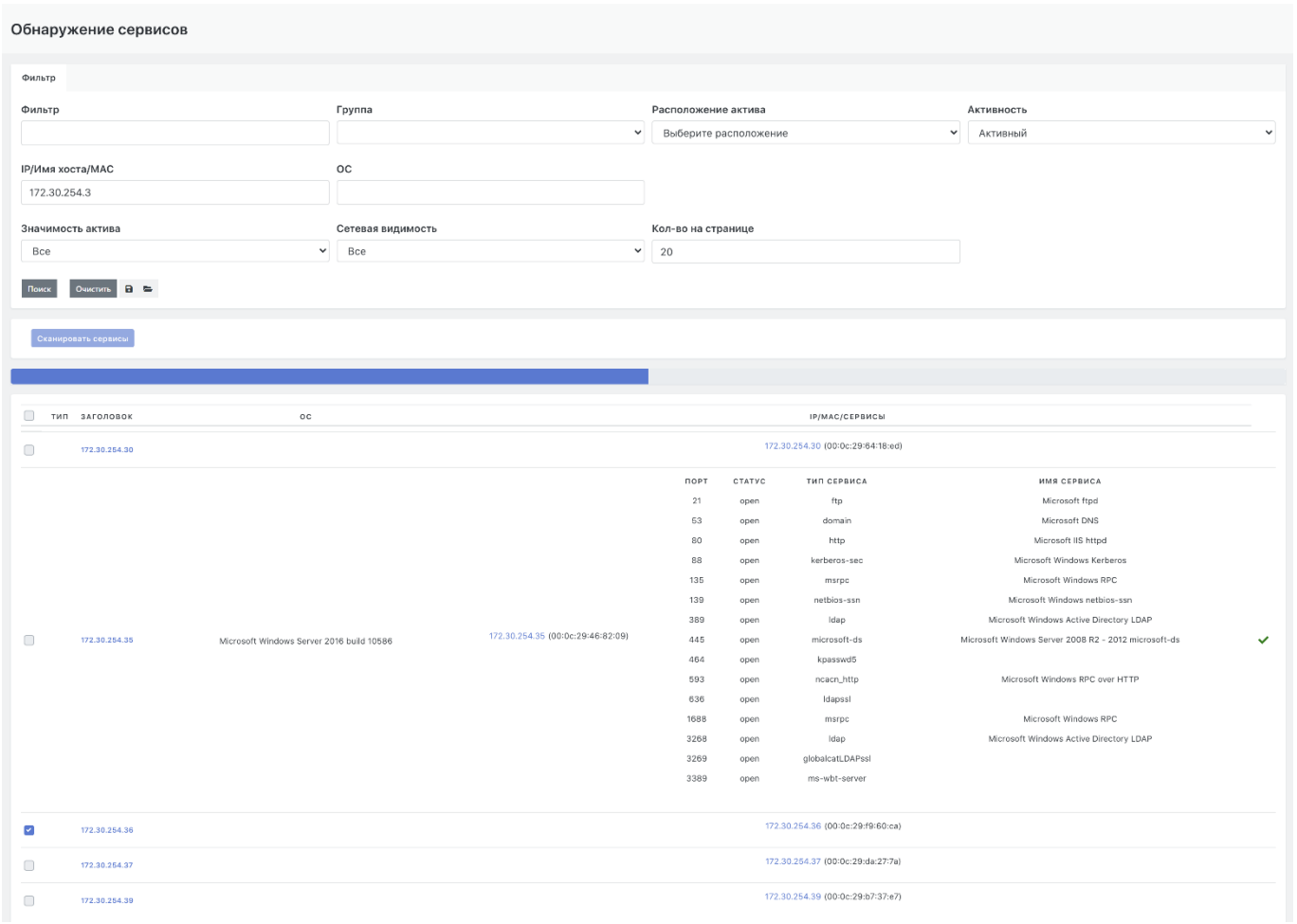



**Рисунок 142 - Экран сканирования сетевых сервисов в процессе сканирования**

После завершения сканирования прогресс бар исчезнет и в списке активов появятся детали проведенного сканирования, а именно атрибуты:

- Найденные открытые порты и их статус;
- Определенные типы сервисов на этих портах;
- Имена сервисов на этих портах;
- Статус исполнения сканирования.

Сканирование сервисов происходит на основе открытых данных, и детальная информация про ОС или сервисы берется на основе обученных эвристических алгоритмов. Для более точной информации пользуйтесь сбором данных с авторизацией.

## 16.3 Обнаружение ПО на хосте с авторизацией

Для запуска сканирования сбора данных о ПО необходимо:

- Перейти на вкладку ***Активы - Инвентаризация - Сбор данных*** (см. рисунок 143);
- Отметить чек-боксами нужные для сканирования активы (при необходимости воспользоваться поиском и фильтрацией);
- Выбрать протокол сканирования, учетную запись и тип сбора данных в форме сбора данных (см. рисунок 144);
- Нажать на кнопку "**Собрать**".

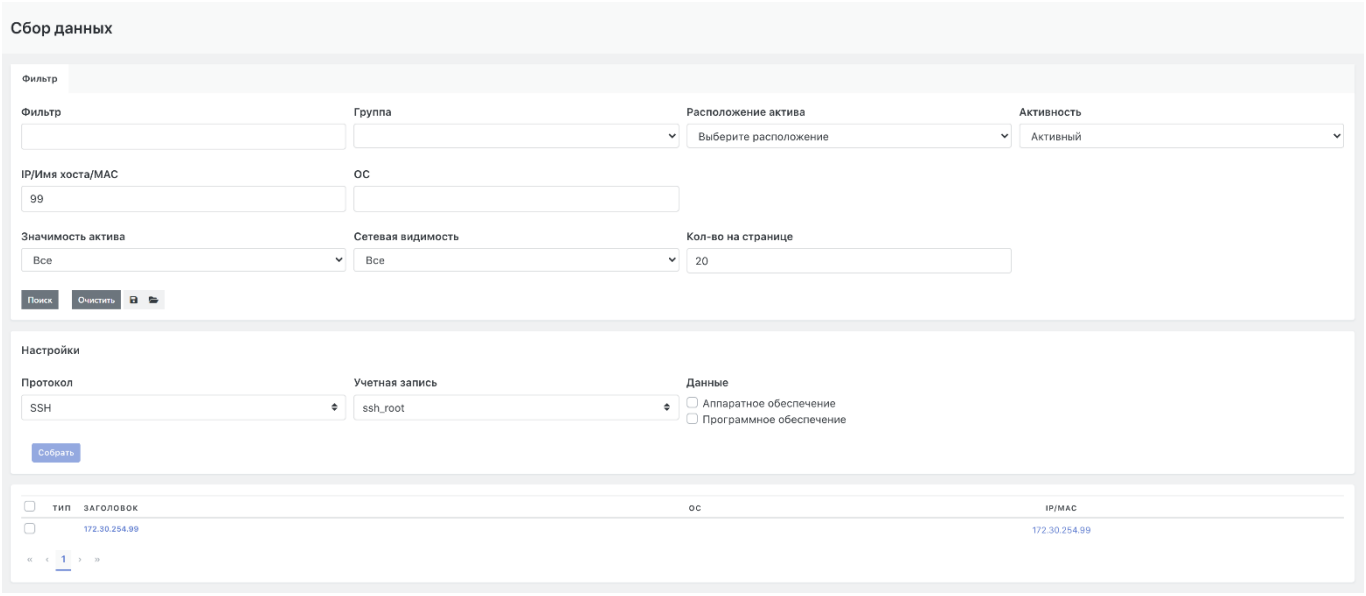



**Рисунок 143 – Экран сбора данных на хосте с авторизацией**

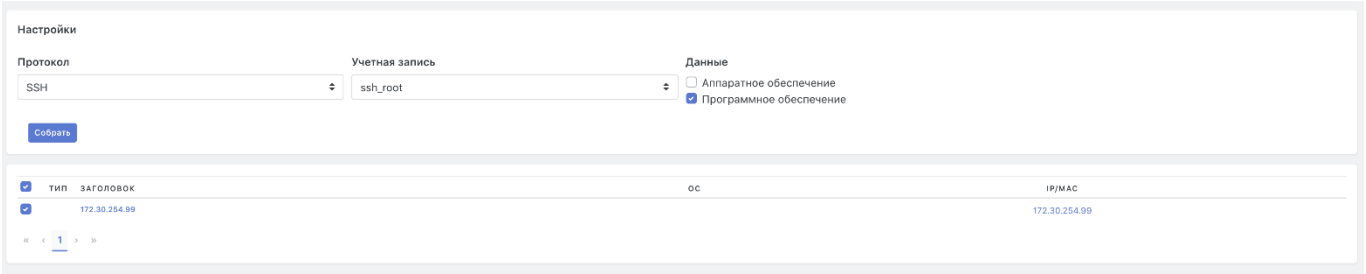



**Рисунок 144 - Форма сбора данных о ПО на хосте с авторизацией**

После завершения сбора данных в деталях актива появится информационный блок с списком программного обеспечения (см. рисунок 145)

Результаты сбора данных с авторизацией перезаписывают результаты сканирования сервисов без авторизации.


**Рисунок 145 – Список найденного программного обеспечения**

## 16.4 Обнаружение аппаратной конфигурации на хосте с авторизацией

Для запуска сканирования сбора данных о ПО необходимо:

- Перейти на вкладку ***Активы - Инвентаризация - Сбор данных***;
- Отметить чек-боксами нужные для сканирования активы (при необходимости воспользоваться поиском и фильтрацией);
- Выбрать протокол сканирования, учетную запись и тип сбора данных в форме сбора данных (см. рисунок 146);
- Нажать на кнопку "**Собрать**".

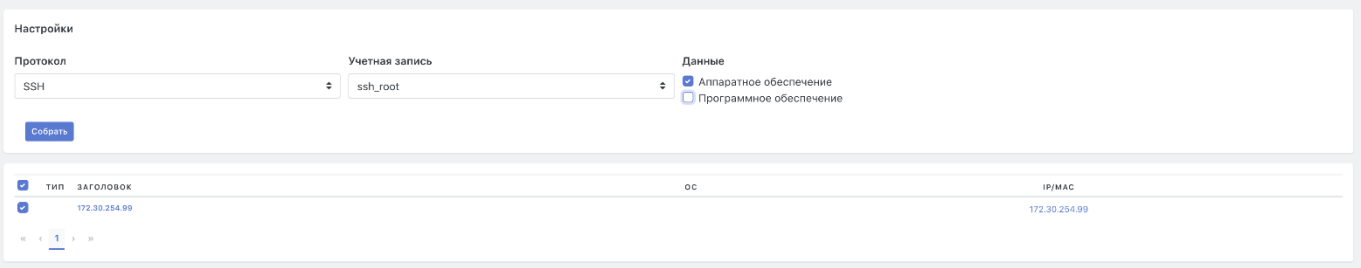



**Рисунок 146 – Форма сбора данных об аппаратном обеспечении на хосте с авторизацией**

После завершения сбора данных в деталях актива появится информационный блок с списком аппаратного обеспечения (см. рисунок 147).

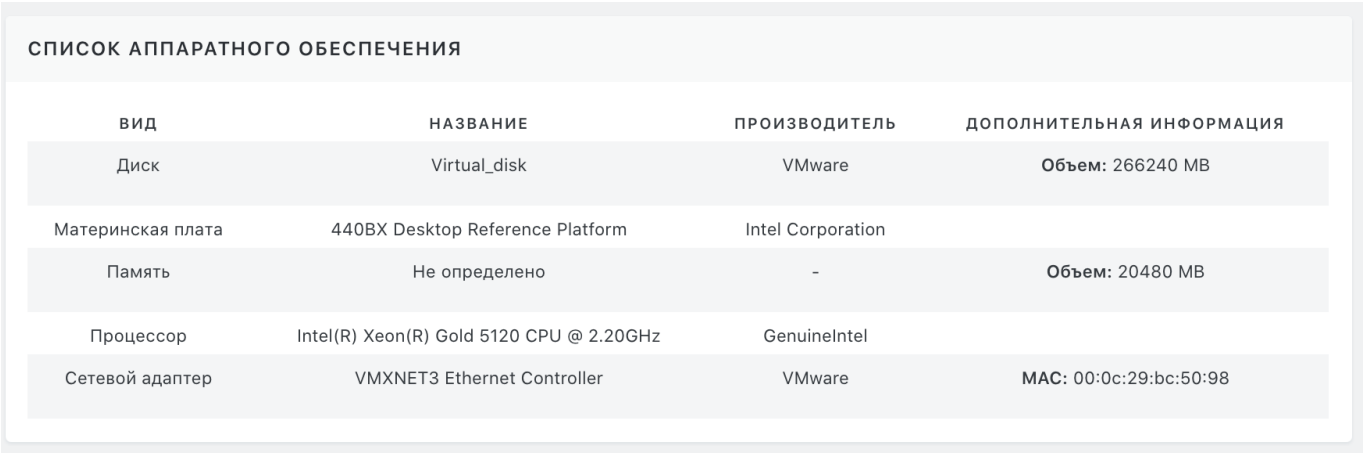



**Рисунок 147 – Список найденного аппаратного обеспечения**

## 16.5 Настройка учетных записей для авторизации на хостах

Данный функционал находится в разделе ***Администрирование - Кластер*** и доступен только администраторам системы.

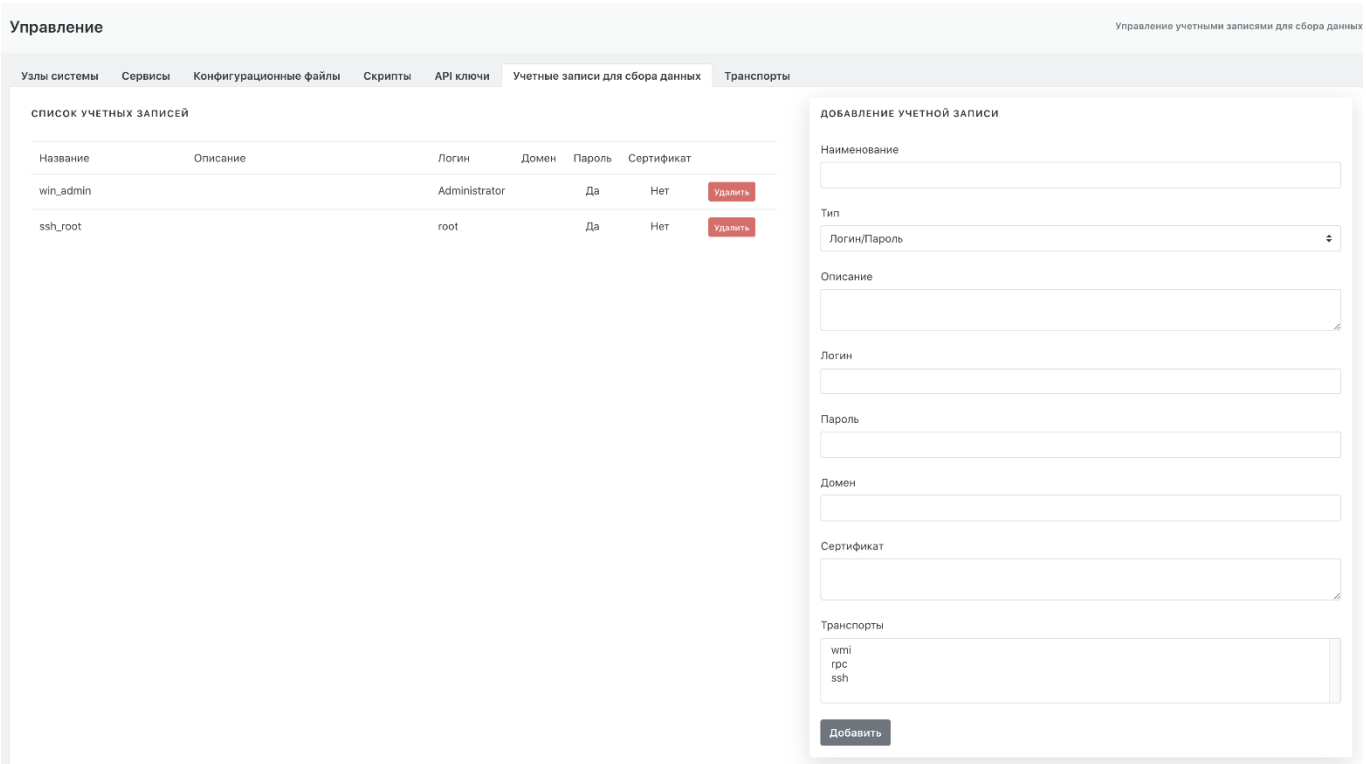



**Рисунок 148 – Экран управления учетными записями для сбора данных**

# 17. Настройка контроля установленного программного обеспечения

## 17.1 Общие положения

В **Платформе Радар** в разделе основного меню "**Оценка соответствия ПО**" реализован функционал контроля списка программного обеспечения установленного на активах по политикам контроля. Политика контроля состоит из набора правил контроля, которые могут отслеживать:

- отсутствие программного обеспечения на активе;
- наличие программного обеспечения на активе.

Политика контроля может быть применена к группе активов. Актив считается соответствующим политике, если все правила контроля дали положительный результат. Группа активов считается соответствующей политике, если все активы группы соответствуют политике. В системе реализована возможность создания инцидентов по результатам проверки соответствия политикам.

## 17.2 Анализ программного обеспечения на активах

### 17.2.1 Просмотр детализации по записи программного обеспечения

В системе доступен перечень всего программного обеспечения, обнаруженного сканерами уязвимостей при сканировании активов. Для просмотра списка ПО необходимо перейти в раздел ***Оценка соответствия ПО - Список ПО*** (см. рисунок 149).

Полное описание табличного списка ПО приведено в разделе «Подраздел "Список ПО"».

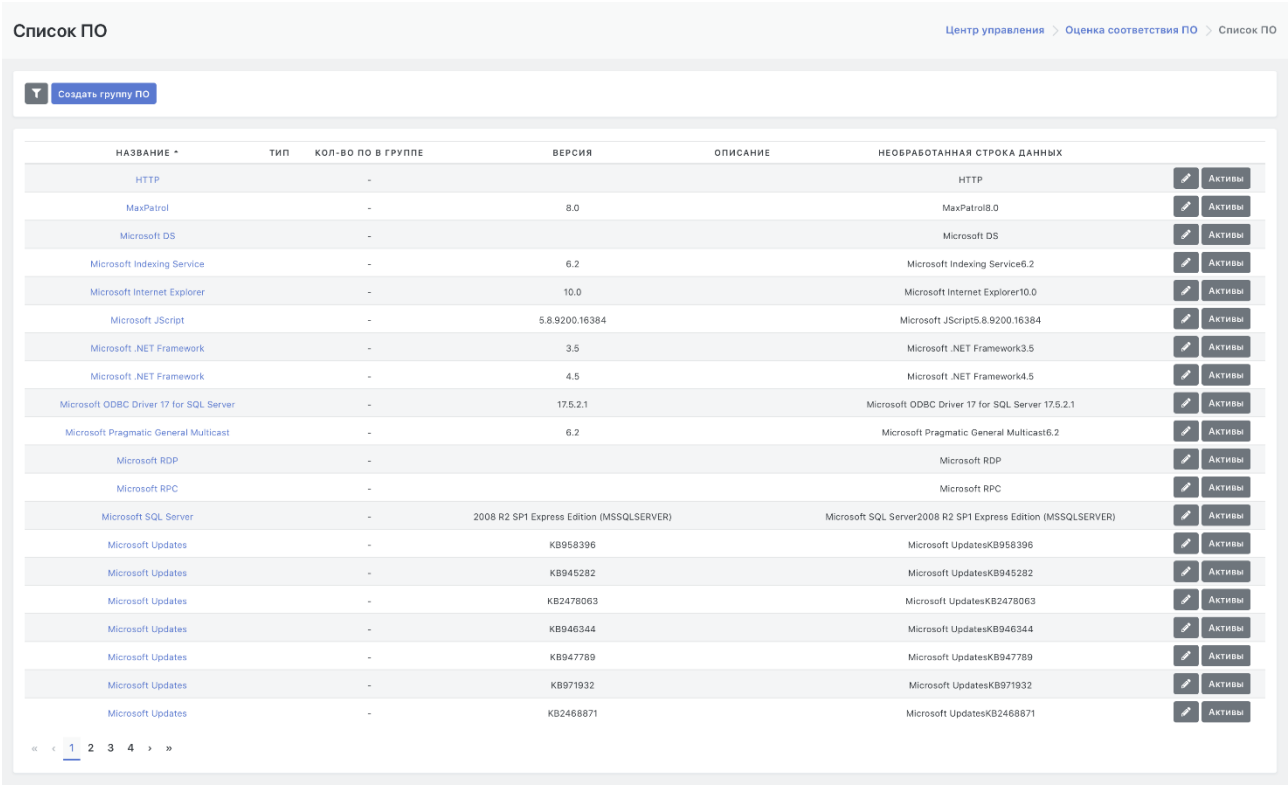



**Рисунок 149 – Окно вкладки «Список ПО»**

Для просмотра детализации по записи о программном обеспечении нужно щелкнуть на название программного обеспечения в поле "**Название**" (см. рисунок 149). На экране откроется форма детализации информации о ПО (см. рисунок 150).

Форма отображает следующие данные:

- **Название клиента** - уникальное название ПО на **Платформе Радар**;
- **Описание** - описание программного обеспечения, написанное пользователем **Платформы Радар**;
- **Название** - название программного обеспечения;
- **ОС** - операционная система, на которой работает ПО;
- **Версия** - версия ПО;
- **Релиз** - данные о релизе;
- **Необработанная строка** - данные, полученные напрямую от сканера уязвимостей.

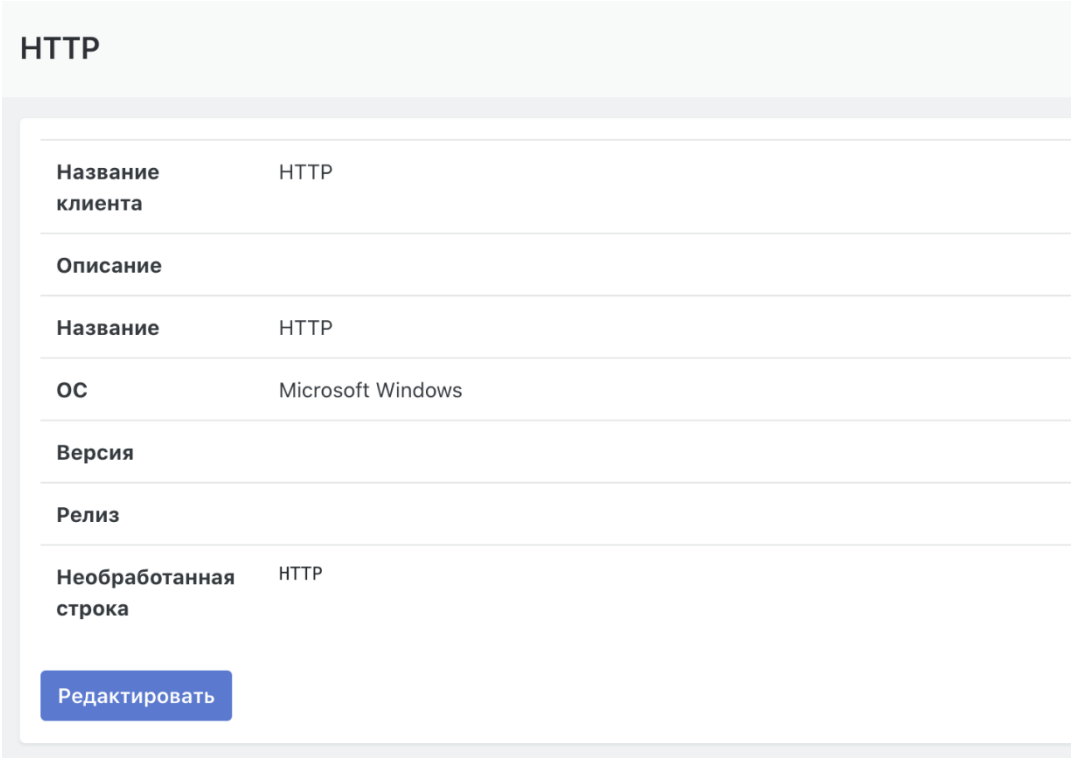



**Рисунок 150 – Форма просмотра деталей записи о программном обеспечении.**

## 17.2.2 Просмотр информации по активам

Для просмотра списка активов, на которых установлено интересующее ПО необходимо:

1. Перейти в раздел ***Оценка соответствия ПО - Список ПО***;
2. Нажать кнопку "**Активы**" в строке интересующего ПО.

На экране откроется перечень активов, на которых найдено данное ПО (см. рисунок 151). Данный перечень представляет собой стандартный для **Платформы Радар** табличный список активов.

Полное описание табличного списка активов приведено в разделе «Подраздел "Активы"».

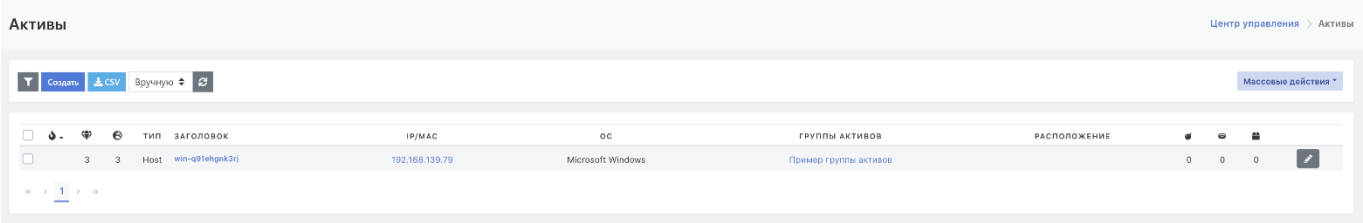



**Рисунок 151 – Перечень активов, на которых найдено при сканировании данное программное обеспечение**

## 17.2.3 Редактирование данных программного обеспечения

В системе реализована возможность внесения изменений в данные о программном обеспечении, полученные от сканера уязвимостей.

Для редактирования данных программного обеспечения необходимо:

1. Перейти в раздел ***Оценка соответствия ПО - Список ПО***;
2. Нажать на кнопку редактирования  в строке ПО, в данные которой нужно внести коррективы.
3. В открывшейся форме редактирования при необходимости можно отредактировать следующие записи о ПО (см. рисунок 152):
    - **Название клиента** - название ПО, которое будет отображаться в деталях инцидента.
    - **Описание** - описание ПО, созданное пользователем **Платформы Радар**.
4. Для сохранения внесенных изменений нажать на кнопку "**Сохранить**".

## 17.2.4 Удаление записи о ПО из списка

Для удаления ПО из списка выполнить следующие действия:

1. Перейти в раздел ***Оценка соответствия ПО - Список ПО***;
2. Нажать на кнопку редактирования  в строке записи ПО, которую необходимо удалить.
3. В открывшейся форме редактирования нажать на кнопку "**Удалить**" (см. рисунок 152).

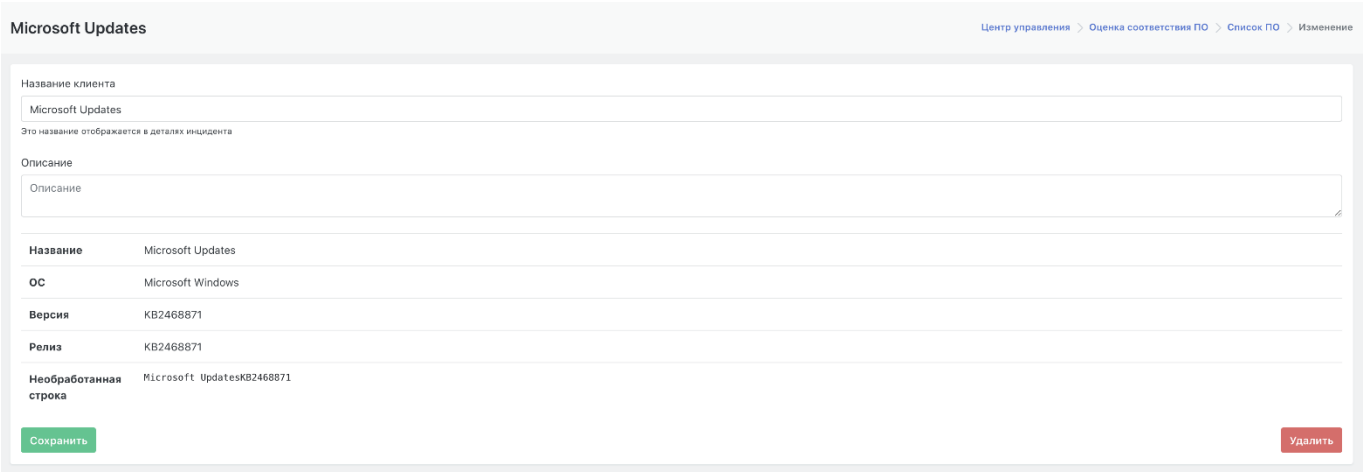



**Рисунок 152 – Окно редактирования программного обеспечения**

## 17.3 Назначение политики проверки соответствия ПО группе активов

Политика проверки назначается группе активов. Для связывания группы активов с одной или несколькими политиками проверки ПО необходимо:

1. Перейти в раздел ***Активы - Группы активов***;
2. Нажать кнопку редактирования  в строке группы активов, для которой конфигурируется политика;
3. В открывшейся форме в блоке "**Набор правил**" сконфигурировать нужные политики (см. рисунок 153):
    - для связывания политики проверки с группой активов необходимо выбрать одну или несколько политик;
    - для отвязывания политики проверки от группы активов необходимо нажать на пиктограмму  справа от имени набора правил.
4. Для сохранения введенных изменений нажать на кнопку "**Сохранить**".

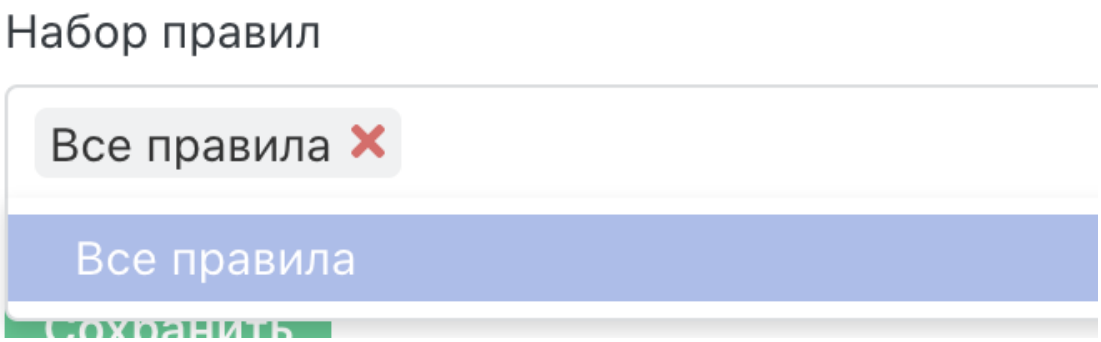



**Рисунок 153 – Назначение политики контроля группе активов**

## 17.4 Запуск процесса проверки соответствия

Процесс проверки соответствия ПО запускается пользователем **Платформы Радар** вручную. Для запуска проверки необходимо:

1. Перейти в раздел ***Активы - Группы активов***;
2. Нажать кнопку "**Проверка соответствия ПО**" в строке группы активов, для которой требуется провести оценку соответствия;
3. Перейти в раздел ***Оценка соответствия ПО - Результаты соответствия ПО*** для просмотра и анализа полученных результатов.

## 17.5 Анализ результатов проверок соответствия ПО

### 17.5.1 Просмотр сводных результатов проверок соответствия ПО

Сводные результаты всех текущих проверок соответствия ПО расположены в разделе ***Оценка соответствия ПО - Результаты соответствия ПО*** (см. рисунок 154).

Полное описание табличного списка результатов проверки соответствия ПО приведено в разделе «Подраздел "Результаты соответствия ПО"».

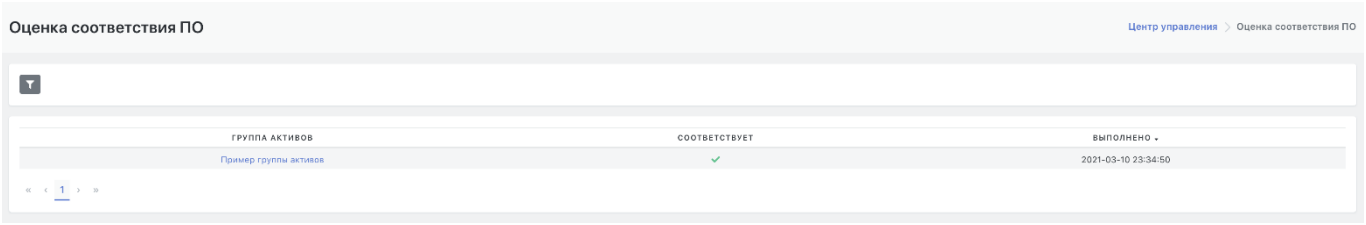



**Рисунок 154 – Окно вкладки «Результаты соответствия ПО»**

## 17.5.2 Просмотр результатов проверок соответствия по группе активов

Для просмотра результатов проверки соответствия ПО по группе активов необходимо:

1. Перейти в раздел ***Оценка соответствия ПО - Результаты соответствия ПО***;
2. В табличном списке результатов щёлкнуть по названию группы активов в поле "**Группа активов**".

Отобразится форма детализации проверки соответствия активов выбранным политикам контроля (см. рисунок 155):

- **Группа активов** - название контролируемой группы активов;
- **Соответствует** - статус соответствия ПО, расположенного на группе активов, заданным политикам проверки ПО;
- **Выполнено** - дата и время последней проверки на соответствие ПО;
- Табличный список активов в составе группы, включающий следующие поля:
    - **Актив** - название актива в **Платформе Радар**;
    - **Соответствует** - количество политик, которые дали положительный (соответствует) результат при проведении проверки соответствия ПО на данном активе;
    - **Не Соответствует** - количество политик, которые дали отрицательный (не соответствует) результат при проведении проверки соответствия ПО на данном активе;
    - **Данные ПО** - наличие/отсутствие данных об установленном программном обеспечении на активе.

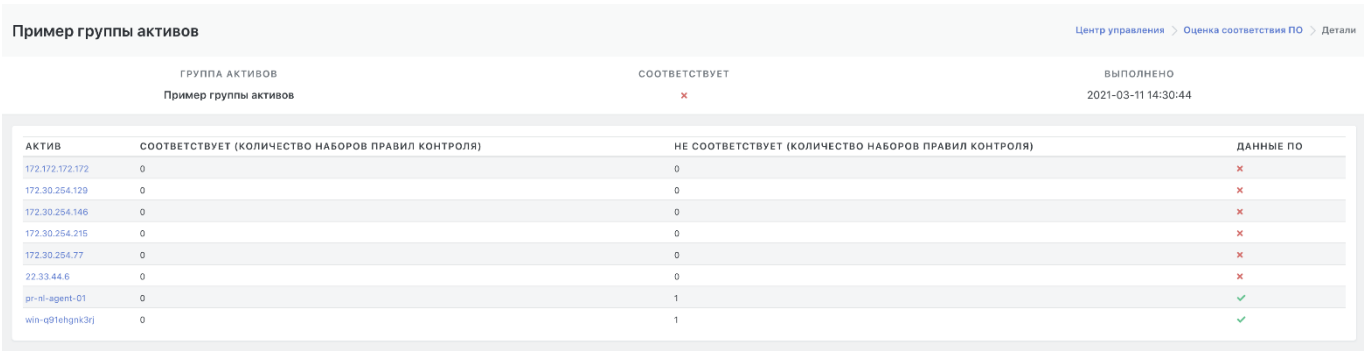



**Рисунок 155 – Просмотр результатов контроля соответствия по группе активов**

# 17.6 Управление политиками проверки соответствия ПО

## 17.6.1 Просмотр текущего списка политик

Текущий список политик расположен в разделе ***Оценка соответствия ПО - Наборы правил*** (см. рисунок 156).

Полное описание табличного списка политик приведено в разделе «Подраздел "Наборы правил"».

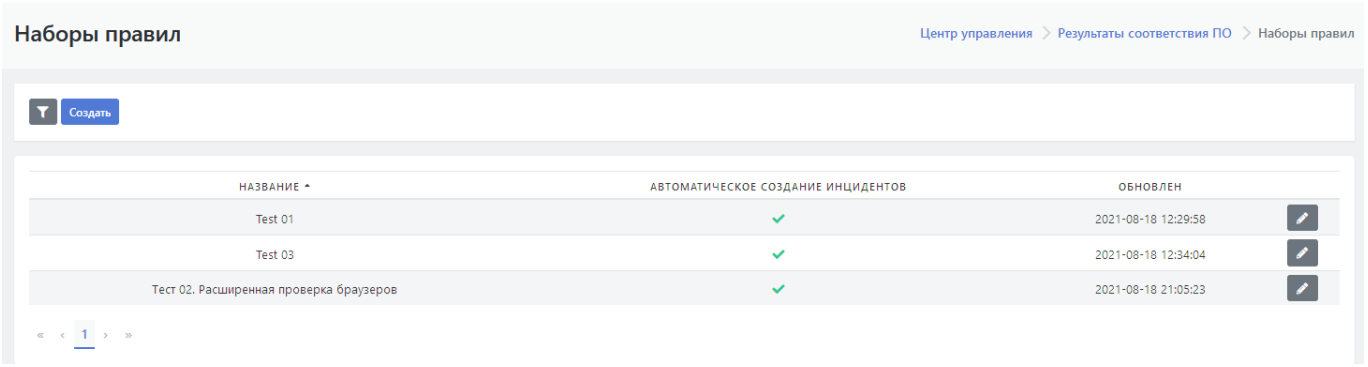



**Рисунок 156 – Список политик проверки соответствия ПО (набор правил)**

## 17.6.2 Создание новой политики

Для создания политики проверки соответствия ПО необходимо:

1. Перейти в раздел ***Оценка соответствия ПО - Наборы правил*** (см. рисунок 156);
2. Нажать на кнопку "**Создать**";
3. Заполнить форму создания политики проверки (см. рисунок 157):
    - **Название клиента** – название политики в **Платформе Радар**;
    - установить флаг "**Автоматическое создание инцидента при несоответствии**", если это необходимо;
    - выбрать для политики одно или последовательно несколько правил проверки из раскрывающегося списка.
4. Сохранить новую политику нажав на кнопку "**Сохранить**".

При выборе правил из списка можно использовать функцию поиска по текстовой строке. Искомая текстовая строка вводится непосредственно в поле списка правил.

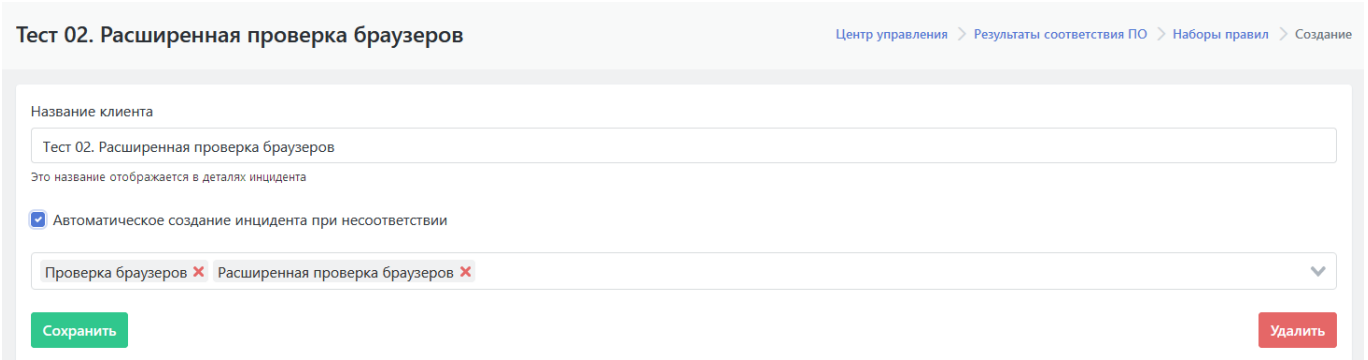



**Рисунок 157 – Создание новой политики (набора правил)**

### 17.6.3 Редактирование параметров политики

Для редактирования параметров политики проверки соответствия ПО из текущего списка необходимо выполнить следующие действия:

1. Перейти в раздел ***Оценка соответствия ПО - Наборы правил***;
2. Нажать на кнопку редактирования  в строке политики, у которой необходимо изменить параметры;
3. В открывшейся форме редактирования внести необходимые изменения параметров политики;
4. Нажать на кнопку "**Сохранить**" (см. рисунок 157).

### 17.6.4 Удаление политики из текущего списка

Для удаления политики проверки соответствия ПО из текущего списка необходимо выполнить следующие действия:

1. Перейти в раздел ***Оценка соответствия ПО - Наборы правил***;
2. Нажать на кнопку редактирования  в строке политики, которую необходимо удалить;
3. В открывшейся форме редактирования параметров политики нажать на кнопку "**Удалить**" (см. рисунок 157).

## 17.7 Управление правилами

### 17.7.1 Просмотр текущего списка правил

Текущий список правил расположен в разделе: ***Оценка соответствия ПО - Правила*** (см. рисунок 158).

Полное описание табличного списка политик приведено в разделе «Подраздел "Правила"».

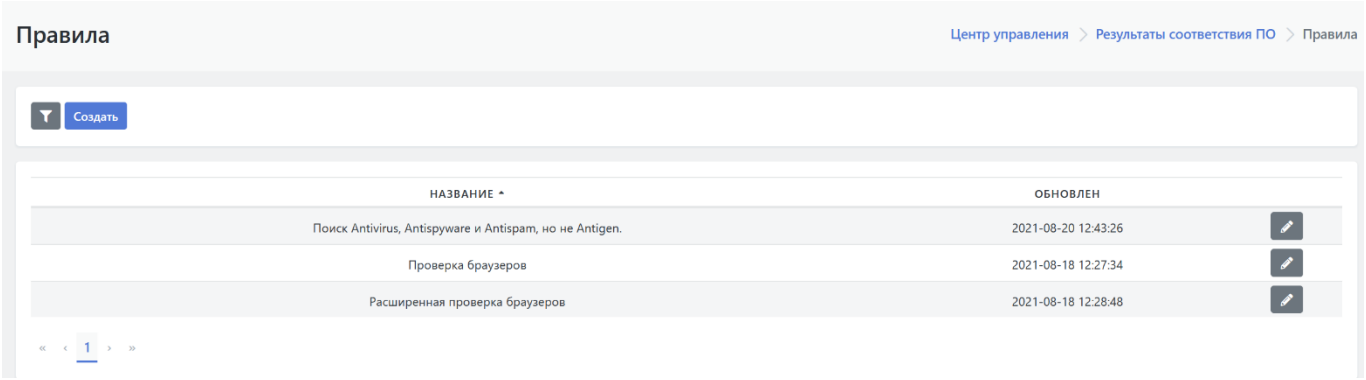



**Рисунок 158 – Текущий список правил проверки**

### 17.7.2 Создание нового правила

Для создания нового правила проверки соответствия ПО необходимо:

1. Перейти в раздел ***Оценка соответствия ПО - Правила*** (см. рисунок 158);
2. Нажать на кнопку "**Создать**";

3. Заполнить форму создания правила (см. рисунок 159):
    - **Название клиента** – название правила в **Платформе Радар**;
    - в поле "**Фильтр**" создать запись, по которой будет работать правило;
    - к полю "**Фильтр**" прикреплена справка по регулярным выражениям, которую при необходимости можно скрыть/раскрыть на экране;
    - при необходимости установить статус правила "**Запись в черном списке**".
4. Сохранить новое правило нажав на кнопку "**Сохранить**".

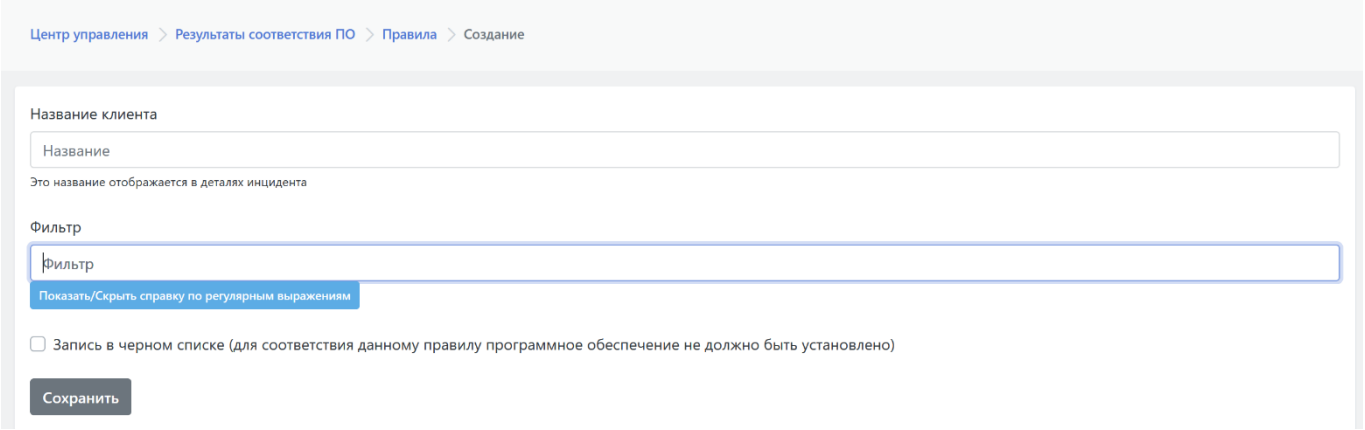



**Рисунок 159 – Создание нового правила**

## 17.7.3 Редактирование данных правила

Для редактирования параметров политики проверки соответствия ПО из текущего списка необходимо выполнить следующие действия:

1. Перейти в раздел ***Оценка соответствия ПО - Правила***;
2. Нажать на кнопку редактирования  в строке правила, которое необходимо изменить;
3. В открывшейся форме редактирования внести необходимые изменения в правило;
4. Нажать на кнопку "**Сохранить**" (см. рисунок 160).

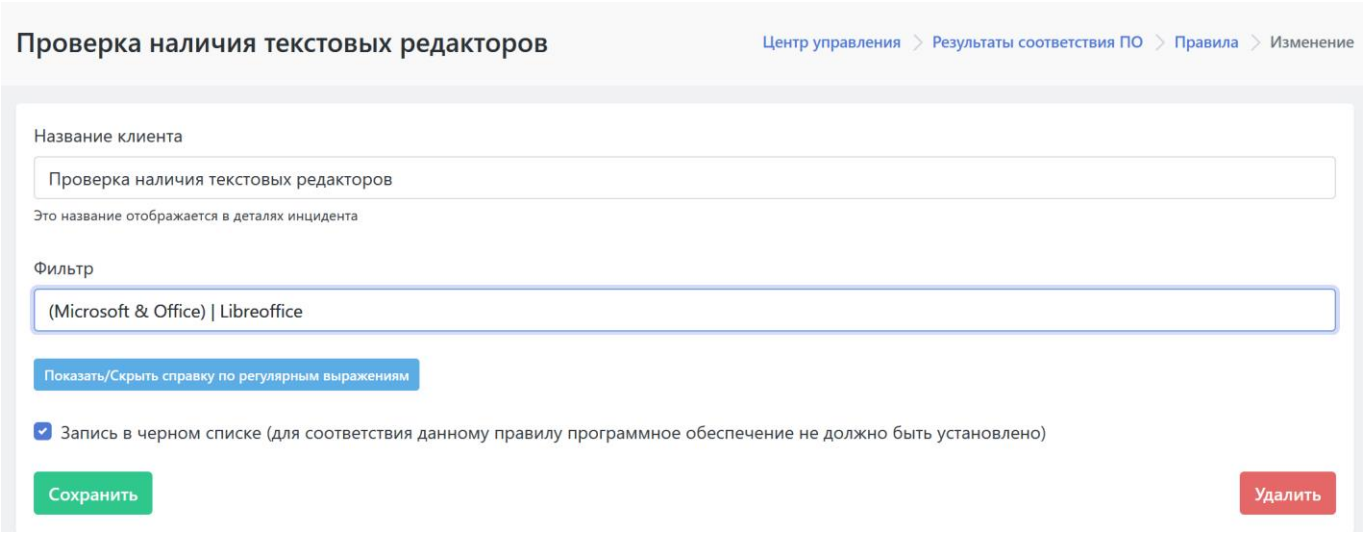



**Рисунок 160 – Редактирование правила**

### 17.7.4 Удаление правила из текущего списка

Для удаления правила из текущего списка необходимо выполнить следующие действия:

1. Перейти в раздел ***Оценка соответствия ПО - Правила***;
2. Нажать на кнопку редактирования  в строке правила, которое необходимо удалить.
3. В открывшейся форме редактирования параметров правила нажать на кнопку "**Удалить**" (см. рисунок 160);
4. В открывшейся форме подтвердить удаление нажав на кнопку "**Да**".

# 18. Интеграция со сканерами уязвимостей

**Сканер уязвимостей** - это специализированное программное обеспечение, предназначенное для поиска хостов в компьютерной сети и поиска уязвимостей в сетевых сервисах и программном обеспечении. **Платформа Радар** обеспечивает интеграцию со сканерами уязвимости Tenable Nessus, Redcheck и MaxPatrol 8 благодаря возможностями разбора отчетов о результатах сканирования выше озвученных сканеров.

## 18.1 Загрузка результатов сканирования

Для импорта результатов сканирования необходимо:

- Перейти в раздел ***Активы - Результаты сканирования***;
- Нажать кнопку "**Создать**";
- Выбрать тип сканера из выпадающего списка (см. рисунок 161);

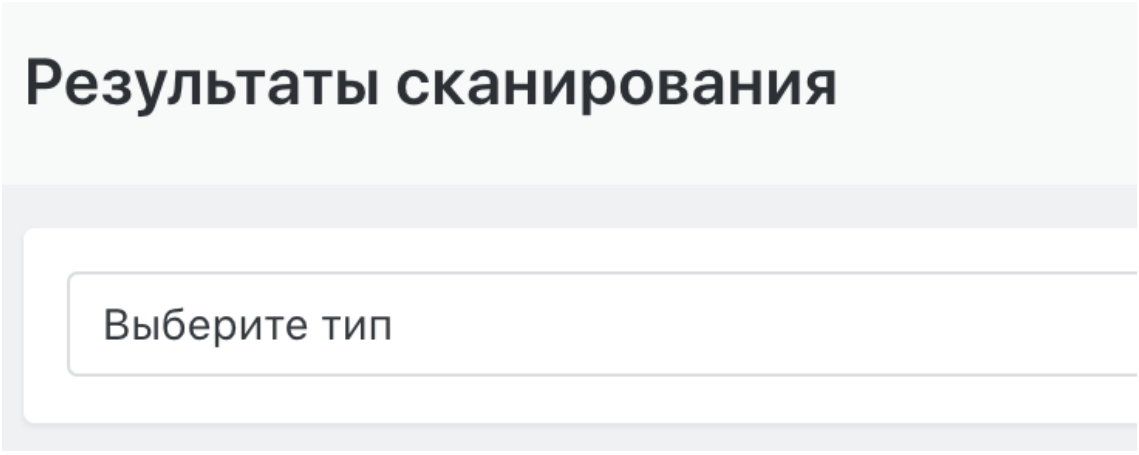



**Рисунок 161 - Форма выбора типа сканера**

- Загрузить через появившуюся форму файл с результатами сканирования (см. рисунок 162);


**Рисунок 162 - Форма загрузки файла результата сканирования**

- В появившемся файле нажать на пиктограмму  (см. рисунок 163).

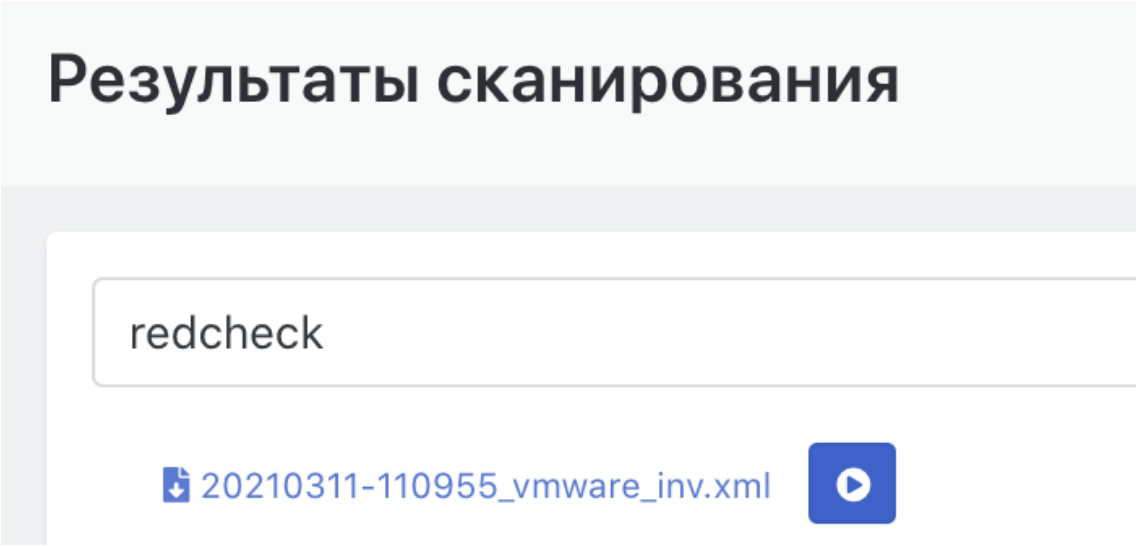



**Рисунок 163 – Список загруженных файлов для старта запуска обработки отчета**

## 18.2 Просмотр результатов сканирования

Для просмотра деталей импортированного сканирования необходимо:

- Перейти в раздел ***Активы - Результаты сканирования***;
- Кликнуть на название импортированной задачи.

В форме отображаются количественные результаты найденных уязвимостей, разделенные на группы важности по цвету согласно оценке CVSS (см. рисунок 164):

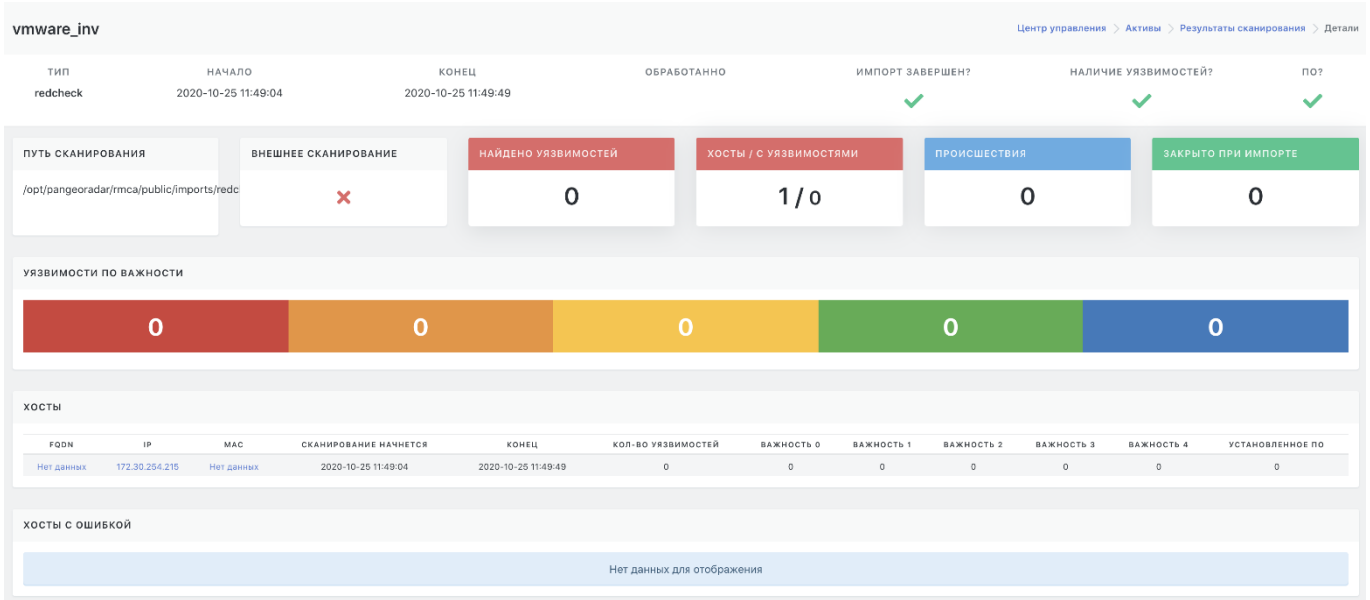



**Рисунок 164 – Окно просмотра результатов сканирования**

# 19. Работа с отчетами

Система позволяет выполнять все работы с отчетами и дашбордами в пользовательском веб-интерфейсе.

## 19.1 Общие данные об отчетах

Раздел "**Отчеты**" предназначен для формирования отчетов типа «дашборд» для наглядной визуализации информации по рабочим метрикам системы.

Отчеты создаются один раз за отчетный период. Отчетные периоды - последовательные интервалы времени, в рамках которых создаются отчеты. Длительность отчетного периода может быть разной. Все созданные отчеты доступны для скачивания для тех пользователей, которые имеют разрешения на данный отчет.

**Важно!** Режим редактирования отчетов, а соответственно функции управления отчетами и виджетами, доступны пользователям только с соответствующими правами.

**Платформа Радар** содержит два типа предустановленных отчетов: "**Главная**" и "**Для печати**".

## 19.2 Просмотр отчетов

### 19.2.1 Вывод отчета на экран

Для просмотра отчетов необходимо выполнить следующие действия (см. рисунок 165):

1. Открыть раздел основного меню "**Отчеты**";
2. В меню отчета в раскрывающемся списке "**Выберите отчет**" выбрать интересующий отчет, который отобразится в рабочей области раздела;
3. При необходимости:
    - провести настройку отчета по временному диапазону отображаемых данных (см. ниже раздел «Настройка временного интервала для отчета»);
    - настроить период обновления данных отчета (см. ниже раздел «Настройка обновления данных отчета»).

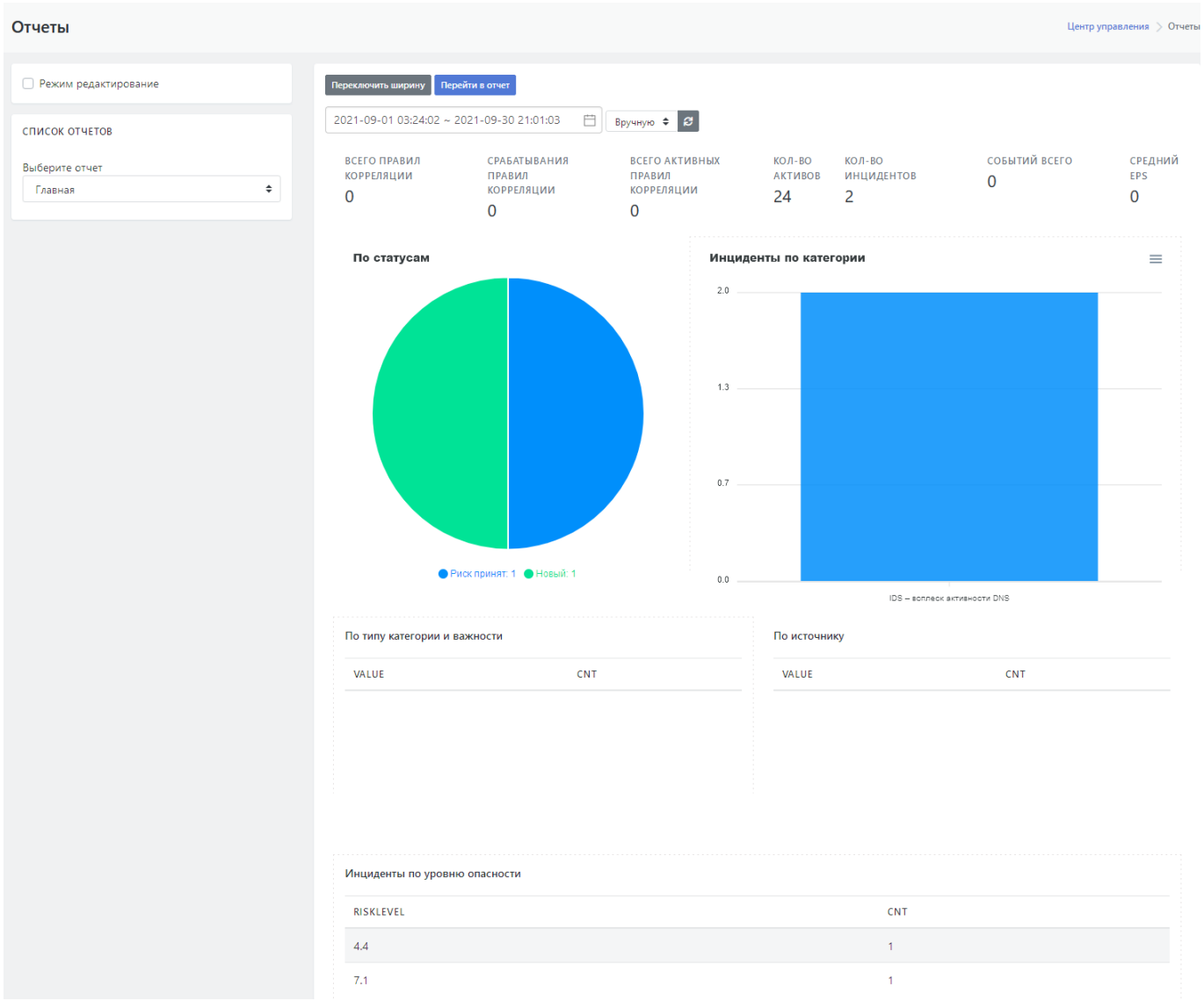



**Рисунок 165 – Просмотр отчета**

## 19.2.2 Настройка временного интервала для отчета

При необходимости можно настроить временной интервал, за который отчет выбирает данные из баз данных.

Для этого необходимо выполнить следующие действия:

1. Щёлкнуть по полю с диапазоном времени, расположенном над отчетом.
2. В открывшемся календаре выбрать дату начал и дату конца временного диапазона (см. рисунок 166). Если необходимо указать один день, то два раза щелкнуть по нужному дню.

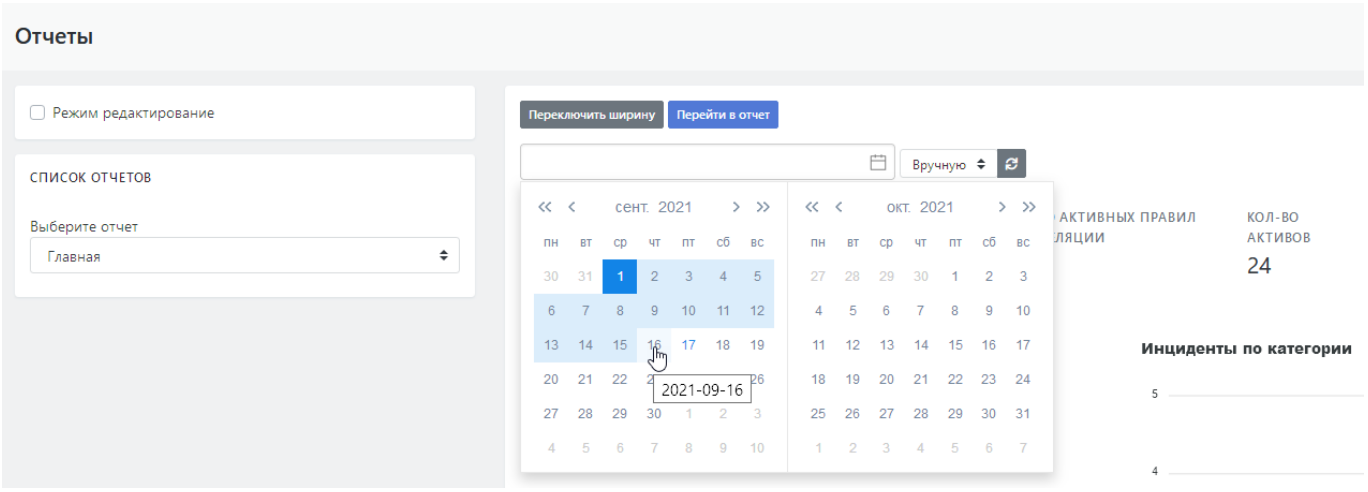



**Рисунок 166 – Установка дат начала и конца временного интервала выборки данных для отчета**

3. После установки дат откроется панель выбора времени для даты начала и конца временного интервала в формате ЧЧ.ММ.СС. Установить время для дат начала и конца временного интервала (см. рисунок 167).

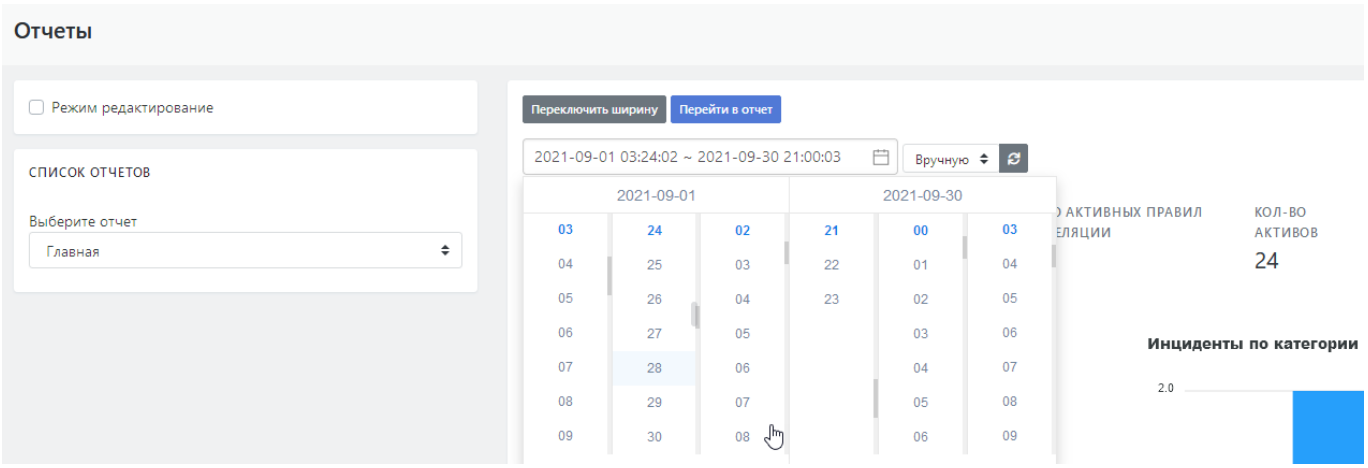



**Рисунок 167 – Установка времени для дат начала и конца временного интервала выборки данных для отчета**

После установки временного интервала в отчете отобразятся данные за указанный интервал.

## 19.2.3 Настройка обновления данных отчета

Над рабочей областью отчета расположена функция обновления данных отчета - поле с пиктограммой ( ). По умолчанию устанавливается режим ручного обновления. Обновление вручную производится при нажатии на пиктограмму.

Для автообновления выбрать временной интервал обновления в раскрывающемся списке:

- 5с
- 15с
- 30с
- 60с

### 19.2.4 Настройка отчета для печати

Перед началом печати отчета желательно сделать предпросмотр выводимого на печать материала. Для этого используются следующие средства раздела "**Отчеты**":

- Кнопка "**Переключить ширину**" сжимает отчет до размера листа А4 для предварительного просмотра расположения виджетов отчета.
- Кнопка "**Перейти в отчет**" открывает страницу отчета, подготовленную для печати стандартными средствами браузера. С помощью встроенных в браузер средств также можно сохранить отчет в формате PDF (см. рисунок 168).

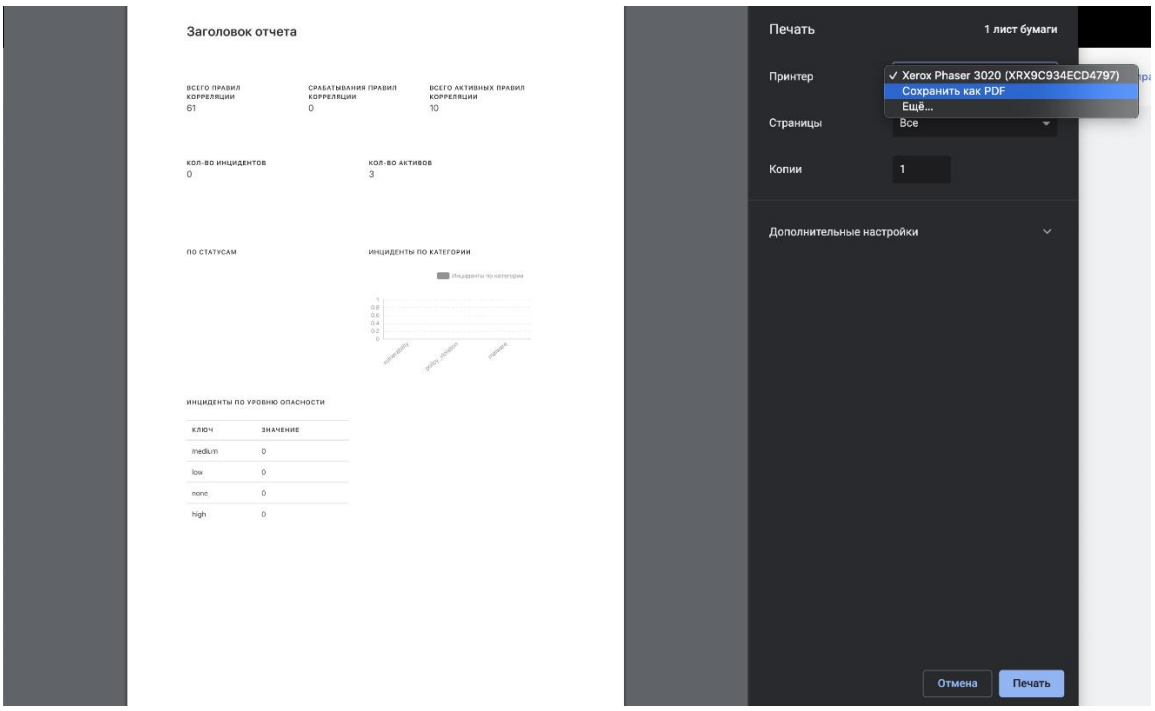



**Рисунок 168 – Печать отчета и сохранение его в PDF**

### 19.2.5 Назначение и описание предустановленных отчетов

**Платформа Радар** содержит два типа предустановленных отчетов: "**Главная**" и "**Для печати**".

Отчет "**Главная**" - это отчет, который по умолчанию выводится на главную страницу веб-интерфейса - **Рабочий стол** пользователя **Платформы Радар** (см. раздел «Рабочий стол»). Предустановленная форма отчета включает в себя стандартный набор основных данных по инцидентам (см. рисунок 169):

- **Всего правил корреляции** - количество правил корреляции.
- **Срабатывание правил корреляции** - количество сработавших правил.
- **Всего активных правил корреляции** - количество активных правил корреляции.
- **Количество активов** - количество активов, на которых произошло срабатывание правил корреляции.
- **Количество инцидентов** - количество зафиксированных инцидентов.
- **Событий всего** - всего событий.
- **Средний EPS** - число событий в секунду.

- **По статусам** - круговая диаграмма распределения инцидентов по их статусам.
- **Инциденты по категории** - столбчатая диаграмма распределения инцидентов по категориям.
- **Незакрытые инциденты по критичности** - табличный список распределения инцидентов по критичности.
- **По источнику** - табличный список распределения инцидентов по источникам.
- **CLOSED** - количество закрытых инцидентов.
- **По типу категории и важности** - табличный список распределения инцидентов по категории и важности.
- **Инциденты по уровню опасности** - табличный список распределение инцидентов по уровню опасности.

При необходимости предустановленный состав данных в отчете "**Главная**" можно изменить.

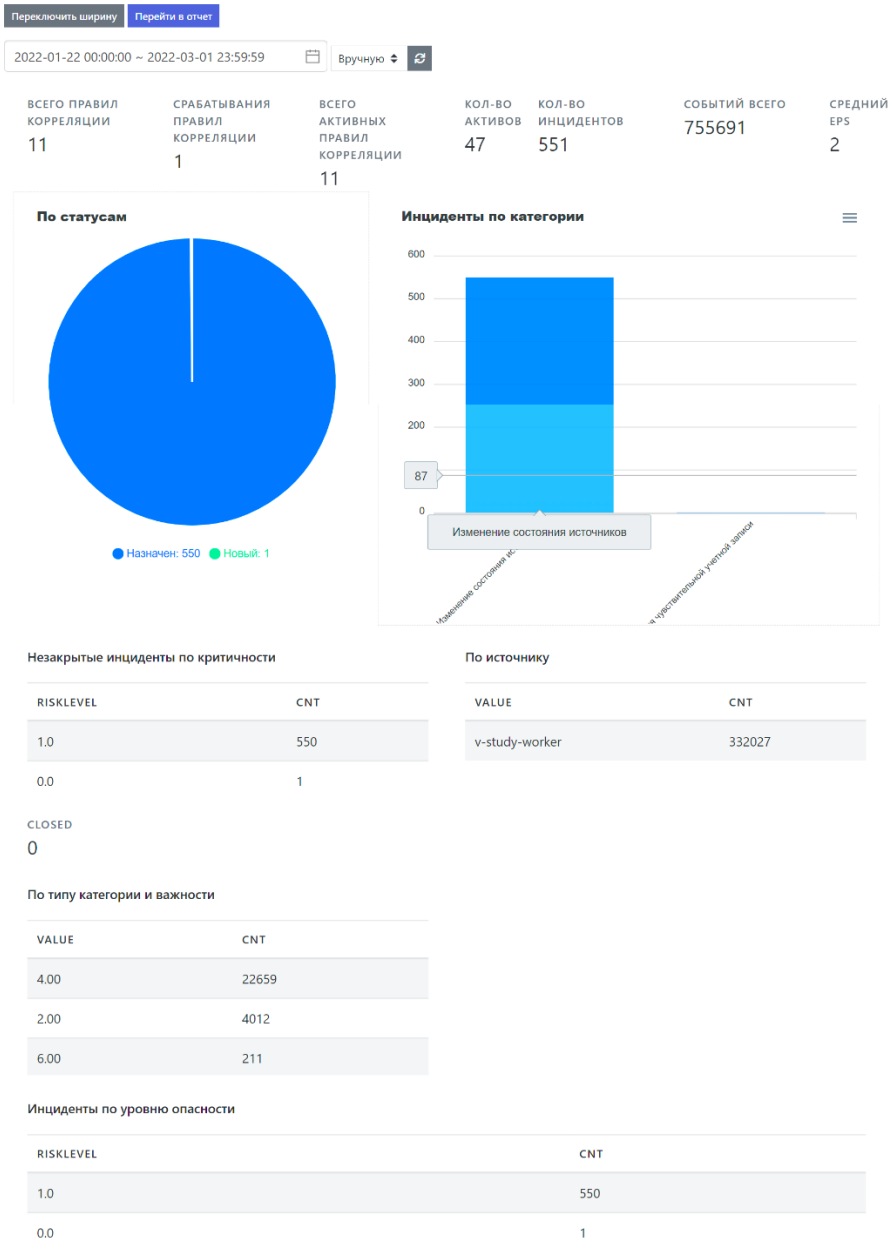



**Рисунок 169 - Отчет "Главная", предустановленный состав полей отчета**

Отчет "**Для печати**" - это отчет, в котором набор данных скомпонован для условий вывода на печать или просмотра в виде PDF-файла (под формат А4). Подробно вывод отчета на печать приведен выше в разделе «Настройка отчета для печати». Предустановленная форма отчета включает в себя следующий стандартный набор данных (см. рисунок 170):

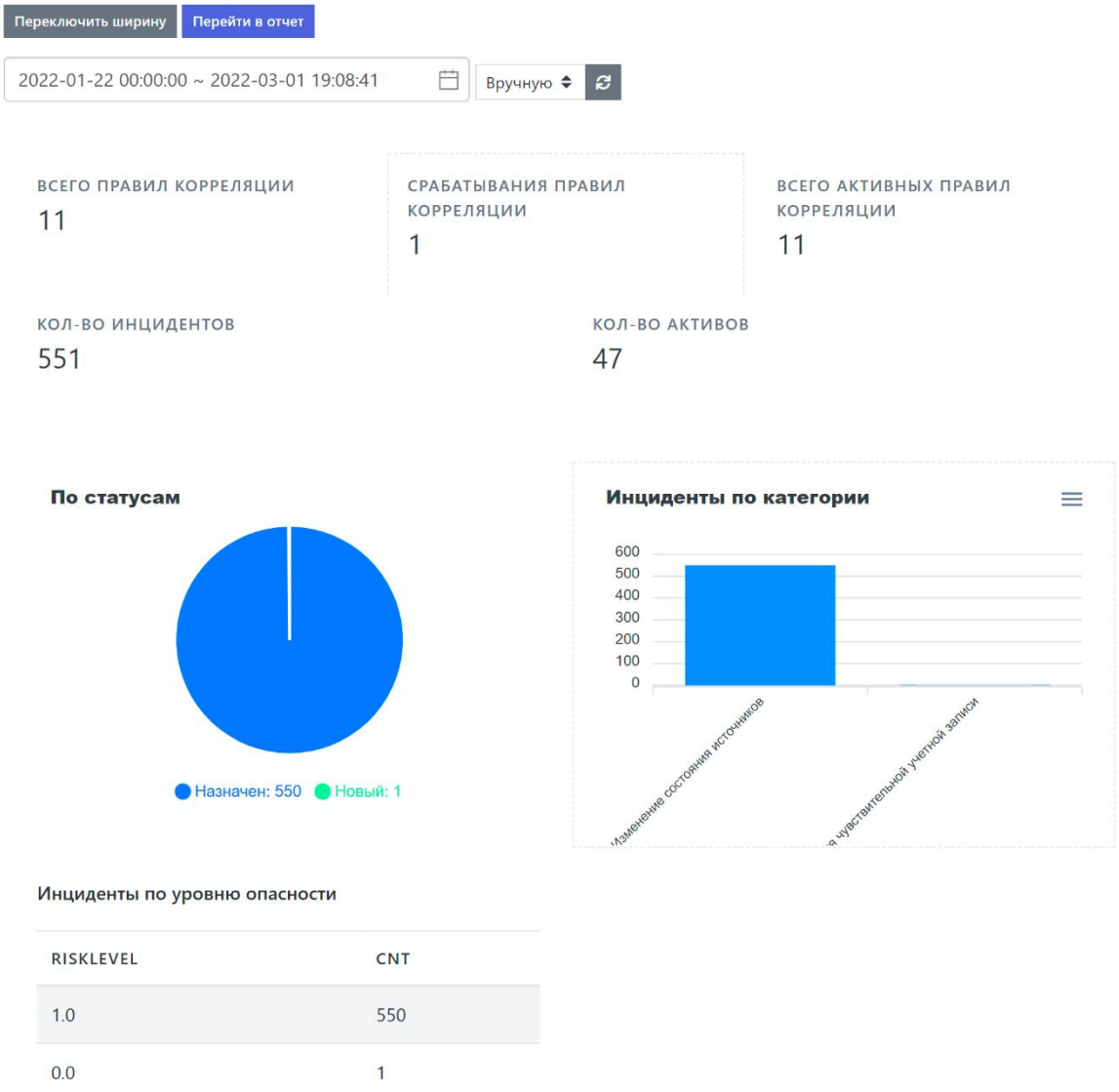



**Рисунок 170 - Отчет "Для печати", предустановленный состав полей отчета**

- **Всего правил корреляции** - количество правил корреляции.
- **Срабатывание правил корреляции** - количество сработавших правил.
- **Всего активных правил корреляции** - количество активных правил корреляции.
- **Количество активов** - количество активов, на которых произошло срабатывание правил корреляции.
- **Количество инцидентов** - количество зафиксированных инцидентов.
- **По статусам** - круговая диаграмма распределения инцидентов по их статусам.
- **Инциденты по категории** - столбчатая диаграмма распределения инцидентов по категориям.

- **Инциденты по уровню опасности** - табличный список распределение инцидентов по уровню опасности.

При необходимости предустановленный состав данных в отчете "**Для печати**" можно изменить.

## 19.3 Управление отчетами

### 19.3.1 Закрепление отчета на рабочем столе

Для закрепления отчета на рабочем столе как отчета по умолчанию необходимо выполнить следующие действия (см. рисунок 171):

1. Перейти в режим редактирования, установив флажок в поле "**Режим редактирования**".
2. Выбрать отчет в списке текущих отчетов.
3. Нажать на кнопку "**Поставить на главную**".
4. Перейти в любой другой раздел интерфейса **Платформы Радар**.
5. Вернуться в раздел "**Отчеты**" и убедиться, что в рабочей области раздела отображается заданный отчет.

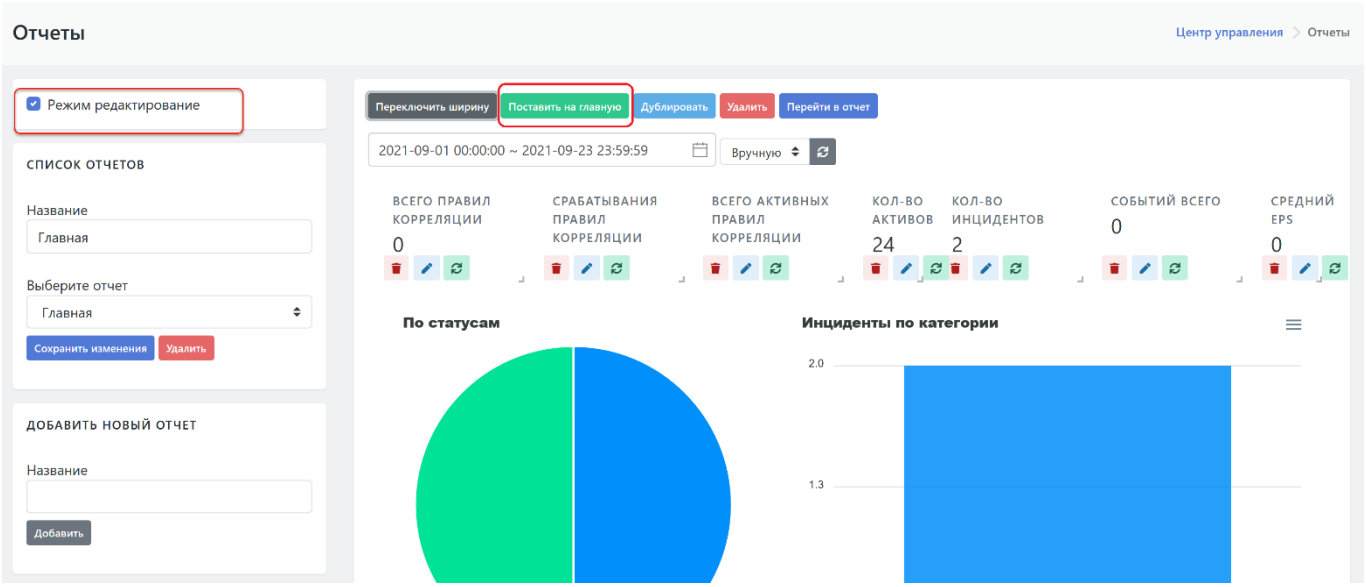



**Рисунок 171 – Работа с отчетами в режиме редактирования**

### 19.3.2 Дублирование отчета

Создание копии отчета со всеми виджетами предназначено для безопасного редактирования состава отчета.

Для дублирования отчёта необходимо выполнить следующие действия:

1. Перейти в режим редактирования, установив флажок в поле "**Режим редактирования**".
2. Выбрать отчет в списке текущих отчетов.
3. Нажать на кнопку "**Дублировать**".
4. Открыть список текущих отчетов. В списке должен появится дубль указанной отчета с пометкой *copied* (см. рисунок 172).

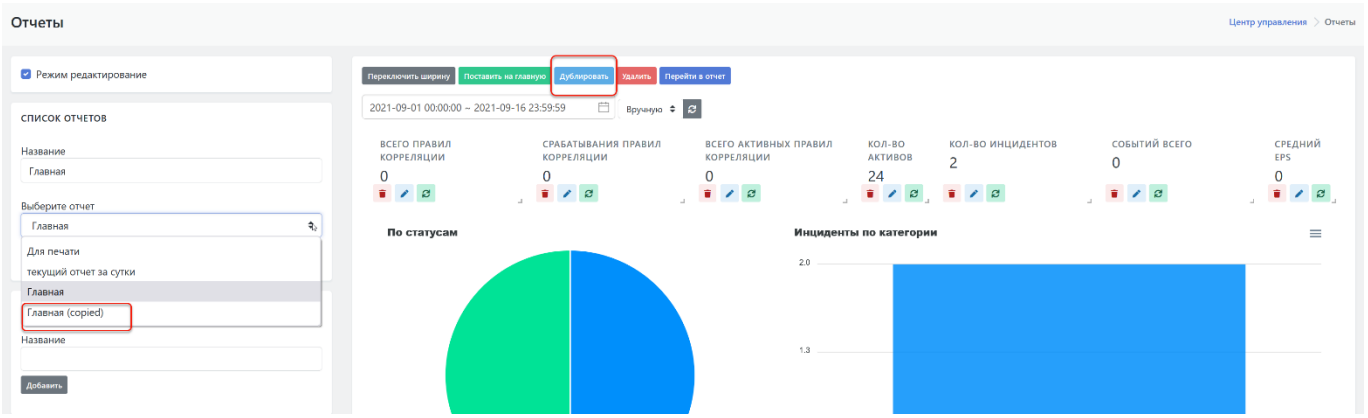



**Рисунок 172 – Дублирование отчета**

## 19.3.3 Создание нового отчета

Для создания нового отчета необходимо выполнить следующие действия:

1. Перейти в режим редактирования, установив флажок в поле "**Режим редактирования**".
2. В блоке "**Добавить новый отчет**" указать название нового отчета и нажать на кнопку "**Добавить**".
3. Выбрать вновь созданный отчет в списке текущих отчетов.
4. Добавить в отчет необходимые виджеты, используя блок "**Добавить новые виджеты**":
5. Нажать на кнопку "**Сохранить изменения**", расположенную под списком отчетов.

Работа с виджетами подробно приведена в разделе «Управление виджетами».

## 19.3.4 Редактирование отчета

Для редактирования отчета необходимо выполнить следующие действия:

1. Перейти в режим редактирования, установив флажок в поле "**Режим редактирования**".
2. При необходимости провести редактирование следующих параметров отчета:
    - изменить имя отчета в поле "**Название**";
    - отредактировать параметры виджетов в рабочей области;
    - изменить состав виджетов в отчете - удалить существующие или добавить новые виджеты.
3. Нажать на кнопку "**Сохранить изменения**", расположенную под списком отчетов.

Работа с виджетами подробно приведена в разделе «Управление виджетами».

## 19.3.5 Удаление отчета

Для удаления отчета с **Платформы Радар** необходимо выполнить следующие действия:

1. Перейти в режим редактирования, установив флажок в поле "**Режим редактирования**".
2. Выбрать отчет в списке текущих отчетов.
3. Нажать либо на кнопку "**Удалить**", расположенную под списком текущих отчетов, либо на аналогичную кнопку, расположенную над рабочей областью.

**Важно!** *Удаление отчета происходит без подтверждения удаления*.

## 19.4 Управление виджетами

**Важно!** *Все действия по управлению виджетами в отчетах совершаются в режиме редактирования. Для этого необходимо установить флажок в поле "**Режим редактирования**".*

### 19.4.1 Добавление нового виджета

Добавление в отчет нового виджета приведено ниже в разделе «Добавление в отчет нового виджета».

### 19.4.2 Изменение положения виджета в отчете

Для изменения положения виджета на странице отчета необходимо:

1. Выбрать в списке текущих отчетов необходимый отчет.
2. Навести курсор мыши на виджет.
3. Удерживая нажатой левую кнопку мыши перетащить виджет в другое место отчета.
4. Для сохранения нового положения виджета в отчете нажать на кнопку "**Сохранить изменения**".

### 19.4.3 Изменение размеров виджета в отчете

Для изменения размеров виджета на странице отчета необходимо:

1. Выбрать в списке текущих отчетов необходимый отчет.
2. Навести курсор мыши на нижний правый угол виджета.
3. Удерживая нажатой левую кнопку перетащить правый нижний угол виджета и тем самым изменить его размер (см. рисунок 173).

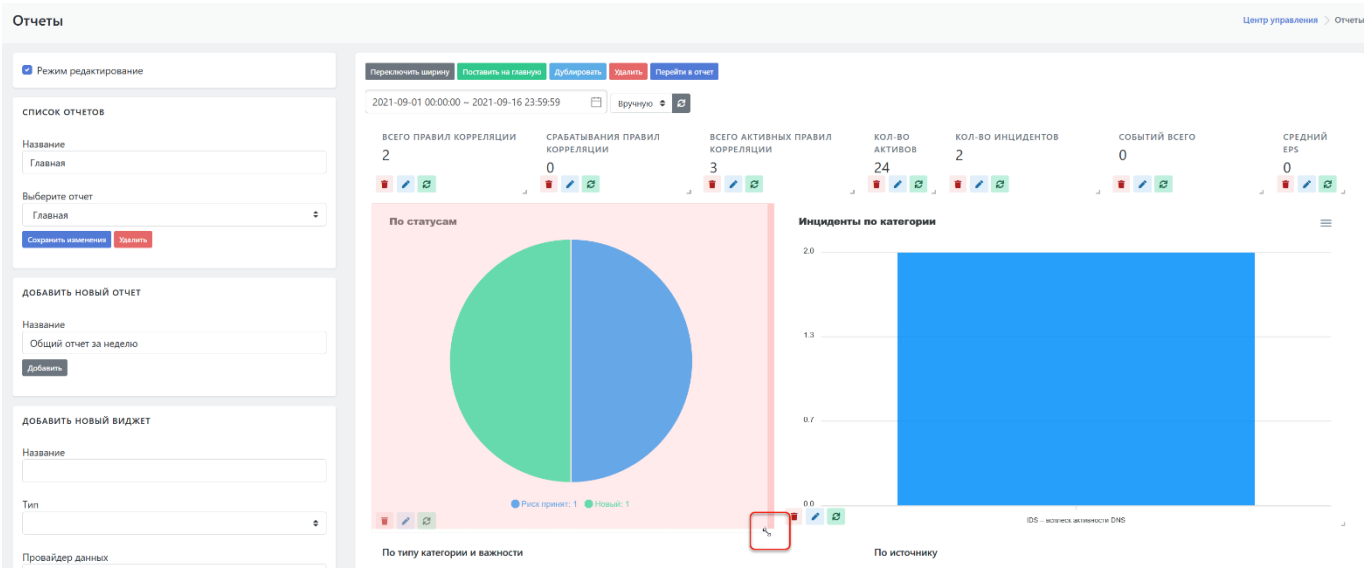



**Рисунок 173 – Изменение размера виджета**

4. Для сохранения нового размера виджета в отчете нажать на кнопку "**Сохранить изменения**".

### 19.4.4 Редактирование параметров виджета

Для редактирования параметров виджета на странице отчета необходимо:

1. Выбрать в списке текущих отчетов необходимый отчет.
2. В рабочей области выбрать нужный виджет и щелкнуть по соответствующей ему пиктограмме  в левом нижнем углу виджета.

   Откроется форма с параметрами данного виджета. Состав параметров формы аналогичен составу параметров формы создания нового виджета (см. раздел «Добавление в отчет нового виджета»).
3. Внести необходимые изменения в параметры виджета.
4. Для внесения изменений в параметры виджета нажать на кнопку "**Изменить**", расположенную внизу формы с параметрами.
5. Нажать на пиктограмму  для принудительного обновления данных виджета после изменения его параметров.

### 19.4.5 Удаление виджета

Для удаления виджета со страницы отчета необходимо:

1. Выбрать в списке текущих отчетов необходимый отчет.
2. В рабочей области выбрать нужный виджет и щелкнуть по соответствующей ему пиктограмме  в левом нижнем углу виджета. Внести необходимые изменения в параметры виджета.
3. Для внесения изменений в параметры виджета нажать на кнопку "**Изменить**".

### 19.4.6 Типы виджетов

#### 19.4.6.1 Перечень типов виджетов

Перечень типов виджетов представлен в раскрывающемся списке "**Тип**" (см. рисунок 174).

**Платформа Радар** поддерживает следующие типы виджетов:

- Численное значение;
- Круговая диаграмма;
- Столбчатая диаграмма;
- Столбчатая диаграмма (stacked);
- Линейная диаграмма;
- Радар диаграмма;
- Обручевая диаграмма;
- Radial Area диаграмма;
- Таблица;

- Заголовок;
- Абзац текста.

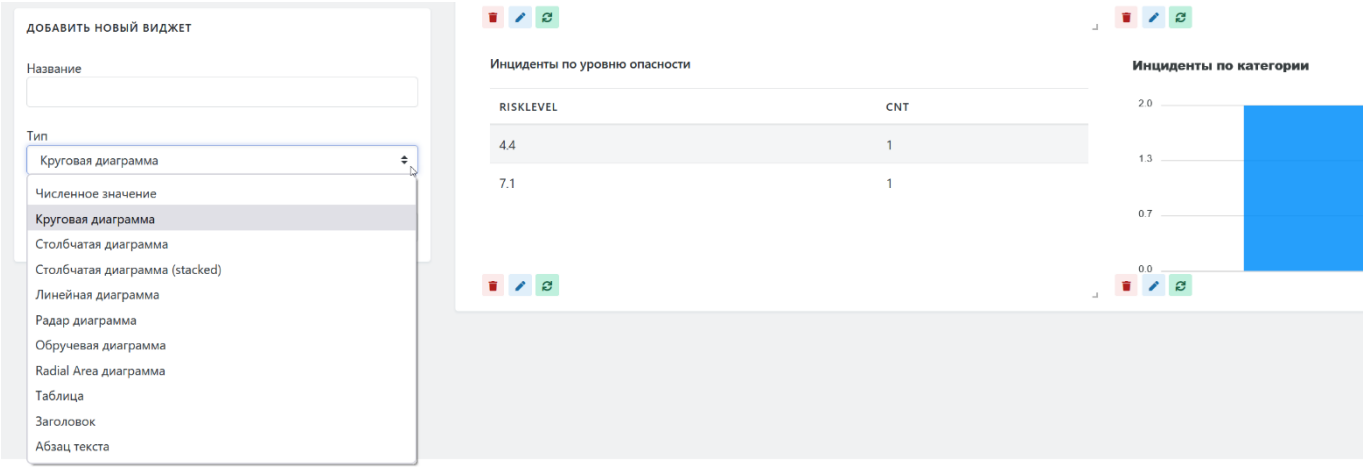



**Рисунок 174 – Типы виджетов**

### 19.4.6.2 Численное значение

Данный виджет содержит в себе целое число из результата запроса к базе данных (см. рисунок 175).

Поддерживается провайдерами:

- SIEM;
- Коррелятор;
- События;
- Сохраненные фильтры.

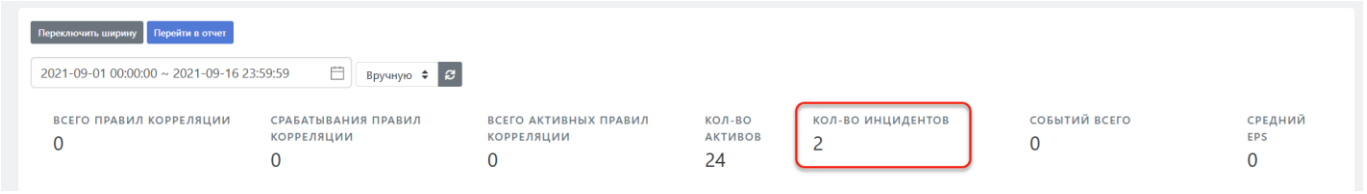



**Рисунок 175 – Пример виджетов типа «Численное значение»**

### 19.4.6.3 Круговая диаграмма

Тит виджета "Круговая диаграмма" (см. рисунок 176) поддерживается провайдерами:

- SIEM;
- Коррелятор;
- События.

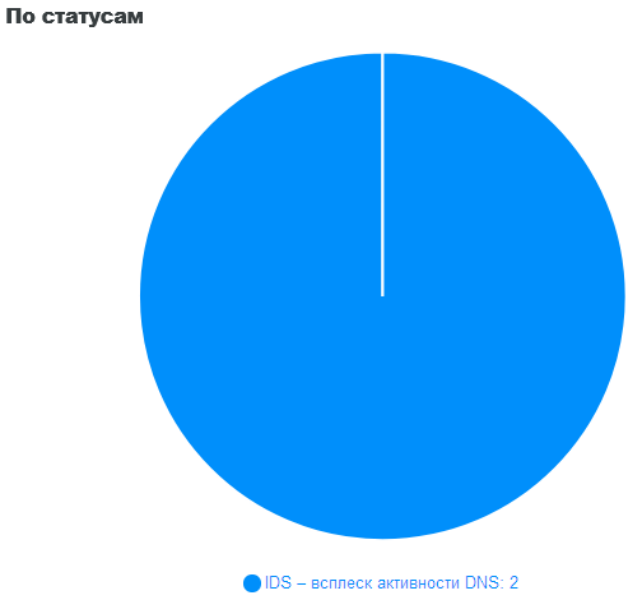



**Рисунок 176 - Пример виджета типа «Круговая диаграмма»**

### 19.4.6.4 Столбчатая диаграмма

Тит виджета "Столбчатая диаграмма" (см. рисунок 177) поддерживается провайдерами:

- SIEM;
- Коррелятор;
- События.

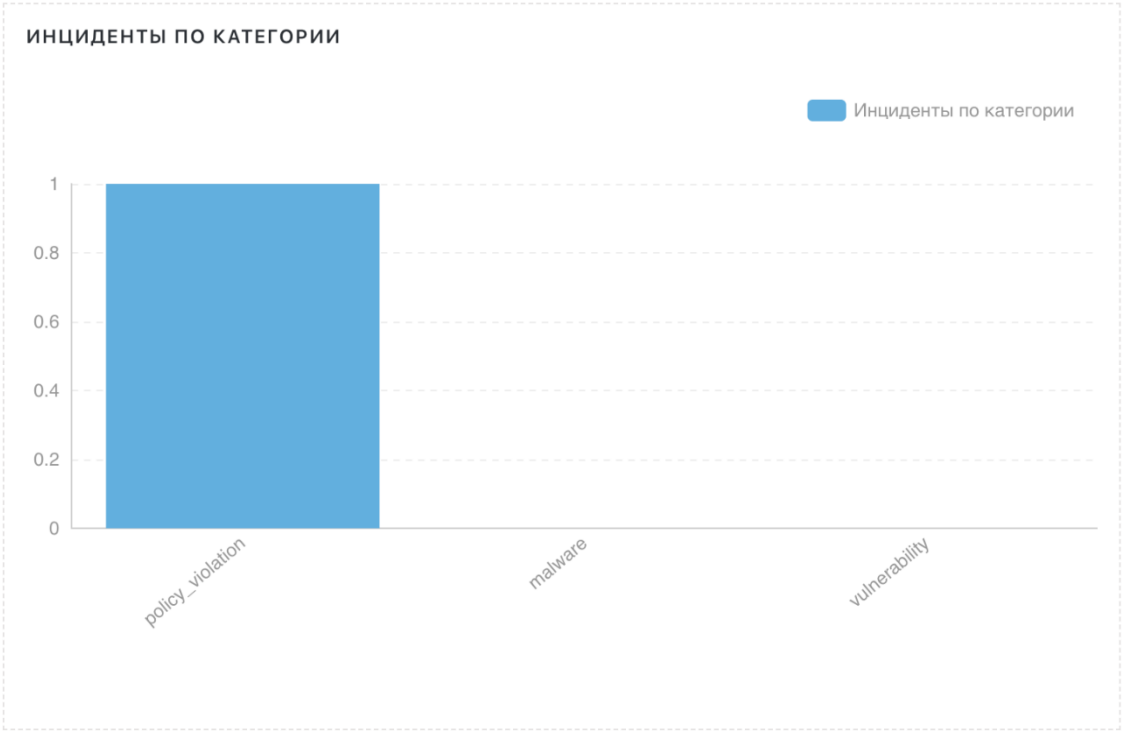



**Рисунок 177 - Пример виджета типа «Столбчатая диаграмма»**

#### 19.4.6.5 Таблица

Тит виджета "Таблица" (см. рисунок 178) поддерживается провайдерами: :

- SIEM;
- Коррелятор.

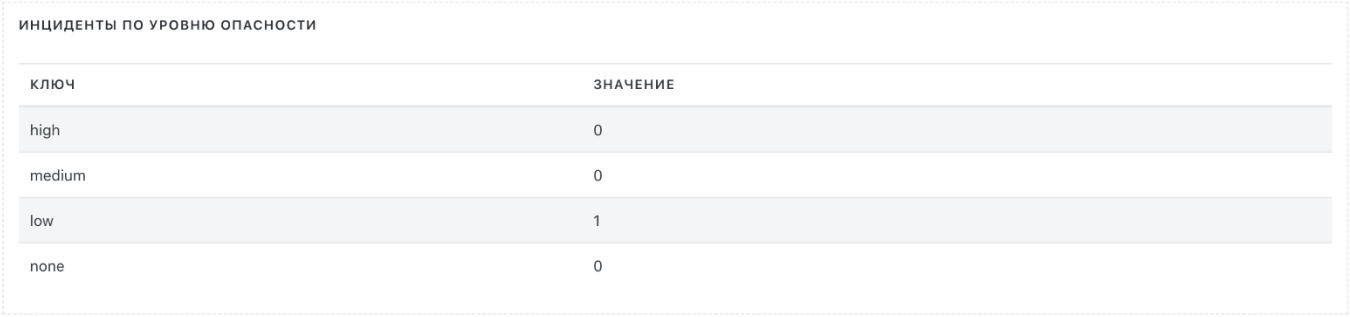



**Рисунок 178 - Пример виджета типа «Таблица»**

#### 19.4.6.6 Заголовок

Информационный виджет - отображает заранее сохраненный текст в настройках виджета (см. рисунок 179).


**Рисунок 179 – Пример виджета типа «Заголовок»**

# 19.5 Провайдеры

## 19.5.1 Общее описание

**Платформа Радар** в режиме редактирования отчетов (флажок "**Редактирование отчета**") поддерживает возможность создания новых виджетов:

- на основе сохраненных фильтров;
- на основе запросов к хранилищу данных.

У каждого из перечисленных выше провайдеров есть ограниченный набор своих типов «запросов».

Для провайдера **на основе фильтра** может быть использован запрос на такие данные как:

- Инциденты;
- Активы;
- Результаты корреляции;
- Правила корреляции;
- События.

Для данных от провайдера на основе фильтра доступная визуализация только в рамках численного значения. В качестве провайдеров могут быть использованы фильтры созданные и сохраненные

при работе с любым типом данных из вышеуказанного перечня. Например, фильтр, созданный и сохраненный в разделе интерфейса "Просмотр событий".

Для провайдера **на основе запроса к хранилищу данных** может быть использован запрос на такие данные как:

- Инциденты;
- Типы инцидентов;
- Статусы инцидентов;
- Уровни угрозы инцидентов;
- Затронутые активы;
- Затронутые группы активов;
- Активы;
- Правила;
- Правила корреляции с небольшим количеством инцидентов;
- Результаты;
- Все события;
- Средний поток событий;
- Все события по источнику;
- Все события по источнику, группировка по важности;
- Все события с группировкой;
- Все события с группировкой (счетчик);
- Все события с группировкой (Stacked);
- Все события с группировкой (счетчик по доп. группировке).

### 19.5.2 Добавление в отчет нового виджета

Для добавления нового виджета в отчет при создании отчета или редактировании необходимо:

1. Выбрать в списке текущих отчетов необходимый отчет.
2. В блоке "**Добавить новый виджет**" ввести в поле "**Название**" название нового виджета под которым он будет отображаться в отчете.
3. Из раскрывающегося списка "**Тип**" выбрать тип нового виджета. Если далее в качестве провайдера будет использоваться фильтр, то надо выбрать тип данных "**Численное значение**".
4. Выбрать провайдера данных для нового виджета - раскрывающийся список "**Провайдер данных**".
5. В списке "**Запрос**" указать тип данных для создания виджета.

6. Если в качестве провайдера был указан готовый запрос - то указать значение в строке "**Поле**", откорректировать данные, если это необходимо, и нажать кнопку "**Добавить виджет**" (см. рисунок 180).
7. Если в качестве провайдера был указа фильтр, то выбрать нужный фильтр из предложенного списка, нажать кнопку "**Загрузить фильтр**", откорректировать данные, если это необходимо, и нажать кнопку "**Добавить виджет**".

Виджет с заданными характеристиками должен появится в отчете.

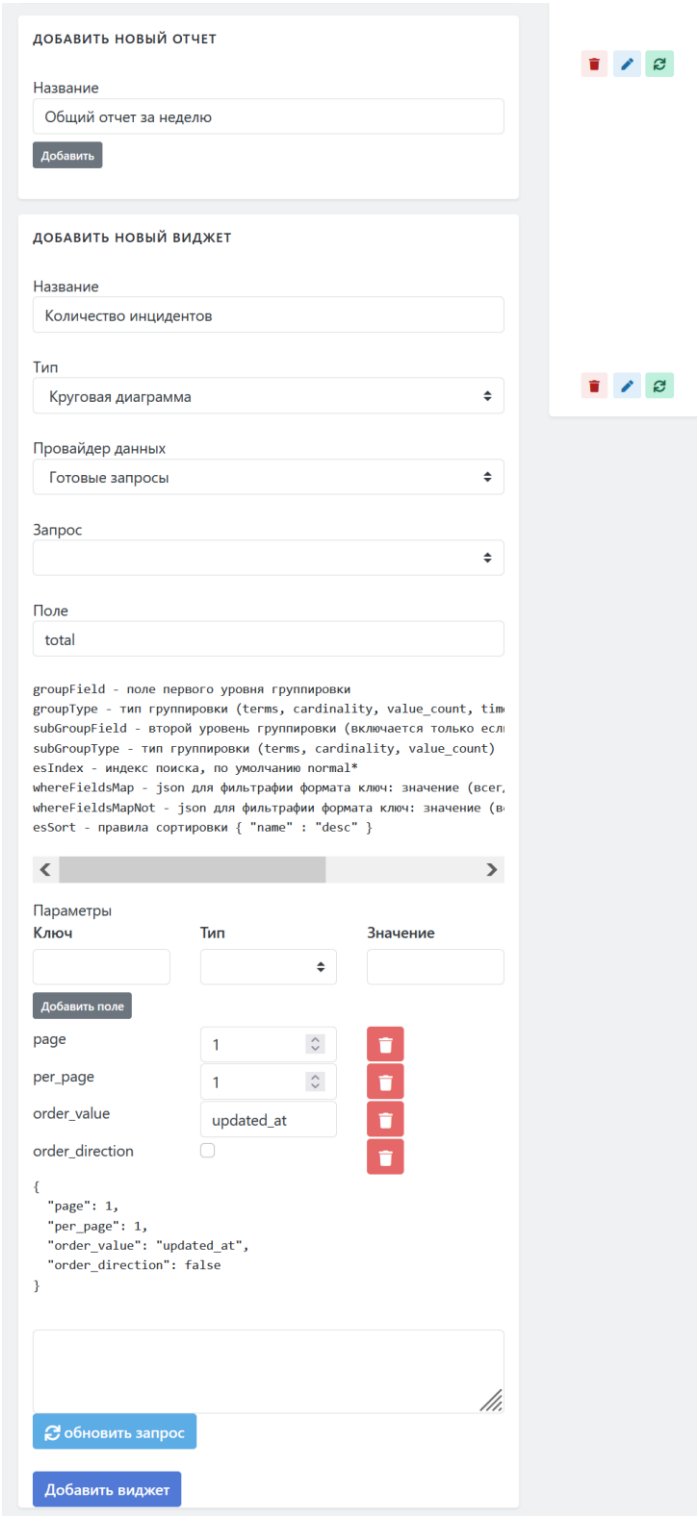



**Рисунок 180 - Добавление нового виджета**

# 20. Работа с правилами корреляции

Раздел содержит описание процессов, связанных с настройкой и обслуживанием правил корреляции.

## 20.1 Предустановленные правила корреляции. Разработка правил корреляции

**Платформа Радар** поставляется с набором готовых правил, которые при необходимости можно быстро включить, следующих категорий:

- обнаружение вредоносного кода;
- обнаружение подозрительных объектов в сетевом трафике;
- обнаружение подозрительной активности;
- аномалии в событиях аутентификации;
- контроль изменения конфигураций.

При необходимости можно разработать собственные правила корреляции.

## 20.2 Управление правилами корреляции

### 20.2.1 Параметры правила корреляции

Перечень правил корреляции представлен на рисунке 181.

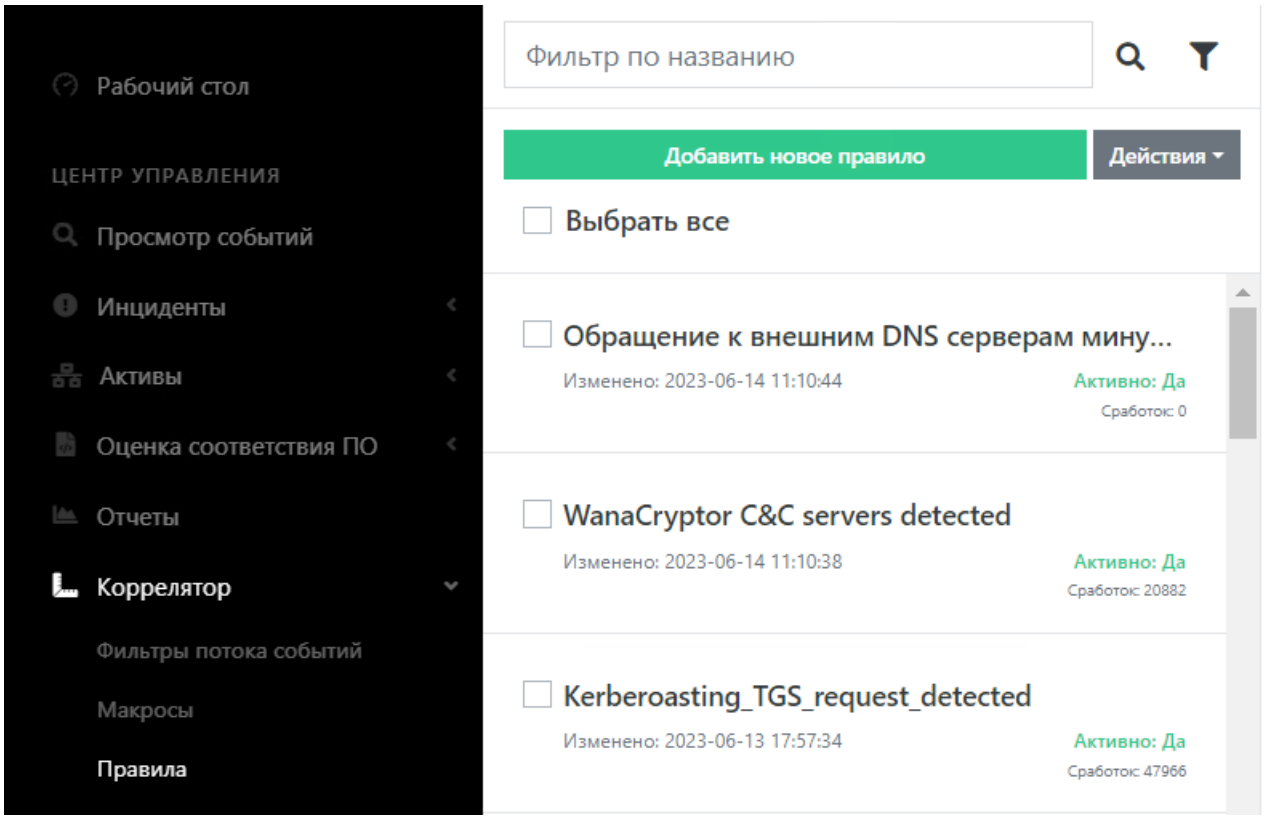



**Рисунок 181 – Перечень правил корреляции**

Для управления правилами корреляции при нажатии на кнопку "**Действие**" разворачивается перечень пунктов:

- **Активировать** - позволяет включить выбранные правила корреляции;
- **Выключить** - позволяет выключить выбранные правила корреляции;
- **Экспортировать** - позволяет экспортировать выбранные правила корреляции в файл;
- **Импортировать** - позволяет импортировать правила корреляции из файла;
- **Удалить** - позволяет удалить выбранные правила корреляции;
- **Экспортировать всё** - позволяет экспортировать все правила корреляции в файл;
- **Удалить всё** - позволяет удалить все правила корреляции.

В перечне доступна фильтрация по наименованию правила корреляции. Для поиска подходящего правила введите часть его названия и кликните на иконку поиска . Для сброса условий поиска очистите поле ввода наименования правила и снова кликните на иконку поиска.

Также при клике на иконку установки фильтра можно задать дополнительную фильтрацию (см. рисунок 182).

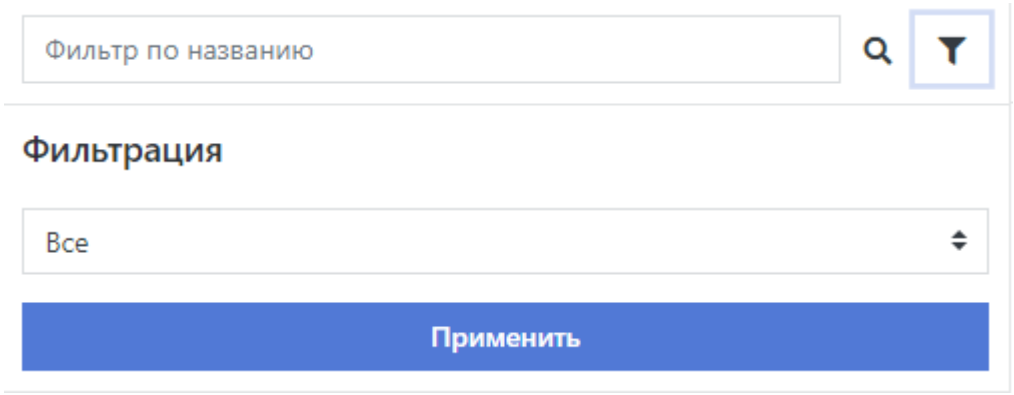



**Рисунок 182 - Фильтрация правил корреляции**

Выберите из списка статус правил корреляции (все, активные, выключенные) и нажмите кнопку "**Применить**", после чего в списке будут отображены только правила корреляции, удовлетворяющие установленным фильтрам.

Для добавления нового правила корреляции кликните на кнопку "**Добавить новое правило**", после чего откроется окно редактирования нового правила корреляции.

Для настройки параметров правила корреляции выберите правило из перечня. При клике на правило корреляции откроются свойства правила (см. рисунок 183).

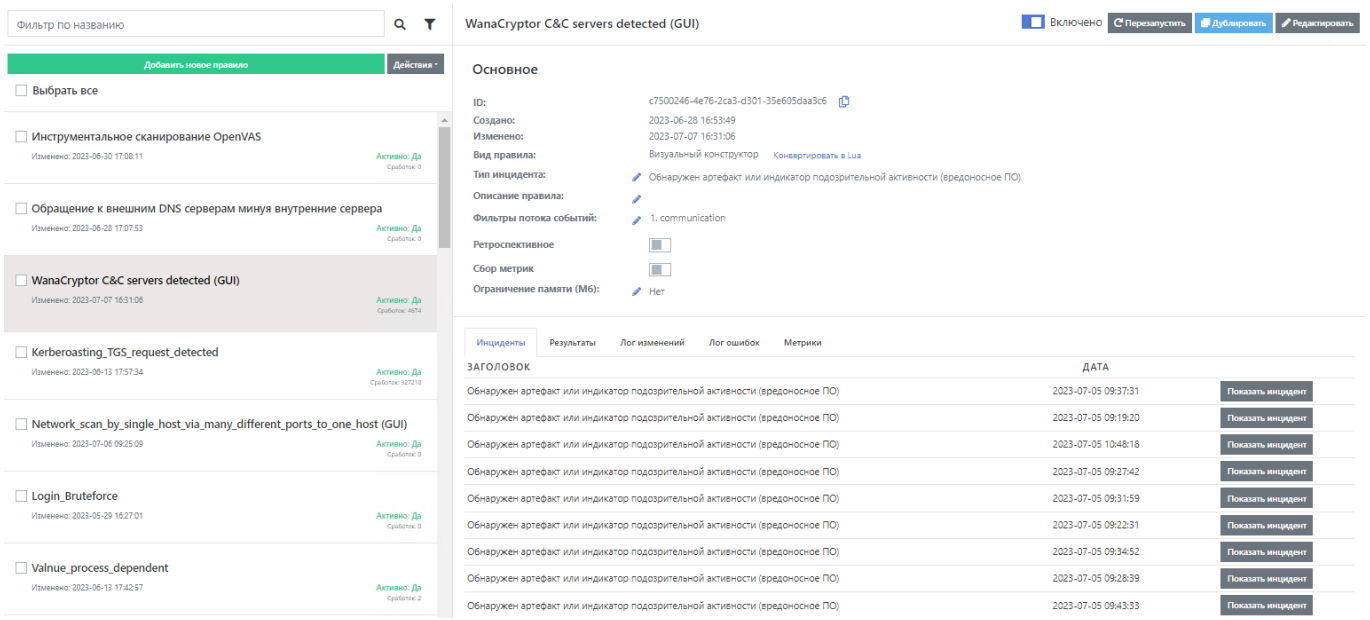



**Рисунок 183 - Свойства правила корреляции.**

На экране отображаются:

- ползунок активации или деактивации правила корреляции;
- кнопка "**Перезапустить**", клик по которой перезапустит правило корреляции;
- кнопка "**Дублировать**", клик по которой сделает копию правила корреляции;
- кнопка "**Редактировать**", которая откроет окно редактирования правила корреляции;
- **ID** - идентификатор правила корреляции;
- **Создано** - дата создания правила;
- **Изменено** - дата последнего изменения правила;
- **Вид правила** - может принимать значения "Визуальный конструктор" или "Скрипт Lua";
- надпись с действием по конвертации правила в скрипт Lua (доступно только для правила, выполненного в виде визуального конструктора);
- **Тип инцидента** - тип иницдента, связанного с правилом (может быть изменено);
- **Описание правила** (необязательное поле);
- **Фильтры потока событий** - подключенные к правилу фильтры потока событий;
- **Ретроспективное** - такое правило обрабатывает уже существующие исторические события;
- **Сбор метрик**;
- **Ограничение памяти** (в мегабайтах) для правила;
- вкладки с информацией по работе правила корреляции.

Включенное правило корреляции начинает работать сразу же, результат работы правила отображается на вкладках с информацией по его работе.

При включении правила корреляции проверяются условия указания типа инцидента и фильтра потока событий. Если хотя бы одно условие не выполнено, то при попытке активации правила появляется сообщение об ошибке (см. рисунок 184).

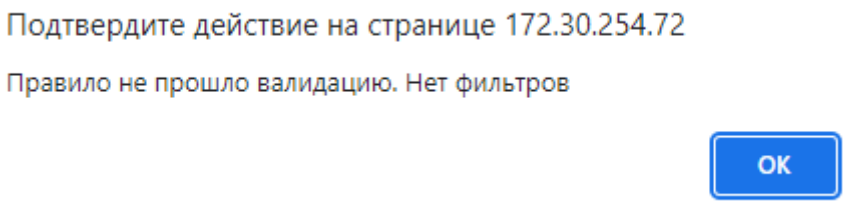



**Рисунок 184 - Ошибка активации правила корреляции.**

Для установки типа инцидента кликните на иконку редактирования напротив текста "**Тип инцидента**" и в открывшемся окне (см. рисунок 185) выберите тип инцидента.

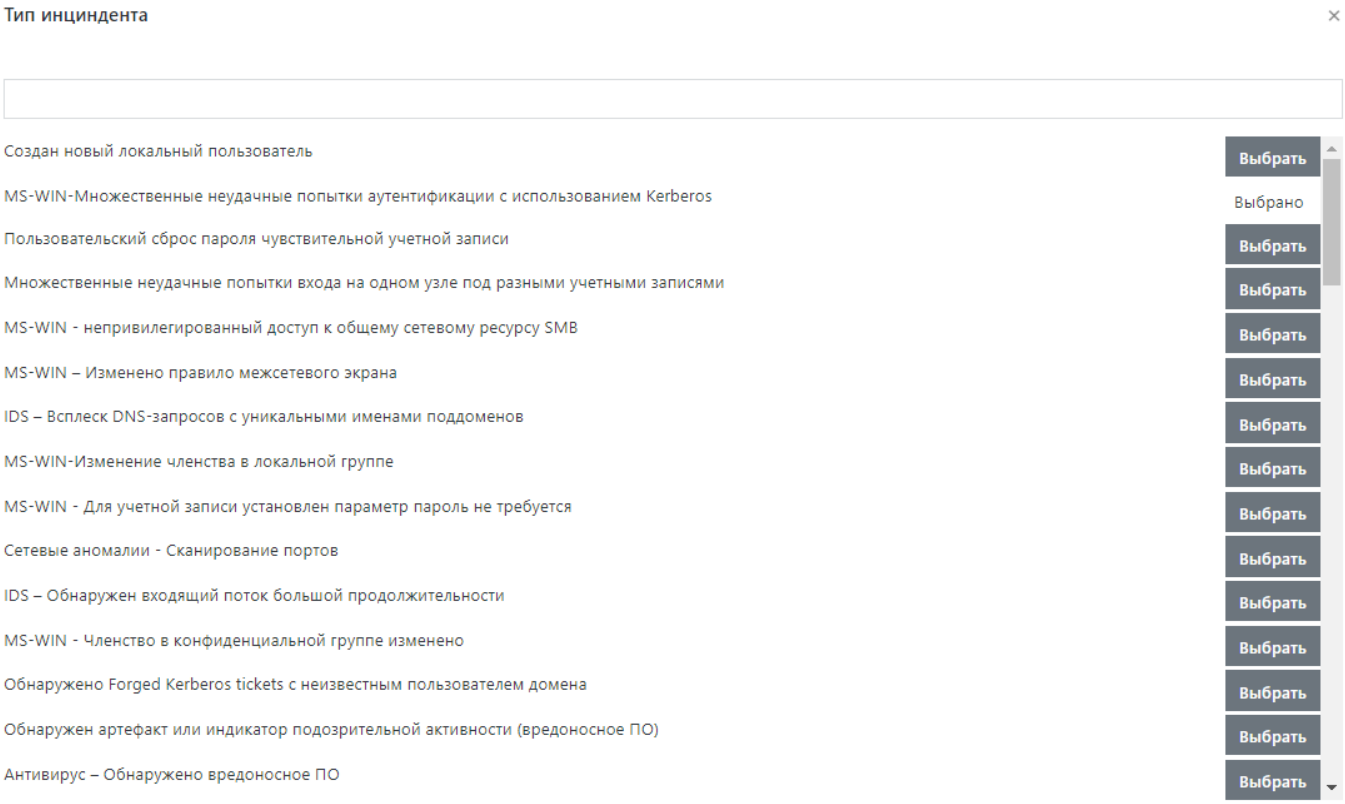



**Рисунок 185 – Выбор типа инцидента**

Напротив выбранного типа инцидента не будет отображаться кнопка "**Выбрать**", а будет отображен текст "**Выбрано**".

Для установки фильтров кликните на иконку редактирования напротив текста "**Фильтры потока событий**" и в открывшемся окне (см. рисунок 186) выберите необходимые фильтры.

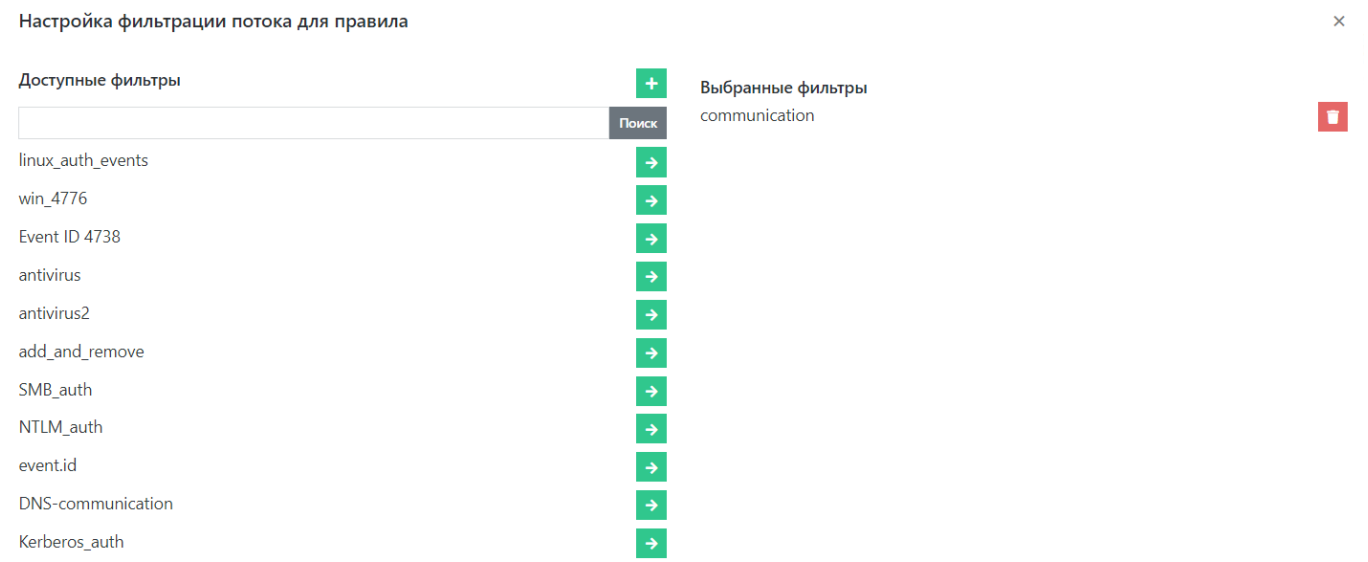



**Рисунок 186 – Выбор фильтров потока событий**

В левой части отображены доступные фильтры, в правой - подключенные к правилу фильтры потока событий. Иконка → позволяет привязать выбранный фильтр потока событий к правилу корреляции, иконка 🗑 - отвязать фильтр от правила.

На вкладках с информацией о работе правила корреляции доступна информация:

- **Инциденты** - перечень созданных инцидентов по результатам работы правила;
- **Результаты** - результаты работы коррелятора;
- **Лог изменений** - журнал изменений правила корреляции;
- **Лог ошибок** - журнал ошибок отработки правила корреляции;
- **Метрики**.

Вкладка "**Инциденты**" (см. рисунок 187) содержит перечень всех созданных уникальных инцидентов.

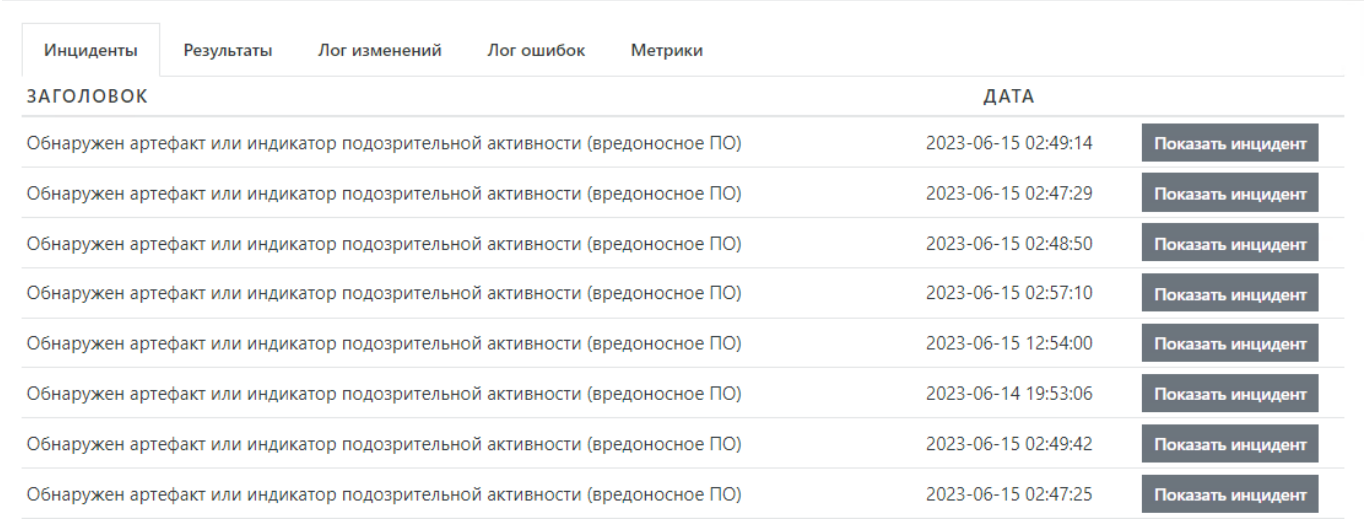



**Рисунок 187 - Вкладка "Инциденты"**

При клике на кнопку "**Показать инцидент**" будет осуществлен переход к созданному правилом корреляции инциденту.

Вкладка "**Результаты**" (см. рисунок 188) содержит перечень срабатываний правила корреляции.

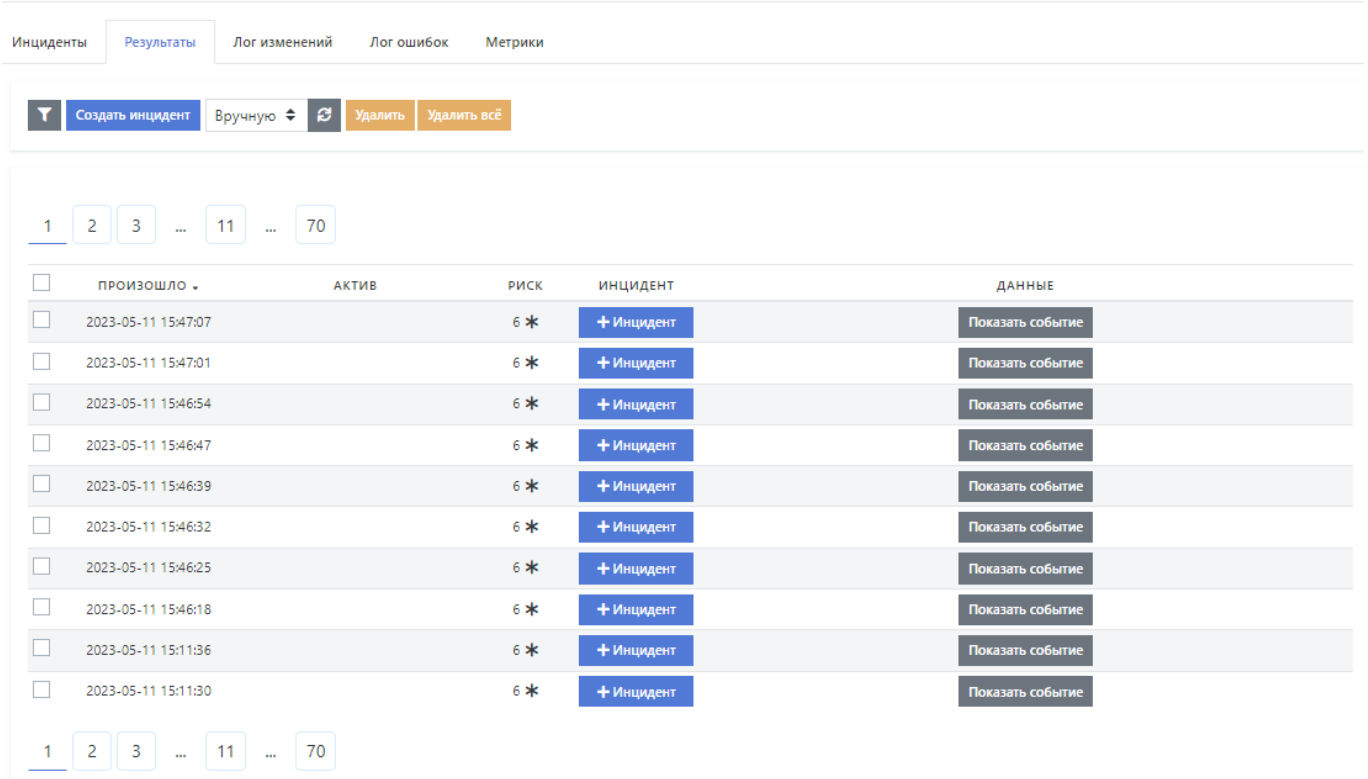



**Рисунок 188 – Вкладка "Результаты"**

В таблице результатов доступны действия:

- фильтрация результатов ( );
- создание инцидента (кнопка "**Создать инцидент**") по выбранным результатам корреляции;
- функция обновления перечня результатов ( );
- удаление выбранных результатов (кнопка "**Удалить**");
- удаление всех результатов (кнопка "**Удалить всё**").

При установке фильтров открывается окно фильтрации, содержащее три вкладки (см. рисунок 189):

- вкладка "**Фильтр**", содержащая настройки фильтрации:
  - фильтр по дате срабатывания (текстовое поле, поиск идет по вхождению);
  - фильтр по уровню риска (выбирается из списка);
  - фильтр по действующим активам (выбирается из списка).
- вкладка "**Активы**", на которой можно указать, по каким группам активов отобразить результаты срабатывания правил корреляции;
- вкладка "**Дополнительно**", содержащая дополнительные параметры:

- фильтр "**Произошло после**", задающий фильтрацию по дате событий после указанной даты;
- фильтр "**Произошло до**", задающий фильтрацию по дате событий до указанной даты;
- количество результатов на одной странице.

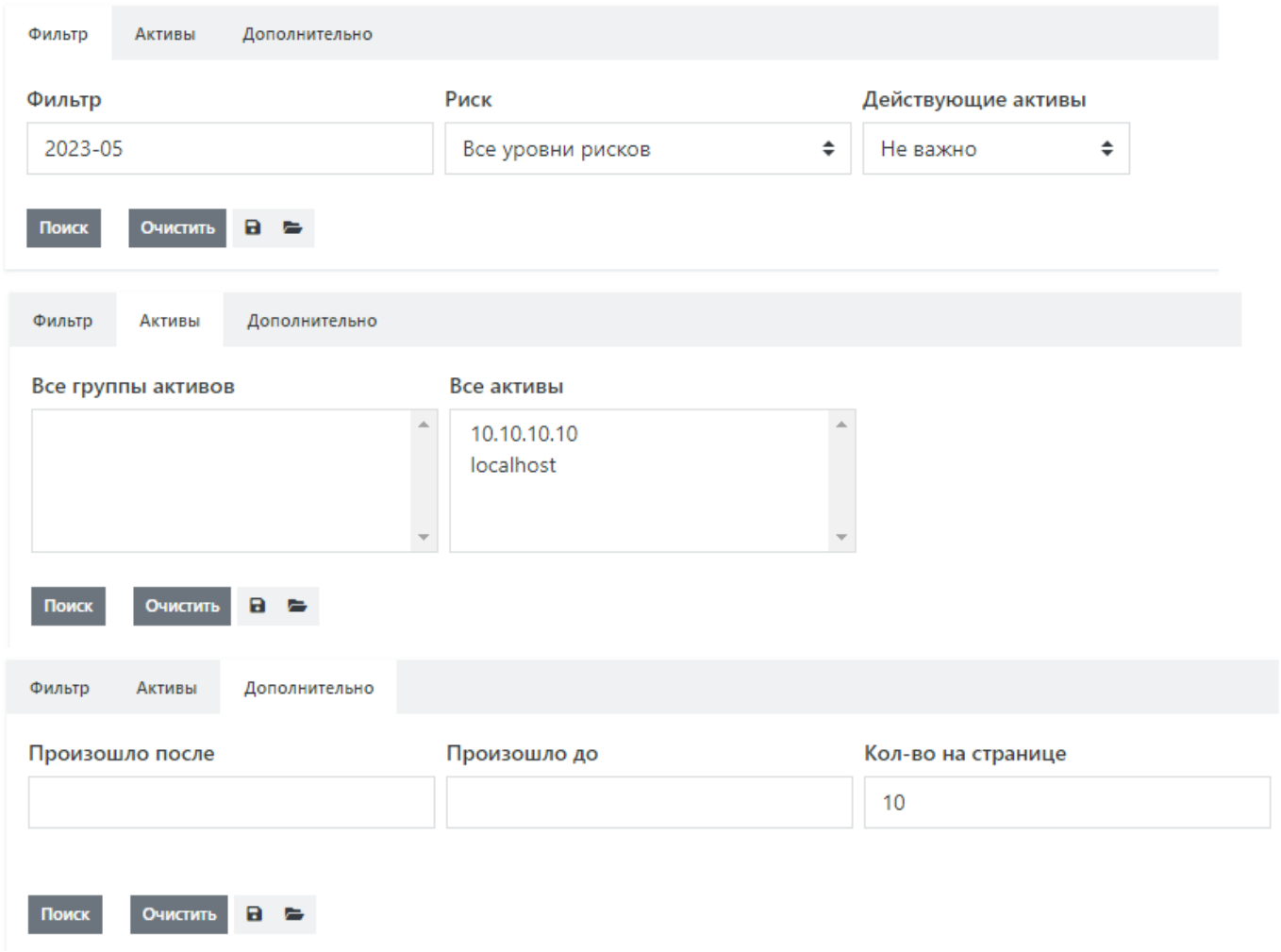



**Рисунок 189 – Фильтры вкладки "Результаты"**

При установке фильтров доступны действия:

- установка заданных фильтров кнопкой "**Поиск**";
- отмена фильтрации кнопкой "**Очистить**";
- сохранение условий фильтрации иконкой ;
- восстановление условий фильтрации иконкой .

Кнопка "**Показать событие**" в таблице результатов позволяет просмотреть событие, которое было отобрано и обработано правилом (см. рисунок 190).

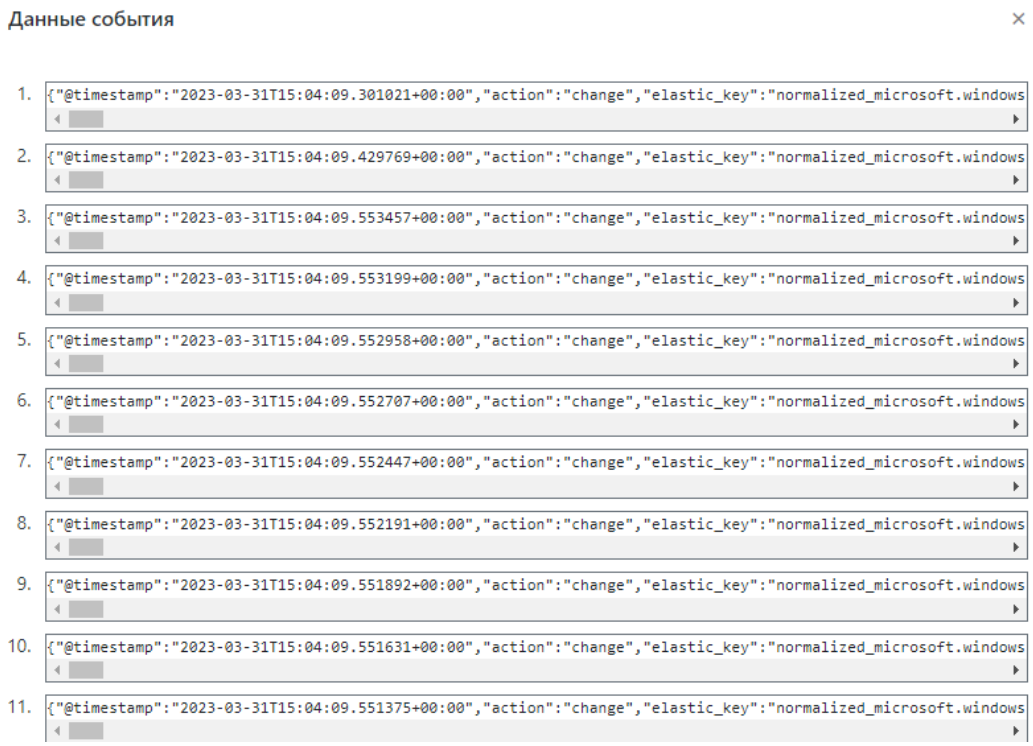
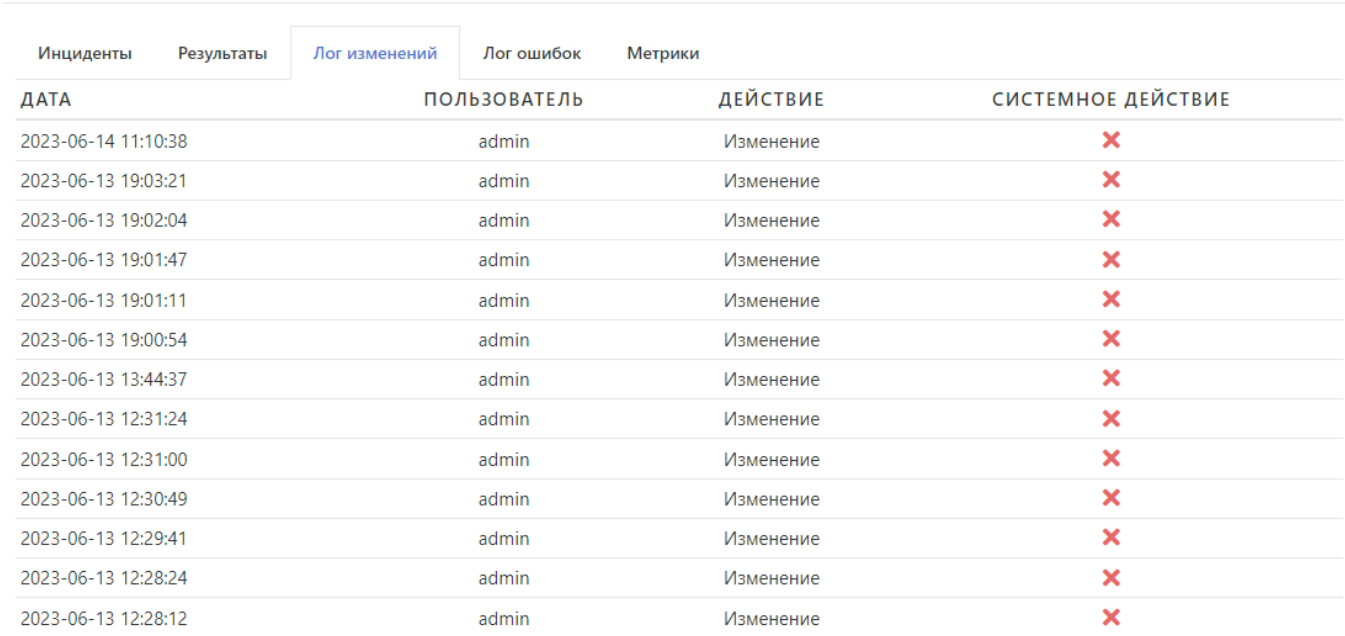



**Рисунок 190 – Просмотр события**

Кнопка "**Инцидент**" в таблице результатов отображается, если по результату не был создан инцидент. Кнопка позволяет создать инцидент по результату обработки. Если инцидент уже создан, то на кнопке будет отображен текст "**Инцидент**". При клике на эту кнопку будет осуществлен переход к созданному правилом корреляции инциденту.

Вкладка "**Лог изменений**" (см. рисунок 191) содержит дату изменения; имя пользователя, внесшего изменение; вид действия; системное действие.




| ДАТА | ПОЛЬЗОВАТЕЛЬ | ДЕЙСТВИЕ | СИСТЕМНОЕ ДЕЙСТВИЕ |
|---|---|---|---|
| 2023-06-14 11:10:38 | admin | Изменение | ✗ |
| 2023-06-13 19:03:21 | admin | Изменение | ✗ |
| 2023-06-13 19:02:04 | admin | Изменение | ✗ |
| 2023-06-13 19:01:47 | admin | Изменение | ✗ |
| 2023-06-13 19:01:11 | admin | Изменение | ✗ |
| 2023-06-13 19:00:54 | admin | Изменение | ✗ |
| 2023-06-13 13:44:37 | admin | Изменение | ✗ |
| 2023-06-13 12:31:24 | admin | Изменение | ✗ |
| 2023-06-13 12:31:00 | admin | Изменение | ✗ |
| 2023-06-13 12:30:49 | admin | Изменение | ✗ |
| 2023-06-13 12:29:41 | admin | Изменение | ✗ |
| 2023-06-13 12:28:24 | admin | Изменение | ✗ |
| 2023-06-13 12:28:12 | admin | Изменение | ✗ |

**Рисунок 191 – Вкладка "Лог изменений"**

Вкладка "**Лог ошибок**" (см. рисунок 192) содержит график изменения количества ошибок при срабатывании правила корреляции.

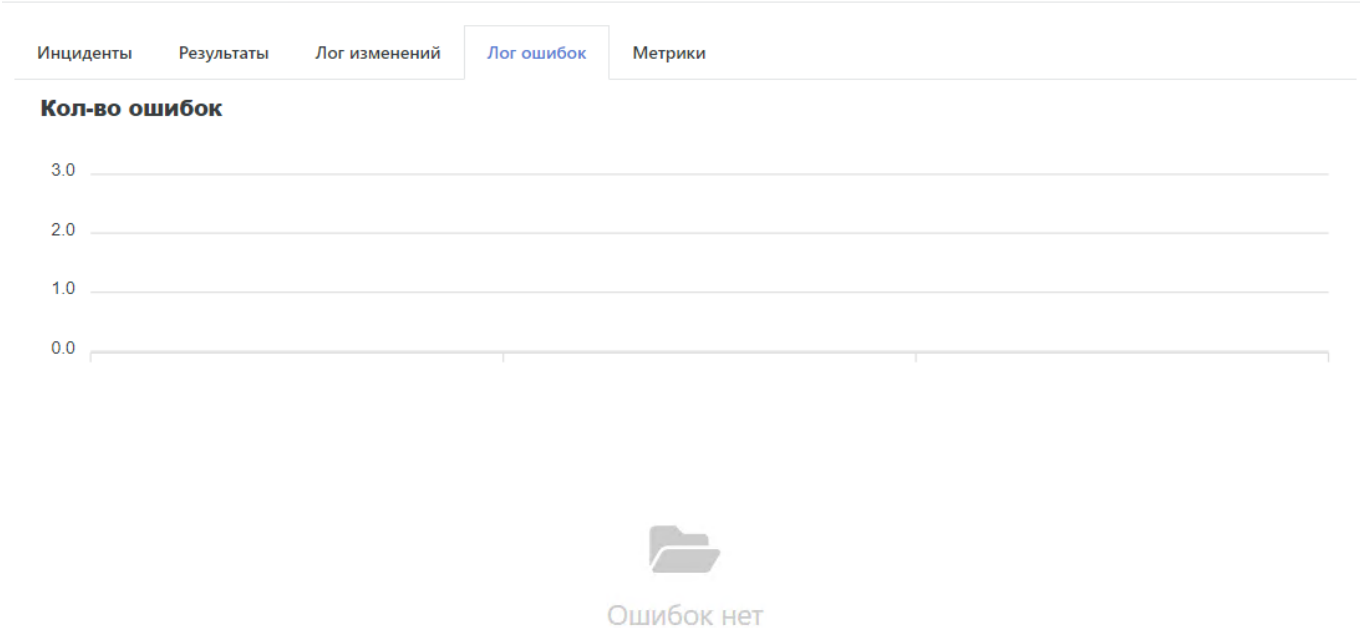



**Рисунок 192 – Вкладка "Лог ошибок"**

Вкладка "Метрики" (см. рисунок 193) содержит график обработки событий.

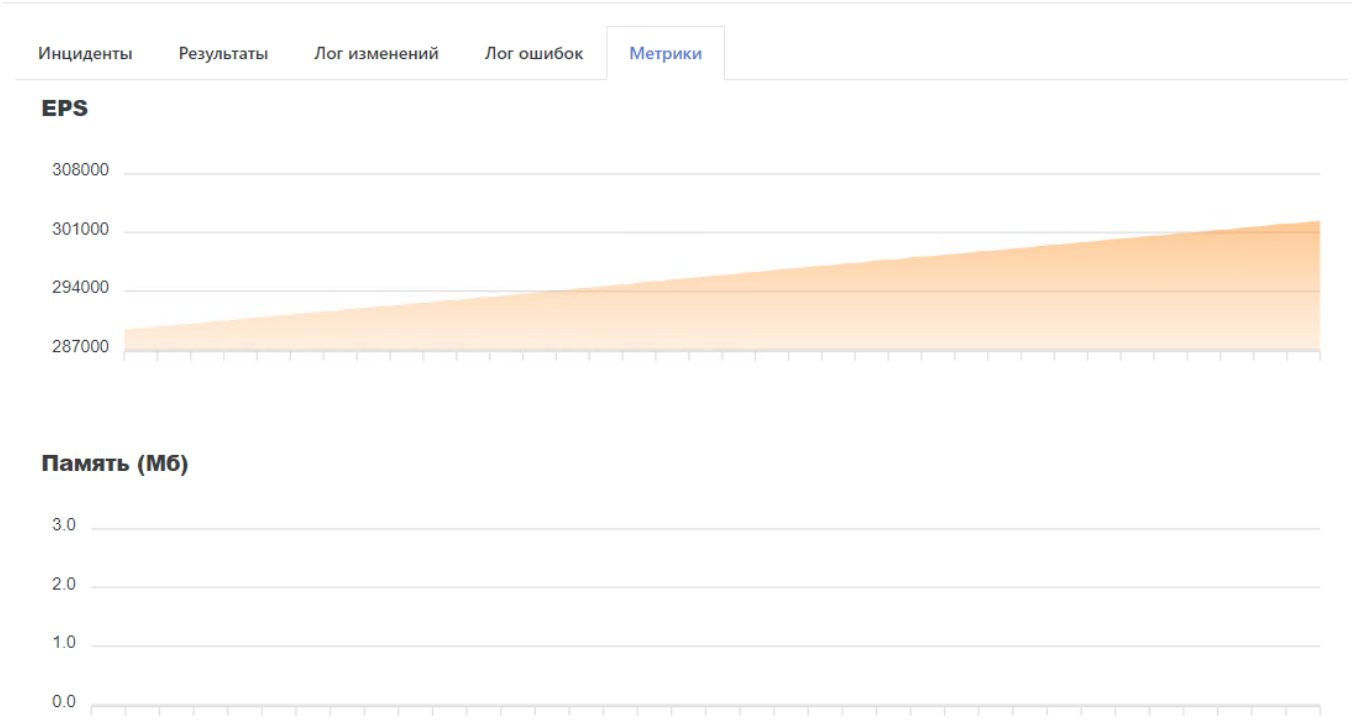



**Рисунок 193 – Вкладка "Метрики"**

На вкладке доступны графики:

- по уровню EPS;
- по количеству занимаемой памяти;
- по количеству накопленных событий в группере;
- по времени выполнения.

## 20.2.2 Создание правила корреляции

При клике по кнопке "**Добавить новое правило**" откроется окно создания нового правила корреляции (см. рисунок 194).

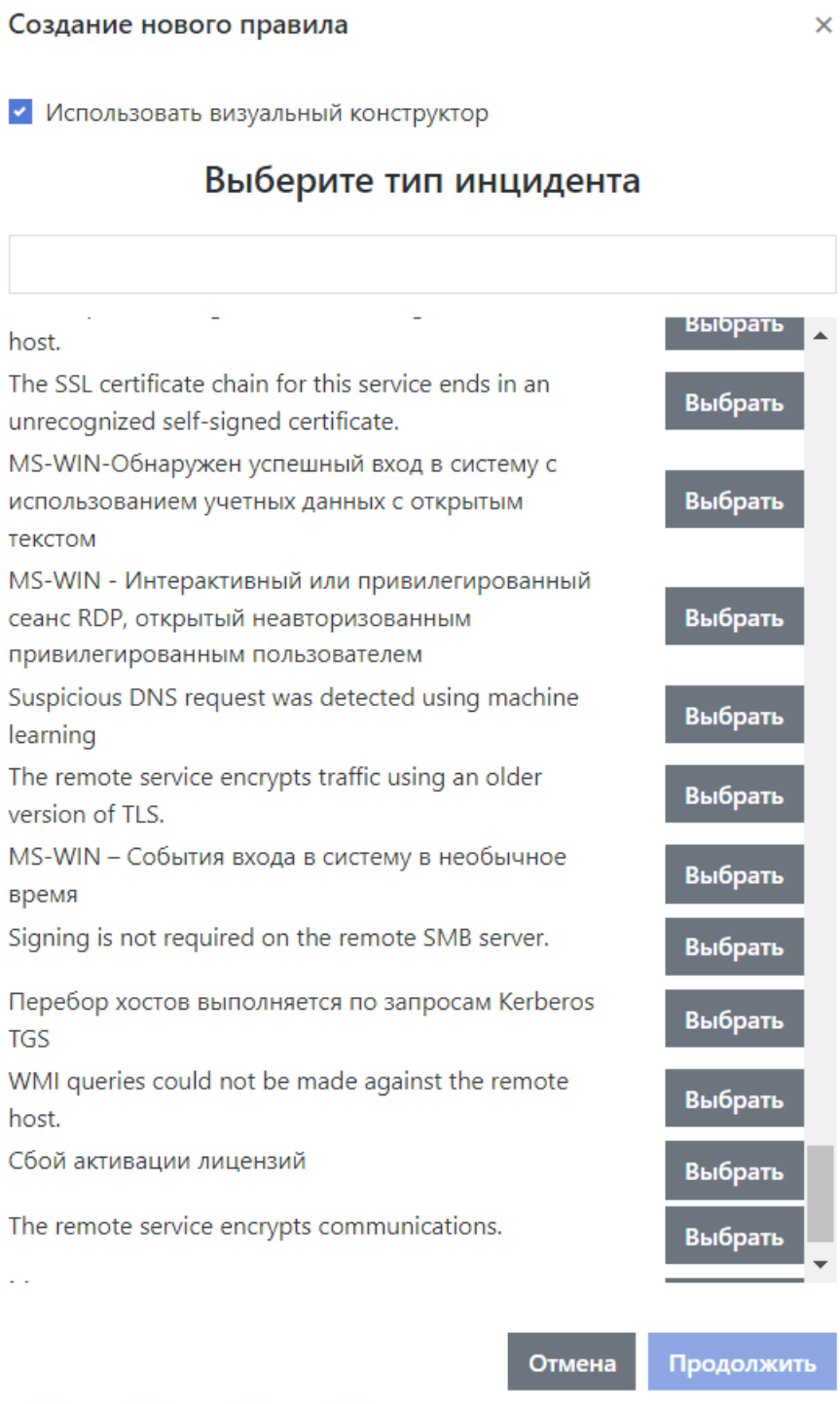



**Рисунок 194 -Создание правила корреляции**

Выберите вид правила: с использованием визуального конструктора или без его использования. В первом случае для создания правила не используется скриптовый язык, само правило настраивается с помощью визуальных блоков.

Для более гибкого описания правила отключите использование визуального конструктора. В этом случае правило необходимо будет описать с помощью скриптового языка Lua.

Любое правило, созданное с помощью визуального конструктора, можно сконвертировать в скрипт Lua.

Далее выберите инцидент с помощью кнопки "**Выбрать**" напротив его наименования и нажмите кнопку "**Продолжить**", после чего откроется окно редактирования правила.

### 20.2.3 Редактирование правила корреляции

При клике по кнопке "**Редактирование**" уже существующего правила корреляции или создании нового правила корреляции откроется окно его редактирования.

При редактировании правил корреляции во многих полях используется список, содержащий предопределенный набор полей. Описание этих полей представлено в «Руководстве по подключению источников» → «Описание полей нормализации».

При редактировании и тестировании правил используется логлайн событий. Сами события можно просмотреть в разделе «Просмотр событий». Логлайн представляет из себя одну строчку записи "сырого" события из всего массива строк события.

Вид окна редактирования зависит от вида правила корреляции (визуальный конструктор или скрипт Lua).

Одинаковыми будут общие элементы управления и параметры правила (см. рисунок 195).

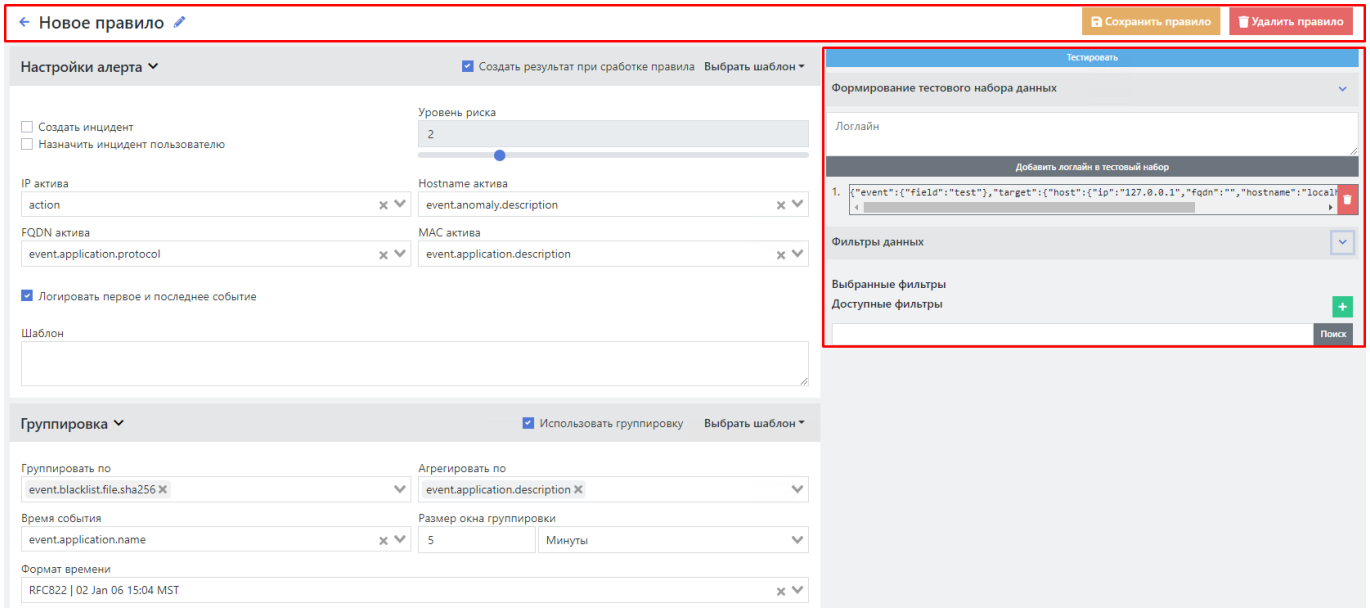



**Рисунок 195 - Параметры правила корреляции**

С помощью иконки  можно изменить имя правила корреляции.

Кнопки "**Сохранить**" и "**Удалить**" позволяют, соответственно, сохранить или удалить правило корреляции.

Кнопка "**Тестировать**" запускает режим тестирования (см. рисунок 196).

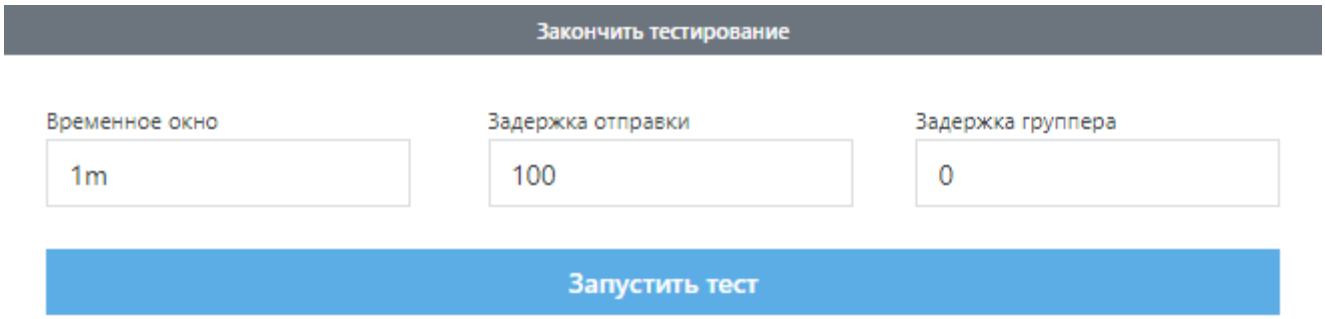



**Рисунок 196 - Режим тестирования правила корреляции**

Для запуска теста задайте параметры:

- размер временного окна выполнения правила корреляции;
- задержка отправки событий;
- задержка работы групера.

После задания параметров нажмите кнопку "**Запустить тест**" и дождитесь выполнения теста и получения его результата (см. рисунок 197).

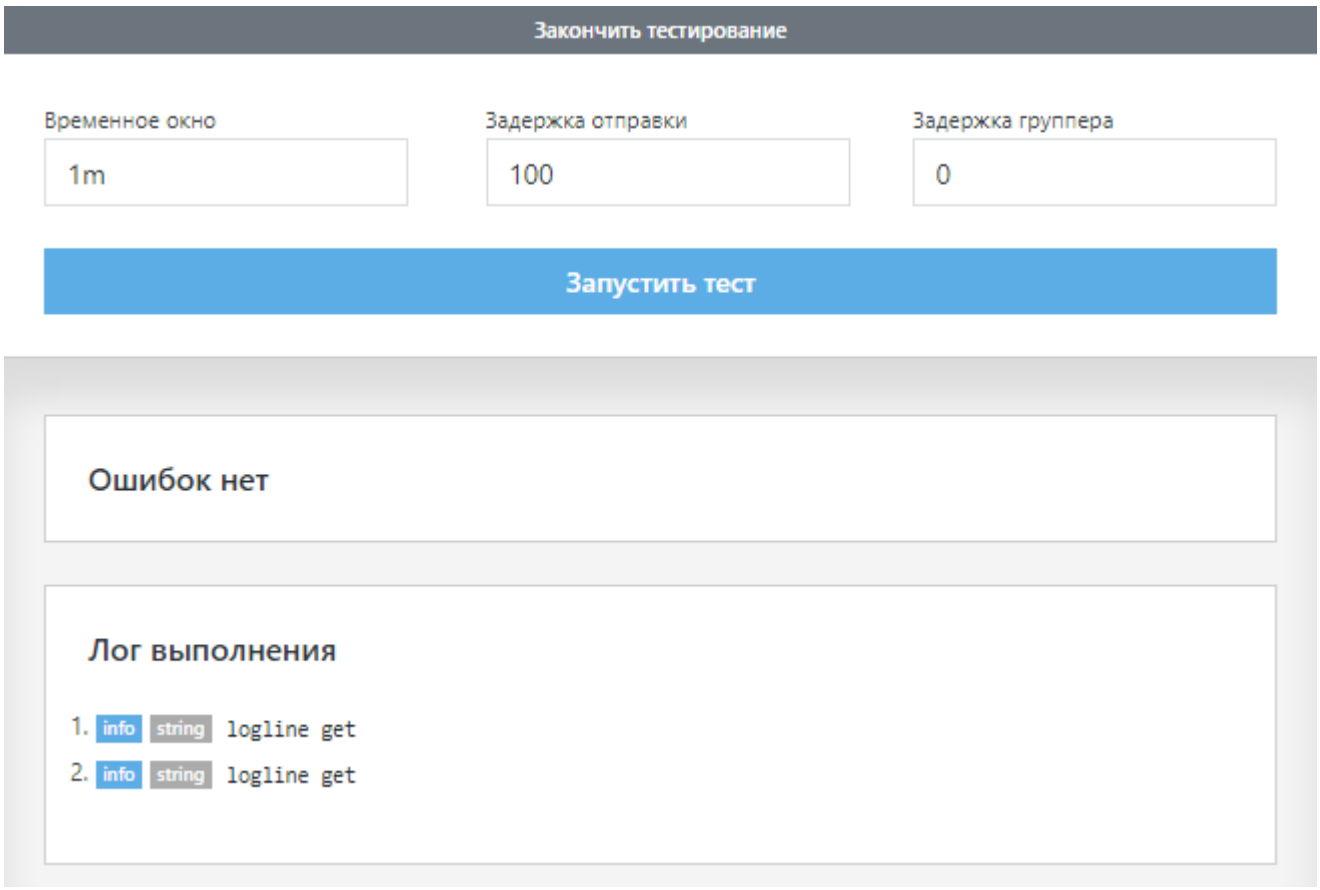



**Рисунок 197 – Результаты тестирования правила корреляции**

По окончании тестирования нажмите кнопку "**Закончить тестирование**", чтобы выйти из режима тестирования.

Далее располагаются параметры, разбитые на группы:

- формирование тестового набора данных;
- фильтры данных;

- макросы.

### 20.2.3.1 Формирование тестового набора данных

Тестовый набор данных содержит набор событий в формате JSON, подаваемых на вход правилу корреляции для проведения тестирования (см. рисунок 198).

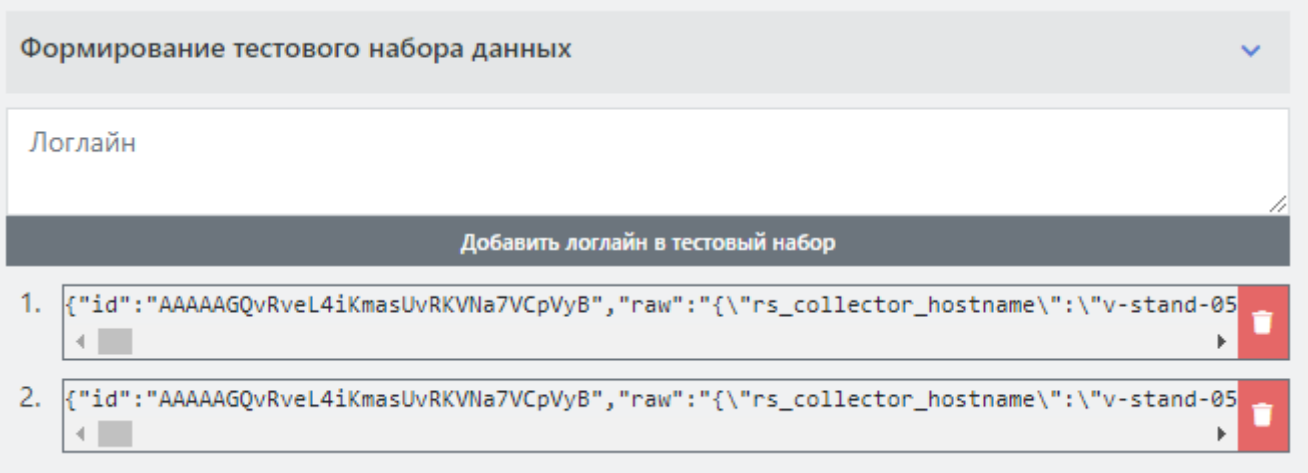



**Рисунок 198 – Тестовый набор данных**

Вставьте событие в строку логлайна и нажмите кнопку "**Добавить логлайн в тестовый набор**" после чего введенное событие будет добавлено к набору тестовых данных. В качестве тестового события берется набор данных в виде "сырого" события в формате JSON.

Иконка  позволяет удалить событие из тестового набора данных

### 20.2.3.2 Фильтры данных

Фильтры отвечают за предфильтрацию логлайнов по правилам, описанным в настройке фильтра. По возможности переносите часть условий из правила в фильтр, это позволит более эффективно разбирать поток.

Управление фильтрами описано в разделе «Управление фильтрами потока событий».

К правилу корреляции можно добавить один или несколько фильтров (см. рисунок 199).

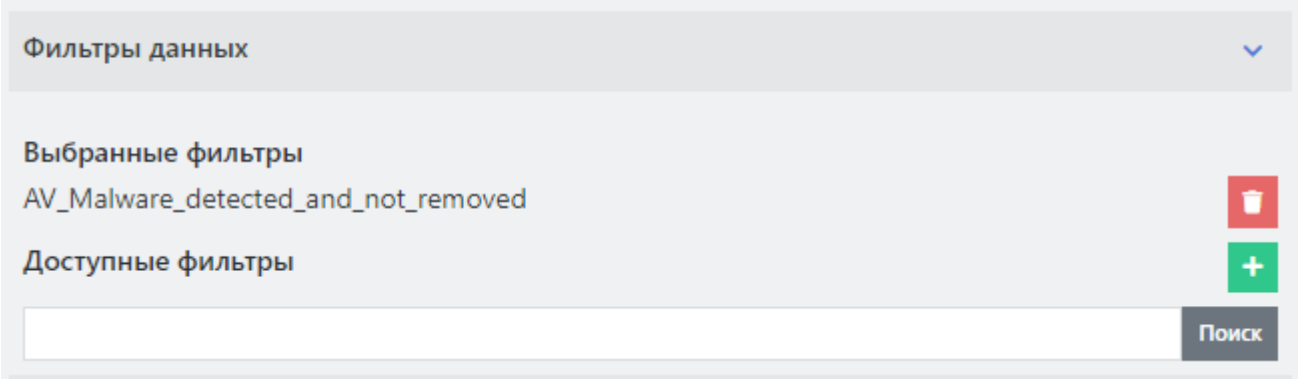



**Рисунок 199 – Перечень фильтров потока событий правила корреляции**

С помощью иконки  можно добавить фильтр потока событий, с помощью иконки  - удалить фильтр из набора.

### 20.2.3.3 Макросы

**Примечание**: Данная функция доступна только для правил с использованием языка Lua

Макросы - подключаемые модули, которые могут содержать как и переменные, так и расширять функционал с помощью функций. Импортируется как есть, целиком. Соответственно, если в макросе есть определение функции *function test*, то и использовать ее в правиле следует напрямую: *test()*.

К правилу корреляции можно добавить один или несколько макросов (см. рисунок 200).

Для управления макросами при нажатии на кнопку "**Действие**" разворачивается перечень пунктов:

- **Экспортировать** - позволяет экспортировать выбранные макросы в файл;
- **Импортировать** - позволяет импортировать макросы из файла;
- **Удалить** - позволяет удалить выбранные макросы;
- **Экспортировать всё** - позволяет экспортировать все макросы в файл;
- **Удалить всё** - позволяет удалить все макросы.

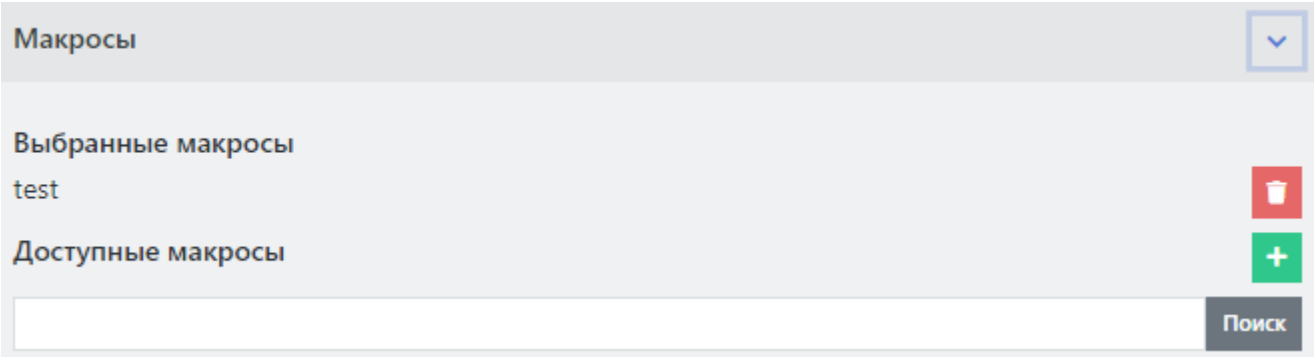



**Рисунок 200 – Перечень макросов правила корреляции**

С помощью иконки  можно добавить макрос, с помощью иконки  - удалить макрос из набора.

### 20.2.3.4 Редактирование правила на основе скриптового языка Lua

В режиме разработки правила на основе скриптового языка Lua окно редактирования правила корреляции имеет вид, представленный на рисунке 201.

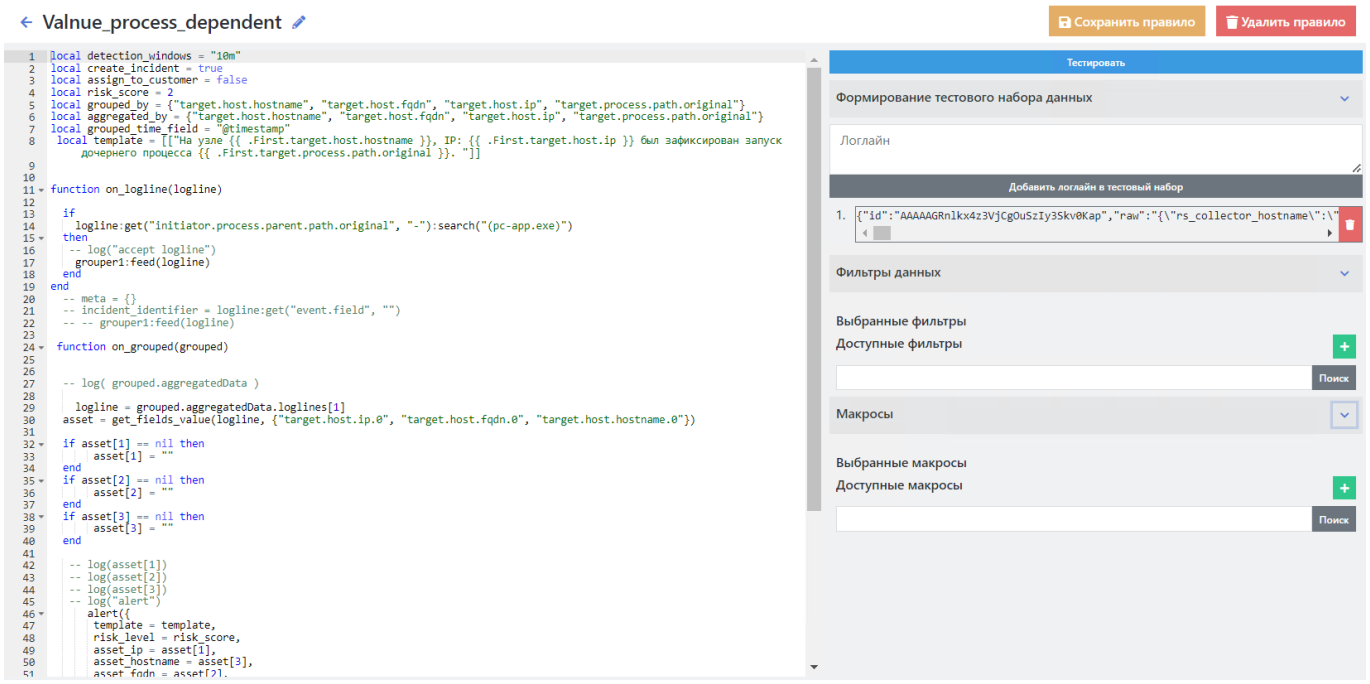



**Рисунок 201 – Вид правила с использованием языка Lua**

Разработка текста правила корреляции рассмотрена в руководстве «Описание редактора Lua для правил корреляции».

### 20.2.3.5 Редактирование правила корреляции с помощью конструктора

В режиме разработки правила с помощью конструктора окно редактирования правила корреляции имеет вид, представленный на рисунке 202.

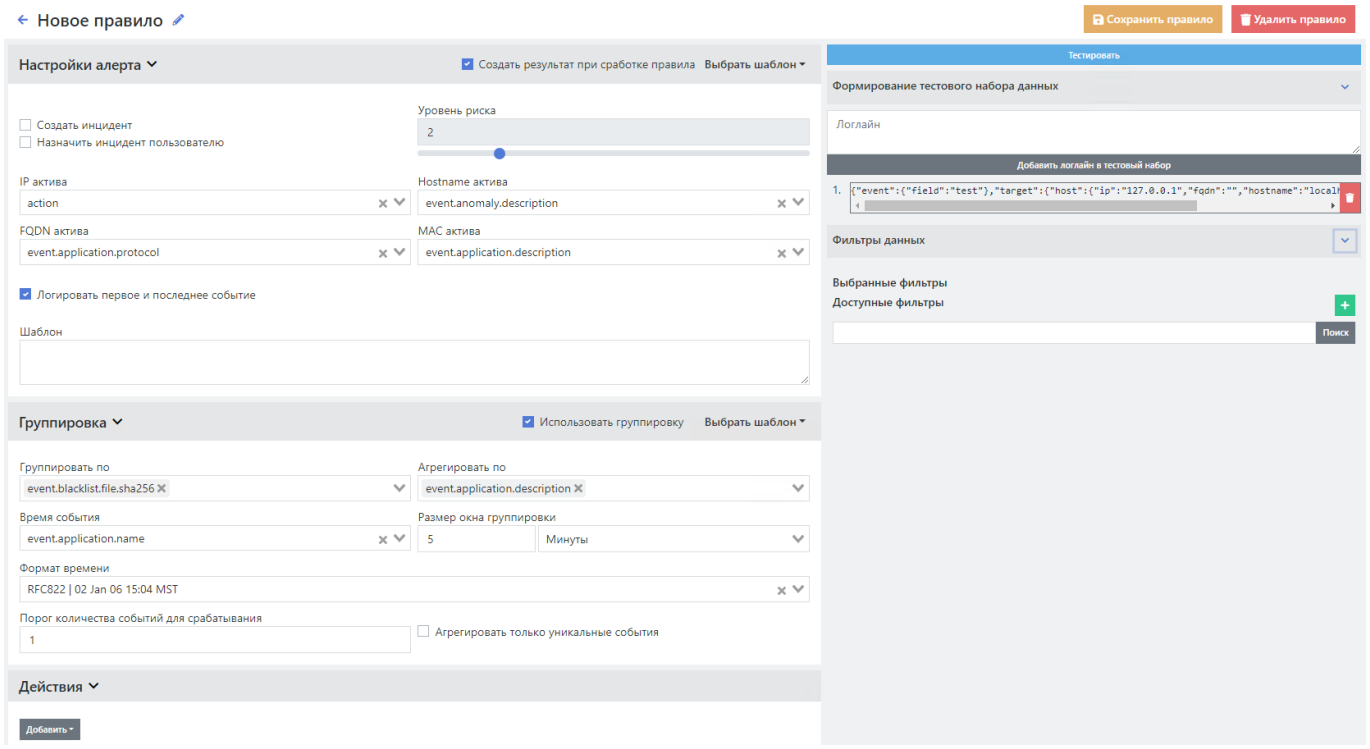



**Рисунок 202 – Вид правила с использованием конструктора**

В режиме конструктора для настройки правила доступны блоки:

- настройка алерта;
- настройка группировки;
- действия;
- конструктор условий.

#### 20.2.3.5.1 Блок настройки алерта

Блок настройки алерта (см. рисунок 203) позволяет настроить реакцию на срабатывание правила корреляции.

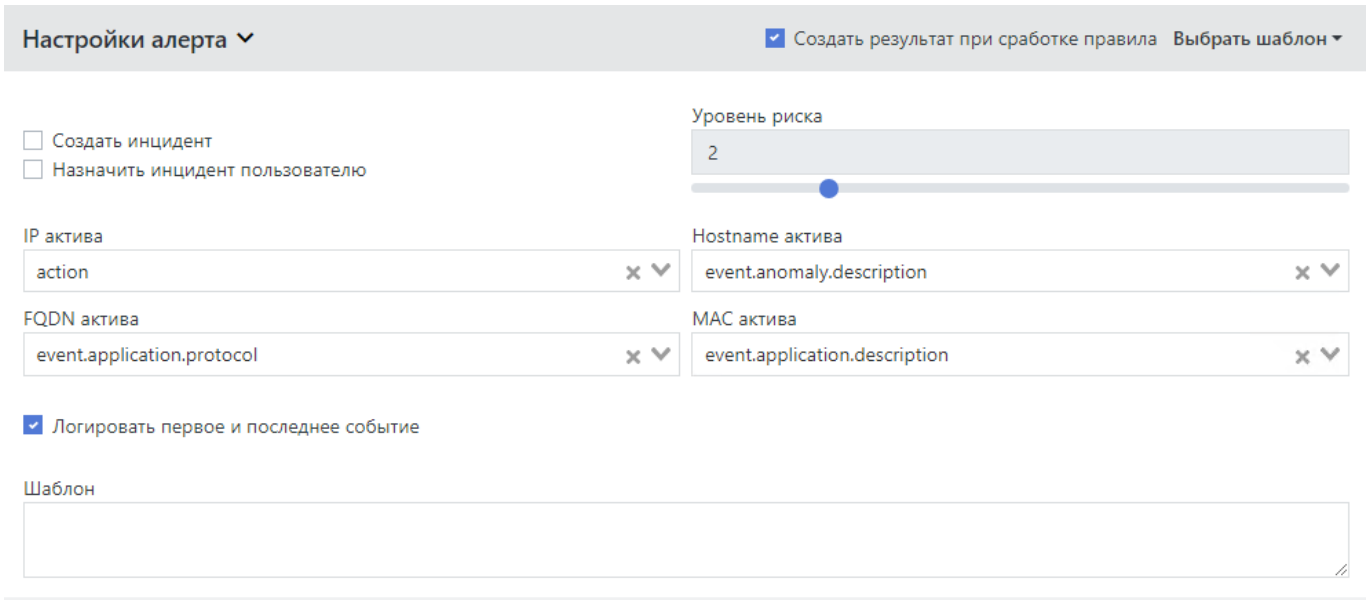



**Рисунок 203 – Блок настройки алерта**

Среди настроек блока алерта доступны параметры:

- **Создать результат при сработке правила** - признак позволяет создать алерт при срабатывании правила корреляции;
- **Выбрать шаблон** - действие позволяет заполнить параметры алерта из готового шаблона;
- **Создать инцидент** - признак показывает, что при срабатывании правила корреляции будет создан инцидент;
- **Назначить инцидент пользователю** - признак показывает, что при срабатывании правила корреляции и создании инцидента необходимо инцидент назначить пользователю;
- **Уровень риска** - параметр задает уровень риска для алерта. Параметр задается пользователем самостоятельно, исходя из критичности события для инфраструктуры;
- **IP актива** - в параметре выбирается из списка поле в качестве ip-адреса актива. **Поле является обязательным для заполнения.** Поле может являться частью сводной таблицы событий;
- **Hostname актива** - в параметре выбирается из списка поле в качестве наименования хоста актива. Поле может являться частью сводной таблицы событий;
- **FQDN актива** - в параметре выбирается из списка поле в качестве наименования домена актива. Поле может являться частью сводной таблицы событий;

- **MAC актива** - в параметре выбирается из списка поле в качестве mac-адреса актива. Поле может являться частью сводной таблицы событий;
- **Логировать первое и последнее события** -при установленном признаке логируются только первое и последнее события. При снятом - все события;
- **Логировать указанное количество событий** - в параметре задается количество логируемых первых событий;
- **Шаблон** - в параметре задается шаблон алерта (инцидента).

В качестве шаблона алерта используется предопределенный текст. Кроме самого текста в шаблон могут быть вставлены поля логлайна. Сами поля могут быть взяты из отдельных записей события:

- `.First` - первый логлайн;
- `.Last` - последний логлайн;
- `.Loglines` - массив логлайнов событий;
- `.Meta` - дополнительные поля.

Пример шаблонов:

```
Результат анализа

На рабочей станции {{ .First.observer.host.ip }} (FQDN: "{{
.First.observer.host.fqdn }}") обнаружена успешная попытка запуска HACK утилиты


На узле {{ .First.target.host.fqdn |}}, IP: {{ .First.target.host.ip }} были
зафиксированы многочисленные неуспешные попытки аутентификации от {{
.Meta.uniq_users }} уникальных УЗ
```

#### 20.2.3.5.2 Блок группировки

Блок группировки (см. рисунок 204) позволяет задавать правила группировки событий и правила агрегации сгруппированных событий. Блок группировки может быть отключен признаком "**Использовать группировку**".

Группировка позволяет группировать однотипные события по выбранному полю. Внутри сгруппированных событий блок позволяет провести агрегацию по указанным полям. **Платформа Радар** подсчитывает количество уникальных полей агрегации внутри уникальных групп. В случае, если поле группировки и поле агрегации совпадают, **Платформа Радар** посчитает количество уникальных групп и количество уникальных значений в каждой группе.

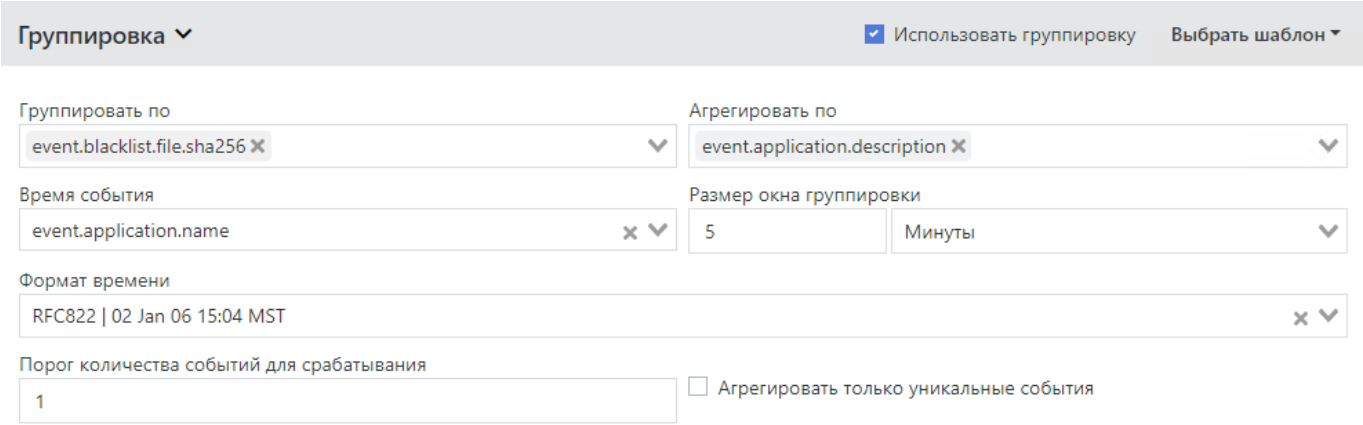



**Рисунок 204 – Блок группировки**

Среди настроек блока группировки доступны параметры:

- **Выбрать шаблон** - действие позволяет заполнить параметры группировки из готового шаблона;
- **Группировать по** - параметр задает одно или несколько выбираемых из списка полей группировки;
- **Агрегировать по** - параметр задает одно или несколько выбираемых из списка полей агрегации;
- **Время события** - параметр задает поле, в котором хранится время события;
- **Размер окна группировки** - параметр задает время, в течение которого после срабатывания правила группировать входящие события;
- **Формат времени** - параметр задает формат времени события, выбирается из списка;
- **Порог количества событий при срабатывании** - параметр задает максимальное количество группируемых событий в рамках временного окна;
- **Агрегировать только уникальные события** - параметр позволяет указать, группировать повторяющиеся события или нет.

Максимальное количество срабатываний правил корреляции в секунду задается глобальном параметре конфигурации: ***Кластер - Управление конфигурацией - Logmule2 - Максимальное количество сработок***.

**20.2.3.5.3 Блок действий**

Необязательный блок действий (см. рисунок 205) задает операции с табличными списками (добавление или удаление записей, очистка табличных списков) при срабатывании правила корреляции. Табличные списки описаны в разделе «Управление табличными списками».

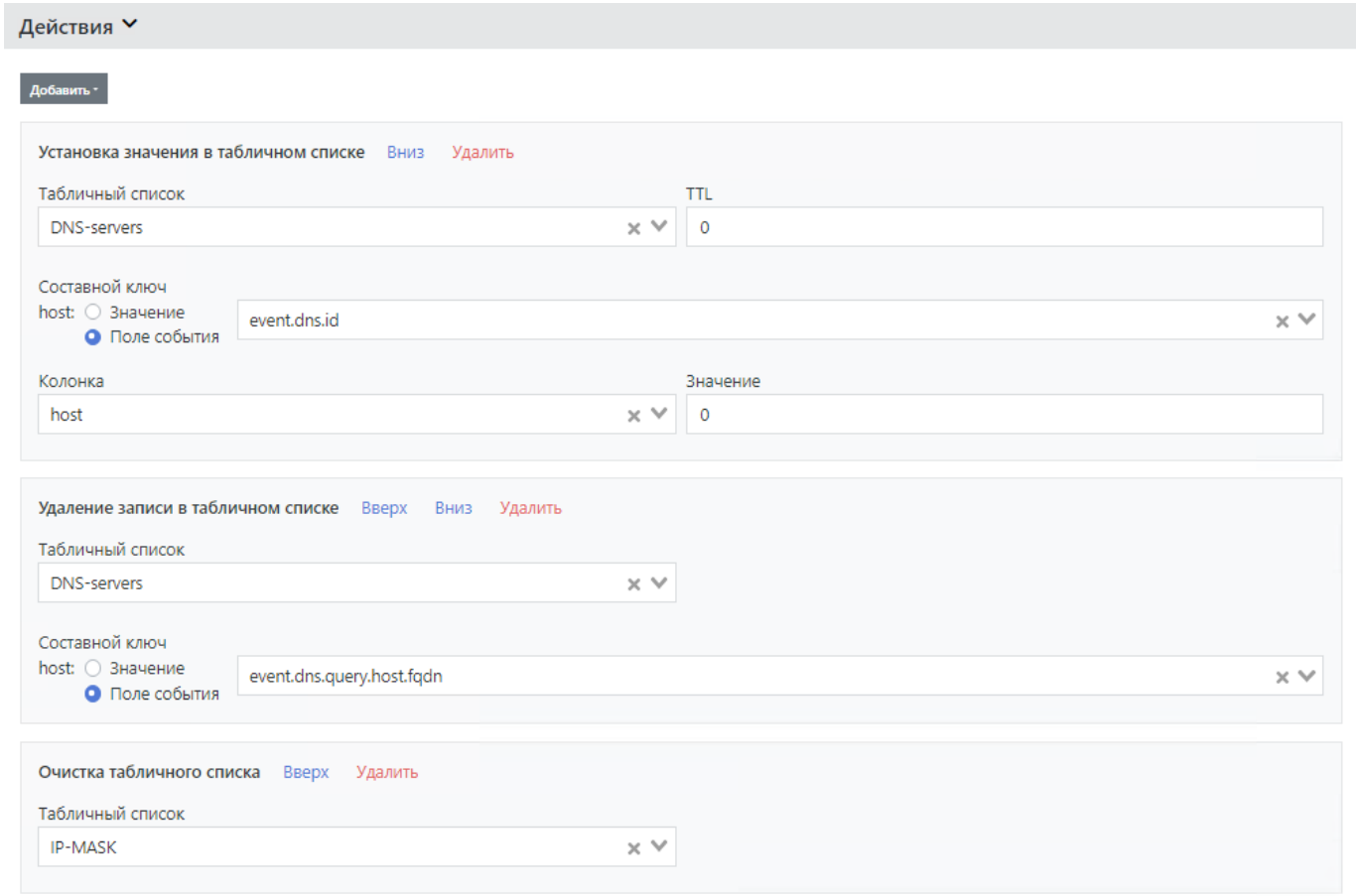



**Рисунок 205 - Блок действий**

Можно добавить неограниченное количество действий через кнопку с меню "**Добавить**". Все действия выполняются последовательно, поэтому доступно перемещение действий вверх или вниз для выстраивания очередности выполнения действий. При необходимости действие можно удалить.

Действие "**Установка значения в табличном списке**". Для выполнения этого действия укажите параметры:

- **Табличный список** - список, в котором устанавливается значение;
- **TTL** - размер окна времени отбора в миллисекундах. События старше указанного времени не будут отбираться для установки значения. По умолчанию 0 - без ограничения;
- **Составной ключ** - указывается значение ключа вручную или выбирается из поля события;
- **Колонка** - указывается колонка для установки значения;
- **Значение** - записываемое значение.

Действие "**Удаление записи в табличном списке**". Для выполнения действия укажите параметры:

- **Табличный список** - список, в котором удаляется значение;
- **Составной ключ** - указывается значение ключа вручную или выбирается из поля события.

Действие "**Очистка табличного списка**". Для выполнения действия укажите параметры:

- "**Табличный список**" - очищаемый список.

### 20.2.3.5.4 Блок конструктора условий

Конструктор условий (см. рисунок 206) позволяет гибко настроить условия отбора событий. Блок является необязательным.

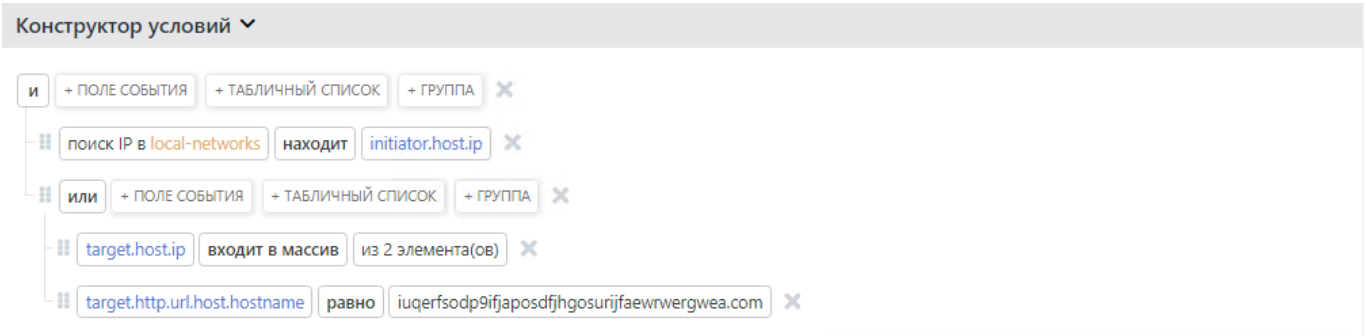



**Рисунок 206 – Блок конструктора условий**

Конструктор представляет из себя набор правил в иерархическом виде. За перемещение условия вверх, вниз или выше, ниже по уровню иерархии отвечает иконка . Для перемещения зажмите левой кнопкой мыши условие и перетащите в нужное место.

Событие включается в отбор, когда выполнены условия в соответствии с заданной логикой. В условиях задается сравнение выбранного поля с указанным значением. При сравнении используются операторы (для каждого оператора доступно отрицание):

- **равно** - проверяется полное равенство поля указанному значению. При равенстве поля значению условие считается выполненным. В качестве значения указывается введенное вручную значение или значение выбранного поля.
- **равно (без регистра)** - проверяется равенство поля указанному значению. При этом не учитывается регистр для строковых значений. При равенстве поля значению условие считается выполненным. В качестве значения указывается введенное вручную значение или значение выбранного поля.
- **существует** - проверяется существование поля. При существовании поля условие считается выполненным.
- **равно значению в массиве** - осуществляется поиск указанного значения поля в массиве. При успешном поиске условие считается выполненным.
- **элемент массива имеет подстроку** - проверяется вхождение значения поля в указанный вручную массив. При вхождении значения поля в массив условие считается выполненным.
- **элемент массива начинается с** - проверяется вхождение значения поля в начало строки каждого элемента массива. При вхождении значения поля в массив условие считается выполненным.
- **элемент массива заканчивается на** - проверяется вхождение значения поля в конец строки каждого элемента массива. При вхождении значения поля в массив условие считается выполненным.
- **имеет подстроку** - проверяется вхождение указанной в значении подстроки в выбранное поле. При вхождении подстроки в поле условие считается выполненным. В качестве подстроки указывается введенное вручную значение или значение выбранного поля.

- **проходит regexp** - проверяется проверка соответствия поля регулярному выражению, указанному в значении. При соответствии условие считается выполненным. В качестве регулярного выражения указывается введенное вручную значение или значение выбранного поля.
- **больше** - проверяется сравнение поля и указанного значения. Если поле больше значения, условие считается выполненным. В качестве значения указывается введенное вручную значение или значение выбранного поля.
- **больше или равно** - проверяется сравнение поля и указанного значения. Если поле больше или равно значению, условие считается выполненным. В качестве значения указывается введенное вручную значение или значение выбранного поля.
- **меньше** - проверяется сравнение поля и указанного значения. Если поле меньше значения, условие считается выполненным. В качестве значения указывается введенное вручную значение или значение выбранного поля.
- **меньше или равно** - проверяется сравнение поля и указанного значения. Если поле меньше или равно значению, условие считается выполненным. В качестве значения указывается введенное вручную значение или значение выбранного поля.
- **начинается с** - проверяется наличие указанного значения в начале значения поля. Если указанное значение находится в начале поля, то условие считается выполненным.
- **заканчивается на** - проверяется наличие указанного значения в конце значения поля. Если указанное значение находится в конце поля, то условие считается выполненным.

На каждом уровне иерархии можно добавить одно из трех условий.

Условие "**Поле события**". Добавляет проверку с полем события (см. рисунок 207).

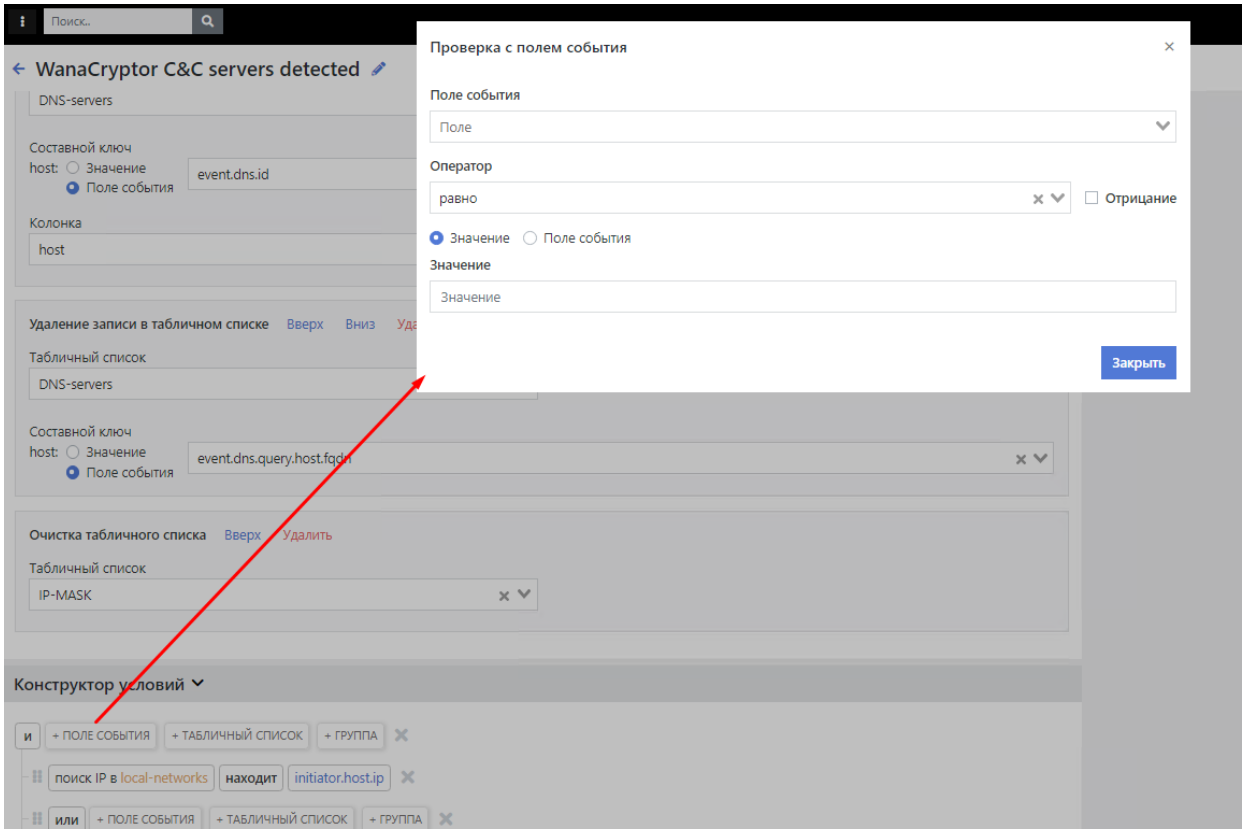



**Рисунок 207 – Проверка с полем события**

Условие добавляет в набор условий проверку отдельного поля события. Для этого настраиваются параметры:

- **Поле события** - выбираемое из списка поле события, по которому проводится проверка;
- **Оператор**- оператор сравнения;
- прочие параметры в зависимости от выбранного оператора.

Условие "**Поле табличного списка**". Добавляет проверку с полем табличного списка (см. рисунок 208).

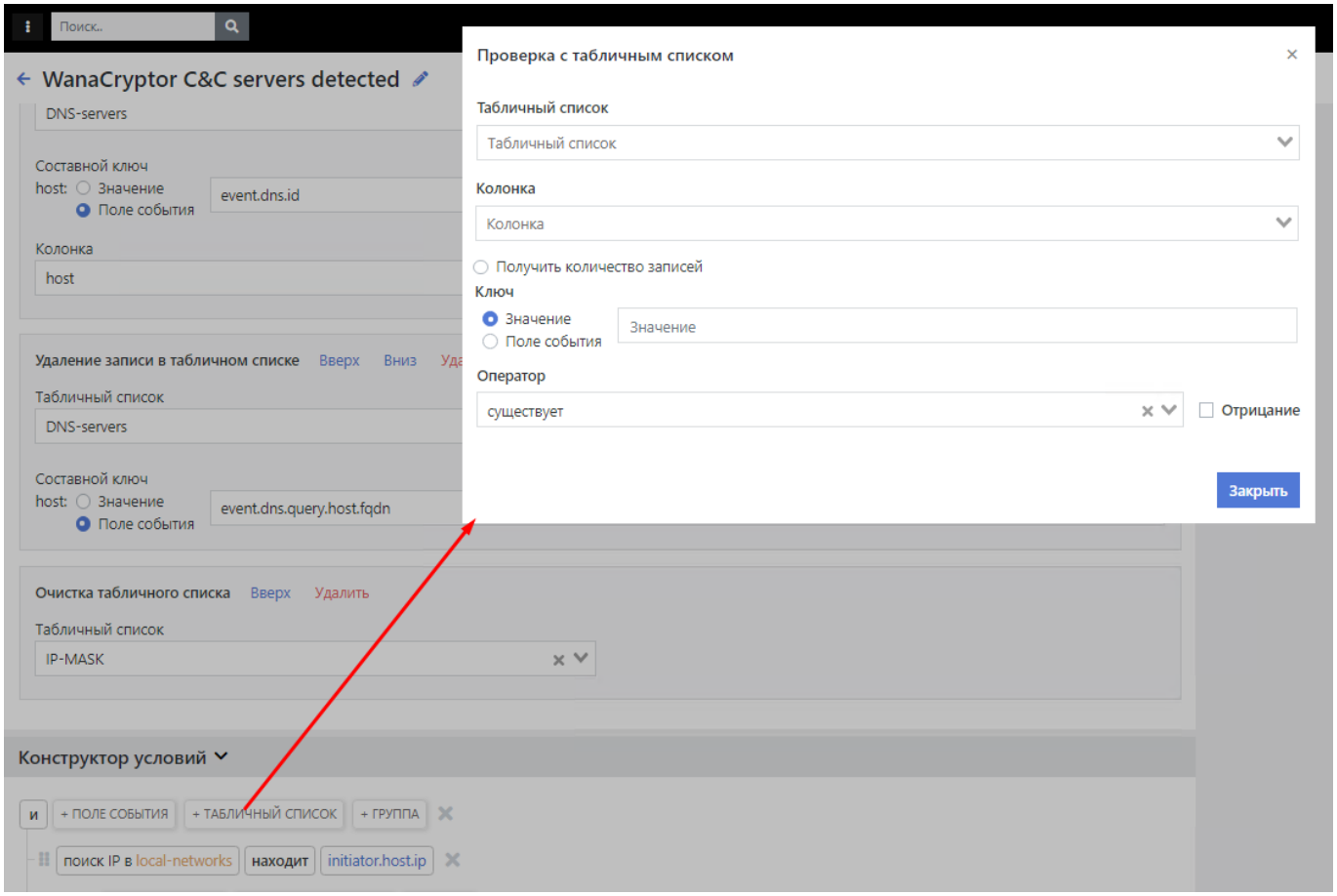



**Рисунок 208 – Проверка с полем табличного списка**

Условие добавляет в набор условий проверку отдельного поля табличного списка. Для этого настраиваются параметры:

- **Табличный список** - выбираемый из списка табличный список;
- **Колонка** - колонка табличного списка;
- **Получить количество записей** - параметры действий с табличным списком с применением оператора и заданием значения;
- **Оператор** или условия поиска (значение или поле события);
- прочие параметры в зависимости от выбранного оператора.

Условие "**Группа**". Добавляет группировку для нескольких условий (см. рисунок 209).

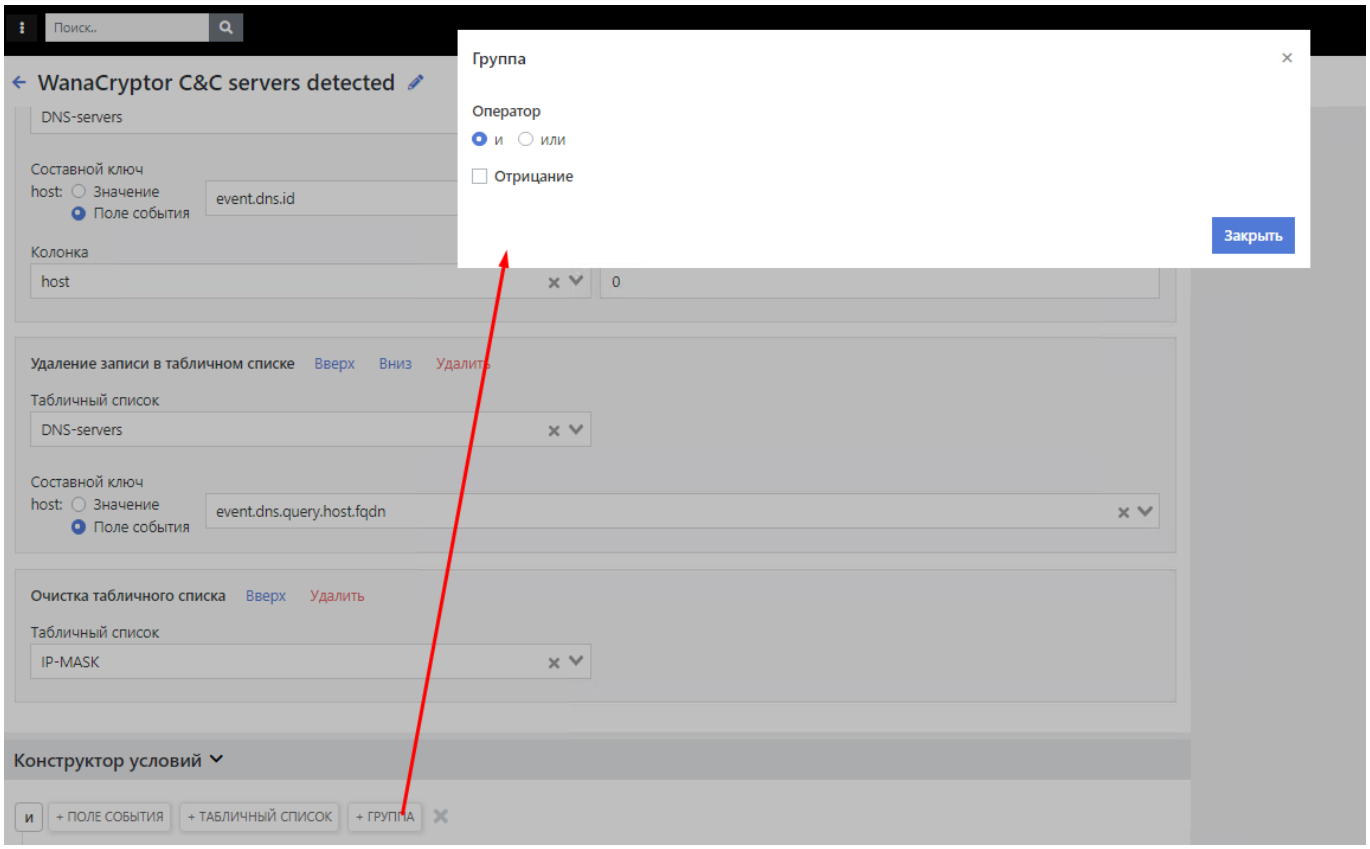



**Рисунок 209 – Группировка условий**

При группировке условий применяется объединение:

- **И** - в этом случае группа условий выполняется и событие отбирается, если выполнены все условия в группе условий;
- **ИЛИ** - в этом случае группа условий выполняется и событие отбирается, если выполнено хотя бы одно условие в группе условий.

Также доступно отрицание результата объединения условий в группу.

# 20.3 Управление табличными списками

## 20.3.1 Создание нового табличного списка

При клике на кнопку "Создать новое хранилище" откроется форма ввода параметров для нового хранилища (см. рисунок 210).

При создании хранилища задайте параметры:

- **Наименование хранилища** (произвольное).
- **Описание** (произвольное).
- Чекбокс "**Под большой объем данных?**" необходим если предполагается, что объем данных будет больше миллиона записей. При этом будет использоваться другой механизм работы с данными.
- **Схема данных** - в схеме через запятую задаются столбцы с данными. Тип может быть указан строчный (*string*), целочисленный (*integer*, *bigint*), вещественное число с переменной

точностью (*double*), для IP-адресов (*IP*), для подсетей IPv4 и IPv6 (*CIDR*). Поле "**Ключ?**" используется для обеспечения уникальности значения.

- Чекбокс "**Скрыть данные?**" необходим, если предполагается, что данные в интерфейсе **Платформы Радар** необходимо отображать в маскированном виде.

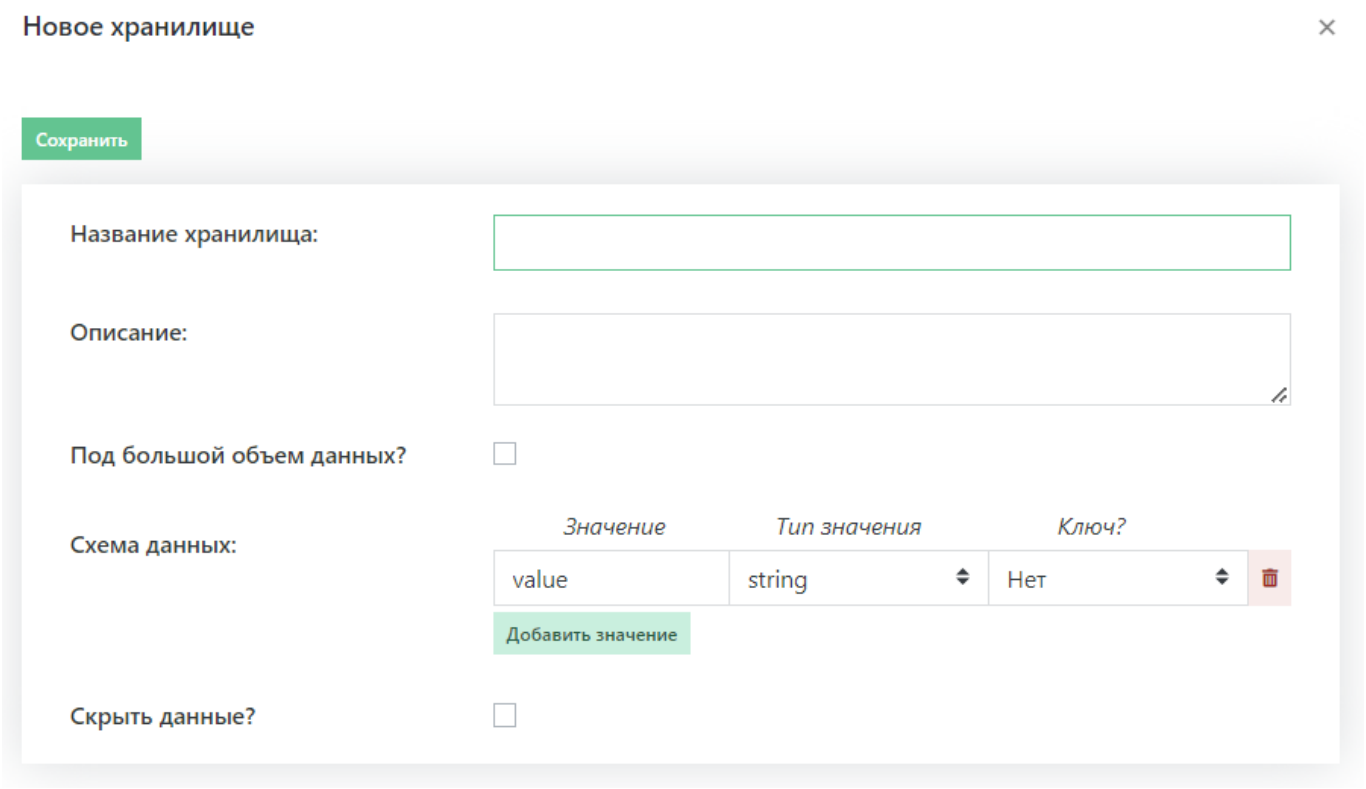



**Рисунок 210 – Создание нового хранилища**

## 20.3.2 Управление табличным списком

При клике на иконку просмотра табличного списка откроется его содержимое (см. рисунок 211).

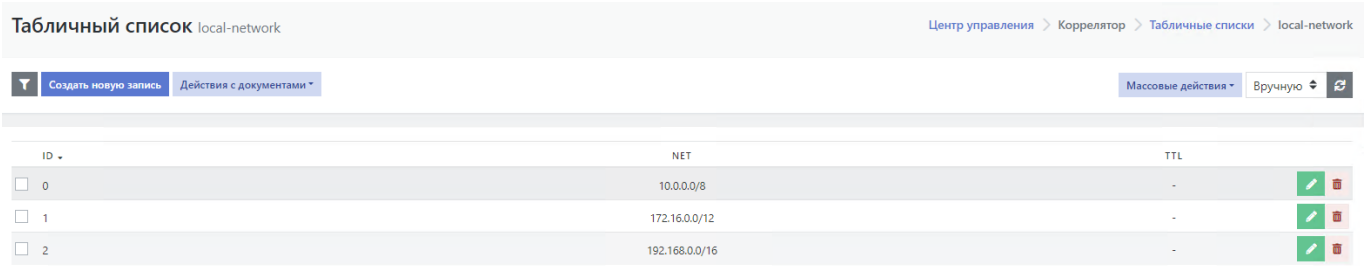



**Рисунок 211 – Просмотр табличного списка.**

Для табличного списка доступны действия:

- добавление нового значения;
- действия с документами;
- установка фильтра;
- массовые действия;
- выбор строки;
- редактирование отдельной строки;

- удаление отдельной строки.

При добавлении нового значения откроется форма ввода нового значения (см. рисунок 212).

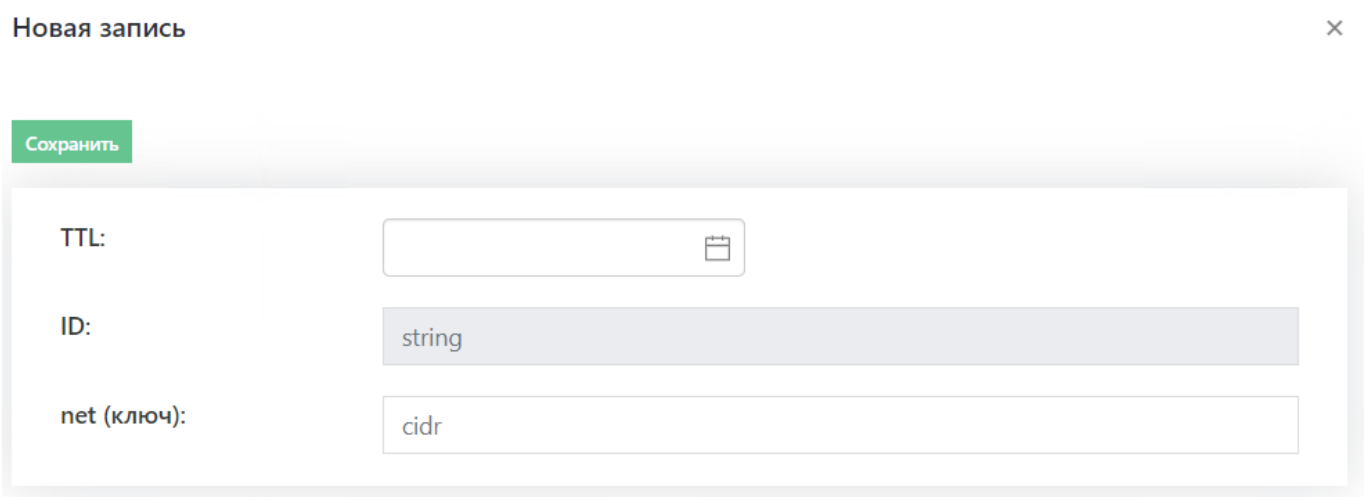



**Рисунок 212 – Добавление нового значения**

В поле "**TTL**" устанавливается дата, до наступления которой запись табличного списка будет действительна.

Для каждой строки табличного списка автоматически задается значение поля "**ID**". Для полей со значением "**Ключ**" с параметром "**Да**" (см. раздел «Создание нового табличного списка»), необходимо соблюдать уникальность значений. Также необходимо соблюдать уникальность значений поля "**ID**" при импорте списка данных. При создании новой записи в табличном списке необходимо заполнять все значения полей с пометкой "**Ключ**".

По клику на кнопку "**Действия с документами**" доступна загрузка и выгрузка табличного списка. Доступные форматы для выгрузки и загрузки: CSV, Excel, JSON.

**Важно!** *При импорте документа в нём должны присутствовать все поля табличного списка (включая поле «ID»).*

При установке фильтра  откроется строка "**Найти совпадение**" с установкой фильтра по ID и значению (см. рисунок 213).

Кнопка "**Показать все**" позволяет сбросить фильтр.

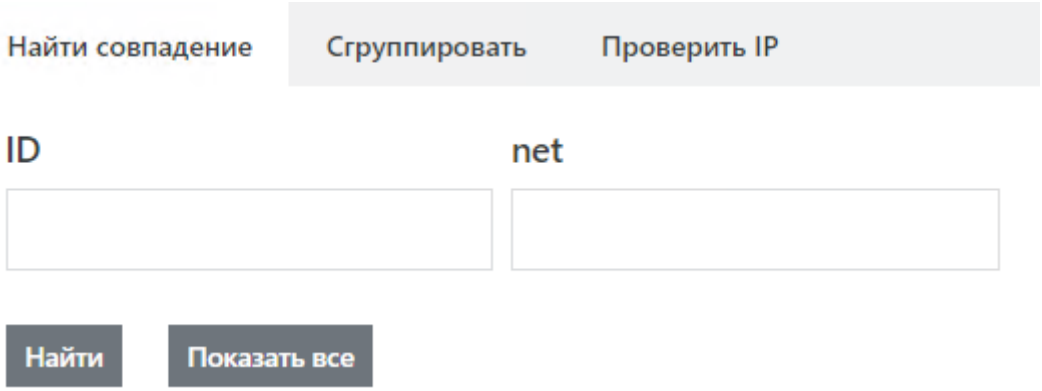



**Рисунок 213 – Фильтр табличного списка**

В строке "**Сгруппировать**" можно установить фильтр группировки столбцов по возрастанию или убыванию (см. рисунок 214).

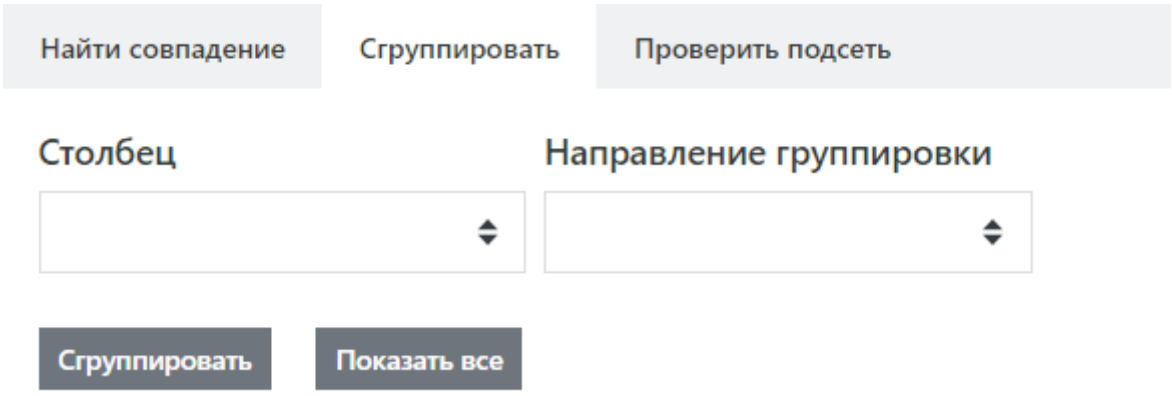



**Рисунок 214 – Группировка табличного списка**

Если в табличном списке есть поле с типом данных IP, то появляется вкладка фильтра "**Проверить подсеть**", где, указав столбец и подсеть, можно проверить принадлежность подсети к выбранному столбцу (см. рисунок 215).

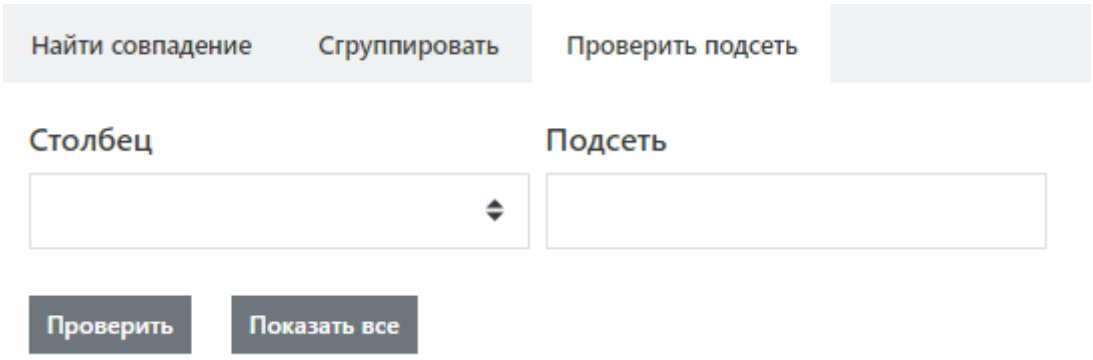



**Рисунок 215 – Проверка подсети**

Если в табличном списке есть поле с типом данных CIDR, то появляется вкладка фильтра "**Проверить IP**", где, указав столбец и IP-адрес, можно проверить IP-адрес на принадлежность к выбранному столбцу (см. рисунок 216).

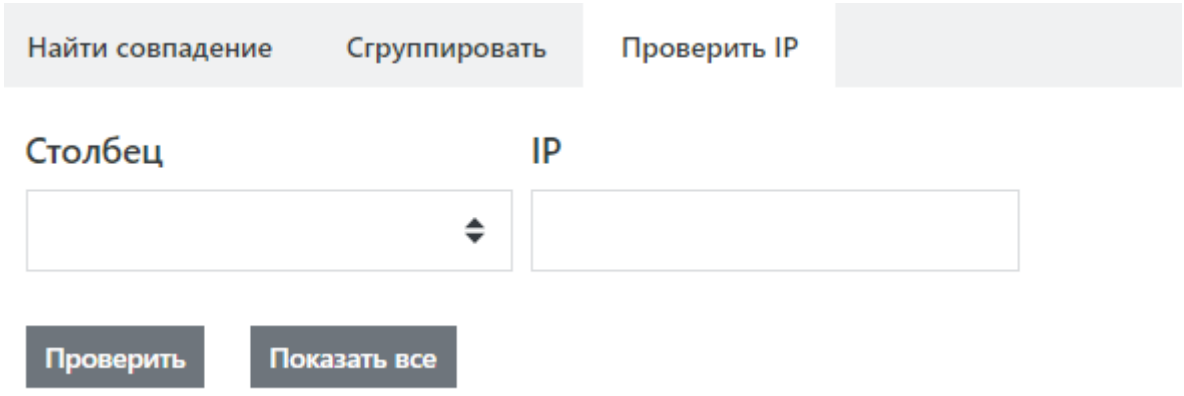



**Рисунок 216 – Проверка IP**

В массовых действиях доступно удаление выбранных или всех строк.
При редактировании отдельной строки отобразится та же форма, что и при добавлении нового значения (см. рисунок 212).

## 20.4 Управление фильтрами потока событий

Перечень фильтров потока событий представлен на рисунке 217.

Для управления фильтрами потока событий при нажатии на кнопку "**Действие**" разворачивается перечень пунктов:

- **Экспортировать** - позволяет экспортировать выбранные фильтры в файл;
- **Импортировать** - позволяет импортировать фильтры из файла;
- **Удалить** - позволяет удалить выбранные фильтры;
- **Экспортировать всё** - позволяет экспортировать все фильтры в файл;
- **Удалить всё** - позволяет удалить все фильтры.

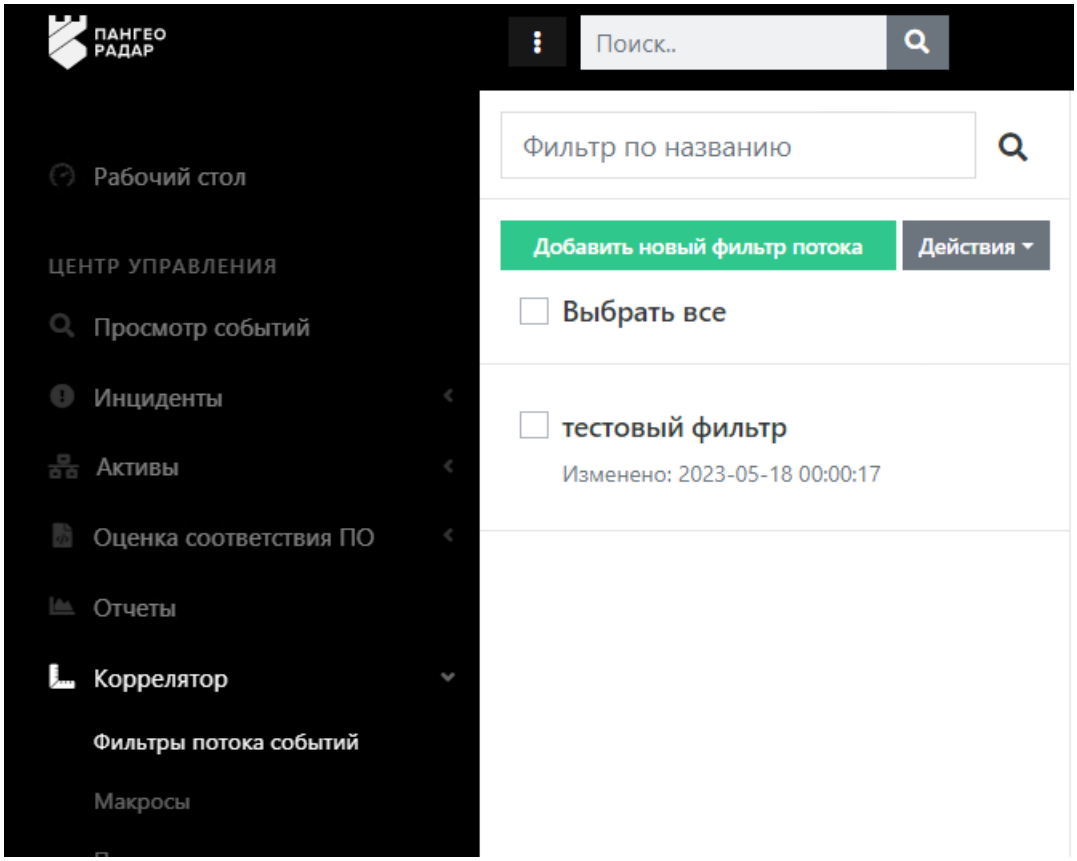



**Рисунок 217 – Перечень фильтров потока событий**

В перечне доступна фильтрация по наименованию фильтра. Для поиска подходящего фильтра введите часть его названия и кликните на иконку поиска . Для сброса условий поиска очистите поле ввода наименования фильтра и снова кликните на иконку поиска.

Для добавления нового фильтра кликните на кнопку "**Добавить новый фильтр потока**" и введите наименование добавляемого фильтра. Новый фильтр потока будет добавлен в перечень (см. рисунок 218).

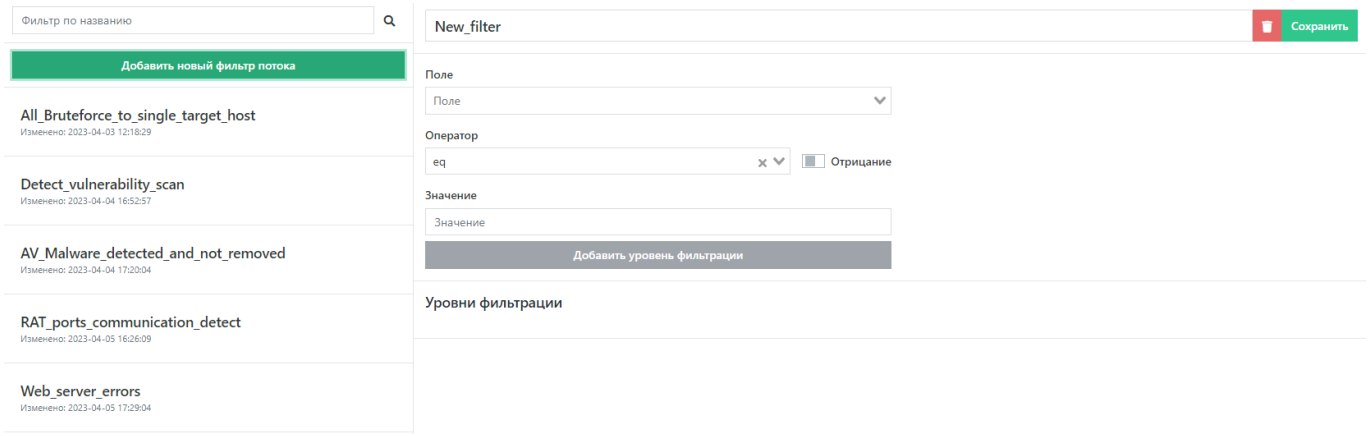



**Рисунок 218 – Добавление нового фильтра потока**

При добавлении фильтра потока событий будут отображены его параметры.

В параметрах задается:

- имя фильтра потока (можно указать любое);
- иконка удаления фильтра потока событий  ;
- кнопка сохранения параметров фильтра потока событий;
- уровни фильтрации.

Для добавления уровня фильтрации выберите поле из списка, затем выберите один из операторов сравнения:

- **eq** - сравнивает поле со значением;
- **in** - проверяет вхождение поля в список значений;
- **substr** - проверяет, входит ли значение в поле.

Для оператора можно установить признак отрицания, в результате чего смысл проверки поменяется на противоположный (операция неравенства и отсутствия вхождения).

Введите вручную значение, с которым сравнивать, после чего кликните кнопку "**Добавить уровень фильтрации**", после чего уровень фильтрации будет добавлен (см. рисунок 219).

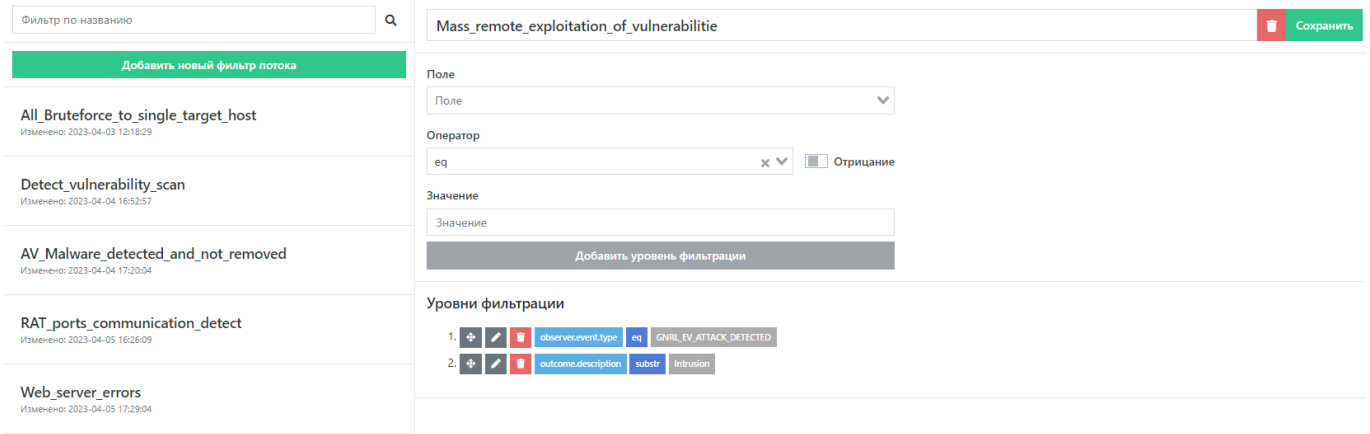



**Рисунок 219 – Уровни фильтрации**

Для каждого уровня доступны действия:

- Перемещение на уровень выше или ниже иконкой . Фильтры потока событий будут применяться в порядке установленной очередности.
- Редактирование иконкой .
- Удаление иконкой . **Уровень удаляется без предупреждения.**

**Платформа Радар** позволяет менять одновременно несколько фильтров. При переходе от настроек одного фильтра потока к настройкам другого фильтра внесенные изменения сохраняются. После окончания внесения изменений сохраните их кликом по кнопке "Сохранить".

**Внимание!!!** *Если не сохранить настройки, то при переходе к другому разделу или странице* ***Платформы Радар*** *изменения не будут сохранены.*

В результате работы фильтра потока события будут отбираться в соответствии с настроенными уровнями фильтрации. В отбор будут попадать события, удовлетворяющие всем уровням фильтрации.

## 20.5 Управление макросами

Чтобы увидеть перечень макросов необходимо перейти ***Коррелятор - Макросы*** (см. рисунок 220).

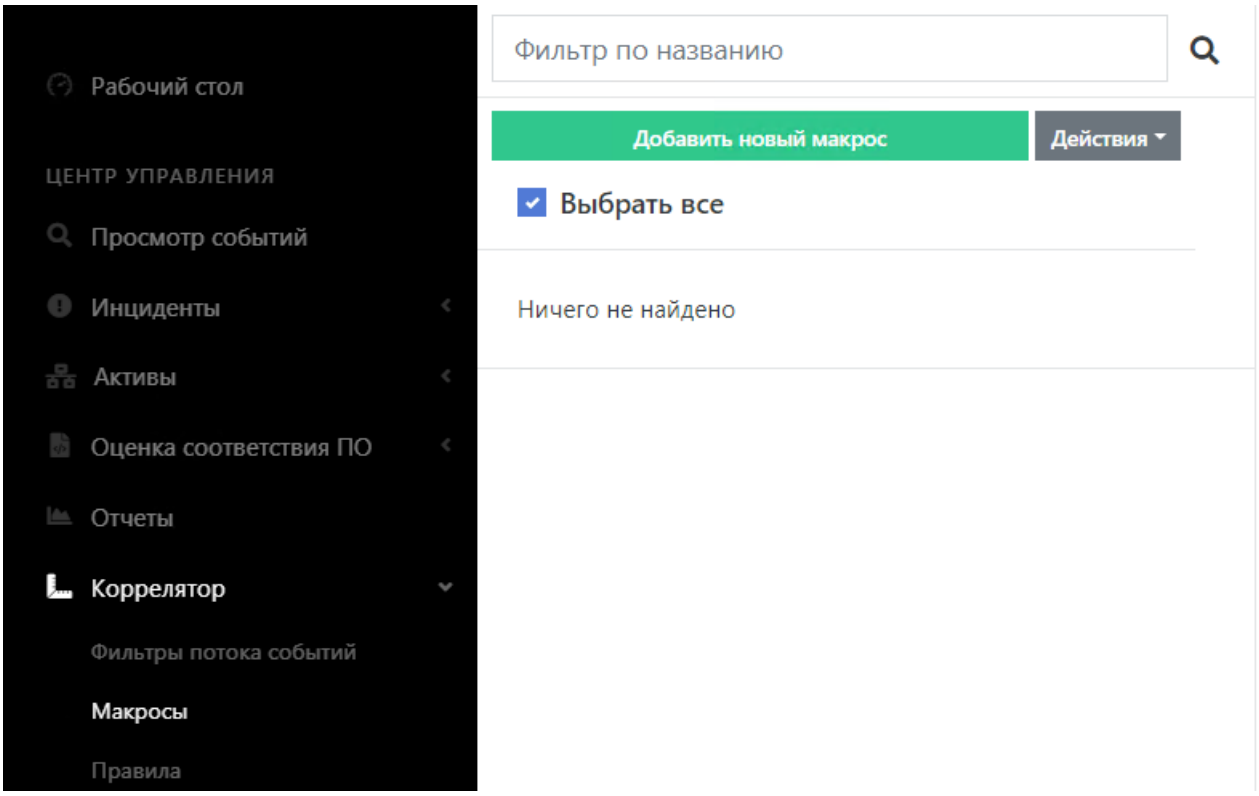



**Рисунок 220 – Перечень макросов**

В перечне доступна фильтрация по наименованию макроса. Для поиска подходящего макроса введите часть его названия и кликните на иконку поиска . Для сброса условий поиска очистите поле ввода наименования макроса и снова кликните на иконку поиска.

Для добавления нового макроса кликните на кнопку "**Добавить новый макрос**" и введите наименование добавляемого макроса. Новый макрос будет добавлен в перечень.

Для редактирования макроса выберите его в списке и нажмите кнопку "**Редактировать**" (см. рисунок 221).


**Рисунок 221 – Параметры макроса**

В режиме редактирования доступно изменение имени макроса и его текста (см. рисунок 222).

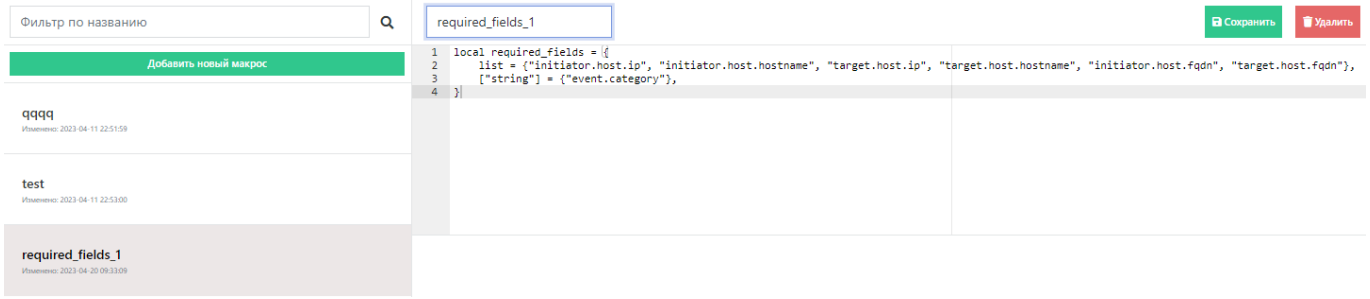



**Рисунок 222 – Редактирование макроса**

В режиме редактирования доступны действия сохранения изменений и удаления макроса.

## 20.6 Ретроспективная корреляция

**Платформа Радар** позволяет осуществлять проверку гипотез на основе исторических данных, хранимых в системе. Для осуществления ретроспективного анализа можно использовать как существующие правила корреляции, так и вновь созданные.

Для перевода правила в режим ретроспективного анализа необходимо изменить ключ очереди, на которую подписывается правило и создать задачу по ретроспективному анализу. Рассмотрим работу в режиме ретроспективного анализа на примере существующего правила. В примере будет использовано правило "Event_logs_cleared".

В разделе ***Коррелятор - Правила*** найти нужное правило и в настройках установить признак ретроспективной корреляции.

Далее необходимо создать задачу по ретроспективному анализу. Для этого нужно перейти в раздел ***Коррелятор - Ретроспективная корреляция*** (см. рисунок 223).

На странице создания задач по ретроспективному анализу необходимо указать следующие параметры параметры:

- **Период** - указать значения начала и конца необходимого промежутка времени, в котором будет проводиться анализ;
- **Название задачи** - указать имя задачи для ее идентификации в списке задач;
- **Правило** - выбрать правило ретроспективной корреляции для задачи, по которому будет проведена корреляция ретроспективных данных;

- **Индекс** - указать индексы событий, по которым необходимо произвести анализ (поддерживается wildcard символ "*").

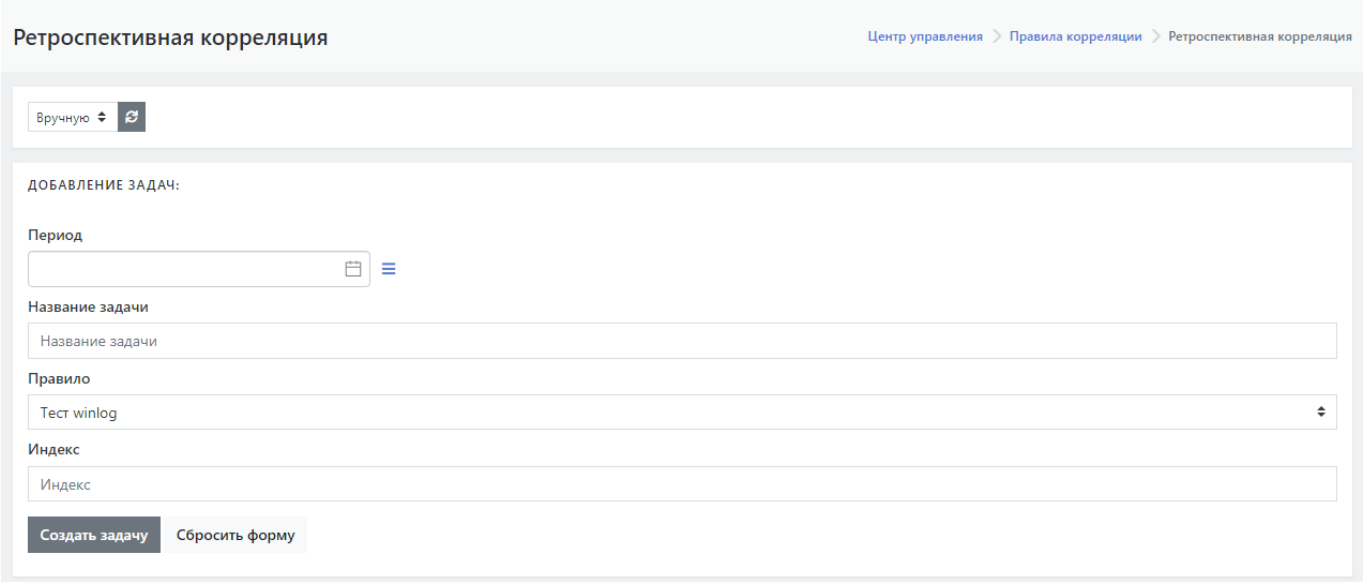



**Рисунок 223 – Ретроспективная корреляция.**

После настройки параметров необходимо нажать кнопку "**Создать задачу**".

После выполнения вышеописанных действий система запустит созданную задачу с указанными параметрами.

# 20.7 Управление шаблонами

**Платформа Радар** позволяет управлять двумя видами шаблонов: шаблоны алертов, шаблоны группировки.

## 20.7.1 Шаблоны алертов

Перечень шаблонов алертов представлен на рисунке 224.

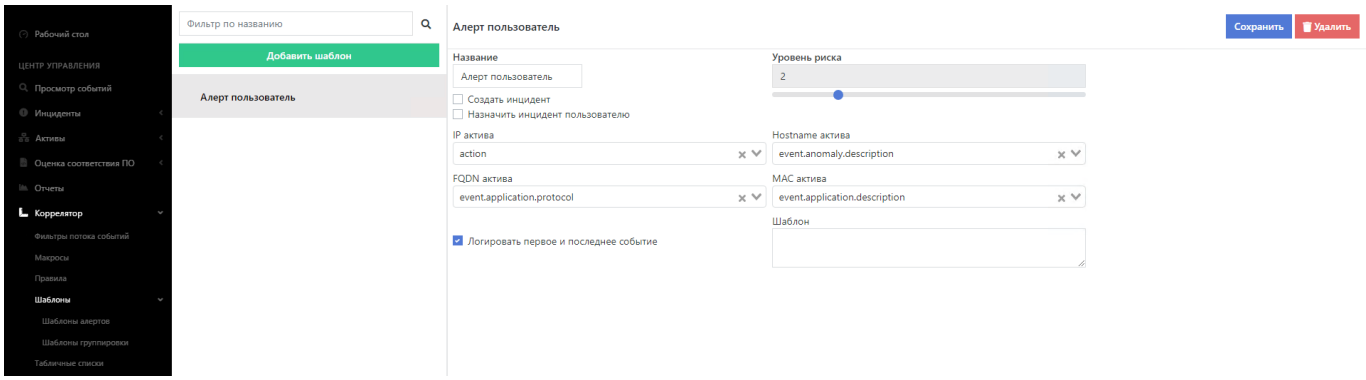



**Рисунок 224 – Перечень шаблонов алертов**

В перечне доступна фильтрация по наименованию шаблона. Для поиска подходящего шаблона введите часть его названия и кликните на иконку поиска  . Для сброса условий поиска очистите поле ввода наименования шаблона и снова кликните на иконку поиска.

Для добавления нового шаблона кликните на кнопку "**Добавить шаблон**". Во вновь открывшемся окне (см. рисунок 225) введите параметры шаблона алертов:

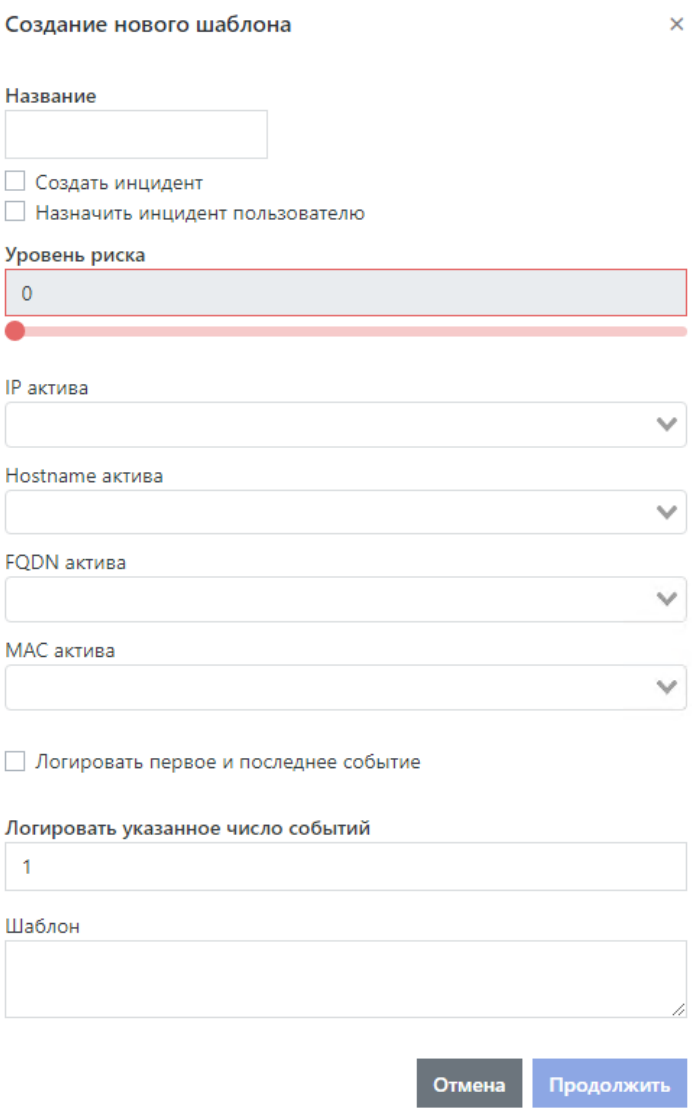



**Рисунок 225 - Создание шаблона алерта**

- **Название** - название нового шаблона алерта.
- **Создать инцидент** - при срабатывании правила корреляции будет создан инцидент.
- **Назначить инцидент пользователю** - при срабатывании правила корреляции и создании инцидента необходимо инцидент назначить пользователю.
- **Уровень риска** - задает уровень риска для алерта. Параметр задается пользователем самостоятельно, исходя из критичности события для инфраструктуры.
- **IP актива** - выбирается из списка поле в качестве ip-адреса актива. **Поле является обязательным для заполнения.** Поле может являться частью сводной таблицы событий.
- **Hostname актива** - выбирается из списка поле в качестве наименования хоста актива. Поле может являться частью сводной таблицы событий.
- **FQDN актива** - выбирается из списка поле в качестве наименования домена актива. Поле может являться частью сводной таблицы событий.
- **MAC актива** - выбирается из списка поле в качестве mac-адреса актива. Поле может являться частью сводной таблицы событий.

- **Логировать первое и последнее события** - при установленном признаке логируются только первое и последнее события. При снятом - все события.
- **Логировать указанное количество событий** - в параметре задается количество логируемых первых событий.
- **Шаблон** - в параметре задается шаблон алерта (инцидента).

В качестве шаблона алерта используется предопределенный текст. Кроме самого текста в шаблон могут быть вставлены поля логлайна. Сами поля могут быть взяты из отдельных записей события:

- `.First` - первый логлайн.
- `.Last` - последний логлайн.
- `.Loglines` - массив логлайнов событий.
- `.Meta` - дополнительные поля.

Пример шаблонов:

```
Результат анализа

На рабочей станции {{ .First.observer.host.ip }} (FQDN: "{{
.First.observer.host.fqdn }}") обнаружена успешная попытка запуска HACK утилиты


На узле {{ .First.target.host.fqdn |}}, IP: {{ .First.target.host.ip }} были
зафиксированы многочисленные неуспешные попытки аутентификации от {{
.Meta.uniq_users }} уникальных УЗ
```

Чтобы изменить шаблон, выберите его из перечня (см. рисунок 224). В правой половине экрана появятся параметры шаблона. Внесите изменения в параметры и нажмите кнопку "**Сохранить**".

Для удаления шаблона нажмите кнопку "**Удалить**".

## 20.7.2 Шаблоны группировки

Перечень шаблонов группировки представлен на рисунке 226.

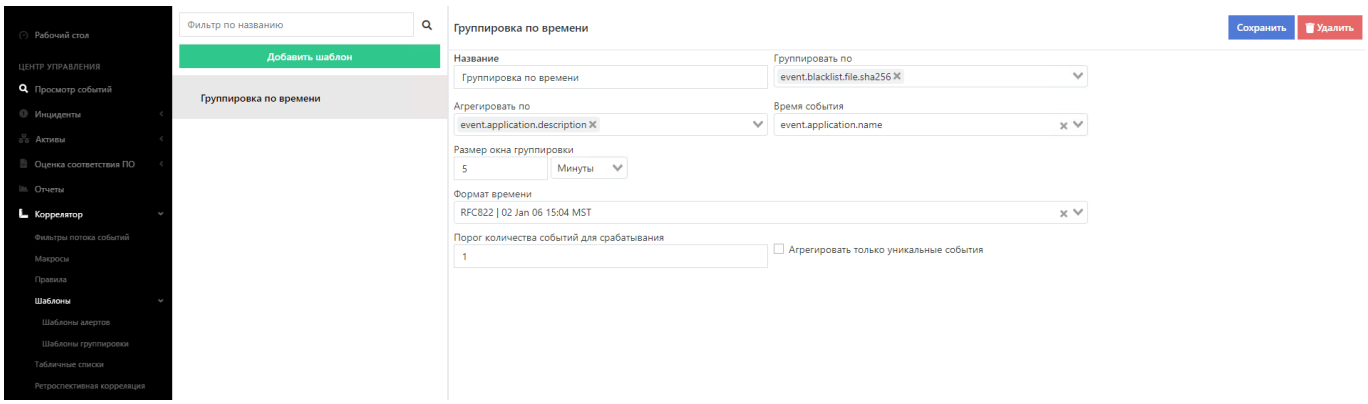



**Рисунок 226 – Перечень шаблонов группировки**

В перечне доступна фильтрация по наименованию шаблона. Для поиска подходящего шаблона введите часть его названия и кликните на иконку поиска  Для сброса условий поиска очистите поле ввода наименования шаблона и снова кликните на иконку поиска.

Для добавления нового шаблона кликните на кнопку "**Добавить шаблон**". Во вновь открывшемся окне (см. рисунок 227) введите параметры шаблона группировки:

- **Название** - название нового шаблона алерта;
- **Группировать по** - параметр задает одно или несколько выбираемых из списка полей группировки;
- **Агрегировать по** - параметр задает одно или несколько выбираемых из списка полей агрегации;
- **Время события** - параметр задает поле, в котором хранится время события;
- **Размер окна группировки** - параметр задает время, в течение которого после срабатывания правила группировать входящие события;
- **Формат времени** - параметр задает формат времени события, выбирается из списка;
- **Порог количества событий при срабатывании** - параметр задает максимальное количество группируемых событий в рамках временного окна;
- **Агрегировать только уникальные события** - параметр позволяет указать, группировать повторяющиеся события или нет.

Максимальное количество срабатываний правил корреляции в секунду задается глобальном параметре конфигурации: ***Кластер - Управление конфигурацией - Logmule2 - Максимальное количество сработок***.

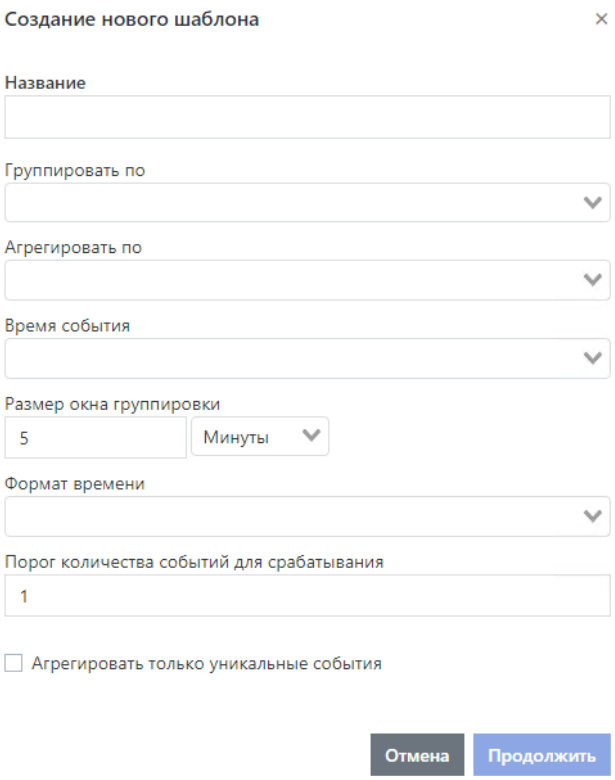



**Рисунок 227 – Создание шаблона группировки**

Чтобы изменить шаблон, выберите его из перечня (см. рисунок 226). В правой половине экрана появятся параметры шаблона. Внесите изменения в параметры и нажмите кнопку "**Сохранить**".

Для удаления шаблона нажмите кнопку "**Удалить**".

# 21. Работа с сообщениями

## 21.1 Общие данные

Сообщение - механизм обмена текстовой информацией между пользователями системы. Сообщение может быть отправлено нескольким получателям.

Адресатами сообщений могут выступать пользователи и группы пользователей. Отправка сообщения группе пользователей равносильна отправке сообщения всем членам этой группы.

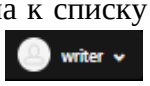
Сообщение может быть отправлено с дополнительной контекстной информацией.

В качестве контекста сообщений могут выступать следующие сущности:

- тип инцидента;
- инцидент;
- актив.

В случае наличия контекста в сообщение добавляется ссылка на соответствующий объект.

## 21.2 Доступ к списку сообщений

Для получения доступа к списку сообщений пользователя необходимо щелкнуть по пиктограмме профиля пользователя 

и в открывшемся меню выбрать пункт "**Сообщения**".

На экране откроется список сообщений пользователя (см. рисунок 228).

Подробное описание интерфейса раздела "**Сообщения**" приведено в отдельном разделе «Пользовательские настройки. Профиль - Сообщения».

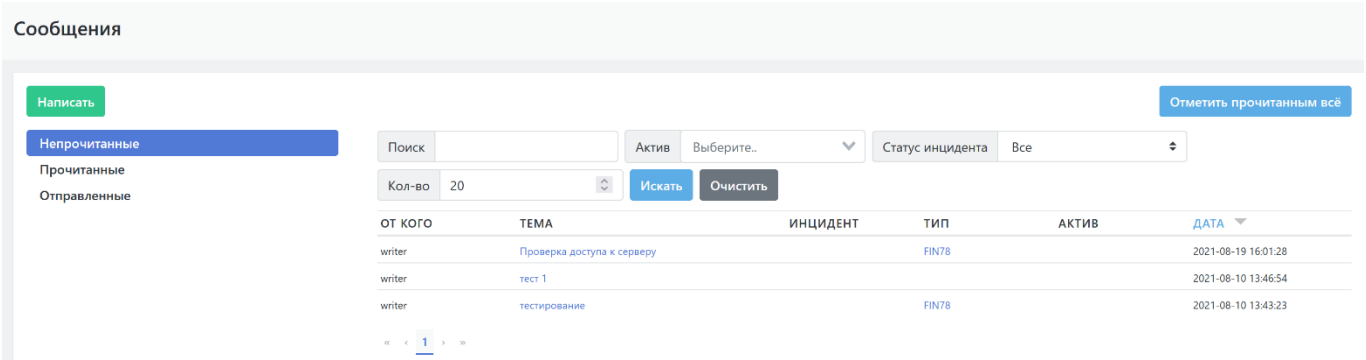



**Рисунок 228 – Список сообщений в профиле пользователя**

## 21.3 Просмотр деталей сообщения

### 21.3.1 Просмотр текста сообщения

Просмотр деталей сообщения доступен для всех типов сообщений: "**Непрочитанные**", "**Прочитанные**", "**Отправленные**".

Для просмотра деталей сообщения необходимо щелкнуть по теме интересующего сообщения в поле "**Тема**". На экране откроется окно с полными данными сообщения (см. рисунок 229):

- **От** - отправитель сообщения;
- **Кому** - адресат сообщения;
- **Дата** - дата и время отправки сообщения;
- Тема сообщения - заголовок, который отображается в списке сообщений пользователя.
- Текст сообщения - непосредственно текст сообщения;
- Связанные объекты - название связанного объекта в виде гиперссылки на данные объекта, для случаев, когда сообщение было отправлено из определенного контекста.

Для возврата к списку сообщений нужно нажать на кнопку "**Закрыть**". Окно просмотра закрывается. Если просматривалось сообщение из списка "**Непрочитанные**", то сообщение автоматически переводится в список прочитанных сообщений.

Если необходимо дать ответ на сообщение, то нажать на кнопку "**Ответить**". Откроется форма создания сообщения.

Процесс создания и отправки нового сообщения подробно описан в разделе «Создание и отправка сообщений».

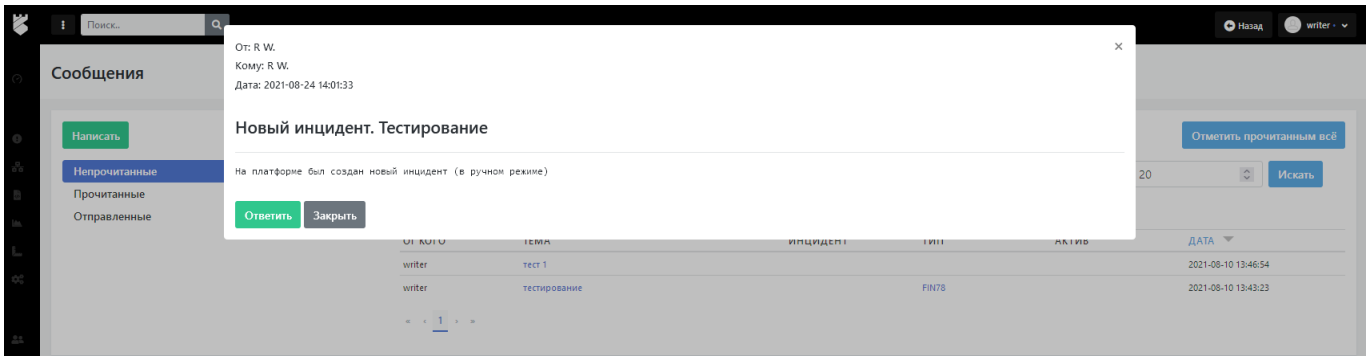



**Рисунок 229 – Окно просмотра сообщения**

## 21.3.2 Просмотр дополнительной контекстной информации

В случае наличия контекста в параметры сообщения добавляется ссылка на соответствующий объект. У сообщений с контекстом буду указаны гиперссылки в соответствующих полях списка (см. рисунок 230):

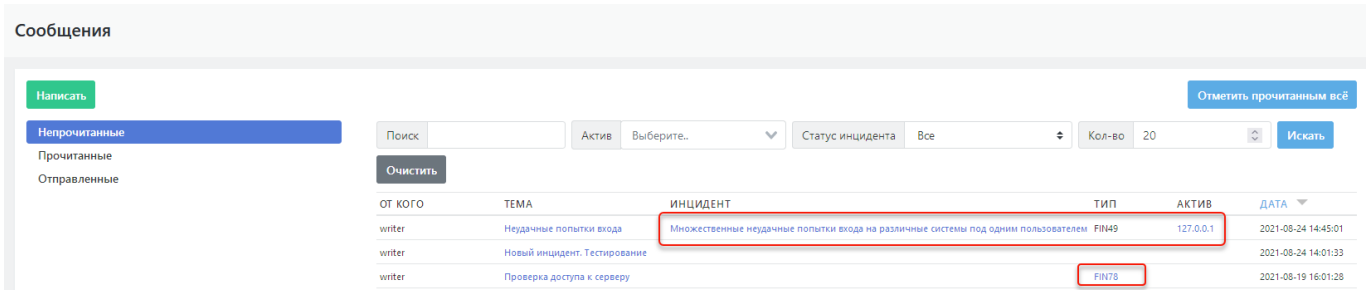



**Рисунок 230 – Гиперссылки сообщений с контекстной информацией**

- **Инцидент** - содержит название инцидента, с которым связано данное сообщение. Гиперссылка ведет на страницу описания данного инцидента;
- **Тип** - содержит идентификатор типа инцидента, с которым связано данное сообщение. Гиперссылка ведет на страницу описания данного типа инцидента;

- **Актив** - содержит идентификатор (например IP-адрес) актива, с которым связано данное сообщение. Гиперссылка ведет на страницу описания данного актива.

# 21.4 Создание и отправка сообщений

## 21.4.1 Отправка сообщения без контекстной информации

Для отправки сообщения без ссылки на объект (без контекстной информации) необходимо:

1. Перейти в раздел "**Сообщения**" в профиле пользователя 

и выбрать пункт "**Сообщения**";
2. Нажать кнопку "**Написать**";
3. В открывшейся форме сообщения заполнить следующие поля (см. рисунок 231):
    - **Получатель** - выбрать адресата из раскрывающегося списка пользователей **Платформы Радар**;
    - **Заголовок** - ввести заголовок сообщения;
    - **Сообщение** - ввести текст сообщения.
4. Нажать на кнопку "**Отправить**".

Данное сообщение должно появится в списке отправленных сообщений пользователя.

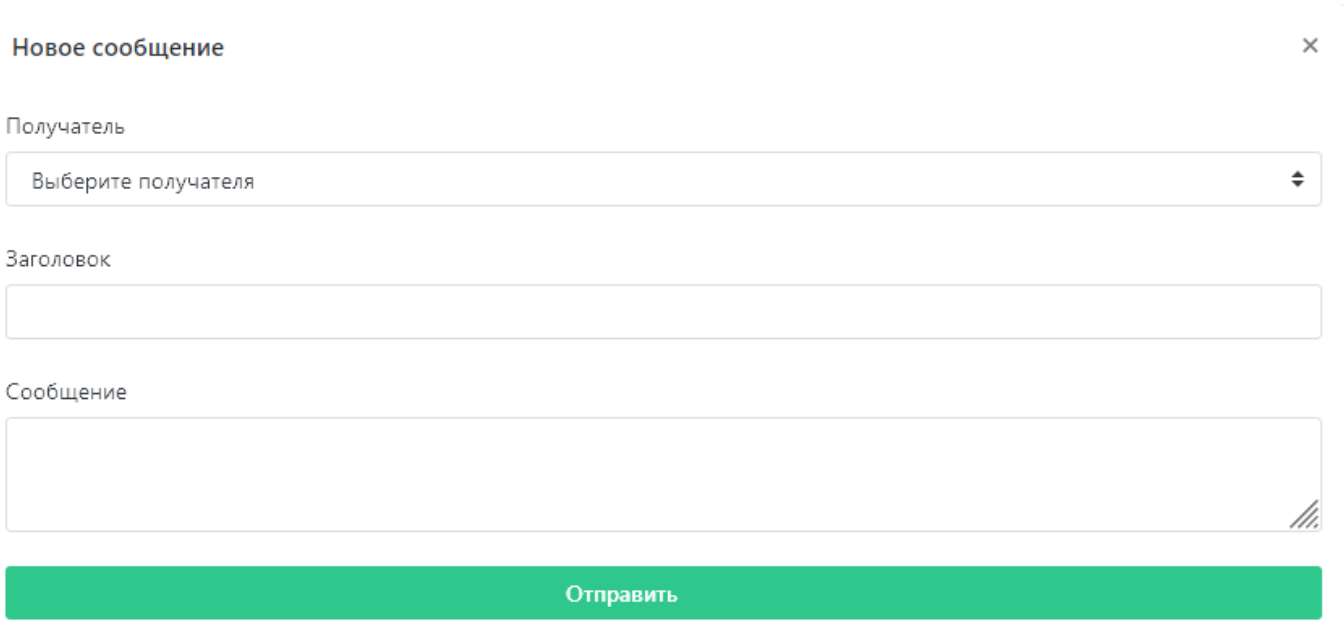



**Рисунок 231 – Отправка сообщения без ссылки на объект**

## 21.4.2 Отправка сообщений с контекстом (ссылкой на объект)

Функция отправки сообщений со ссылкой на инцидент, тип инцидента и актив доступна в соответствующих разделах:

- Кнопка "**Написать сообщение**" для отправки сообщения со ссылкой на инцидент доступна на странице карточки инцидента: ***Инцидент - Инцидент - /щелкнуть по названию интересующего инцидента в списке/***.

- Кнопка "**Написать сообщение**" для отправки сообщения со ссылкой на тип инцидент доступна на странице карточки типа инцидента: ***Инцидент - Инцидент - /щелкнуть по названию интересующего инцидента в списке/***.
- Кнопка "**Написать сообщение**" для отправки сообщения со ссылкой на актив доступна на странице карточки актива: ***Актив - Актив - /щелкнуть по названию интересующего актива в списке/***.

Форма для отправки сообщения с контекстом аналогична форме отправки сообщения без контекста. Все необходимые ссылки на объекты создаются в теле сообщения автоматически при отправке сообщения.

Подробное описание формы создания сообщения приведено в разделе «Отправка сообщения без контекстной информации».

# 22. Работа с НКЦКИ

## 22.1 Общая информация

Национальный координационный центр по компьютерным инцидентам обеспечивает координацию деятельности субъектов критической информационной инфраструктуры Российской Федерации по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

**ГосСОПКА** — государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, создаваемая в целях предотвращения и устранения последствий компьютерных атак на критическую информационную инфраструктуру Российской Федерации.

Концепция **ГосСОПКА** появилась с целью защиты критической информационной инфраструктуры (КИИ) Российской Федерации.

**Платформа Радар** позволяет автоматизировать регистрацию выбранных инцидентов в **ГосСОПКА**.

## 22.2 Настройка интеграции

Перед началом отправки инцидентов в **ГосСОПКА** необходимо произвести настройку **Платформы Радар**:

- настроить сопоставление данных;
- проверить настройку API конструктора;
- настроить группы активов;

### 22.2.1 Настройка сопоставления данных

Для настройки сопоставления данных перейдите в меню ***Параметры - Сопоставление данных*** (см. рисунок 232).

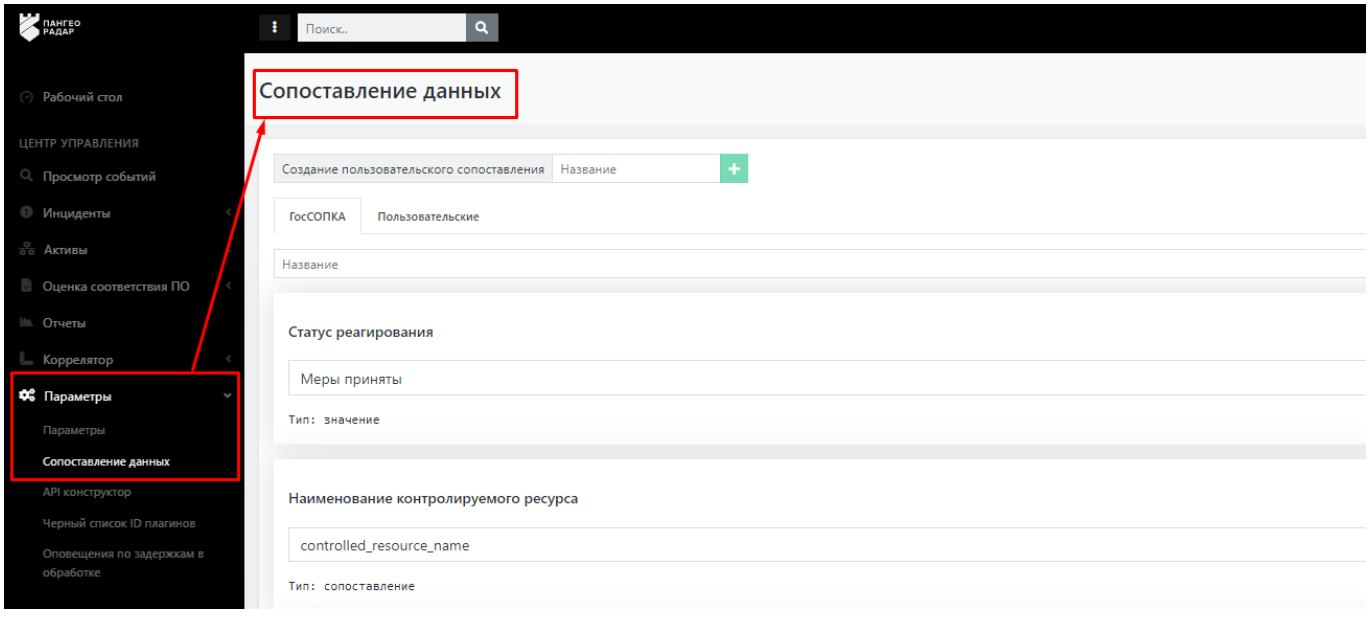



**Рисунок 232 – Сопоставление данных**

**ГосСОПКА** принимает инциденты в определенном формате с определенным набором полей. Все эти поля перечислены на странице.

Всего существует два вида полей:

- **Предопределенные**. В **Платформе Радар** такой тип поля называется **Значение**. Этот тип полей не сопоставляется, а указывается значение, выбранное из списка. Пример представлен на рисунке 233.

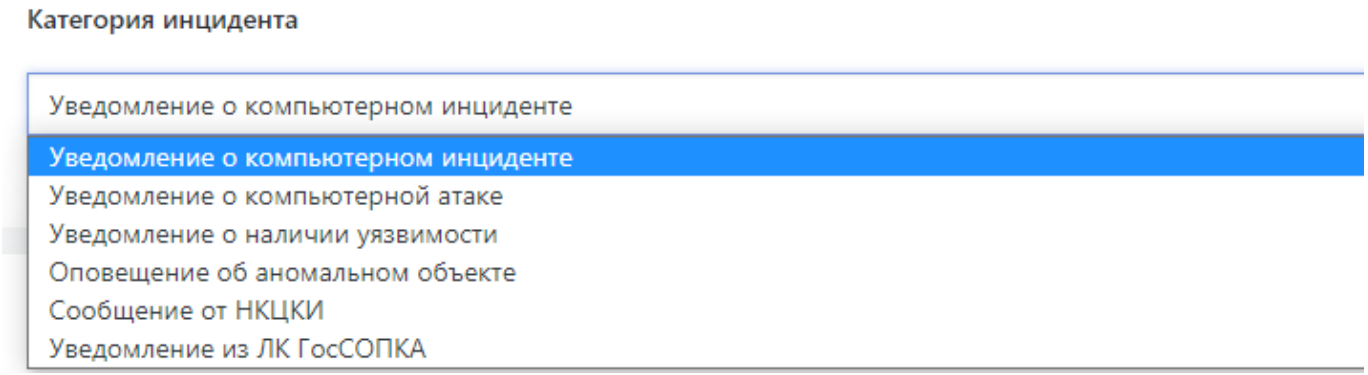



**Рисунок 233 – Выбор из списка для поля типа "Значение"**

- **Сопоставляемые**. В **Платформе Радар** такой тип поля называется **Сопоставление**. Для такого типа полей значение **Платформа Радар** берет из инцидента и помещает в сопоставляемое поле автоматически. Пример представлен на рисунке 234.

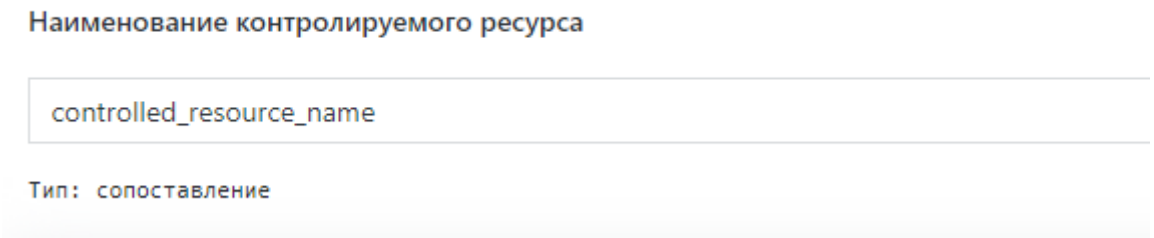



**Рисунок 234 – Указание поля инцидента для типа "Сопоставление".**

При поставке **Платформы Радар** все поля для интеграции с системой **ГоссСОПКА** уже настроены, однако при необходимости можно уточнить предопределенные поля.

## 22.2.2 API конструктор

Для перехода в **API конструктор** перейдите в меню ***Параметры - API конструктор*** (см. рисунок 235).

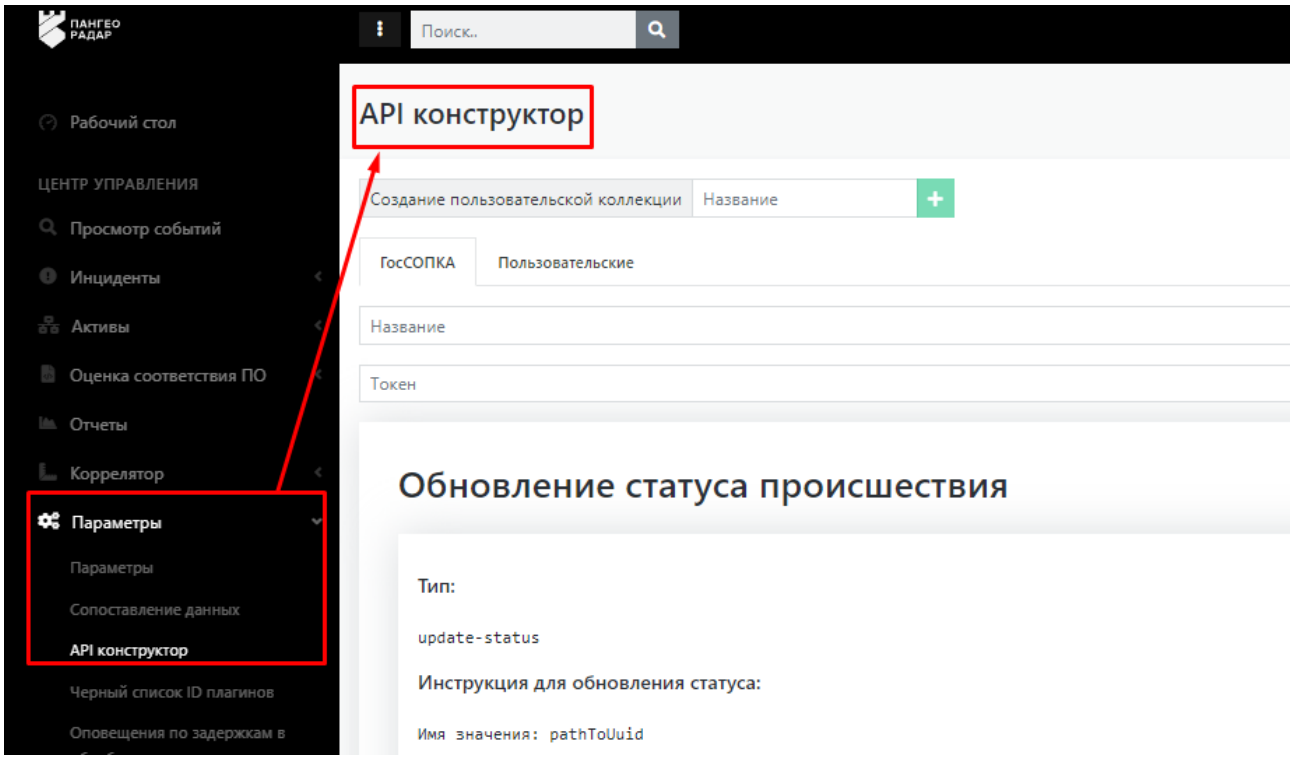



**Рисунок 235 – API конструктор**

Здесь для настройки интеграции вам необходимо указать **Токен** для передачи инцидентов в систему **ГосСОПКА**.

Внимание! После сохранения **Токен** не будет отображаться в интерфейсе **Платформы Радар**.

Ниже показаны два метода передачи инцидентов: метод обновления статуса происшествия (см. рисунок 236) и метод отправки происшествия (см. рисунок 237).

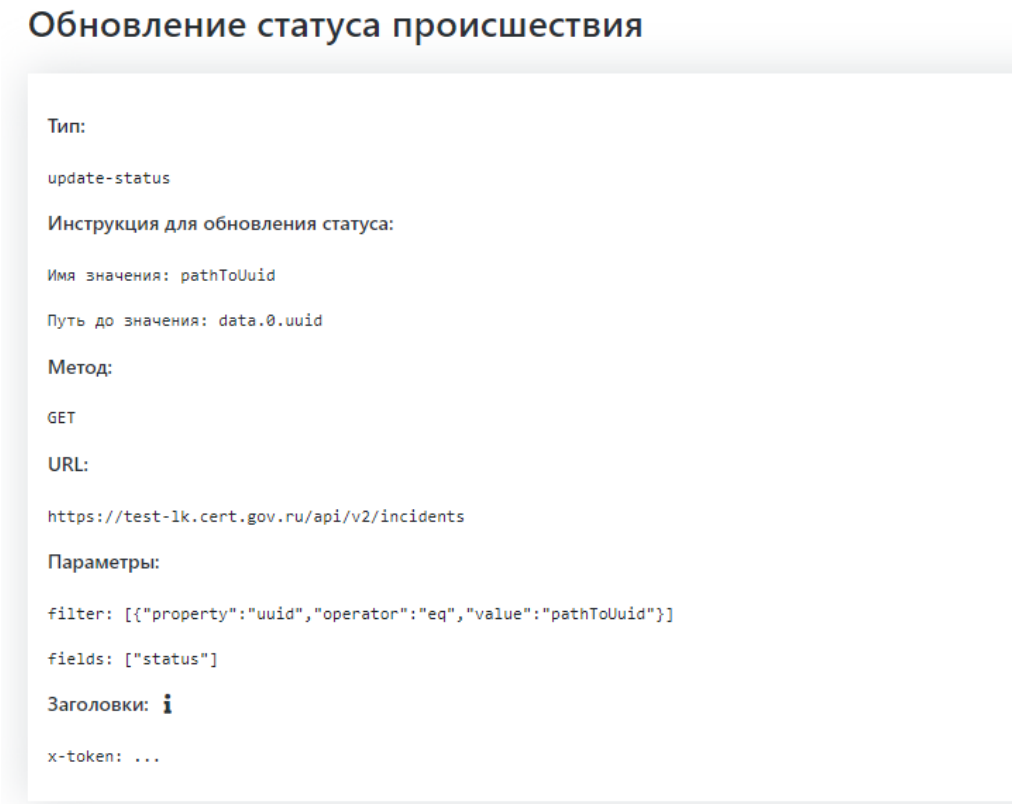



**Рисунок 236 – Метод обновления статуса происшествия**

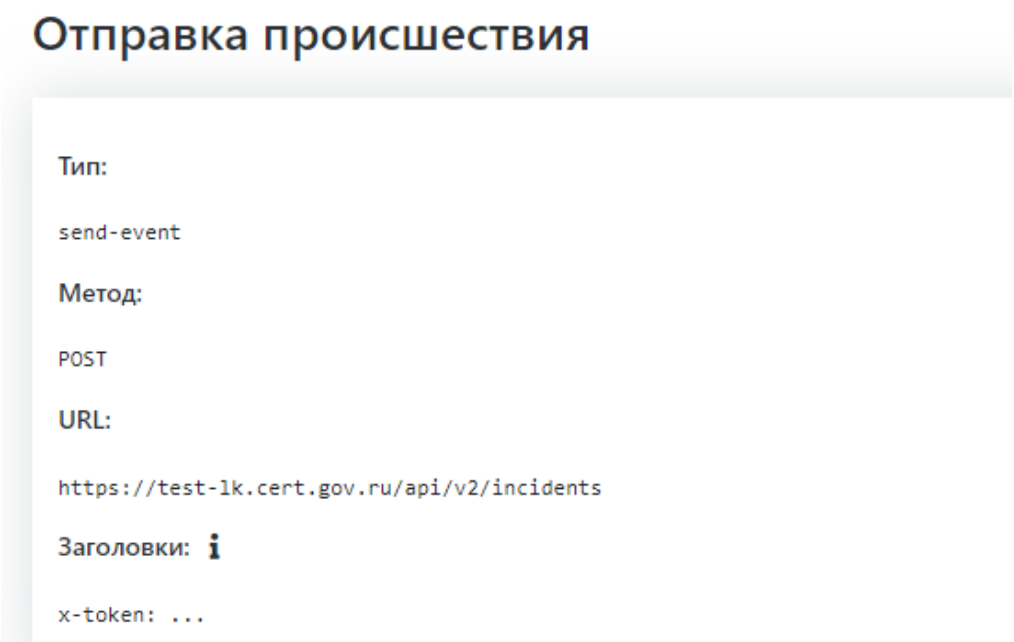



**Рисунок 237 – Метод отправки происшествия**

### 22.2.3 Настройка группы активов

К каждому инциденту привязан свой актив. А сами активы объединяются в группы. Для того, чтобы инциденты могли быть отправлены в систему **ГосСОПКА**, связанные активы должны входить в группы активов с установленным признаком КИИ (критическая информационная инфраструктура).

Убедитесь, что этот признак проставлен в группе активов. Для этого перейдите в меню ***Активы - Группы активов***, найдите необходимую группу и кликните иконку редактирования (см. рисунок 238).

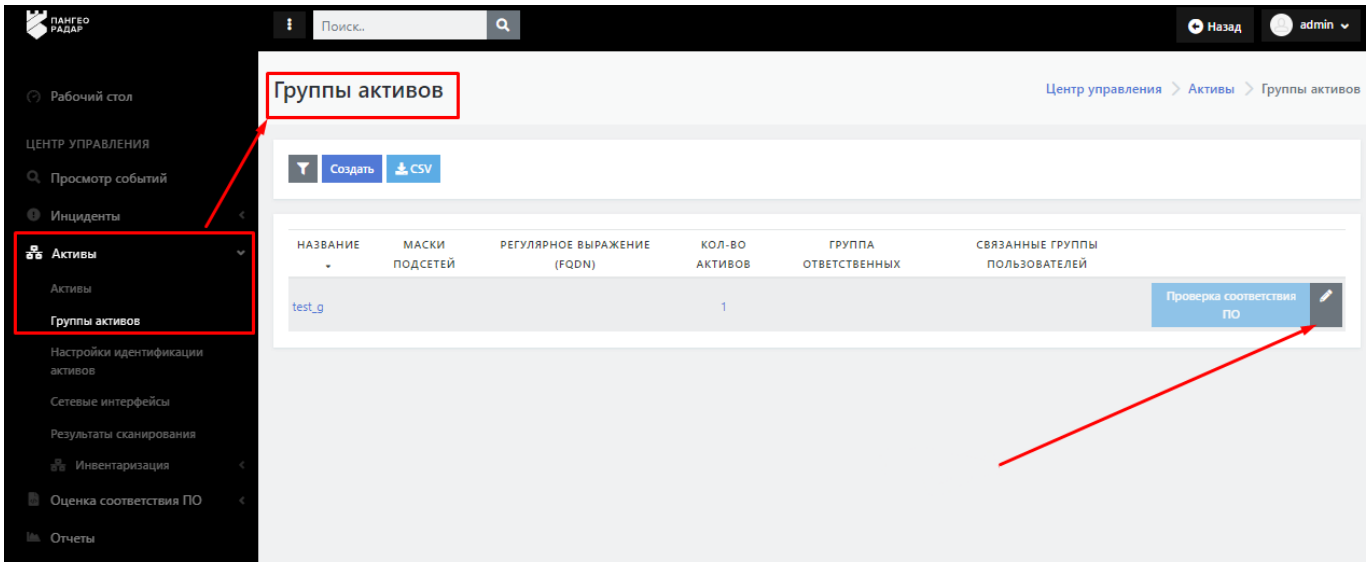



**Рисунок 238 – Редактирование группы активов.**

В настройках группы активов проверьте наличие установленного признака напротив надписи "**КИИ?**" (см. рисунок 239).

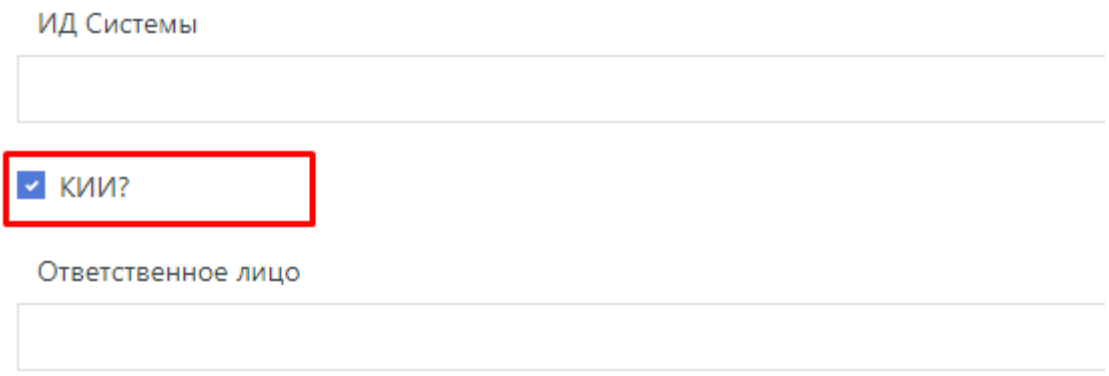



**Рисунок 239 – Признак КИИ**

## 22.3 Передача происшествий в ГосСОПКА

Передача происшествий в **ГосСОПКА** осуществляется в два этапа:

1. Среди инцидентов выбирается необходимый для отправки в качестве происшествия в **ГосСОПКА**;
2. Происшествие валидируется и отправляется в **ГосСОПКА**.

### 22.3.1 Выбор инцидента для отправки

Для выбора инцидента перейдите к инцидентам в меню ***Инциденты*** - ***Инциденты*** (см. рисунок 240).

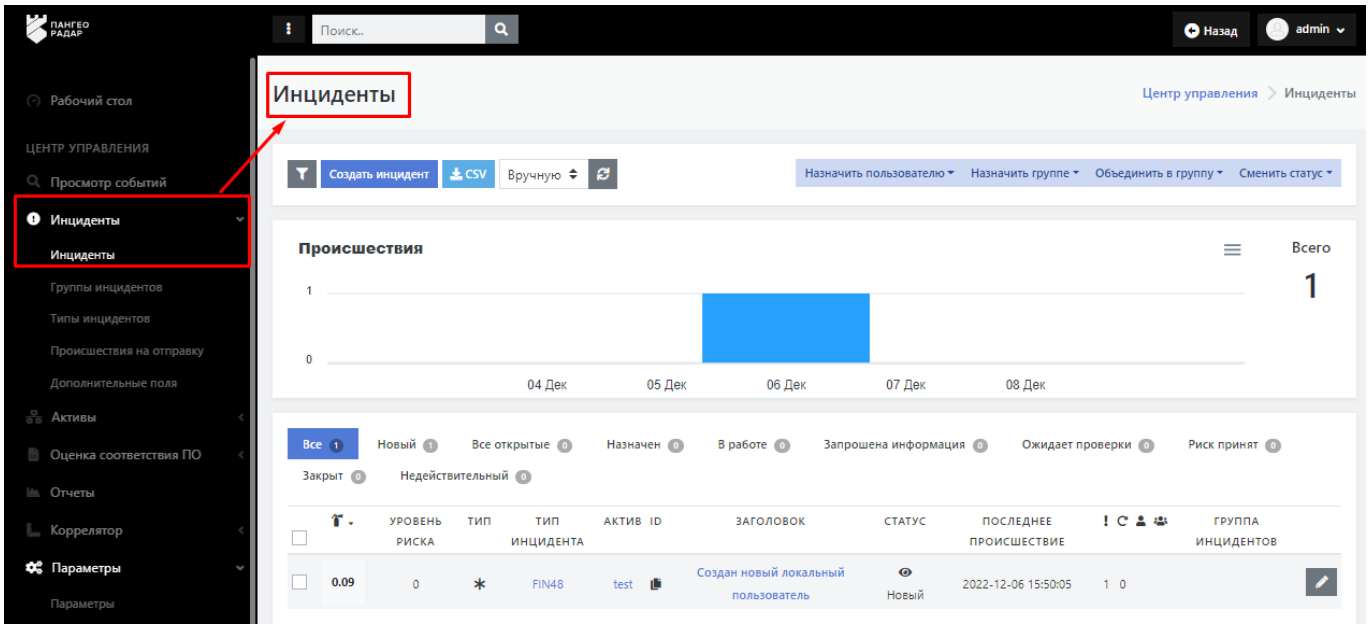



**Рисунок 240 – Перечень инцидентов**

В перечне найдите необходимый инцидент и кликните по его заголовку. В окне с инцидентом найдите блок "**Происшествия**".

Для отправки инцидента в качестве происшествия в **ГосСОПКА** (см. рисунок 241):

1. Установите признак "**Выбрать для отправки**";
2. В поле "**НКЦКИ**" выберите пункт **ГосСОПКА**;
3. Кликните на иконку "**Зарегистрировать для отправки**".

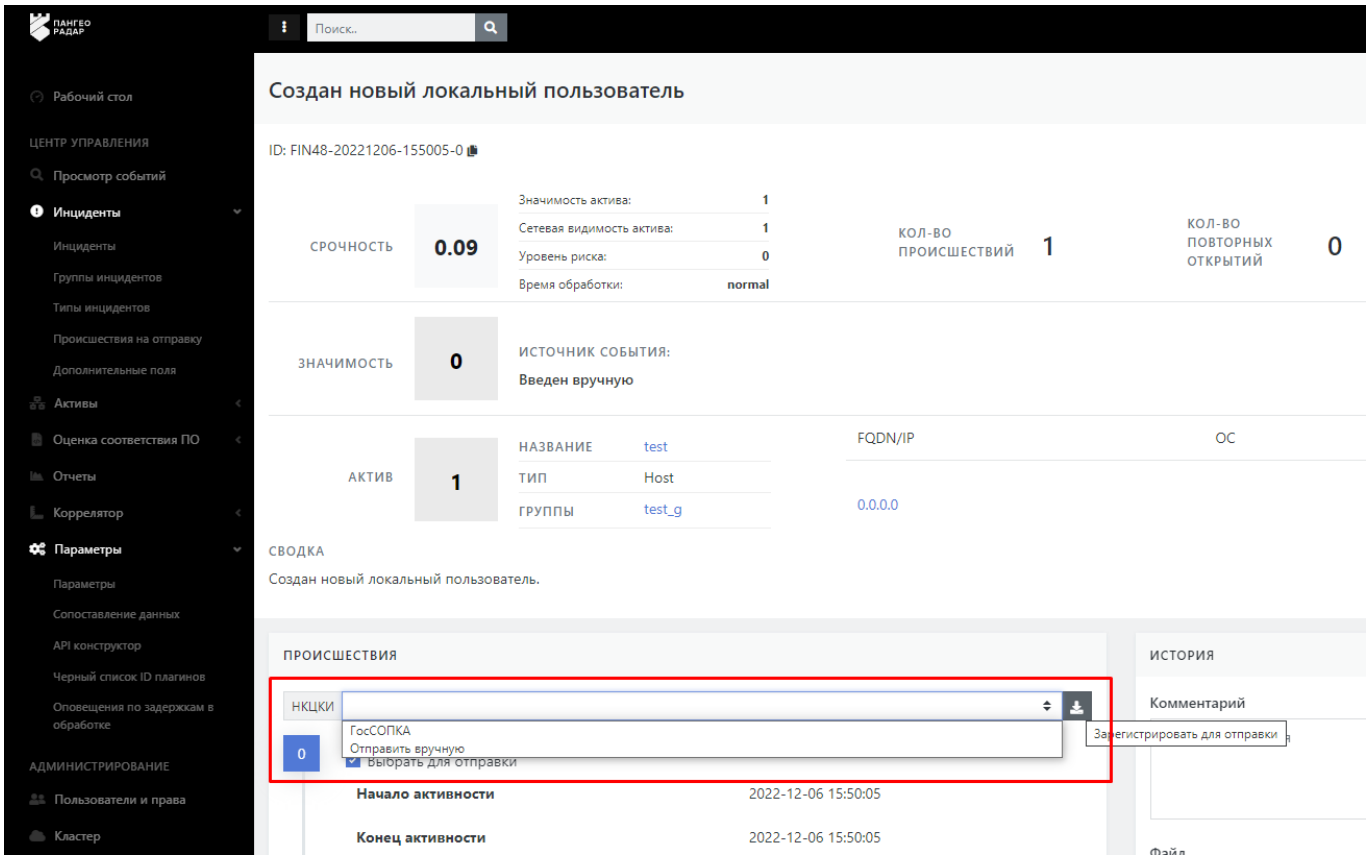



**Рисунок 241 – Регистрация происшествия на отправку**

Настройка отправки инцидента в **ГосСОПКА** будет отображаться только у инцидентов, у которых связанный актив входит в группу активов с установленным признаком "**КИИ**".

## 22.3.2 Управление происшествиями на отправку

Для управления происшествиями перейдите в меню ***Инциденты - Происшествия на отправку*** (см. рисунок 242).

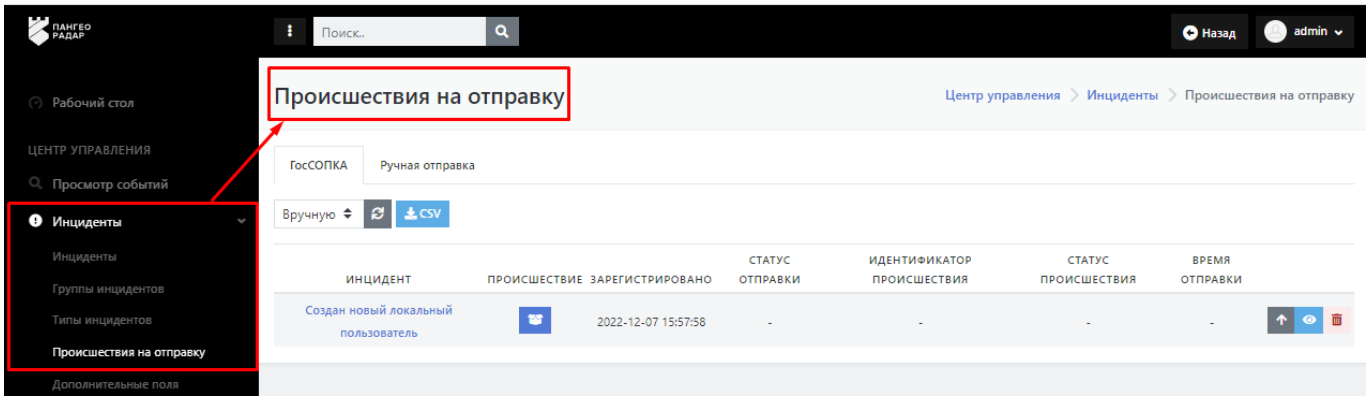



**Рисунок 242 – Происшествия на отправку**

При клике на заголовок инцидента откроется подробная информация об инциденте (см. рисунок 242).

Кликните на иконку просмотра происшествия  чтобы просмотреть подготовленное для отправки происшествие (см. рисунок 243).

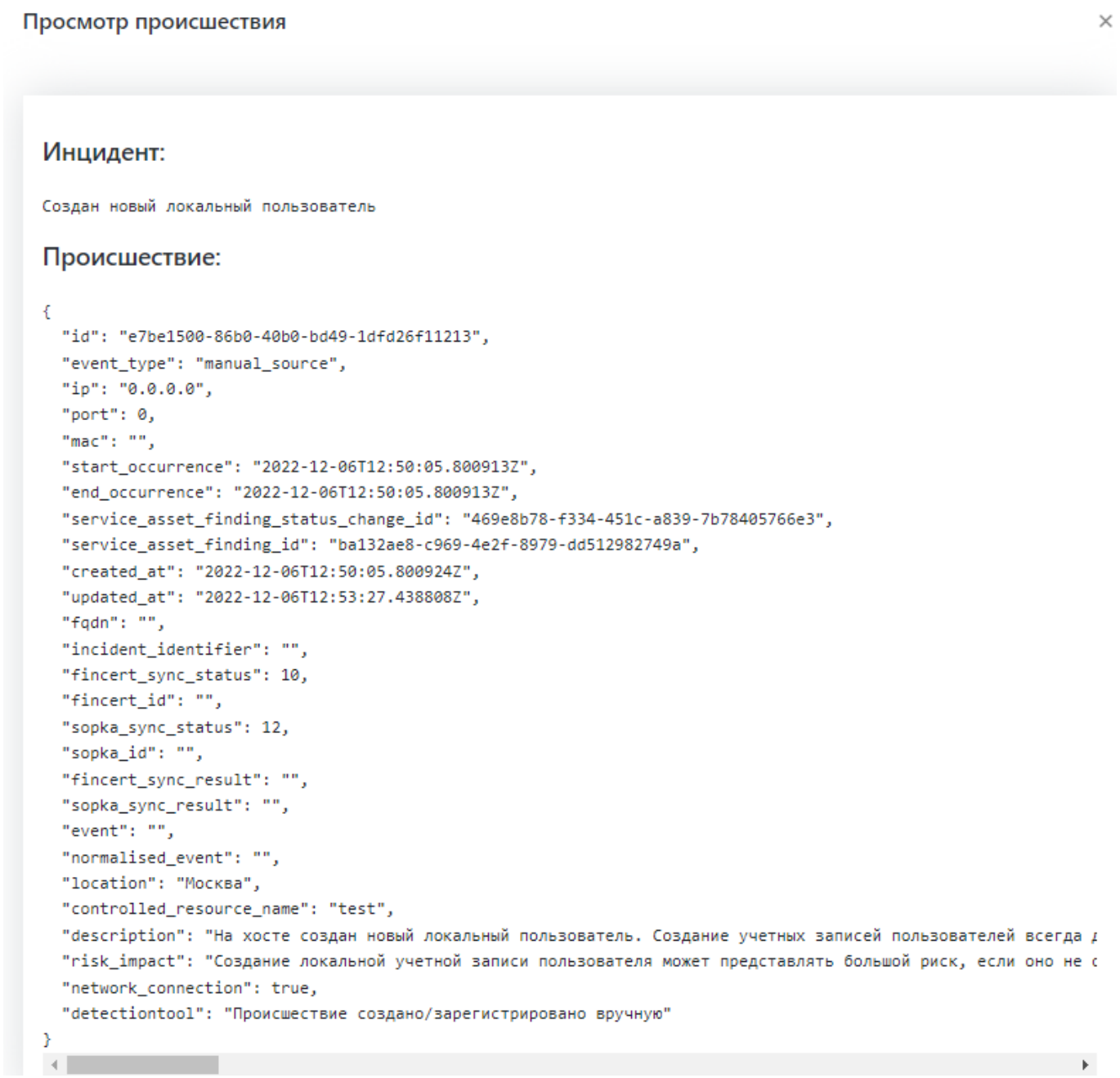



**Рисунок 243 – Просмотр происшествия**

Кликните на иконку отправки сообщения  , при этом откроется окно проверки происшествия (см. рисунок 244).

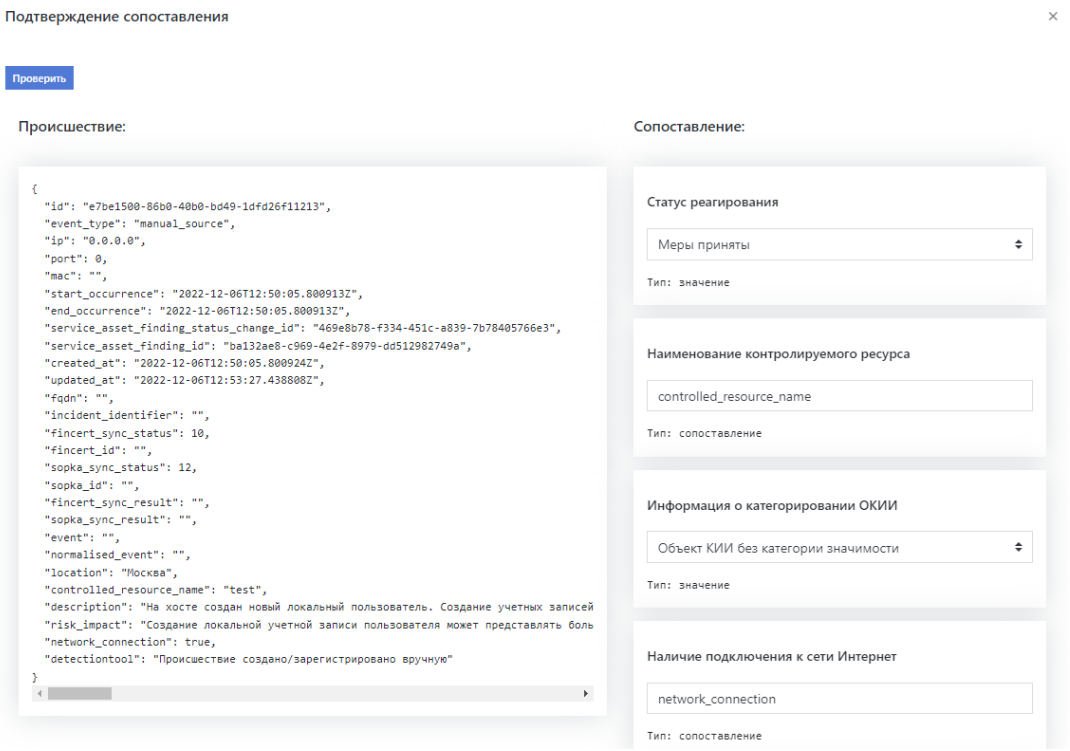



**Рисунок 244 – Подтверждение сопоставления**

В окне проверки происшествия отображается исходное происшествие и поля сопоставления. Нажмите кнопку "**Проверить**" для просмотра результирующего сообщения (см. рисунок 245).

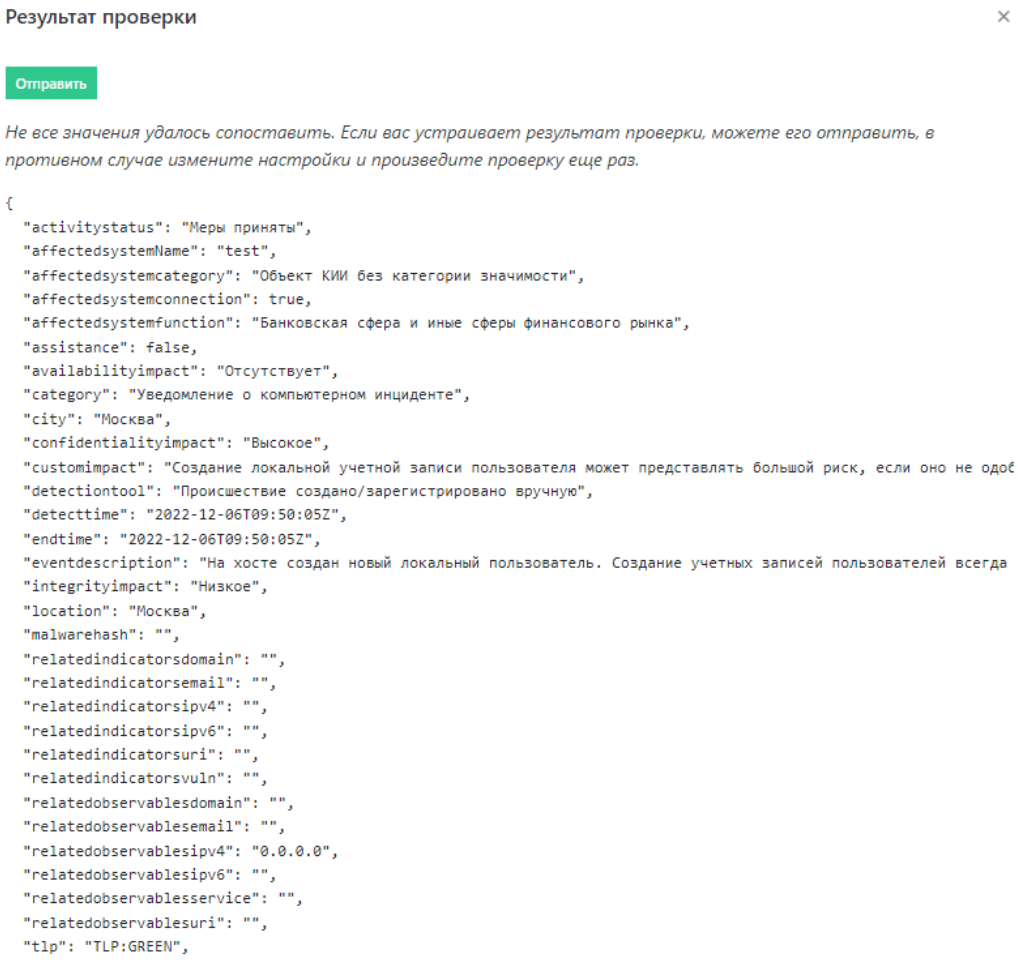



**Рисунок 245 – Просмотр результата проверки**

Поля могут быть не все сопоставлены, но это не мешает отправке данных в НКЦКИ. Если результат сопоставления удовлетворительный, нажмите кнопку "**Отправить**" для отправки сообщения.

После отправки иконка отправки сообщения изменится на иконку обновления статуса , а в происшествии будут указаны дата отправки, статус отправки, идентификатор происшествия, статус происшествия (см. рисунок 246).

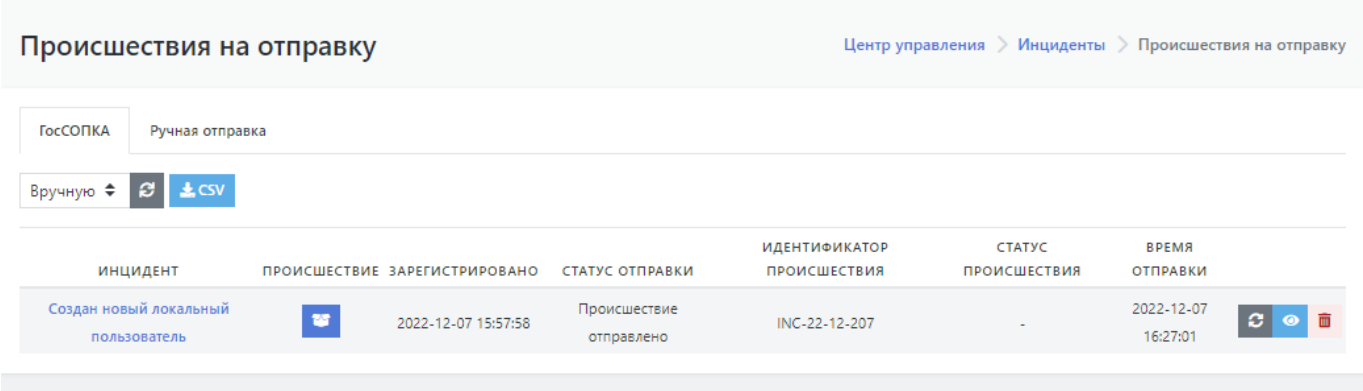



**Рисунок 246 – Изменение статуса отправки**

При клике на иконку обновления статуса статус происшествия будет обновлен.

Подробности обновления статуса можно получить, кликнув на иконку просмотра ответов (см. рисунок 247).

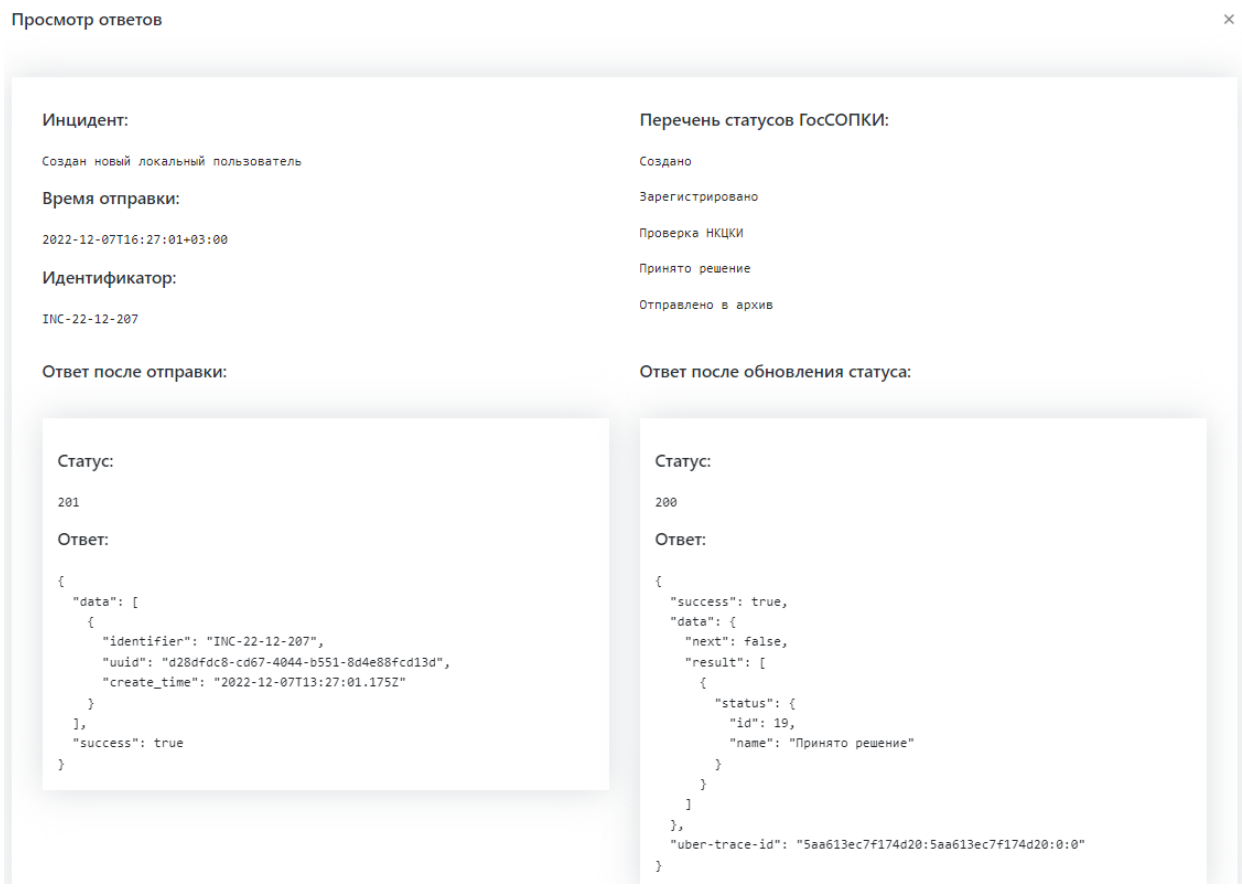



**Рисунок 247 – Просмотр ответов**