Платформа Радар

Руководство оператора

Версия 3.1.0

ООО Пангео Радар

Оглавление

1. Авторизация

1.1. Аутентификация пользователя

По умолчанию интерфейс пользователя доступен по URL: http://<адрес сервера>:8080.

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

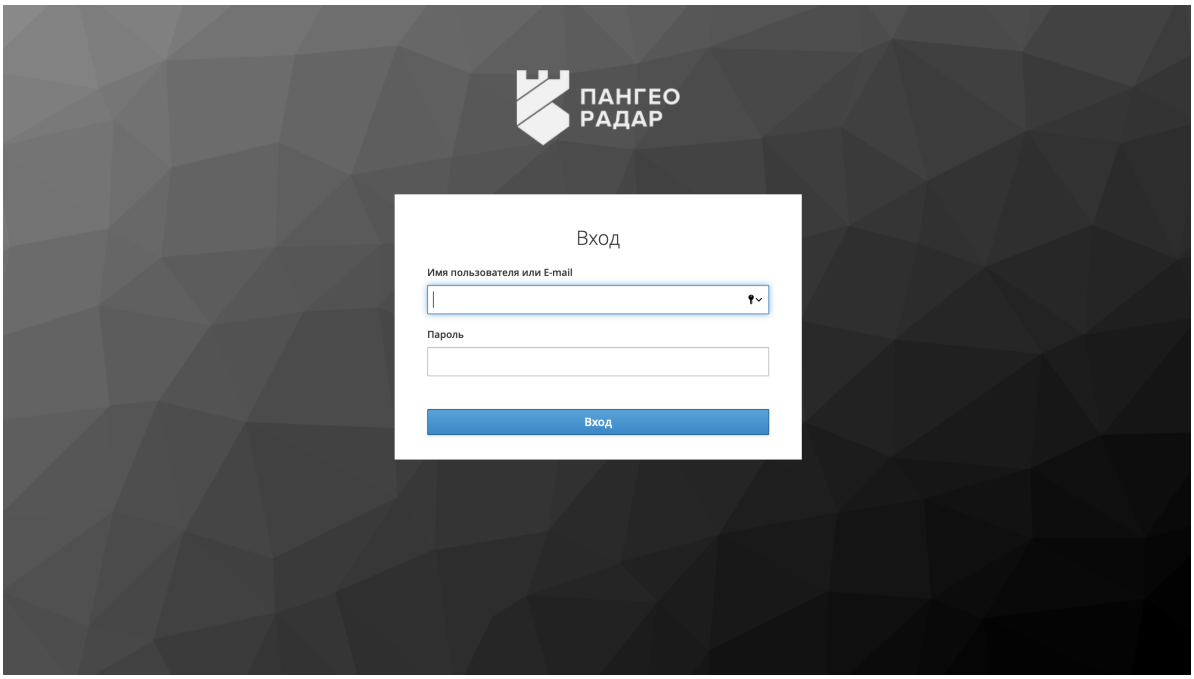


Рисунок 1 - Окно аутентификации Платформы Радар

После успешной аутентификации пользователя на экране откроется рабочий стол пользовательского интерфейса Платформы Радар (см. раздел "Основные элементы интерфейса. Рабочий стол").

При первой авторизации, платформа может потребовать от пользователя сменить пароль (см. Рисунок 2).

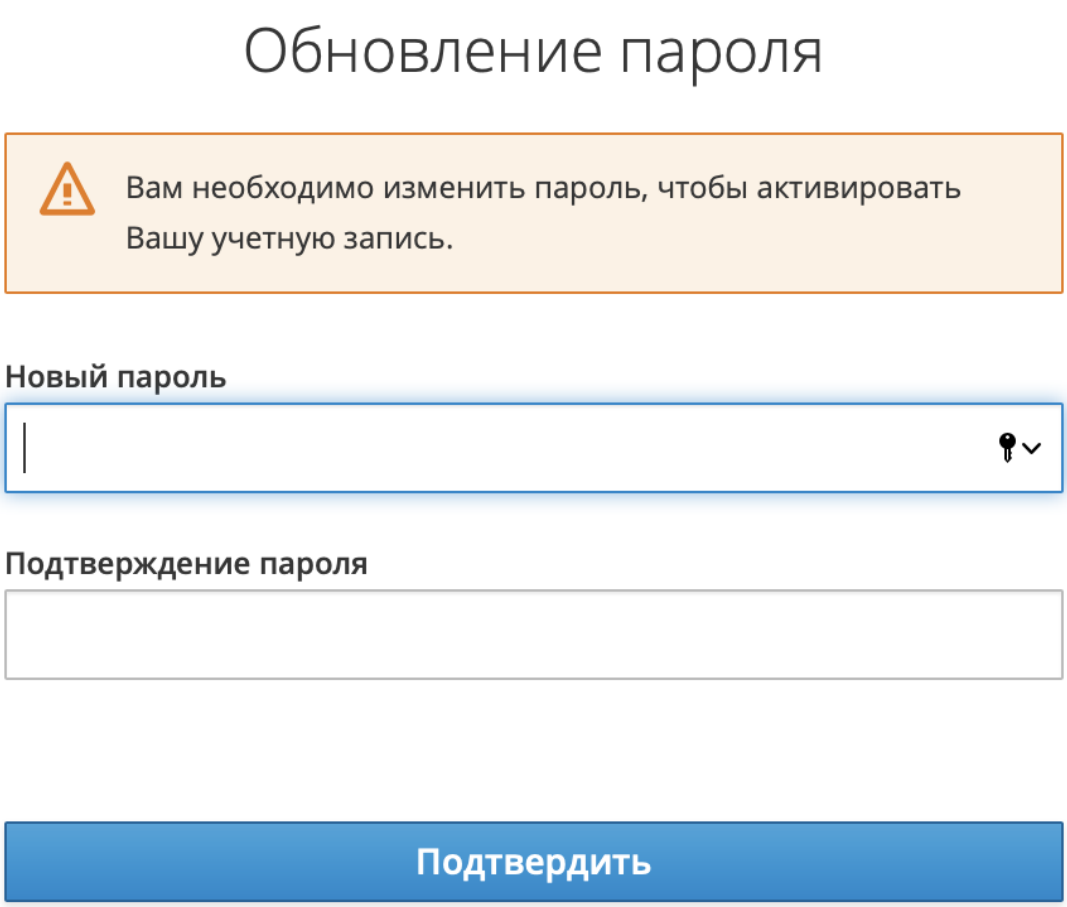


Рисунок 2 - Форма ввода нового пароля

Если при вводе логина и пароля были допущены ошибки, то Платформа выдаст соответствующее предупреждение (см. Рисунок 3).

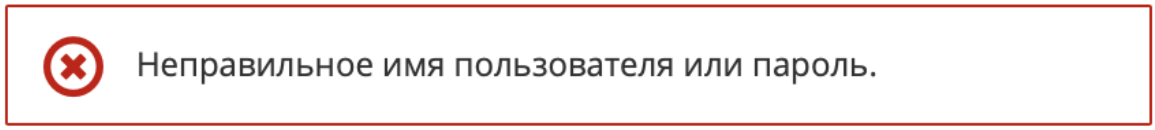


Рисунок 3 - Уведомление об ошибках авторизации

2. Основные элементы интерфейса. Рабочий стол

При входе пользователя в графический пользовательский интерфейс Платформы открывается рабочий стол пользователя (см. Рисунок 4).

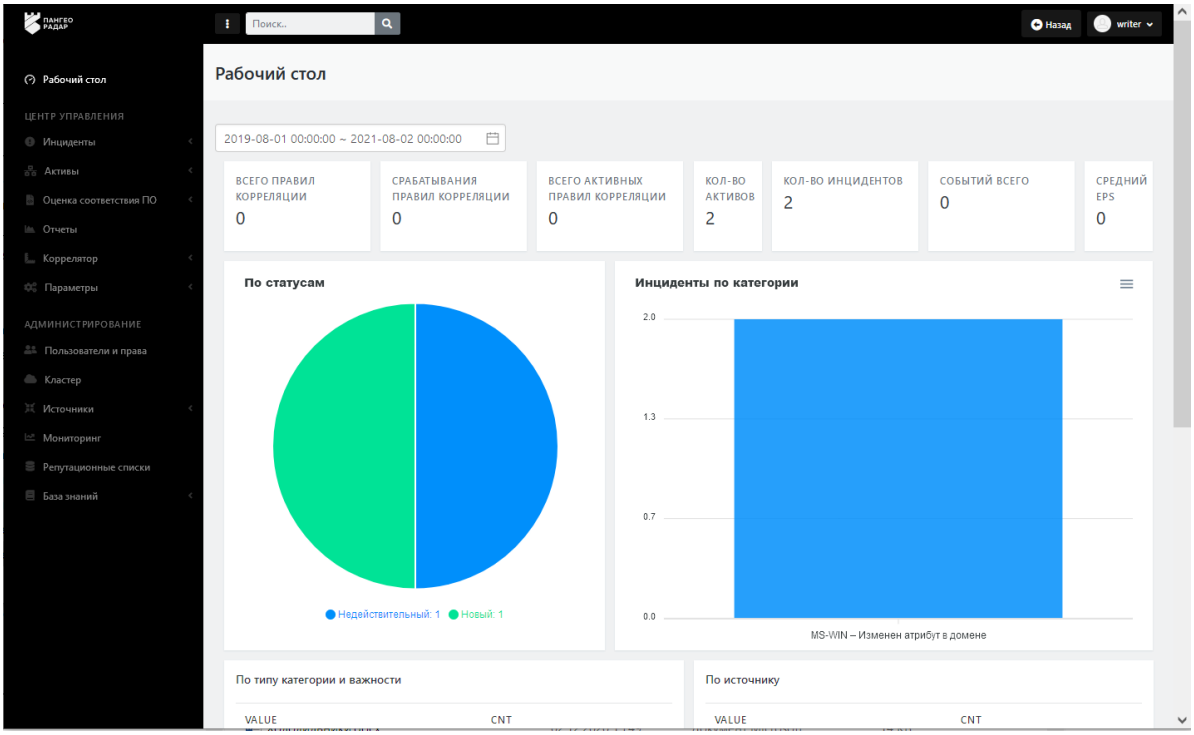
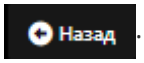


Рисунок 4 - Рабочий стол пользовательского интерфейса Платформы Радар

На верхней панели интерфейса располагаются следующие элементы:

- Пиктограмма для скрытия/разворачивания основного меню Платформы  .
- Функция поиска - стандартное поле ввода поискового запроса (см. Рисунок 4).
- Пиктограмма возврата на предыдущую страницу -  .
- Пиктограмма профиля пользователя с индикацией наличия новых сообщений -  . При нажатии на пиктограмму открывается меню работы с профилем пользователя. Подробное описание работы с профилем пользователя приведено в отдельном разделе "Пользовательские настройки".

Слева располагается основное меню Платформы, которое может находиться в свернутом или раскрытом состоянии.

Основное меню Платформы содержит три раздела:

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

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

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

- "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;
- "Источники" - управление подключением источников событий;
- "Мониторинг" - просмотр метрик работоспособности компонентов Платформы;
- "Репутационные списки" - управление списками индикаторов компрометации;
- "База знаний" - управление базой знаний по типам инцидентов и правилам корреляции.

Непосредственно на рабочем поле располагается актуальная информация (см. Рисунок 4) разных типов и разных способов представления, скомпонованная по принципу приборной доски (дашборда). Информация предоставляется за перид времени, который устанавливается в специальном поле в верхней части рабочего стола. Приборная панель рабочего стола содержит следующие блоки данных:

- диаграмма распределение инцидентов по статусам;
- график распределения инцидентов по категориям;
- таблица распределение инцидентов по типу категории и важности;
- таблица распределение инцидентов по источнику;
- таблица распределение 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. Инциденты

3.1. Раздел "Инциденты"

Для наглядности наши специалисты подготовили видео фрагмент для работы с инцидентами SIEM "Платформа Радар"

3.1.1. Состав раздела "Инциденты"

Раздел «Инциденты» содержит следующие подразделы:

- "**Инциденты**" -- предназначен для работы с инцидентами;
- "**Типы инцидентов**" -- предназначен для работы с типами инцидентов;
- "**Просмотр событий**" -- предназначен для просмотра списка событий. Раздел доступен пользователю только при наличии права на просмотр событий.

3.1.2. Подраздел "Инциденты"

Зарегистрированные инциденты информационной безопасности хранятся в системе в отдельном хранилище. Время хранения инцидентов настраивается независимо от срока хранения событий

3.1.2.1. Основные элементы подраздела

Подраздел "Инциденты" предназначен для оперирования инцидентами.

Подраздел содержит следующие элементы (см. Рисунок 6):

- Текущий список 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 смены статуса -- раскрывающийся список "**Сменить статус**".

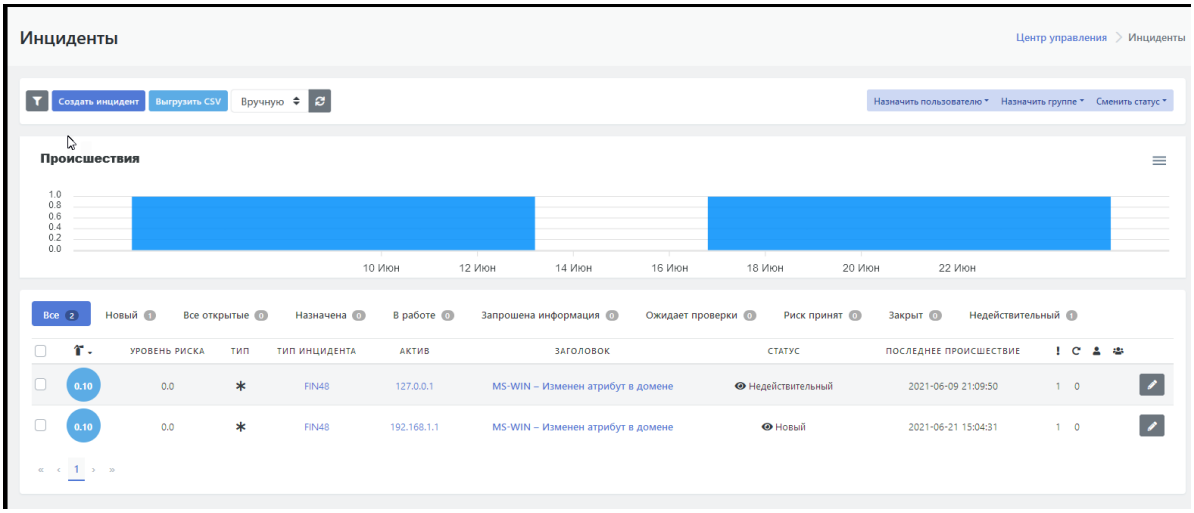


Рисунок 6 - Рабочая область подраздела «Инциденты»

3.1.2.2. 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.

- Поле "**Оценка срочности**" () -- содержит оценку срочности отработки инцидента.
- Поле "**Уровень риска**" -- содержит численную оценку уровня риска.
- Поле "**Тип**" -- содержит пиктограмму - идентификатор типа, к которому принадлежит инцидент.
- Поле "**Тип инцидента**" -- содержит идентификатор инцидента.
- Поле "**Актив**" -- идентификатор сетевого актива на котором произошел инцидент (IP-адрес актива или сетевое имя) .
- Поле "**Заголовок**" -- текстовый заголовок инцидента, под которым он был зафиксирован на Платформе.
- Поле "**Статус**" -- содержит статус в котором находится инцидент в настоящее время.
- Поле "**Последнее происшествие**" -- дата и время когда было зафиксировано последнее происшествие в рамках инцидента.
- Поле "**Кол-во происшествий**" ( ) -- счетчик количества происшествий в рамках инцидента.
- Поле "**Кол-во повторных открытий**" () -- счетчик количества повторных открытий инцидента.
- Поле "**Пользователь**" () -- назначенный ответственный пользователь.
- Поле "**Группа**" () -- назначенная группа ответственных.
- Кнопка () -- функция редактирования параметров инцидента.

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

3.1.2.3. 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 7):

- **"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 7).

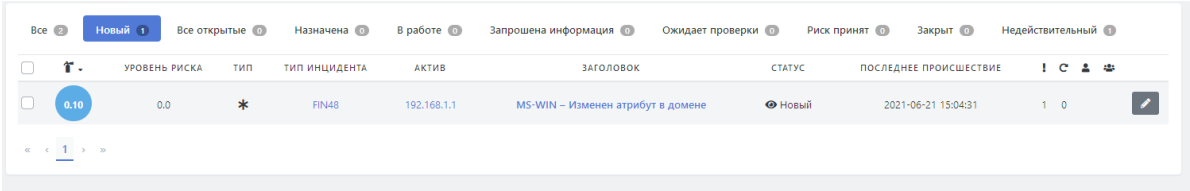


Рисунок 7 - Область быстрого переключения между списками инцидентов, отфильтрованных по текущему статусу

3.1.2.4. Настраиваемые фильтры списка инцидентов

При нажатии на кнопку  открывается область с настраиваемыми фильтрами для табличного списка инцидентов (см. Рисунок 8). Фильтр списка инцидентов разбит на группы и позволяет провести фильтрацию списка по следующим параметрам:

1. Вкладка "**Фильтр**" содержит следующие возможности:

- Фильтр по заголовку инцидента -- свободный текстовый ввод;
- Фильтр по типу инцидента -- раскрывающийся список типов инцидентов;
- Фильтр по времени обработки инцидента -- выбор времени из предустановленного в Платформе списка (раскрывающийся список):
    - Нормальное;
    - Небольшая задержка;
    - Задержка;
    - Неприемлемый.

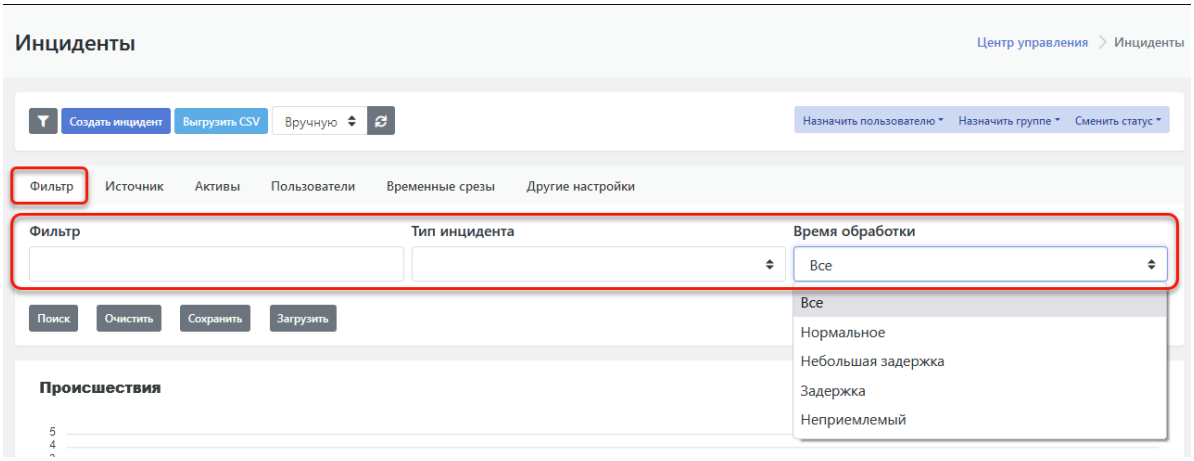


Рисунок 8 - Фильтры для списка инцидентов на вкладке "Фильтры"

2. Вкладка "**Источник**" содержит следующие возможности:

- Фильтр по категории, к которой относится инцидент -- раскрывающийся список со следующими значениями:
    - Уязвимость;
    - Сетевая аномалия;
    - Нарушение политики.
- Фильтр по источнику, создавшему инцидент в Платформе -- раскрывающийся список со следующими значениями:
    - Сканер уязвимостей;
    - Устаревший инцидент;

- Коррелятор событий;
- Введён вручную;
- Контроль соответствия;
- Контроль потока событий.

3. Вкладка "**Активы**" содержит следующие возможности:

- Фильтр по группам активов -- раскрывающийся список, состав списка групп активов определяется Администраторами платформы 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;
  - DNZ, 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).

4. Вкладка "**Пользователи**" содержит следующие возможности:

- Фильтр по логину пользователя, отвечающего за инциденты -- раскрывающийся список логинов пользователей, зарегистрированных на Платформе.
- Фильтр по названию группы, отвечающей за инциденты -- раскрывающийся список групп пользователей, созданных на Платформе.

5. Вкладка "**Временные срезы**" содержит следующие возможности фильтрации (см. Рисунок 9):
   - задать временной срез "**Последнее происшествие с <дата, время> до <дата, время>**";
   - задать временной срез "**Последнее сканирование от <дата, время> до <дата, время>**";
   - задать временной срез "**Сменился статус с <дата, время> до <дата, время>**".

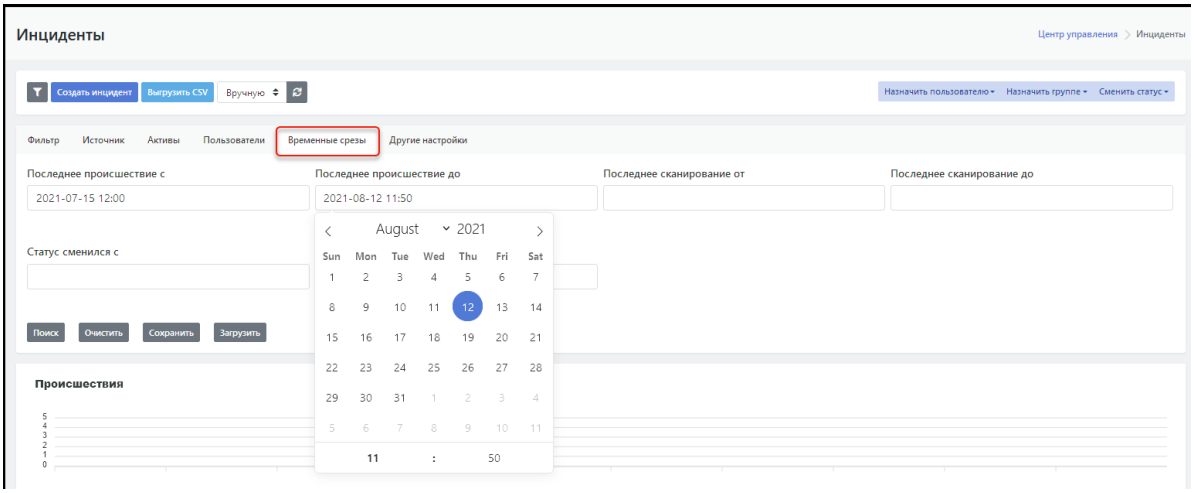


Рисунок 9 - Фильтрация инцидентов по временным срезам. Вкладка "Временные срезы"

6. Вкладка "**Другие настройки**" содержит следующие возможности (см. Рисунок 10):

- 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".

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

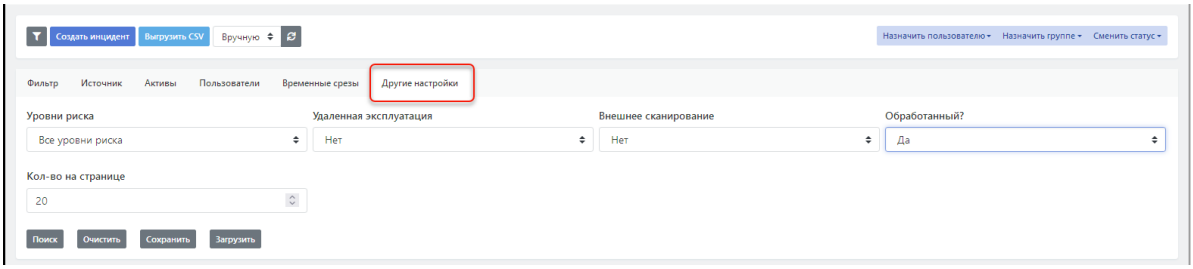


Рисунок 10 - Вкладка фильтра "Другие настройки" и функция редактирования строк табличного списка инцидентов

Для фильтрации табличного списка необходимо установить нужные значения фильтров на всех вкладках и нажать на кнопку "**Поиск**" на любой из вкладок (см. Рисунок 10).
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**".

3.1.2.5. 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.

3.1.2.6. Назначение инцидентов пользователям и группам

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

3.1.2.7. 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 *"Работа с инцидентами. Расследование инцидента. Изменение статуса инцидента"*.

3.1.2.8. Создание инцидента

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

3.1.3. Подраздел "Типы инцидентов"

3.1.3.1. Основные элементы подраздела

Подраздел "Типы инцидентов" предназначен для оперирования типами инцидентов.

Подраздел содержит (см. Рисунок 11):

- 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 "**Выгрузить CSV**".

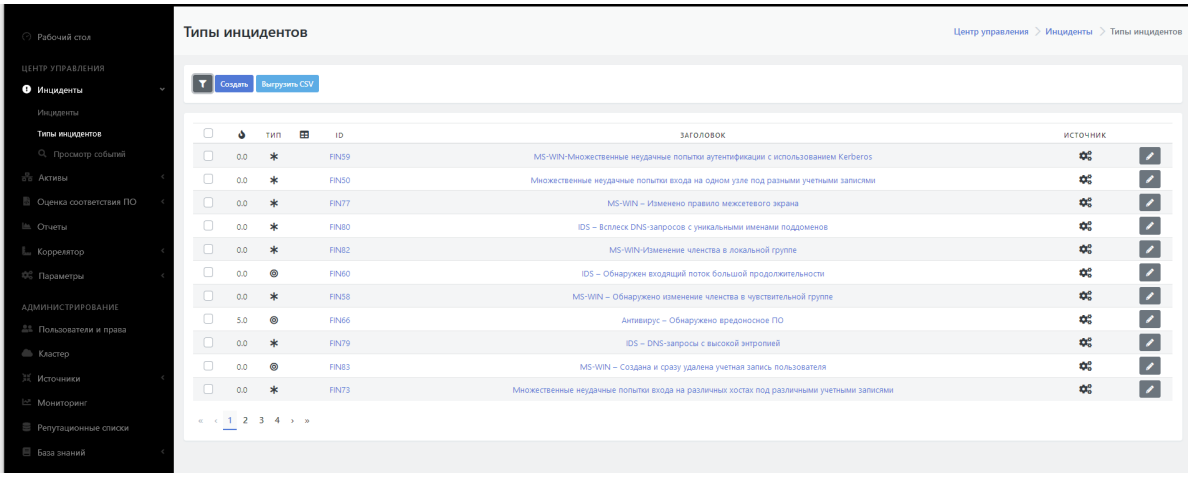


Рисунок 11 - Рабочая область подраздела «Типы инцидентов»

3.1.3.2. 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.
- Поле "**Оценка срочности**" ( ) -- содержит оценку срочности отработки инцидента.
- Поле ( ) -- **"уровень риска"**, содержит численную оценку уровня риска данного типа инцидента.
- Поле "**Тип**" -- содержит пиктограмму - идентификатор типа.
- Поле ( ) -- поле статуса "**Эксплуатируется удаленно**", указывает на возможность удаленной эксплуатации данного типа инцидента.
- Поле **"ID"** -- идентификатор типа инцидента в Платформе.
- Поле "**Заголовок**" -- название типа инцидента, под которым он был заведен в Платформе.
- Поле "**Источник**" -- содержит пиктограммы, соответствующие тому или иному источнику данных.
- Кнопка ( ) -- функция редактирования параметров типа инцидента.

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

3.1.3.3. Настраиваемые фильтры списка типов инцидентов

При нажатии на кнопу открывается область с настраиваемыми фильтрами для табличного списка типов инцидентов (см. Рисунок 12). 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".

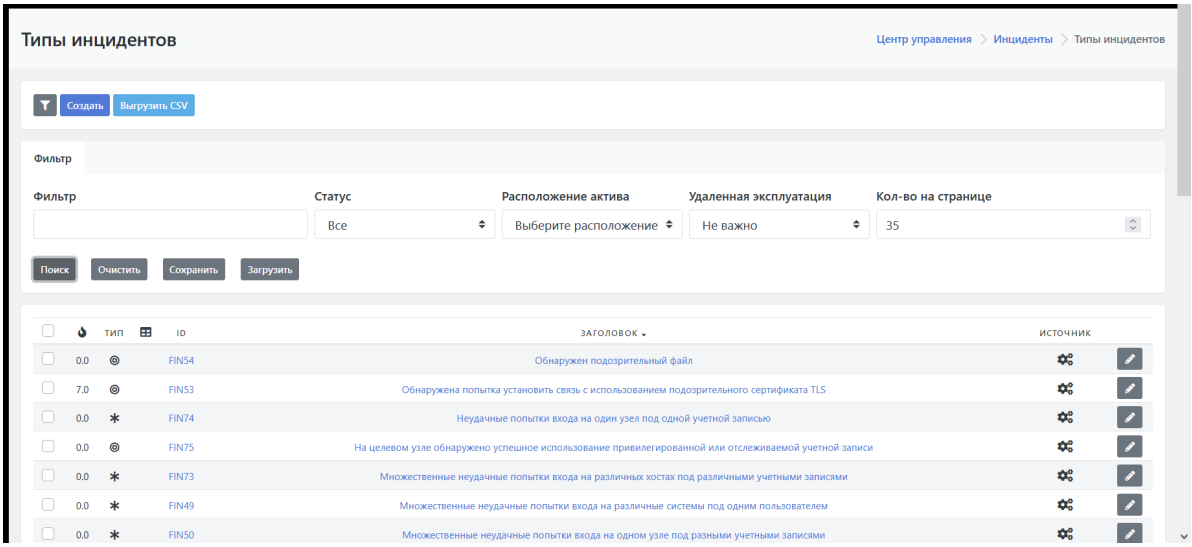


Рисунок 12 - Фильтры для списка типов инцидентов

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 подразделе *"Настраиваемые фильтры списка инцидентов"*.

3.1.3.4. 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 приведено в подразделе *"Работа с базой знаний типов инцидентов. Создание нового типа инцидента вручную"* .

3.1.4. Подраздел "Просмотр событий"

3.1.4.1. Основные элементы подраздела

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

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

Подраздел содержит (см. Рисунок 13):

- Набор настраиваемых фильтров для вывода событий по заданным параметрам (верхняя часть экрана):
    - Поле "**Время**" -- задание временного интервала, на котором надо просмотреть события.
    - Поле "**Индекс**" -- указание индекса ElasticSearch.
    - Поле текстового ввода поискового запроса.
- 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.

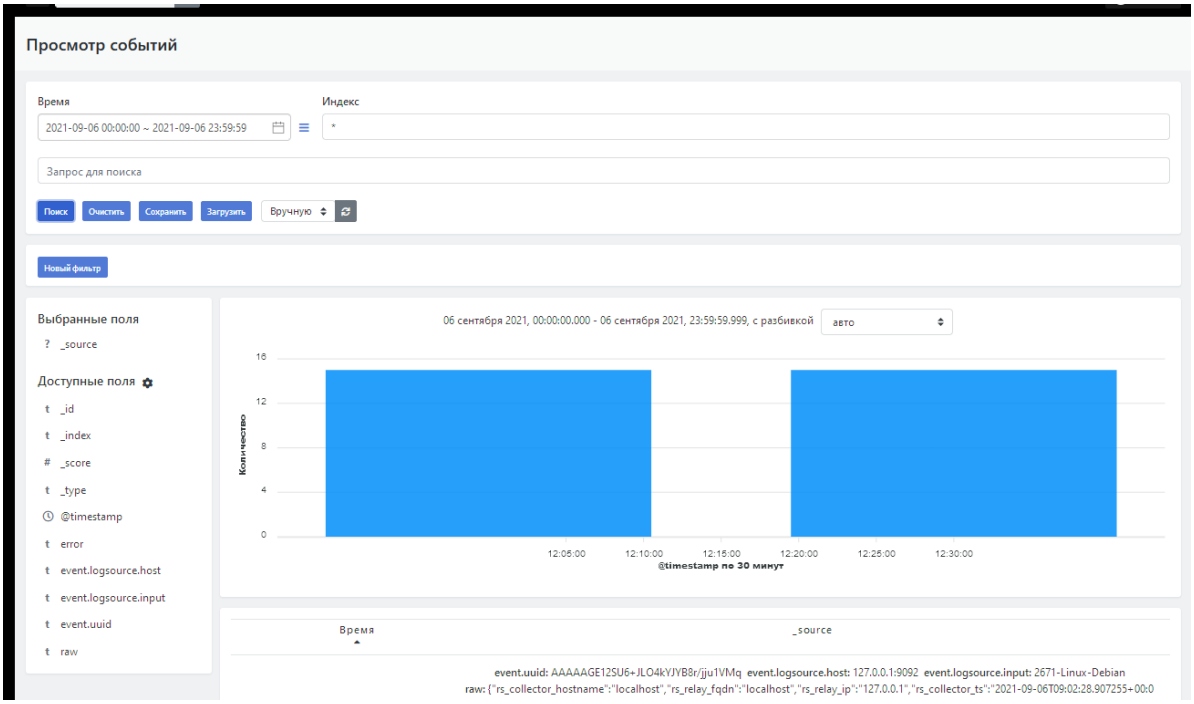


Рисунок 13 - Рабочая область подраздела «Просмотр событий»

3.1.4.2. Настройка просмотра и работа с событиями

Настройка просмотра и работа с просмотрщиком событий подробно рассмотрена в разделе *"Работа с просмотрщиком событий"*.

4. Раздел "Активы"

4.1. 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 так же собираемых данных.

4.2. Подраздел "Активы"

4.2.1. Основные элементы подраздела

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

Подраздел содержит следующие элементы (см. Рисунок 14):

- Текущий список активов, заявленных на Платформе.
- 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 "**Выгрузить 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**".

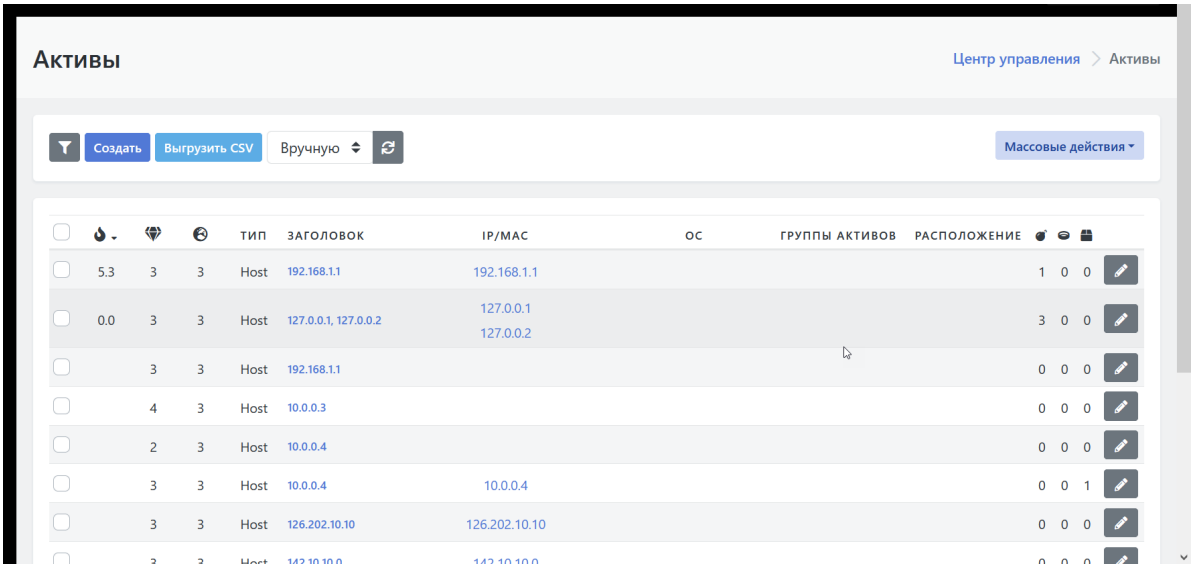


Рисунок 14 - Рабочая область подраздела "Активы"

4.2.2. Список активов. Параметры списка

Текущий список активов представлен в виде табличного списка со следующими основными параметрами (см. Рисунок 14):

- 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 на Платформе.
- 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 на платформе).
- 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 инцидента.

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

4.2.3. Настраиваемые фильтры списка активов {#list_filters}

При нажатии на кнопу  открывается область с настраиваемыми фильтрами для табличного списка активов (см. Рисунок 15). 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 необходимо установить нужные значения фильтров и нажать на кнопку "**Поиск**" (см. Рисунок 15).
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**".

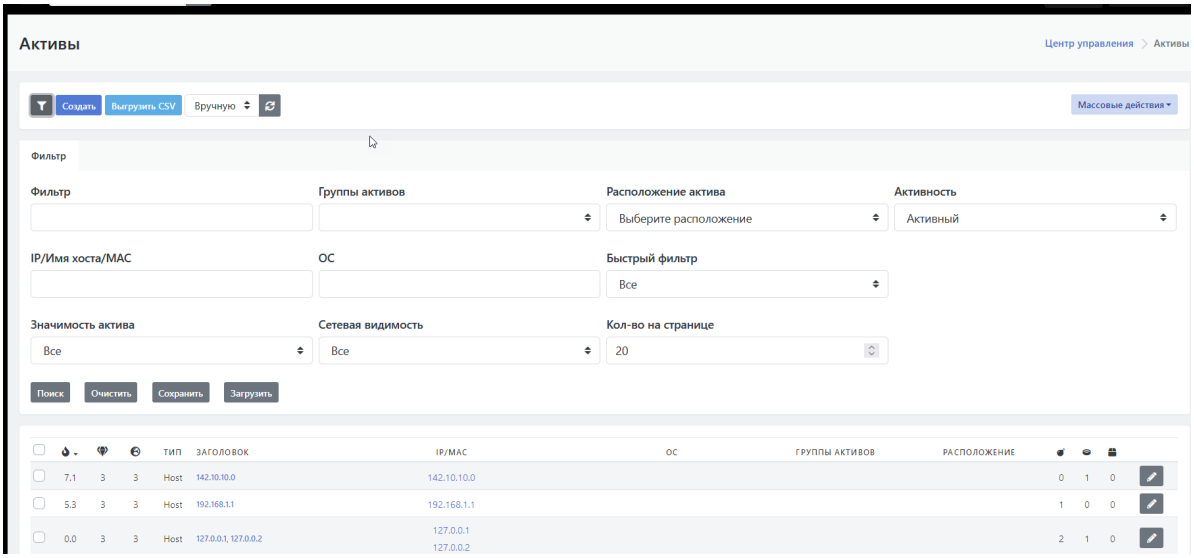


Рисунок 15 - Фильтры для списка активов

4.2.4. 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.

4.2.5. Управление активами

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

4.2.6. Создание актива

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

4.2.7. Редактирование параметров актива

Редактирование параметров актива доступно по нажатию на кнопку  . Подробное описание редактирования параметров группы актива приведено в в разделе *"Работа с активами. Редактирование группы активов"*.

4.3. Подраздел "Группы активов"

4.3.1. Основные элементы подраздела

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

Подраздел содержит следующие элементы (см. Рисунок 16):

- Текущий список групп активов, созданных на Платформе.
- 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**".

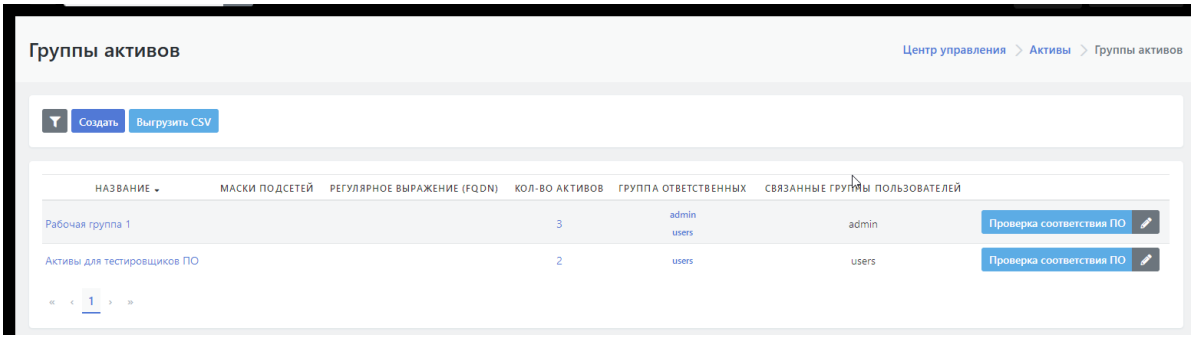


Рисунок 16 - Рабочая область подраздела "Группы активов"

4.3.2. Список групп активов. Параметры списка

Текущий список групп активов представлен в виде табличного списка со следующими основными параметрами (см. Рисунок 14):

- Поле "**Название**" -- название группы активов на Платформе.
- Поле **"Маски подсетей"** -- стратегия автоматического добавления активов в группу по заданной маске подсети. Новые активы, попадающие под указанную сетевую маску, будут автоматически включаться в группу.
- Поле **"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.

- Поле **"Кол-во активов"** -- количество активов в группе.
- Поле **"Группа ответственных"** -- группа пользователей, назначенная ответственными за данную группу активов.
- Поле "**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.

4.3.3. Настраиваемые фильтры списка групп активов

При нажатии на кнопу  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 "*.

4.3.4. 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 на Платформе вручную приведено в в разделе *"Работа с активами. Создание группы активов"*.

4.3.5. Редактирование параметров группы активов

Редактирование параметров группы активов доступно по нажатию на кнопку  . Подробное описание редактирования параметров группы актива приведено в в разделе *"Работа с активами. Редактирование группы активов"*.

4.4. Подраздел "Настройки идентификации активов"

4.4.1. Основные элементы подраздела

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

Подраздел содержит следующие элементы (см. Рисунок 17):

- 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  .

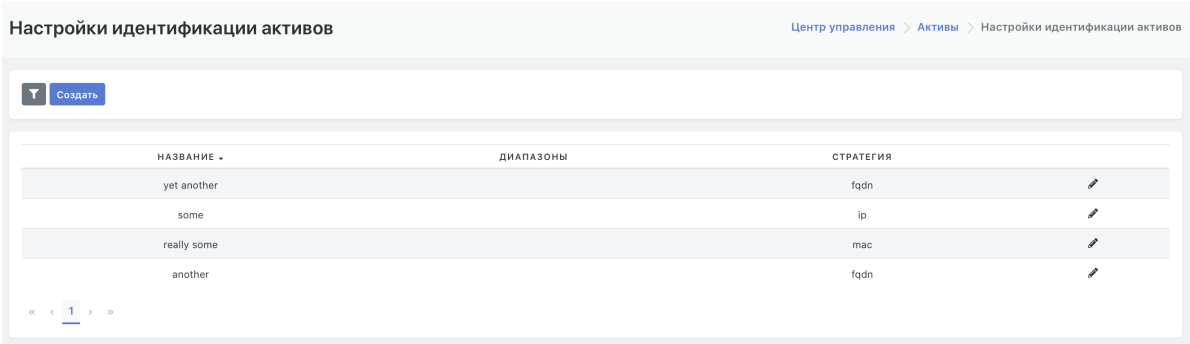


Рисунок 17 - Рабочая область подраздела "Настройка идентификации активов"

4.4.2. Список настроенных сегментов. Параметры списка

Текущий список настроенных сегментов для идентификации активов представлен в виде табличного списка со следующими основными параметрами (см. Рисунок 17):

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

4.4.3. Настраиваемые фильтры списка сегментов

При нажатии на кнопу  открывается область с фильтрами для табличного списка настроенных сегментов (см. Рисунок 18). 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 "*.

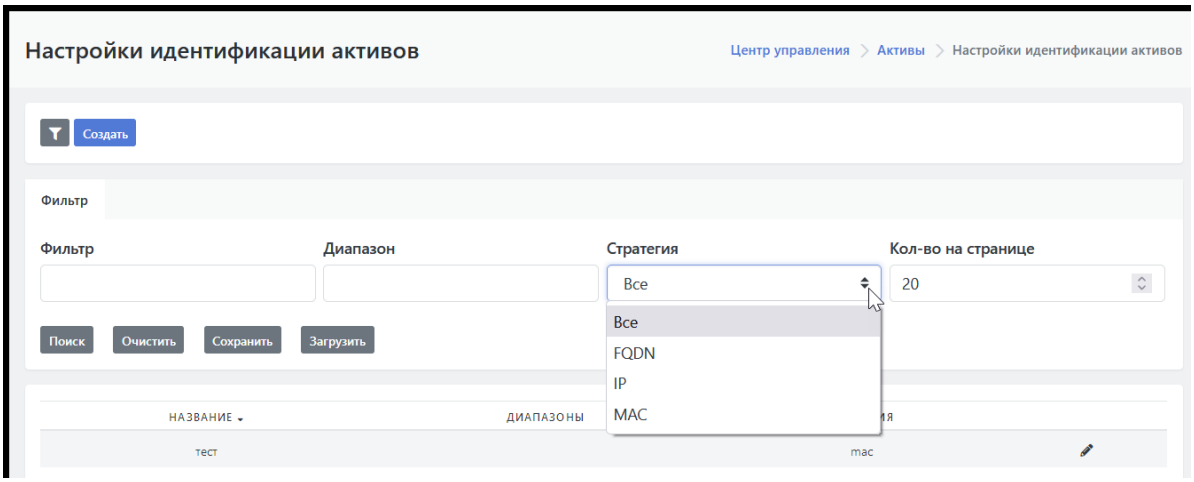


Рисунок 18 - Фильтры подраздела "Настройка идентификации активов"

4.4.4. 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 на Платформе приведено в в разделе *"Работа с активами. Создание и настройка сегмента"*.

4.4.5. Редактирование параметров сегмента

Редактирование параметров настроенного сегмента доступно по нажатию на кнопку  .

Подробное описание редактирования параметров сегмента приведено в в разделе *"Работа с активами. Редактирование параметров сегмента"*.

4.5. Подраздел "Сетевые интерфейсы"

4.5.1. Основные элементы подраздела

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

Подраздел содержит следующие элементы (см. Рисунок 19):

- 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  .

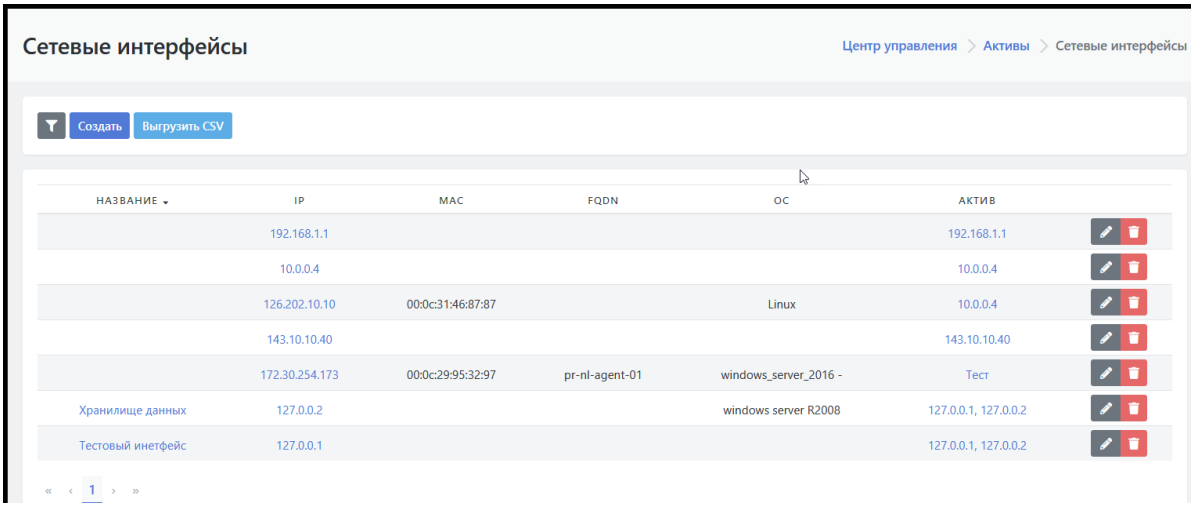


Рисунок 19 - Рабочая область подраздела "Сетевые интерфейсы"

4.5.2. Список сетевых интерфейсов. Параметры списка

Список сетевых интерфейсов представлен в виде табличного списка со следующими основными параметрами (см. Рисунок 17):

- Поле "**Название**" -- имя интерфейса на Платформе.
- Поле **"IP"** -- IP-адрес интерфейса.
- Поле **"MAC"** -- MAC-адрес интерфейса.

- Поле **"FQDN"** -- FQDN, определенный по данному IP-адресу.
- Поле **"ОС"** -- операционная система, обнаруженная при сканировании через данный интерфейс.
- Поле "**Актив**" -- название, связанного с интерфейсом актива (активов).
- Кнопка ( ) -- функция редактирования параметров интерфейса.
- Кнопка ( ) -- функция удаления сетевого интерфейса.

4.5.3. Настраиваемые фильтры списка интерфейсов

При нажатии на кнопу открывается область с настраиваемыми фильтрами для списка интерфейсов (см. Рисунок 20). 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 20).

Стандартные правила работы с фильтрами приведены в разделе *"Настраиваемые фильтры списка активов "*.

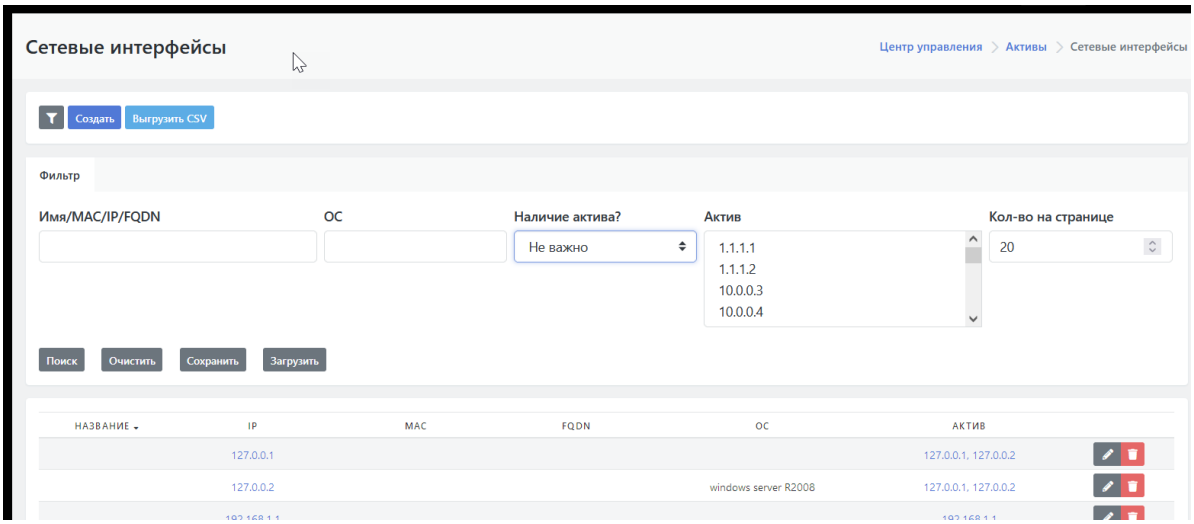


Рисунок 20 - Фильтр подраздела "Сетевые интерфейсы"

4.5.4. 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 на Платформе вручную приведено в в разделе *"Работа с активами. Создание сетевого интерфейса"*.

4.5.5. Редактирование параметров сетевого интерфейса

Редактирование параметров сетевого интерфейса доступно по нажатию на кнопку .

Подробное описание редактирования параметров интерфейса приведено в в разделе *"Работа с активами. Редактирование параметров сетевого интерфейса"*.

4.6. Подраздел "Результаты сканирования"

4.6.1. Основные элементы подраздела

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

Подраздел содержит следующие элементы (см. Рисунок 21):

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

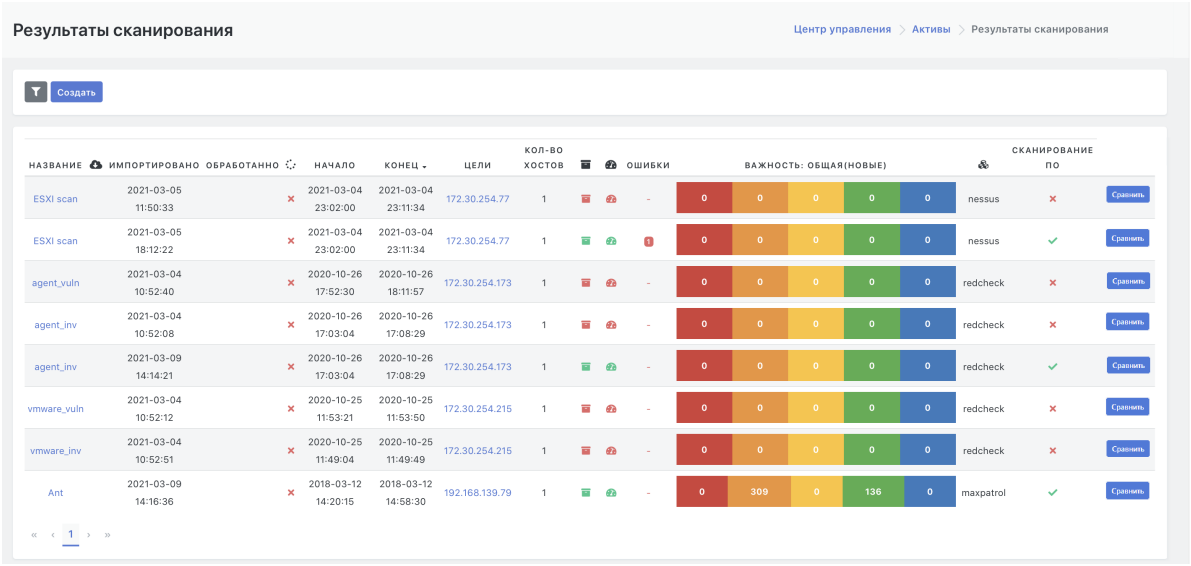


Рисунок 21 - Рабочая область подраздела "Результаты сканирования"

4.6.2. Список результатов сканирований. Параметры списка

Список сетевых интерфейсов представлен в виде табличного списка со следующими основными параметрами (см. Рисунок 17):

- Поле "**Название**" -- уникальное название проведенного сканирования на Платформе.
- Флаг "**Результаты внешнего сканирования**" () -- статус сканирования: "внешнее/ внутреннее" ( / ).
- Поле **"Импортировано"** -- дата и время импорта результатов на Платформу.
- Поле **"Обработано"** -- время обработки результатов оператором.
- Флаг () -- статус обработки результатов сканирования оператором: "обработано/ не обработано" ( / ).
- Поле **"Начало"** -- дата и время начала сканирования.
- Поле **"Конец"** -- дата и время завершения сканирования.
- Поле **"Цели"** -- активы (IP-адреса), указанные в задаче сканирования.
- Поле **"Кол-во хостов"** -- количество хостов в результатах сканирования.
- Поле () -- количество автоматически закрытых инцидентов. Указывается при наведении курсора мыши на пиктограмму в строке:
  -  -- на активе нет автоматически закрытых инцидентов (=0);

-  -- на активе есть автоматически закрытые инциденты (<0).

- Поле () -- количество автоматически прикреплённых происшествий к существующим инцидентам. Указывается при наведении курсора мыши на пиктограмму в строке:
  -  -- на активе нет автоматически прикреплённых происшествий к существующим инцидентам (=0);
  -  -- на активе есть автоматически прикреплённые происшествия к существующим инцидентам (<0).
- Поле **"Ошибки"** -- наличие ошибок в результатах сканирования.
- Поле **"Важность"** -- отображаются количественные результаты найденных уязвимостей, разделенные на группы важности по цвету согласно оценке CVSS.
- Поле **"Тип сканирования"** () -- содержит тип сканирования: "redcheck / maxpatrol / nessus"
- Флаг "**Сканирование ПО**" -- флаг наличия данных о программном обеспечении в результатах сканирования: ( / ).
- Кнопка **"Сравнить"** -- функция просмотра изменений в составе уязвимостей между результатами сканирования и текущими данными в системе.

4.6.3. Настраиваемые фильтры списка результатов сканирования

При нажатии на кнопу  открывается область с настраиваемыми фильтрами для списка результатов сканирования (см. Рисунок 22). 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 "*.

4.6.4. 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 на Платформе вручную приведено в разделе *"Сканирование. Создание записи о сканировании"*.

4.6.5. Сравнение результатов сканирования

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

4.7. Подраздел "Инвентаризация"

4.7.1. 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.

4.7.2. Вкладка "Обнаружение хостов"

4.7.2.1. 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 22):

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

4.7.2.2. Список результатов сканирования хостов. Параметры списка

Результаты сканирования -- табличный список активов, обнаруженных при сканировании заданной подсети, с указанием следующих параметров активов (см. Рисунок 22):

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

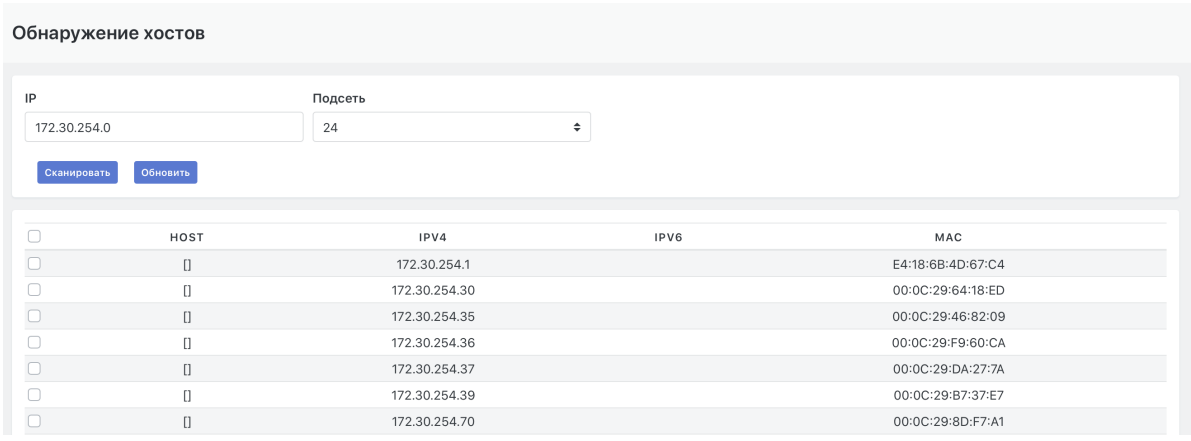


Рисунок 22 - Рабочая область вкладки "Обнаружение хостов"

4.7.2.3. Сканирование активов указанной подсети

Для запуска сканирования с целью обнаружения хостов необходимо нажать на кнопку **"Сканирование"**. Подробное описание проведения обнаружения хостов приведено в разделе *"Сканирование. Обнаружение хостов"*.

4.7.2.4. Обновление данных по результатам сканирования

Процедура обновления данных по результатам сканирования приведена в разделе *"Сканирование. Обновление данных по результатам сканирования"*.

4.7.3. Вкладка "Обнаружение сервисов"

4.7.3.1. 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 софта и ОС по открытым данным актива.

В рабочей области отображаются следующие элементы (см. Рисунок 23):

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

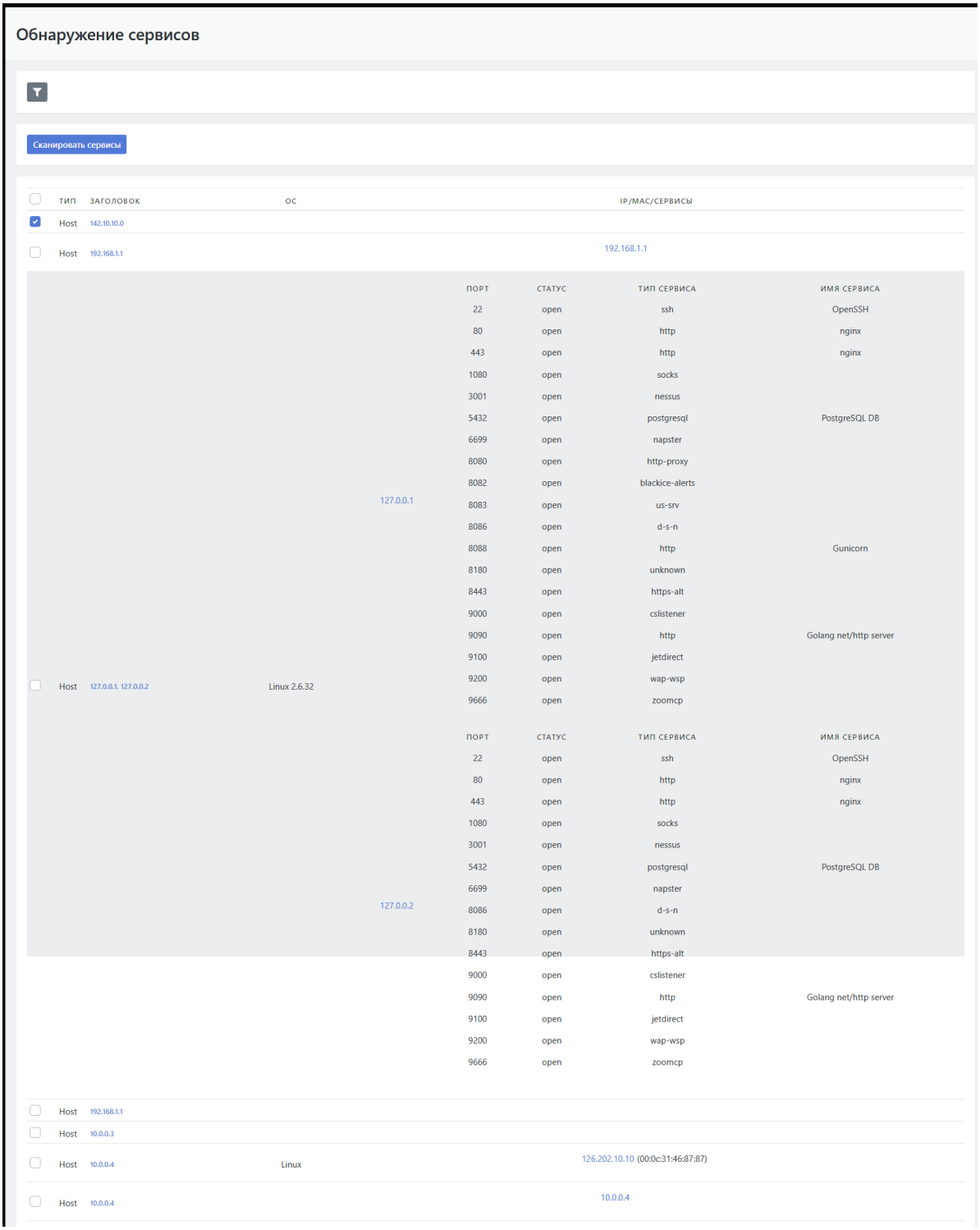


Рисунок 23 - Рабочая область вкладки "Обнаружение сервисов"

4.7.3.2. 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 23):

- Поле (/) -- флаговое поле для выбора строк с активами для проведения с ними действий сканирования сервисов.
- Поле **"Тип"** -- тип актива.
- Поле **"Заголовок"** -- имя актива на Платформе (или IP-адрес).
- Поле **"ОС"** -- операционная система на активе.
- Поле **"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.

4.7.3.3. Настраиваемые фильтры списка активов с результатами сканирования сервисов

При нажатии на кнопу  открывается область с настраиваемыми фильтрами для списка активов с результатами сканирования сервисов (см. Рисунок 24). 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 "*.

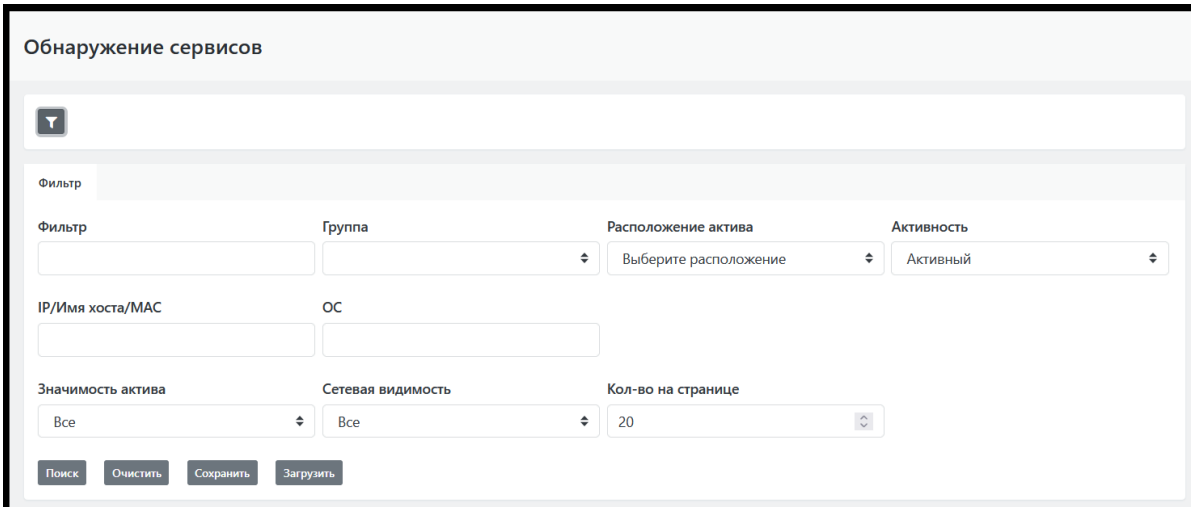


Рисунок 24 - Фильтры для поиска в списке результатов сканирования сервисов

4.7.3.4. 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 *"Сканирование. Обнаружение сервисов"*.

4.7.4. Вкладка "Сбор данных"

4.7.4.1. 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 25):

- Настройки сбора данных, состоящие из следующих элементов:
  - Поле **"Протокол"** -- выбор протокола для сбора данных, раскрывающийся список протоколов: "SSH/ WMI/ RPS".
  - Поле **"Учетная запись"** -- выбор учетной записи для авторизации на активе, раскрывающийся список доступных учетных записей.
  - Поля выбора **"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  .

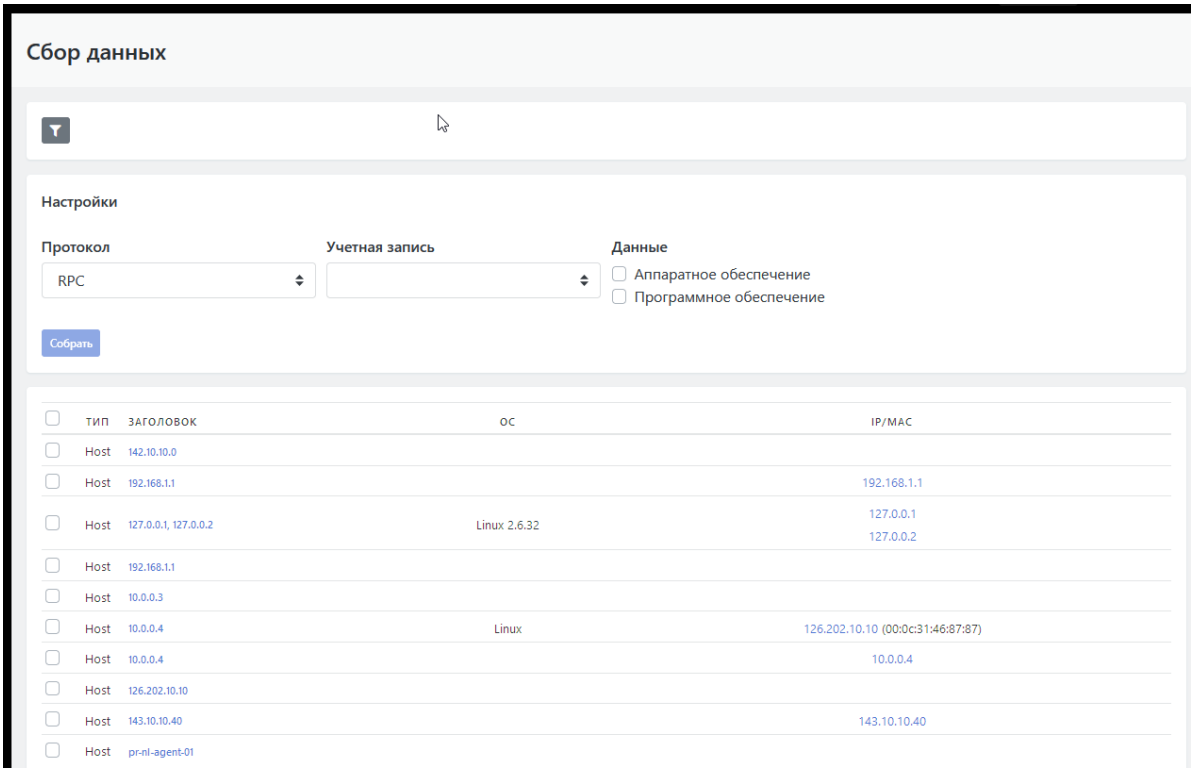


Рисунок 25 - Рабочая область вкладки "Сбор данных"

4.7.4.2. 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 25):

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

4.7.4.3. Настраиваемые фильтры списка активов с результатами сканирования сервисов

При нажатии на кнопу 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 с результатами сканирования сервисов"*.

4.7.4.4. 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 *"Сканирование. Сбор данных"*.

5. Коррелятор

5.1. Раздел "Коррелятор"

5.1.1. Общее описание раздела "Коррелятор"

Раздел основного меню Платформы Радар «**Коррелятор**» включает следующие подразделы:

- "**Правила**" - подраздел предназначен для управления правилами корреляции;
- "**Шаблон**" - подраздел предназначен для управления шаблонами вывода результатов работы правил коррелятора;
- "**Хранилища значений**" - подраздел предназначен для управления хранилищами значений, которые используются в правилах корреляции как конфигурационные значения;
- "**Результаты**" - подраздел предназначен для обработки результатов работы правил корреляции, по которым Инциденты и Оповещения не создаются автоматом.

5.1.2. Подраздел "Правила"

Подраздел «Правила» предназначен для управления правилами корреляции, самим коррелятором и диагностикой работы правил корреляции (см. Рисунок 26).

Подраздел содержит:

- Текущий список правил корреляции.
- Набор фильтров для просмотра списка правил - фильтры открываются по нажатию на кнопку  .
- Функции создания нового правила корреляции в системе - "Создать вручную" и "Создать через конструктор".
- Функцию редактирования правила - окно редактирования открывается по нажатию на кнопку  .
- Функции просмотра логов коррелятора - "Общий лог" и "Лог ошибок".
- Селектор переключения активного узла коррелятора.
- Кнопки включения/выключения правила.

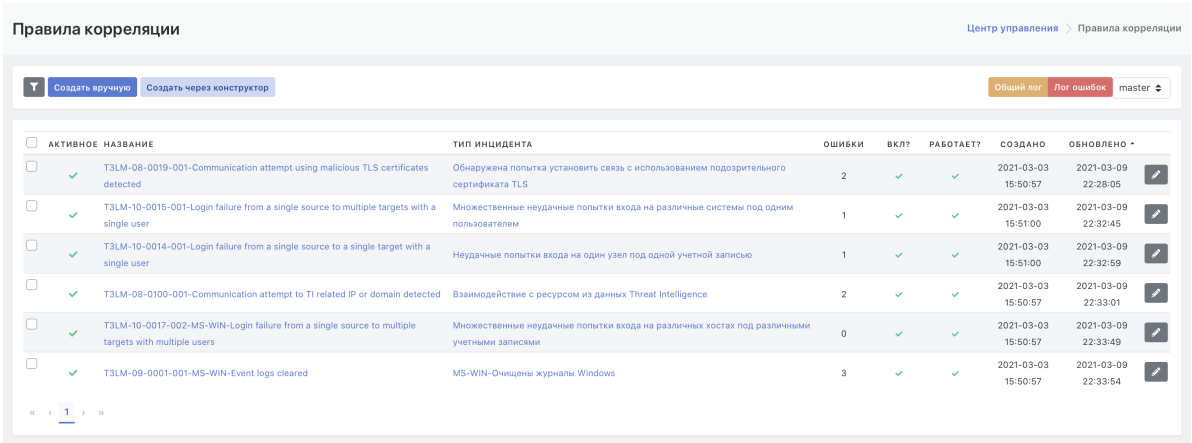


Рисунок 26 - Рабочая область подраздела «Правила»

Текущий список правил корреляции, загруженных в систему, представлен в виде табличного списка со следующими полями:

- флаг "Активное " - текущее состояние правила активное/неактивное (✔ / ✖);
- флаг "Локальное" - текущее состояние правила локальное/глобальное;

- поле "Название" - название правила;
- поле "Тип инцидента" - краткое описание инцидента;
- поле "Ошибки" - количество ошибок;
- поле "Создано" - дата создания правила в системе;
- поле "Обновлено" - дата последнего изменения првила;
- флаги состояния правила на коррелляторе:
    - "Вкл?" - (✔ / ✘);
    - "Работает?" - (✔ / ✘).

Фильтр правил позволяет провести фильтрацию списка по следующим параметрам:

- по параметру Завершенные/Не завершенные;
- по параметру Активные/Неактивные;
- поиск по названию правила (поиск по свободно введенной строке).

5.1.3. Подраздел "Шаблоны"

Подраздел «Шаблоны» предназначен для управления шаблонами вывода результатов работы правил коррелятора (см. Рисунок 27).

Подраздел содержит:

- Текущий список шаблонов, созданных в системе.
- Набор фильтров для просмотра списка шаблонов - фильтры открываются по нажатию на кнопку  .
- Функцию создания нового шаблона в системе - кнопка "Создать".
- Функцию редактирования шаблона - окно редактирования открывается по нажатию на кнопку  .

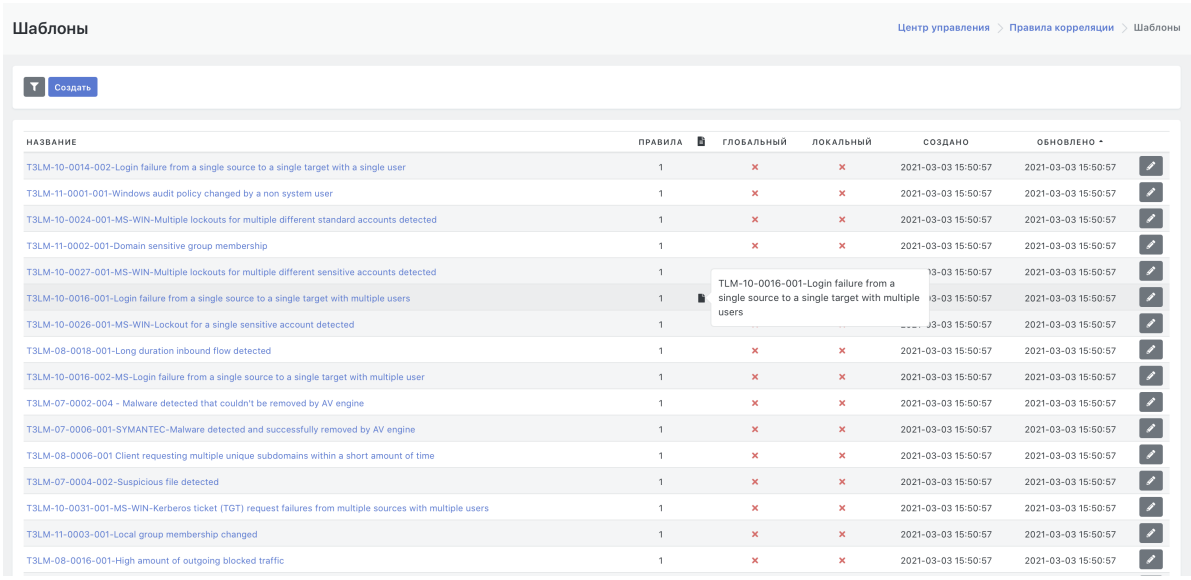


Рисунок 27 - Рабочая область подраздела «Шаблоны»

Текущий список шаблонов, загруженных в систему, представлен в виде табличного списка со следующими атрибутами:

- поле "Название" - название шаблона;
- поле "Правила" - количество правил корреляции, использующих данный шаблон.

- поле  - внутреннее описание, всплывает при наведении курсора на пиктограмму в данном поле:
- флаг "Глобальный" - наличие глобальных значений в полях шаблона ( /);
- флаг "Локальный" - наличие локальных значений в полях шаблона ( / );
- поле "Создано" - дата создания шаблона в системе;
- поле "Обновлено" - дата последнего изменения шаблона.

Фильтр шаблонов позволяет провести фильтрацию списка по названию шаблона (поиск по свободно введенной строке).

5.1.4. Подраздел "Хранилища значений"

Подраздел «Хранилища значений» предназначен для управления хранилищами значений, которые используются в правилах корреляции как конфигурационные значения.

Подраздел содержит:

- Текущий список хранилищ, созданных в системе.
- Набор фильтров для просмотра списка хранилищ - фильтры открываются по нажатию на кнопку  .
- Функцию создания нового хранилища в системе - кнопка "Создать".
- Функцию редактирования данных хранилища - окно редактирования открывается по нажатию на кнопку  .

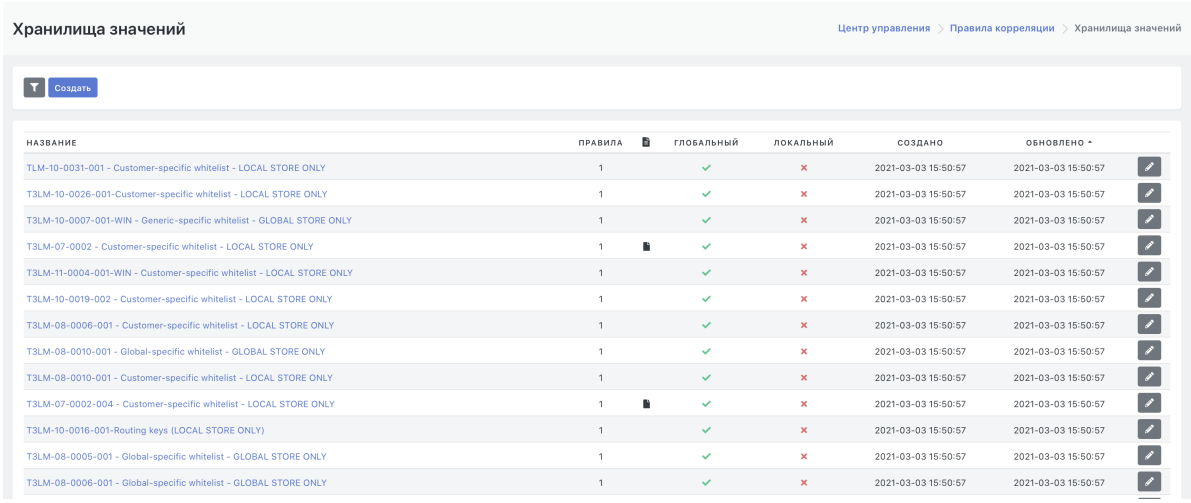


Рисунок 28 - Рабочая область подраздела «Хранилища значений»

Текущий список хранилищ представлен в виде таблицы со следующими атрибутами:

- поле "Название" - название хранилища значений;
- поле "Правила" - количество правил, использующих данное хранилище.
- поле  - внутреннее описание, всплывает при наведении курсора на пиктограмму в данном поле:
- флаг "Глобальный" - указывает, что хранилище содержит глобальный набор значений ( / );
- флаг "Локальный" - указывает, что хранилище содержит локальный набор значений ;
- поле "Создано" - дата создания хранилища;
- поле "Обновлено" - дата последнего изменения хранилища.

Фильтр списка хранилищ позволяет провести фильтрацию списка по следующим параметрам:

- по названию хранилища (поиск по свободно введенной строке);
- по статусу данных в хранилище - Локальные, Глобальные.

5.1.5. Подраздел "Результаты"

Подраздел "Результаты" предназначен для обработки результатов работы правил корреляции, по которым Инциденты и Оповещения не создаются автоматически.

Подраздел содержит:

- Текущий список инцидентов, выявленных как результат срабатывания правил корреляции и оформленных в ручном режиме.
- Набор фильтров для просмотра списка инцидентов - фильтры открываются по нажатию на кнопку  .
- Функция создания нового инцидента в системе по выбранным результатам работы правила - кнопка "Создать инцидент".

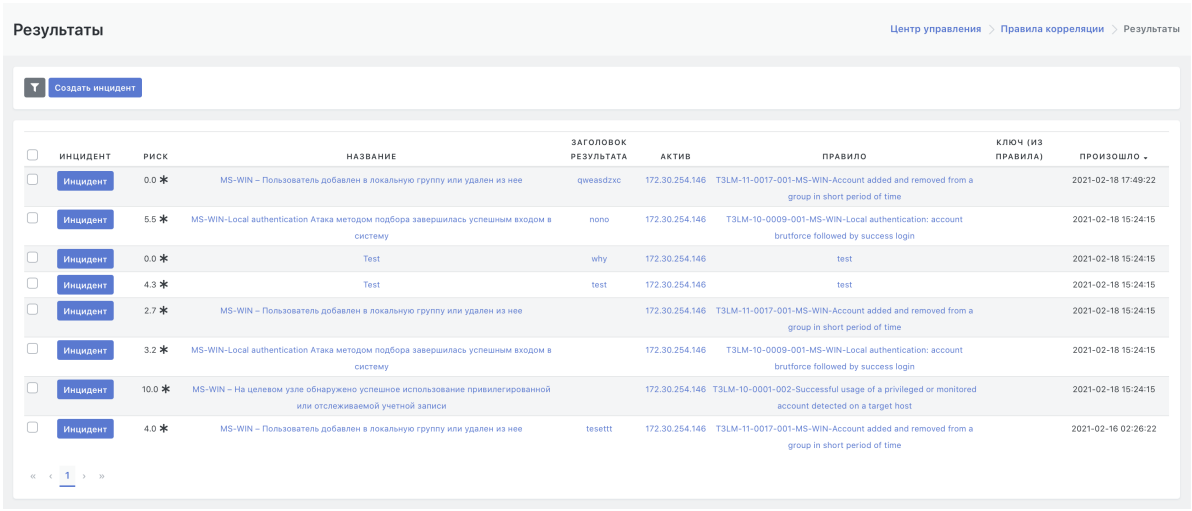


Рисунок 29 - Рабочая область подраздела «Результаты»

Текущий список инцидентов представлен в виде табличного списка со следующими атрибутами:

- поле "Инцидент" - содержит кнопку "Инцидент" для конвертации результатов работы правила в инцидент.
- поле "Риск" - содержит оценку уровня риска.
- поле "Название" - тип инцидента;
- поле "Заголовок результата" заголовок результата.
- поле "Актив" - актив, на котором обнаружена угроза, выявленная правилом;
- поле "Правило" - название правила, с помощью которого была обнаружена угроза;
- поле "Ключ из правила" ;
- поле "Произошло" - дата и время обнаружения инцидента.

Фильтр списка инцидентов разбит на группы и позволяет провести фильтрацию списка по следующим параметрам:

- Вкладка "Фильтр" содержит следующие возможности фильтрации:
    - по типу инцидента (поиск по свободно введенной строке);
    - по уровню риска инцидента;
    - по статусу инцидента - Обработан/Не обработан/Не важно;

    - по статусу актива, но котором выявлен инцидент - Действующий/Не действующий/Не важно.
- Вкладка "Активы" содержит следующие возможности фильтрации:
    - по группе активов;
    - по имени актива;
    - по типу инцидента.
- Вкладка "Дополнительно" содержит следующие возможности фильтрации:
    - по времени обнаружения - по заданному временному интервалу;
    - по статусу принятия в обработку - Принят/Не принят/Не важно.

6. Оценка соответствия ПО

6.1. Раздел "Оценка соответствия ПО"

6.1.1. 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.

6.1.2. Подраздел "Результаты соответствия ПО"

6.1.2.1. 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 30):

- 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 отдельном разделе "Запуск процесса проверки соответствия".

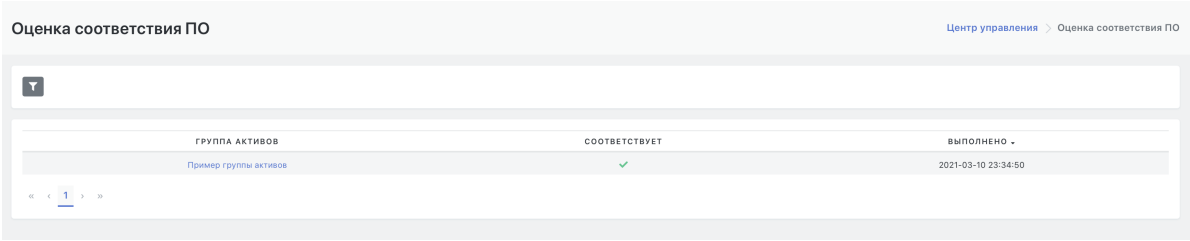


Рисунок 30 - Рабочая область подраздела "Результаты соответствия ПО"

6.1.2.2. Список результатов проверки ПО. Параметры списка

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

- Поле "**Группа активов**" -- название группы активов, на которых проводилась данная проверка, активная ссылка на детализацию результатов проверки соответствия ПО;
- Флаговое поле "**Соответствует**" -- статус соответствия ПО для группы активов по результату проверки;
- Поле "**Выполнено**" -- дата и время время, в которое запускалась проверка соответствия ПО на указанном активе.

6.1.2.3. Настраиваемые фильтры списка результатов проверки ПО

При нажатии на кнопу  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**".

6.1.2.4. 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 *"Настройка контроля установленного программного обеспечения. Анализ результатов проверок соответствия ПО"*.

6.1.3. Подраздел "Список ПО"

6.1.3.1. 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 31):

- 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"**.

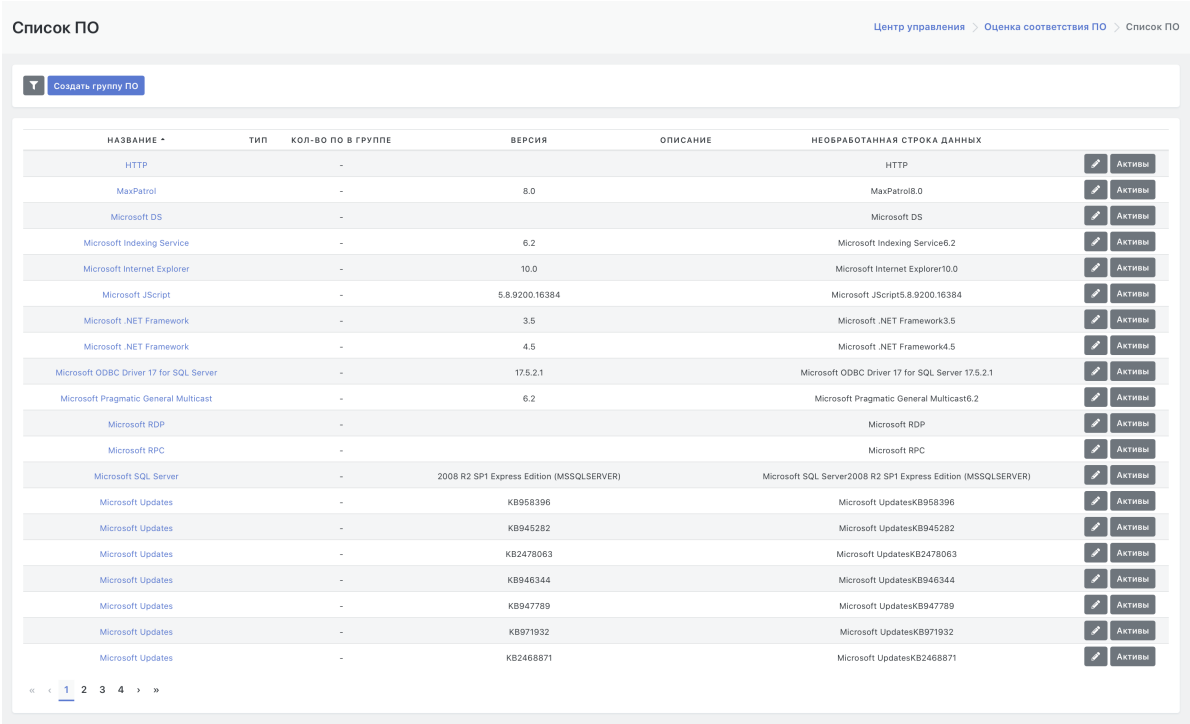


Рисунок 31 - Рабочая область подраздела "Список ПО"

6.1.3.2. Список ПО. Параметры списка

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

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

6.1.3.3. Настраиваемые фильтры списка ПО

При нажатии на кнопу 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"**.

6.1.3.4. 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. Более подробное описание просмотра детализации приведено в разделе "*Настройка контроля установленного программного обеспечения. Анализ программного обеспечения на активах*".

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 списка активов приведено в разделе "*Настройка контроля установленного программного обеспечения. Анализ программного обеспечения на активах*".

6.1.3.5. 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 "*Настройка контроля установленного программного обеспечения. Анализ программного обеспечения на активах*".

6.1.3.6. Редактирование данных ПО

Для редактирования данных о ПО необходимо нажать на кнопку  -- произойдет переход на страницу редактирования данных. Подробное описание функции редактирования приведено в разделе "*Настройка контроля установленного программного обеспечения. Анализ программного обеспечения на активах*".

6.1.4. Подраздел "Наборы правил"

6.1.4.1. 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 32):

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

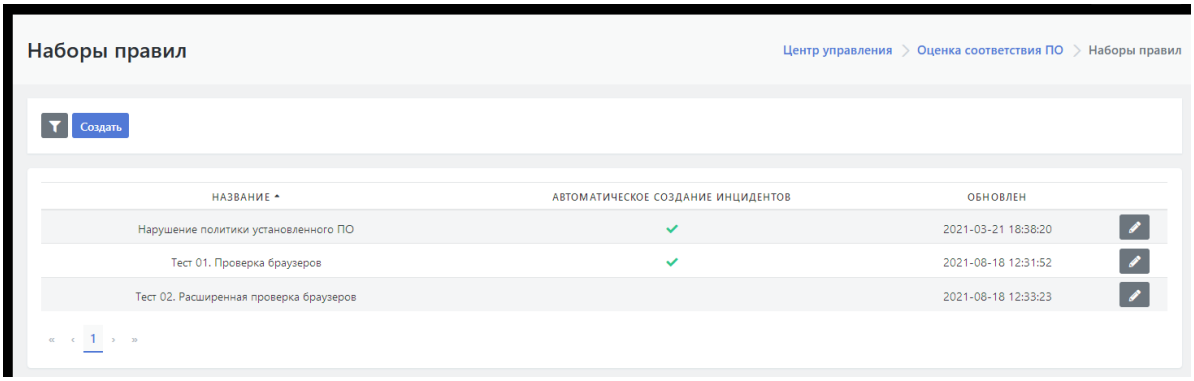


Рисунок 32 - Рабочая область подраздела "Наборы правил"

6.1.4.2. Список политик. Параметры списка

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

- Поле "**Название**" -- название политики (группы правил).
- Флаговое поле "**Автоматическое создание инцидентов**" -- включена/выключена функция автоматического создания инцидентов при выявлении нарушения политики.

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

6.1.4.3. Настраиваемые фильтры списка политик

При нажатии на кнопу 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**".

6.1.4.4. Создание, редактирование, удаление политик

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

При нажатии на кнопу 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*".

6.1.5. Подраздел "Правила"

6.1.5.1. 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 33):

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

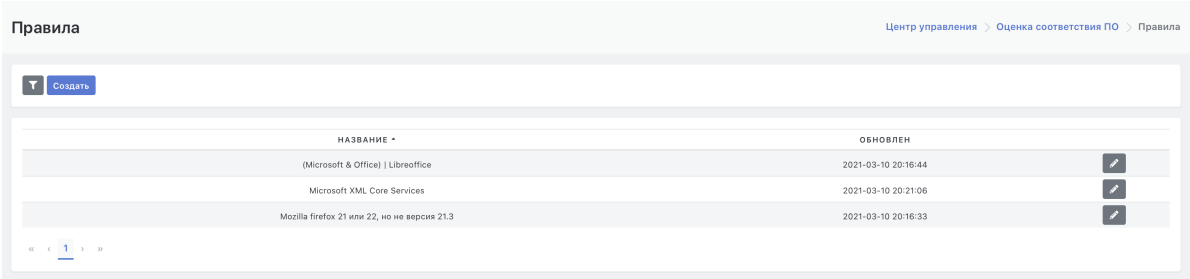


Рисунок 33 - Рабочая область подраздела "Правила"

6.1.5.2. Список правил. Параметры списка

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

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

6.1.5.3. Настраиваемые фильтры списка политик

При нажатии на кнопу  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**".

6.1.5.4. Создание, редактирование, удаление правила

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

При нажатии на кнопу  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*".

7. Параметры

7.1. Раздел «Параметры»

7.1.1. Состав раздела "Параметры"

Раздел «Параметры» состоит из следующих подразделов:

- **"Параметры"** -- подраздел предназначен для настройки общих параметров Платформы.
- **"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 .

7.1.2. Подраздел «Параметры»

7.1.2.1. 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, включая значения по умолчанию (см. Рисунок 34) ;
- **"Обработка уязвимостей"** -- вкладка предназначена для настройки параметров автоматической обработки уязвимостей;
- **"Синхронизация с Базой Знаний"** -- вкладка предназначена для проведения синхронизации с Базой знаний.

7.1.2.2. Вкладка "Общие". Обновление общих параметров

Рабочее поле вкладки "Общие" содержит поля для редактирования следующих общих параметров (см. Рисунок 34):

- "**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 в качестве срока по-умолчанию в параметре "Принять до". Чтобы оставить значение параметра "Принять до" пустым, надо указать в поле "0".
- "**Расположение**" -- текстовое поле ввода, предназначено 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 нажать на кнопку "**Сохранить**".

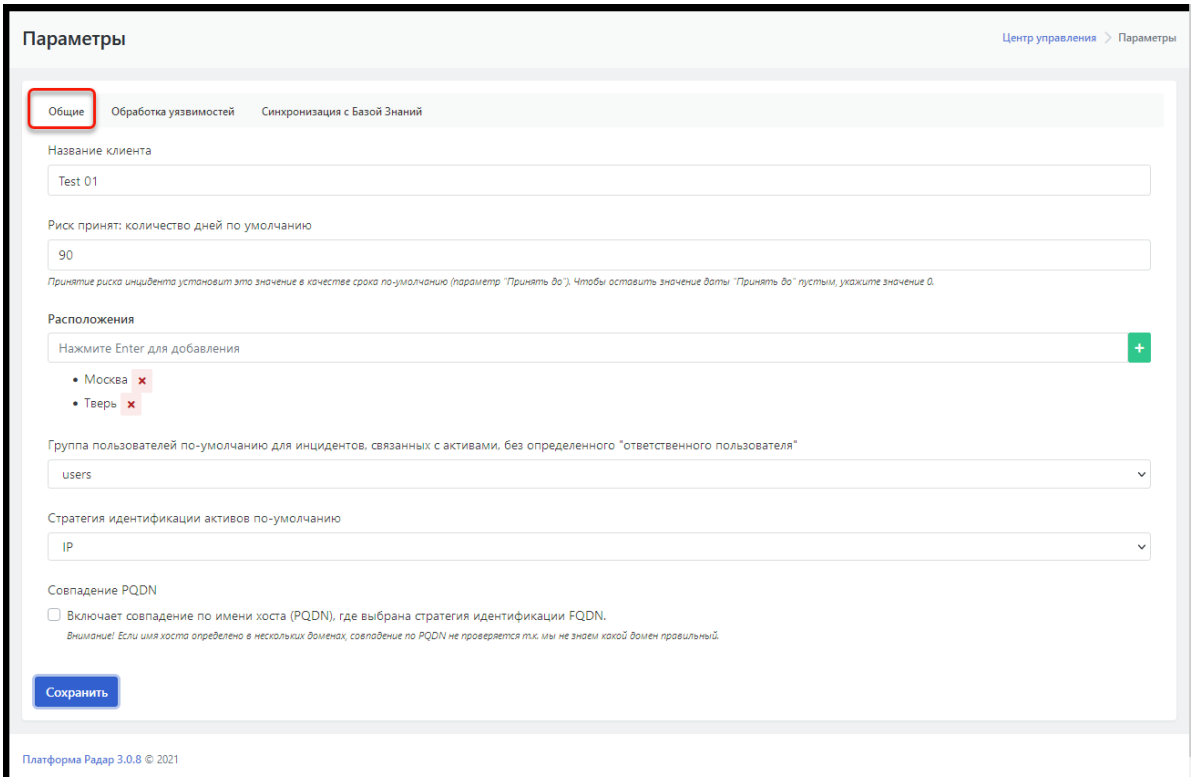


Рисунок 34 - Подраздел "Параметры", вкладка "Общие"

7.1.2.3. Вкладка "Обработка уязвимостей". Обновление общих параметров

Рабочее поле вкладки "Обработка уязвимостей" содержит поля для редактирования параметров автоматического закрытия и автоматического переоткрытия инцидентов (см. Рисунок 35):

- Флаговое поле "**Автоматически закрывать инциденты**" -- включение/ отключение режима автоматического закрытия уязвимостей;
- Флаговое поле "**Закрыть только инциденты со статусом "Ожидает проверки""** " -- включение/ отключение режима , при котором происходит автоматическое закрытие инцидентов только в статусе «Ожидает проверки»;
- "**Минимальный уровень риска для повторного открытия инцидентов**" -- риски ниже указанного уровня не переоткрываются автоматически;
- "**Статус повторно открытых инцидентов**" -- переоткрываемые автоматически инциденты будут переводиться в указанный статус.

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

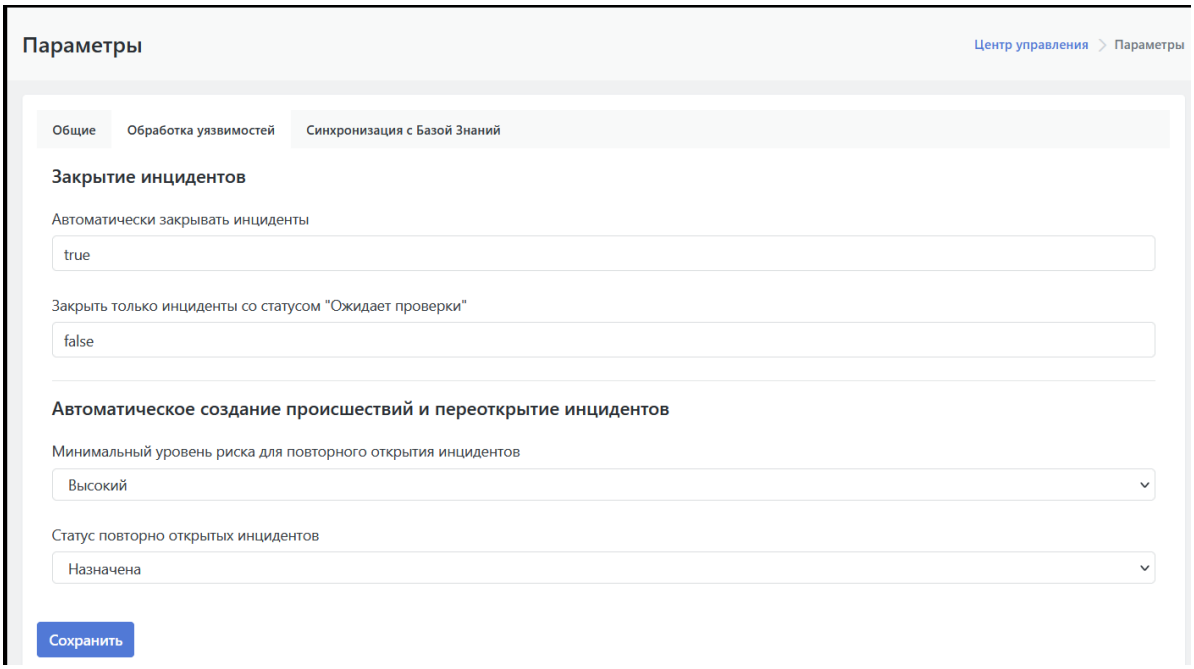


Рисунок 35 - Подраздел "Параметры", вкладка "Обработка уязвимостей"

7.1.2.4. Вкладка "Синхронизация с Базой Знаний"

Рабочее поле вкладки "Синхронизация с Базой Знаний" содержит два функциональных элемента (см. Рисунок 36):

- 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 36).

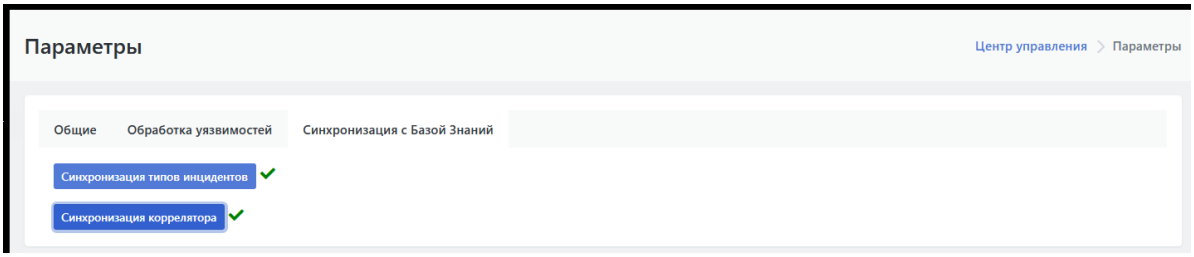


Рисунок 36 - Подраздел "Параметры", вкладка "Синхронизация с Базой Знаний"

7.1.3. Подраздел «Черный список ID плагинов»

7.1.3.1. 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 37):

- 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  .

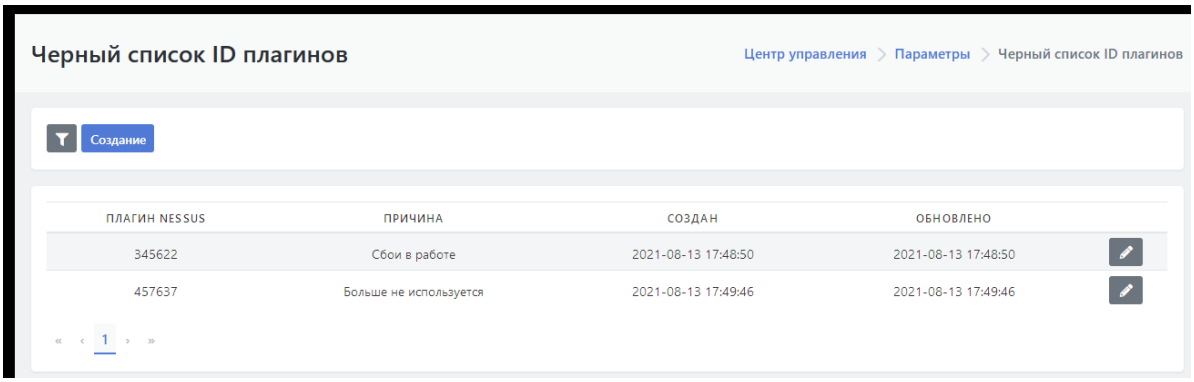


Рисунок 37 - Рабочая область подраздела "Черный список ID плагинов"

7.1.3.2. 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 так же удаление плагина из списка.

7.1.3.3. Настраиваемые фильтры списка плагинов

При нажатии на кнопу  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**".

7.1.3.4. Включение нового плагина в список, удаление плагина из списка

Для включения в черный список нового плагина необходимо (см. Рисунок 38):

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.

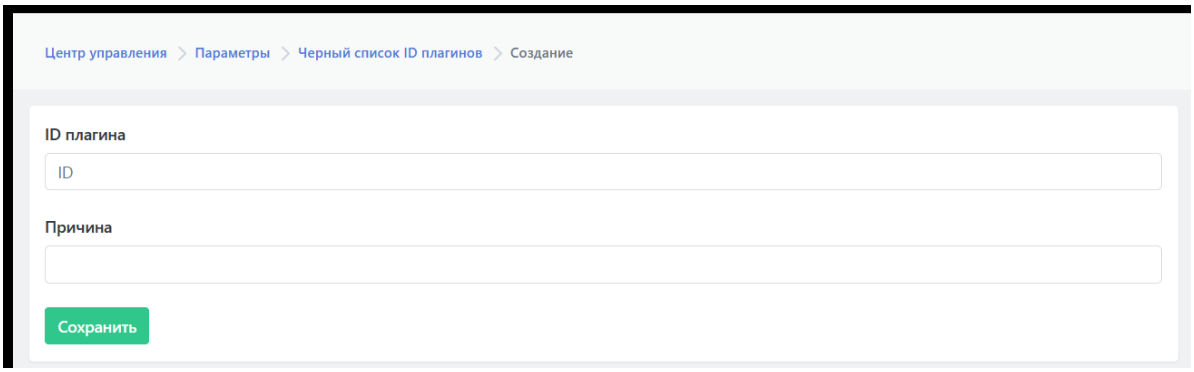


Рисунок 38 - Включение нового плагина в "Черный список ID плагинов"

7.1.3.5. 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 39).
3. Для сохранения изменений нажать на кнопку "**Сохранить**". Для удаления плагина из черного списка нажать на кнопку "**Удалить**".

Откроется обновленный черный список плагинов.

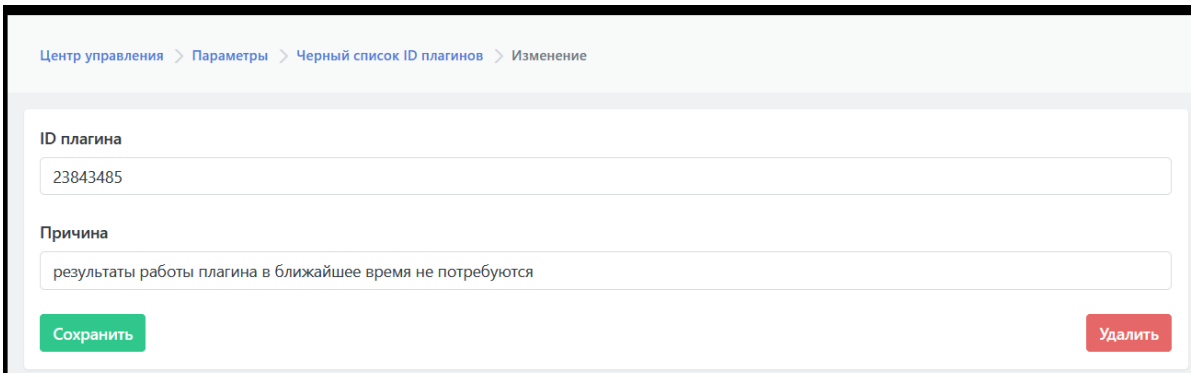


Рисунок 39 - Форма редактирования параметров плагин из черного списка

7.1.4. Подраздел "Оповещения по задержкам в обработке"

7.1.4.1. 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.

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.

7.1.4.2. Настройка временных отсечек для оповещений

В Платформе возможно настроить 3 контрольных отсечки по времени разбора инцидента (см. Рисунок 40):

- "**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.

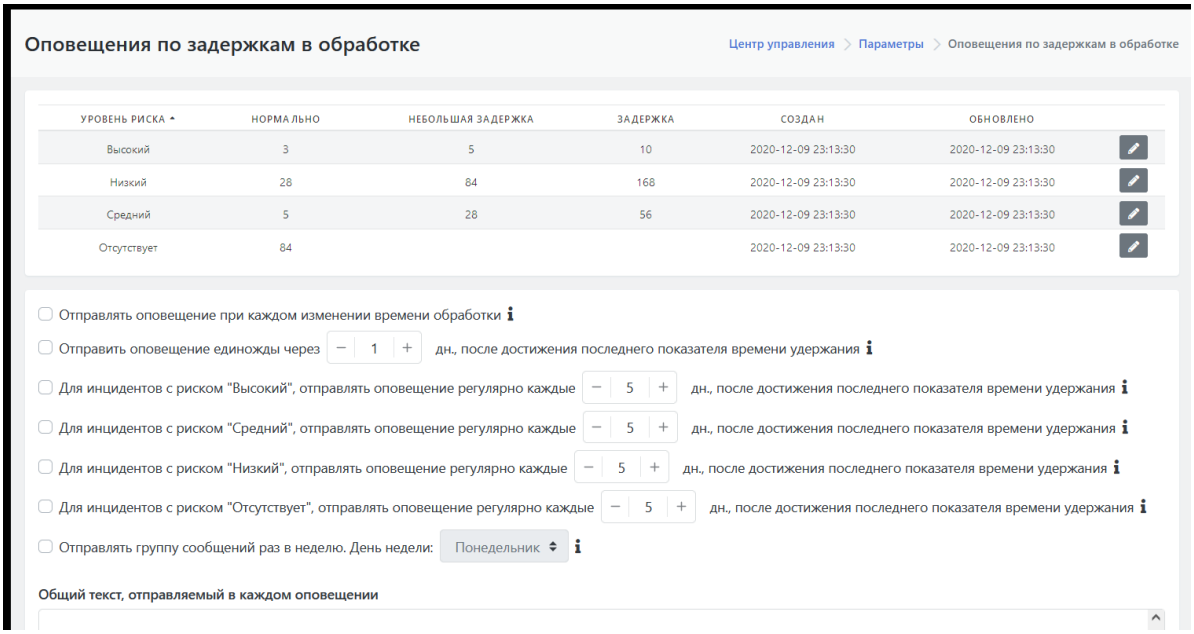


Рисунок 40 - Рабочее поле подраздела "Оповещения по задержкам в обработке", блоки настроек временных отсечек для оповещений и блок настройки параметров отправки оповещений

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 41).
3. Нажать на кнопку **"Сохранить"**.

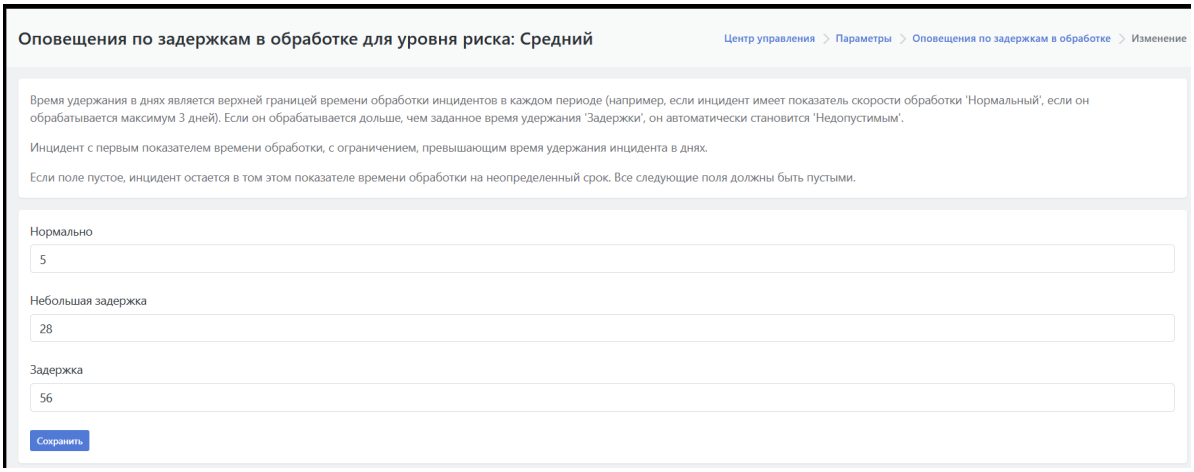


Рисунок 41 - Редактирование времени контрольных отсечек для среднего уровня риска

7.1.4.3. Настройка режима отправки оповещений

В Платформе возможно настроить следующие режимы отправки оповещений (см. Рисунок 42):

- "**Отправлять оповещения при каждом изменении времени обработки *i* **"-- 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 *i*"** -- 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 *i* "** -- 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 *i* "** -- 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 *i* "** -- 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 *i* "** -- 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 <...> *i* "** -- при активации опции все накопившиеся оповещения будут отправляться единожды в указанный день.

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

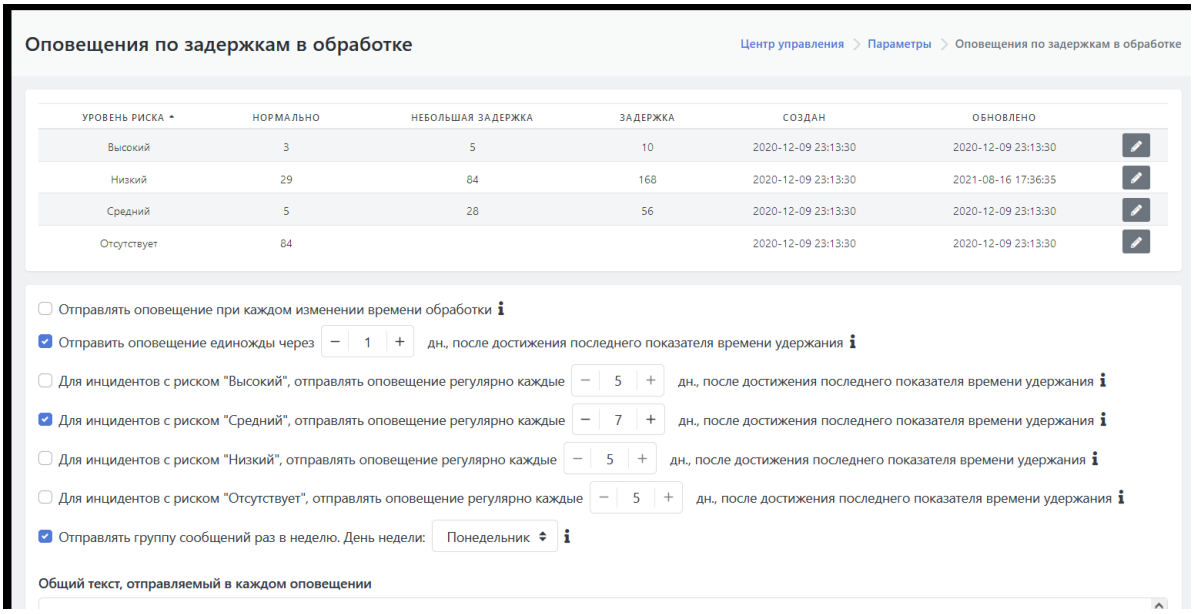


Рисунок 42 - Настройка режимов отправки оповещений

7.1.4.4. Настройка текстов для оповещений

Для оповещений по задержкам в обработке можно настроить следующий текст (см. Рисунок 43):

- **"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 нажать на кнопку **"Сохранить"**, расположенную внизу страницы под всеми блоками настроек (см. Рисунок 43).

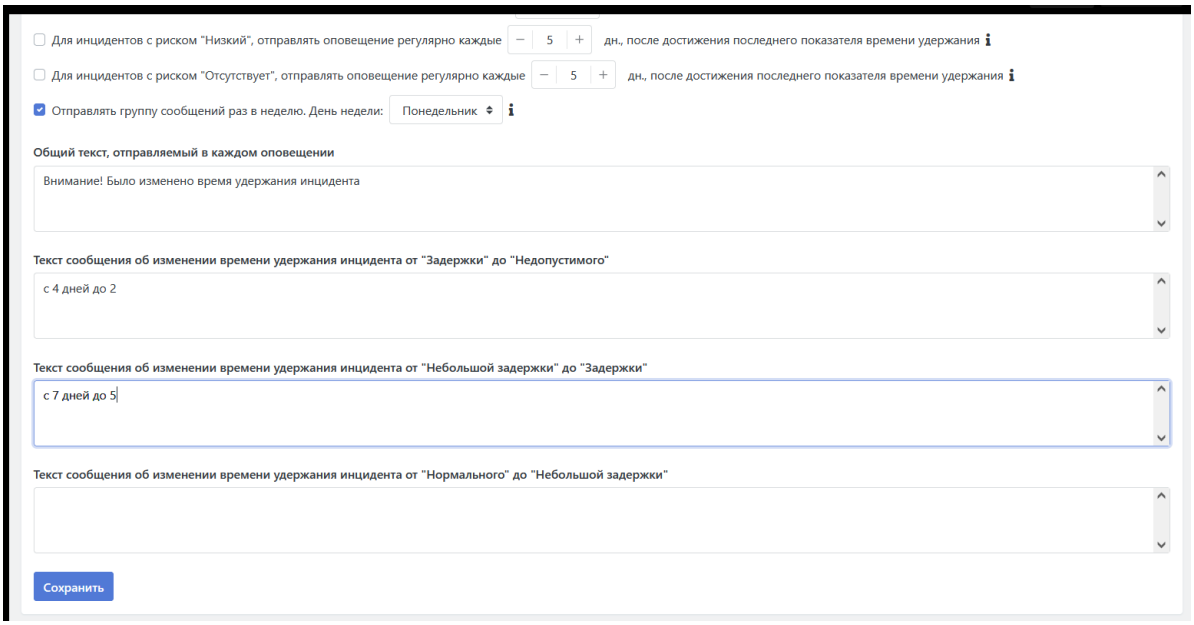


Рисунок 43 - Настройка текстов оповещений

8. Сообщения

8.1. Раздел Сообщения

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

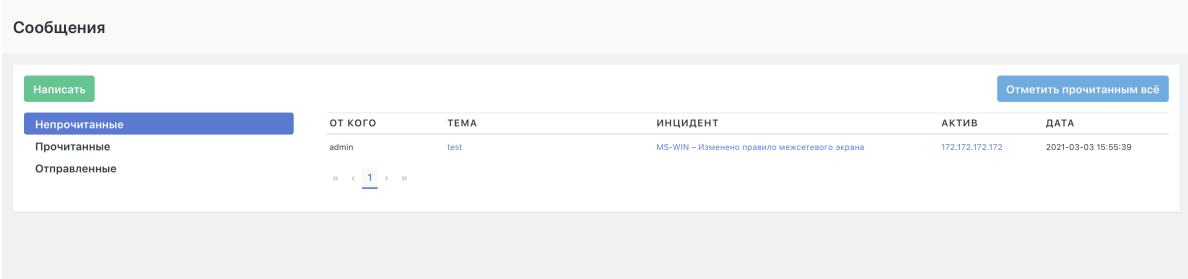


Рисунок 44 - Рабочая область раздела «Сообщения»

В рабочей области отображаются следующие виды сообщений (Рисунок 2):

- Непрочитанные;
- Прочитанные;
- Отправленные;

Список сообщений, содержит следующие поля:

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

Для создания нового сообщения необходимо нажать кнопку "Написать".

В появившемся окне "Новое сообщение" заполнить поля "Получатель " и "Заголовок", ввести новое сообщение и нажать кнопку "Отправить" (Рисунок 3).

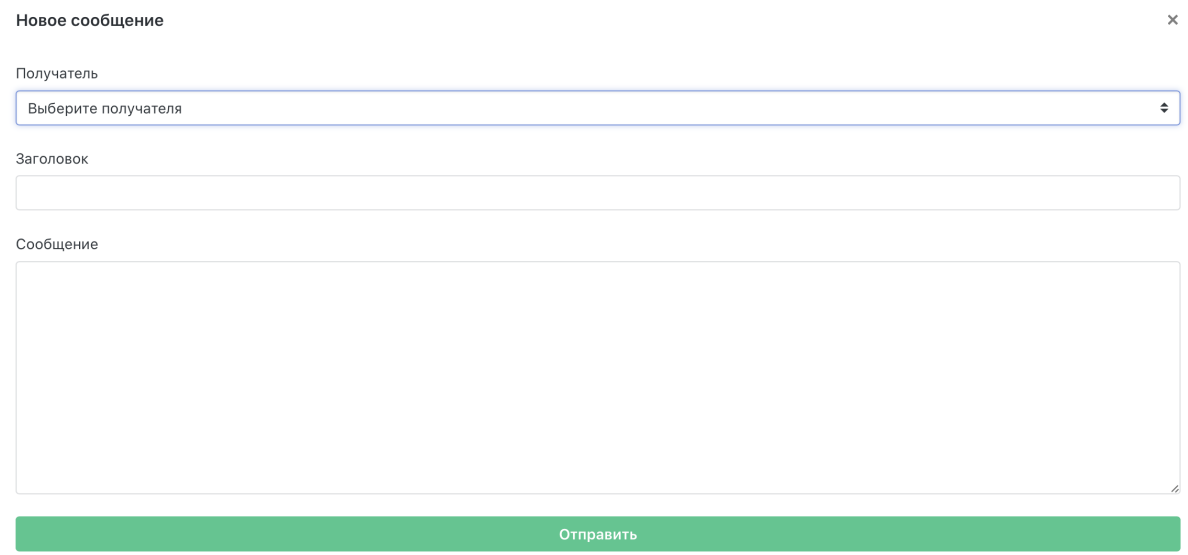


Рисунок 45 - Окно «Новое сообщение»

9. Раздел Отчеты

9.1. Основные элементы раздела

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

Раздел состоит из следующих элементов (см. Рисунок 46):

- 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"**.

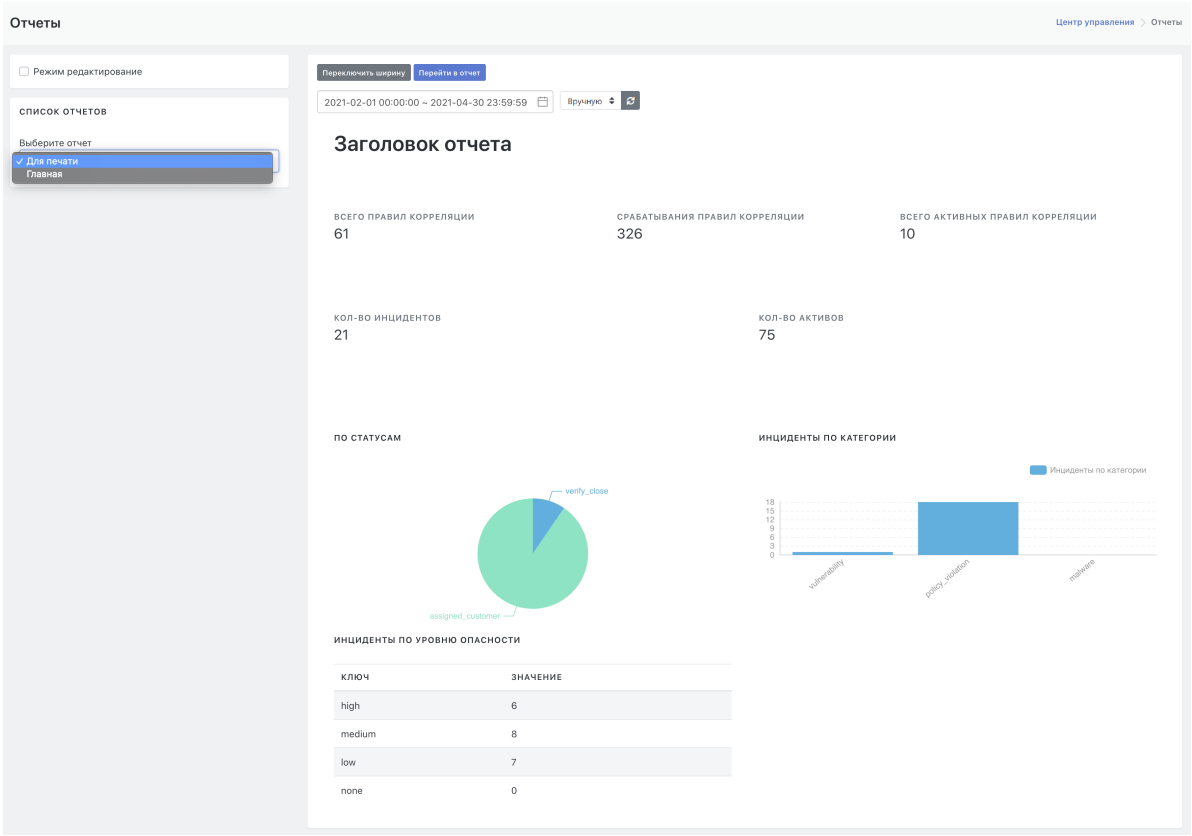


Рисунок 46 - Рабочая область раздела "Отчеты"

9.2. 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 47):

- 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"**.

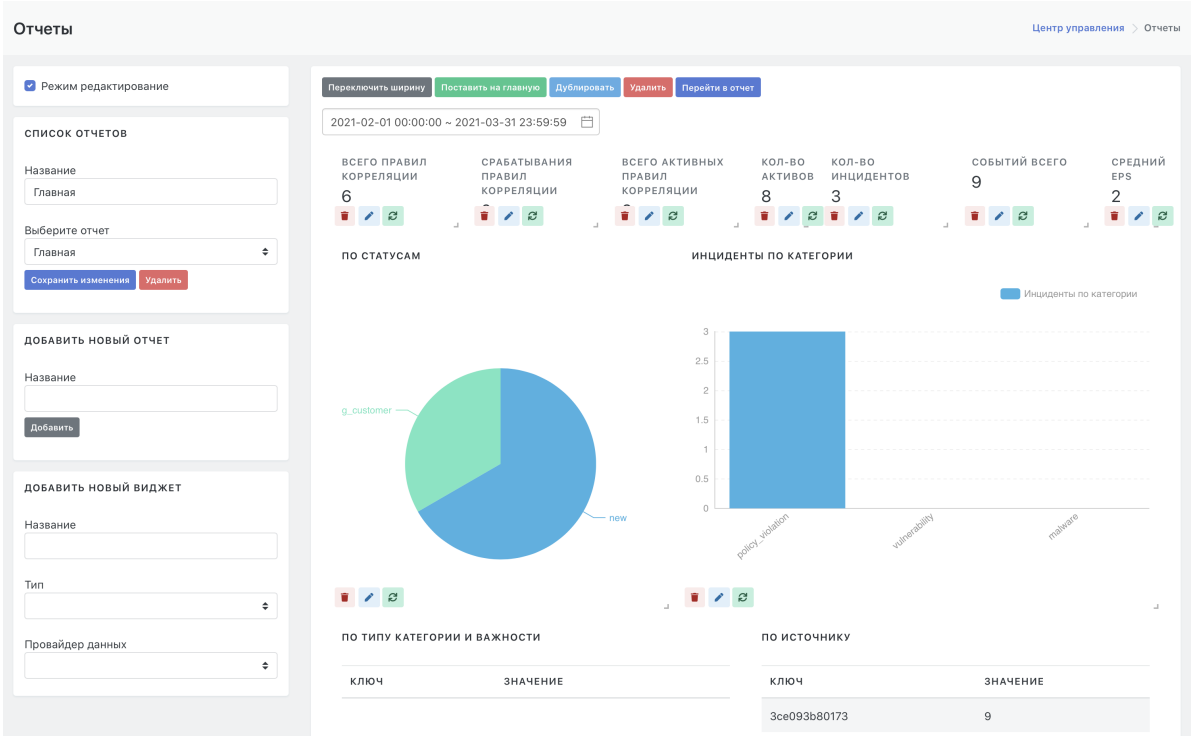


Рисунок 47 - Рабочая область раздела "Отчеты" в режиме редактирования

9.3. 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 советующих пунктах раздела *"Работа с отчётами"* .

9.4. 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.

10. Работа с инцидентами

10.1. 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 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 инцидент всегда имеет определенный тип инцидента и привязку к активу, на котором он выявлен.

10.2. Выявление инцидентов (автоматическое создание инцидентов)

10.2.1. Механизмы выявления инцидентов

В рамках Платформы реализованы следующие механизмы выявления инцидентов:

- правила корреляции -- подробное описание в отдельном документе *"Руководство разработчика правил корреляции"* ;
- данные об уязвимостях -- подробное описание в разделе *"Интеграция со сканерами уязвимостей"*;

- создание инцидента вручную;
- контроль списка программного обеспечения -- подробное описание в разделе *"Настройка контроля установленного программного обеспечения"*;
- контроль потока событий ИБ с источников -- подробное описание в разделе контроль потока событий с источников.

10.2.2. 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.

10.2.3. Происшествия

В Платформе 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 статус инцидента меняется на «Новый» или «ПР Новый» (подробнее о настройке) и для него увеличивается счетчик повторных открытий инцидента.

10.3. Создание инцидента вручную

10.3.1. Общие положения

Создание инцидента вручную может потребоваться в следующих случаях:

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

10.3.2. 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/**.

10.3.3. Создание нового инцидента со страницы списка инцидентов {#create_incident_from_list}

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 48).

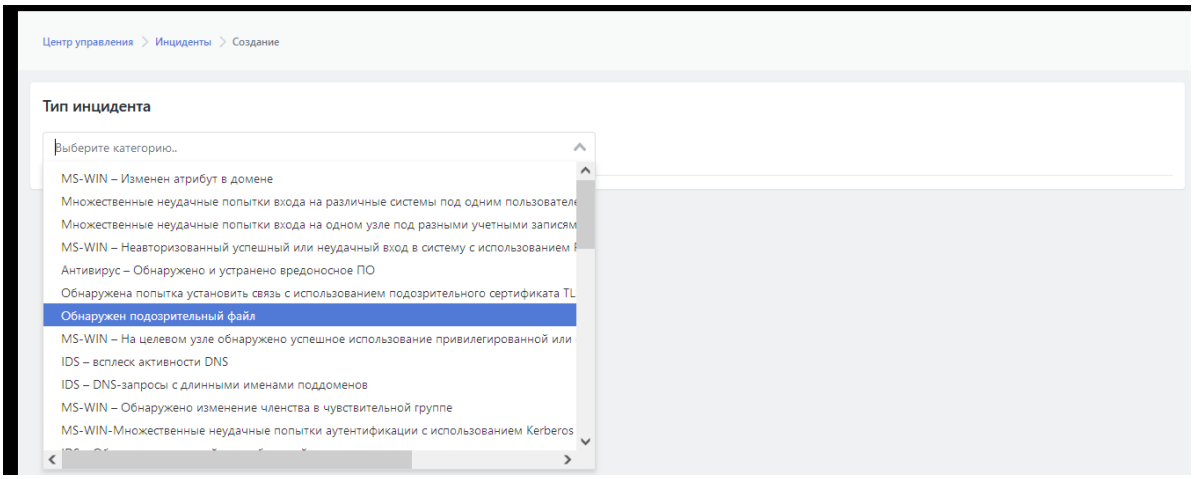


Рисунок 48 - Выбор типа для создаваемого вручную инцидента

4. После выбора типа открывается форма со стандартными параметрами указанного типа инцидента (см. Рисунок 49). Отредактировать стандартные значения полей, если это необходимо. Полное описание параметров типа инцидента приведено в разделе *"Просмотр детализации типа инцидента. Карточка типа"*.

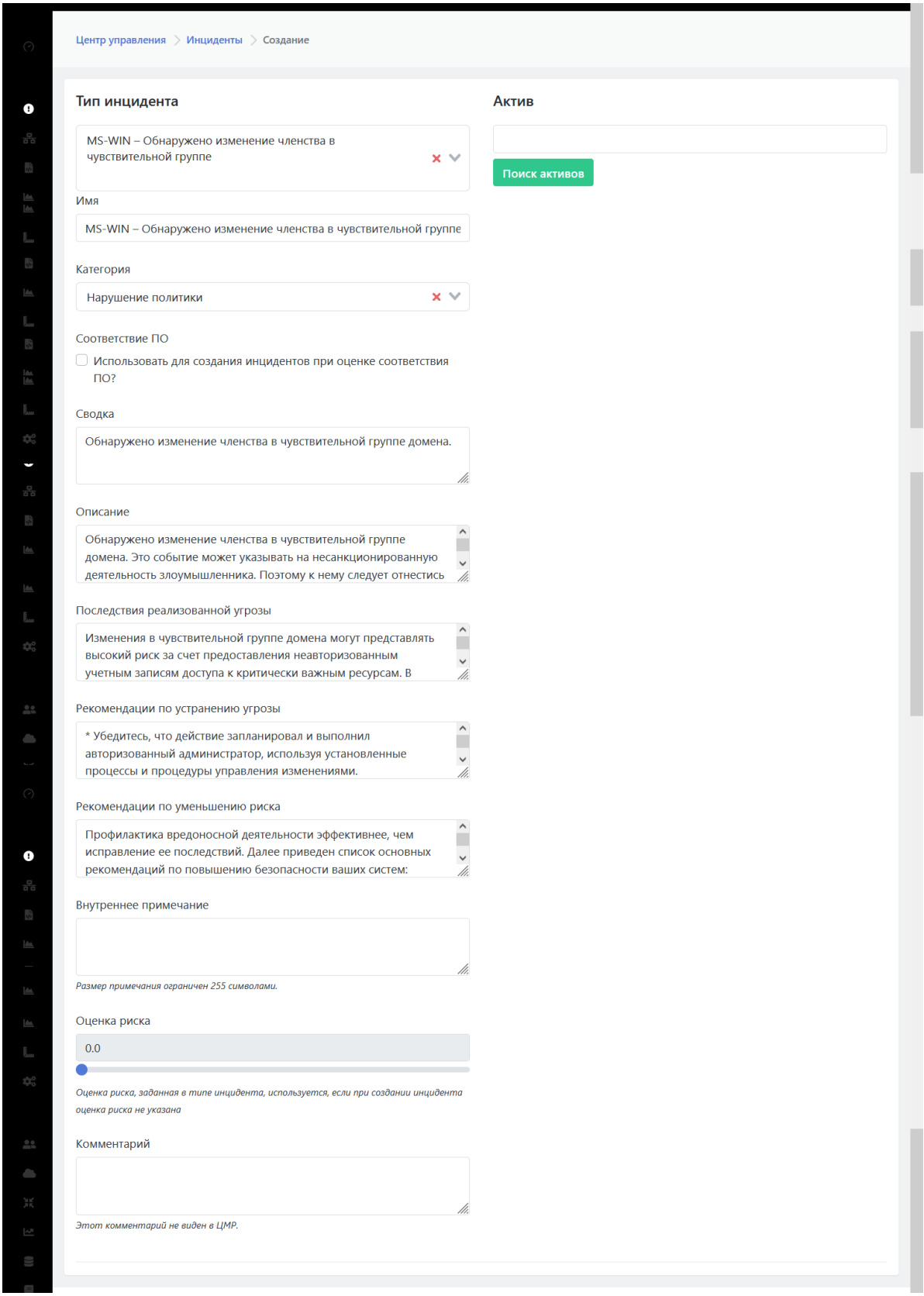


Рисунок 49 - Настройка параметров типа при создании нового инцидента

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 50). При отсутствии регистрации актива на Платформе будет предложено создать актив. Алгоритм создания нового актива на Платформы приведен ниже.
6. Для завершения создания инцидента на Платформы нажать на кнопку "**Сохранить**".

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

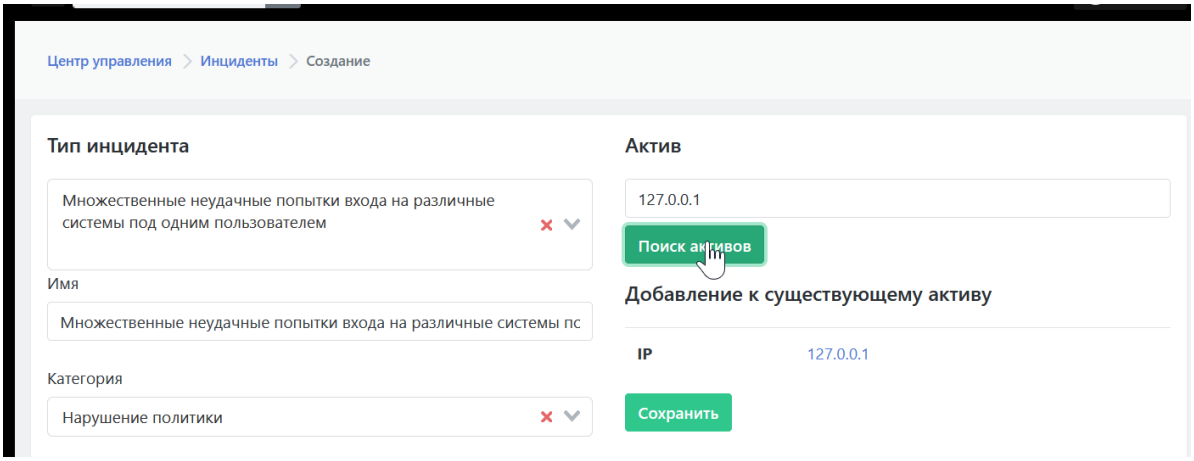


Рисунок 50 - Привязка нового инцидента к активу и сохранение созданного инцидента

При отсутствии на Платформе данных об активе, будет предложено создать новый актив (см. Рисунок 51). На экране откроется область **"Создание нового актива"**. Для нового актива необходимо указать:

- Поле "**Имя**" -- указать имя активы на Платформы
- 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 подразделе *"Управление активами Создание актива"*.

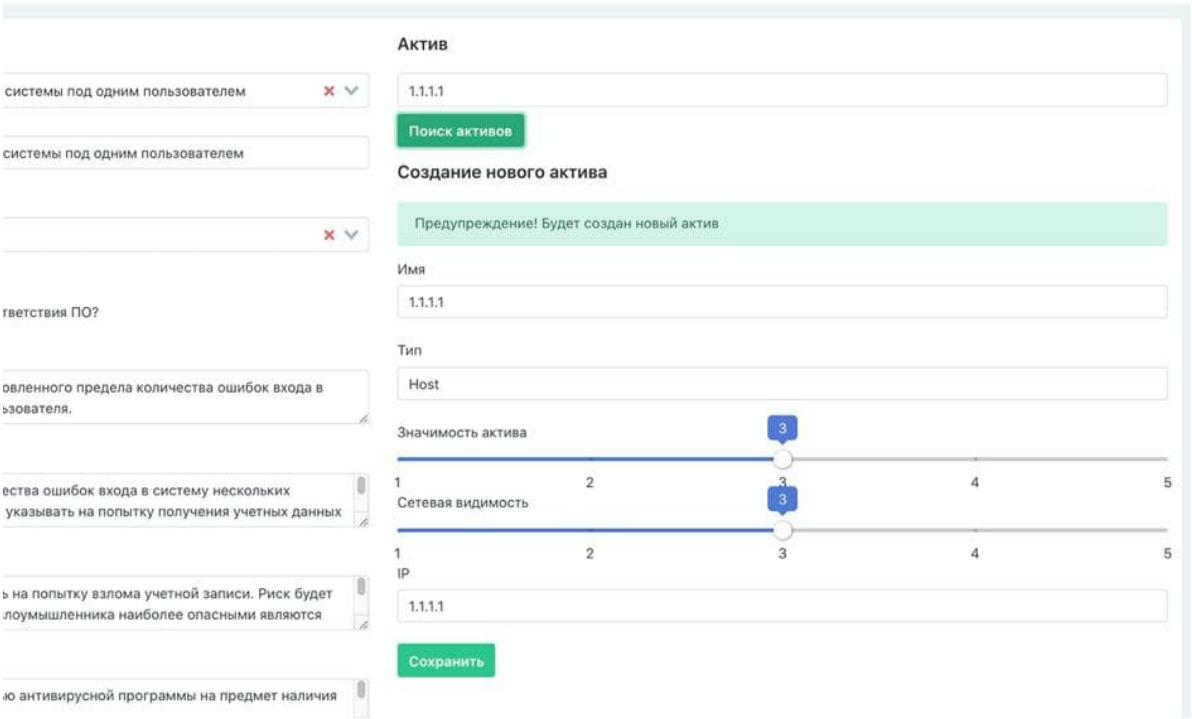


Рисунок 51 - Область с формой создания актива (при создании инцидента)

10.3.4. 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 *"Создание нового инцидента со страницы списка инцидентов"*.

10.3.5. Привязка дополнительных событий вручную для анализа причины инцидента

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 перейти в раздел **"Просмотр событий"**.
2. Открыть интересующее событие, щелкнув по значку - ▶ (см. Рисунок 52).

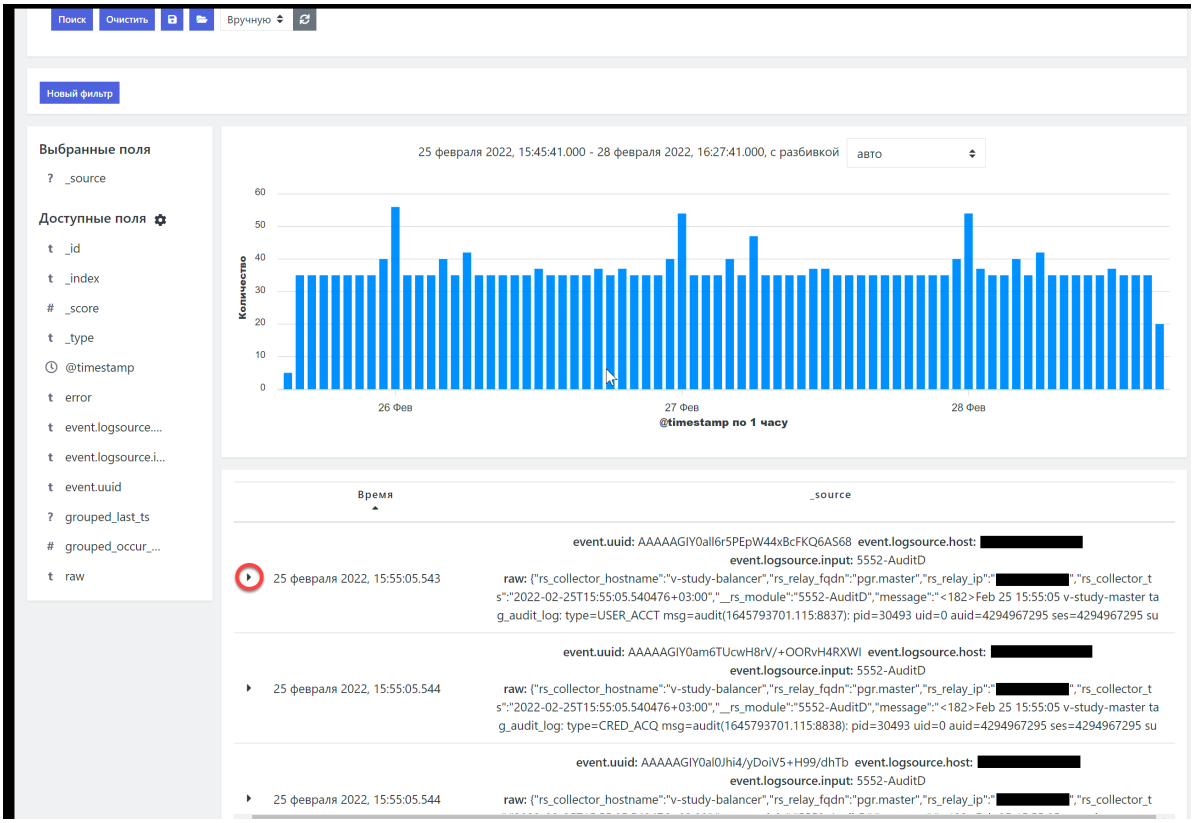


Рисунок 52 - Открытие "сырых" данных события

3. Нажать кнопку **Найти инцидент** (см. Рисунок 53).

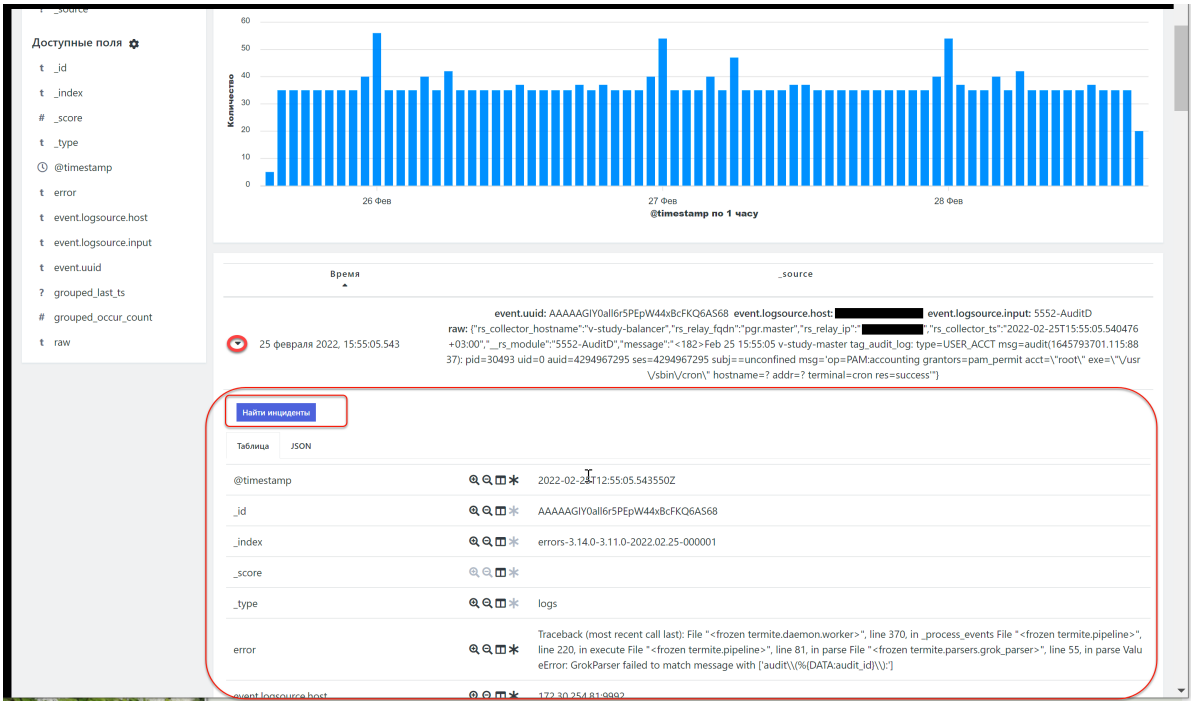


Рисунок 53 - Функция поиска инцидента, которому может принадлежать данное событие

4. Если для данного события связанный с ним инцидент не будет найден, то Платформы предложит (см. Рисунок 54) либо вручную создать инцидент на основе данного события (кнопка **Создать инцидент**), либо добавить событие к существующему инциденту (кнопка **Добавить к существующему**).

Рисунок 54 - Результат работы функции **Найти инциденты**.

5. Нажать кнопку **Добавить к существующему**.
6. В открывшемся окне (см. Рисунок 51):
   - 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.

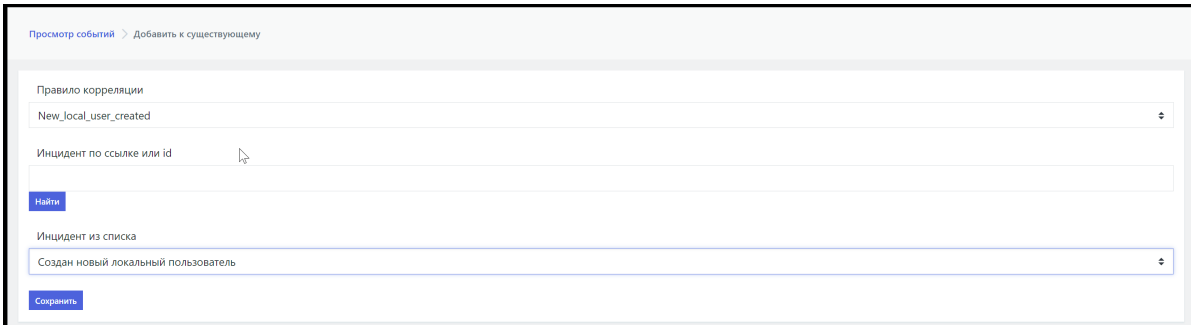


Рисунок 55 - Привязка события к инциденту

8. Для привязки события к инциденту нажать кнопку **Сохранить.**

Для того чтобы проверить что привязка события к инциденту произошла - надо повторить шаги 1-3 приведенного выше алгоритма. По нажатию кнопки **Найти инциденты** откроется имя инцидента, к которому было привязано вручную событие (см. Рисунок 56). По имени инцидента можно перейти на карточку инцидента для просмотра детализации. Описание карточки инцидента приведено в разделе документа *"Анализ инцидента. Просмотр детализации инцидента. Карточка инцидента"*

Рисунок 56 - Просмотр списков инцидентов, к которым привязано событие

10.4. Анализ инцидента

10.4.1. 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 57).

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

Подробное описание табличного списка инцидентов и возможностей фильтрации списка приведены в разделе документации "*Подраздел "Инциденты"* ".

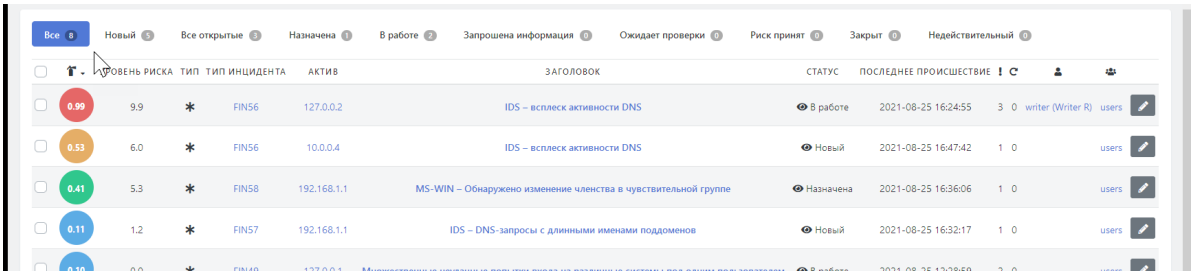


Рисунок 57 - Список инцидентов в разделе "Инциденты" -> "Инциденты"

Гиперссылки в строке инцидента обеспечивают просмотр следующей детальной информации:

- Поле "**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 документа *"Просмотр детализации типа инцидента. Карточка типа"* .
- Поле "**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 документа *"Просмотр детализации актива. Карточка актива"*.
- Поле "**Заголовок**" -- содержит название инцидента. Гиперссылка ведет на карточку инцидента с детальной информацией по данному инциденту. Описание карточки инцидента приведено в разделе документа *"Анализ инцидента. Просмотр детализации инцидента. Карточка инцидента"*.
- Поле "**Пользователь**" () -- содержит имя пользователя Платформы, которому назначен данный инцидент для расследования. Гиперссылка ведет на страницу с краткой информацией по данному пользователю.
- Поле "**Группа**" () -- содержит имя группы пользователей Платформы, 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 *"Расследование инцидента. Редактирование параметров инцидента"*.

10.4.2. Просмотр детализации инцидента. Карточка инцидента

10.4.2.1. 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 58).

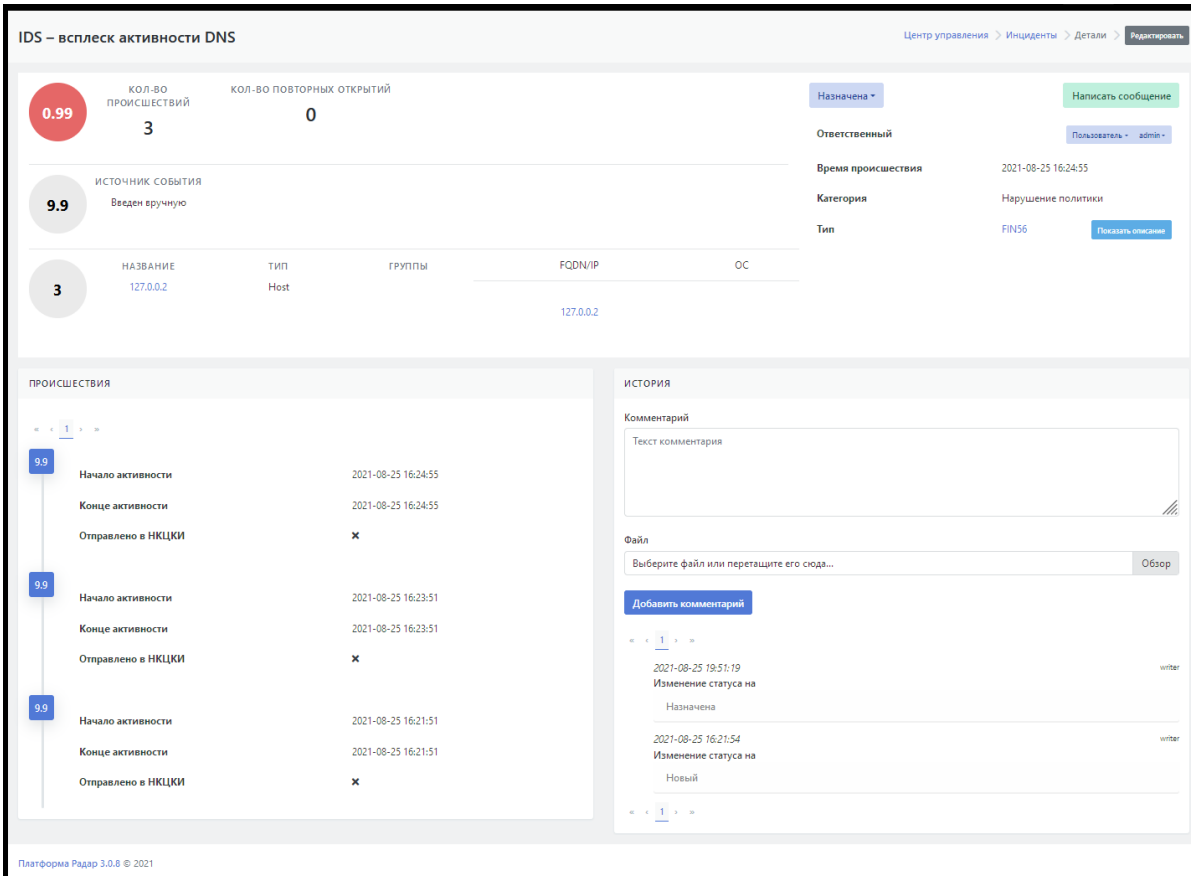


Рисунок 58 - Карточка инцидента с детальной информацией по инциденту

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.

10.4.2.2. Блок сводной информации по инциденту

Блок сводной информации содержит следующие данные по инциденту (см. Рисунок 53):

- **"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 на Платформе. Реализовано в виде гиперссылки, которая ведет на карточку актива. Описание карточки актива приведено в разделе документа *"Просмотр детализации. Карточка 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 59). Список содержит возможные варианты смены текущего статуса и позволяет поменять статус инцидента непосредственно на карточке инцидента.

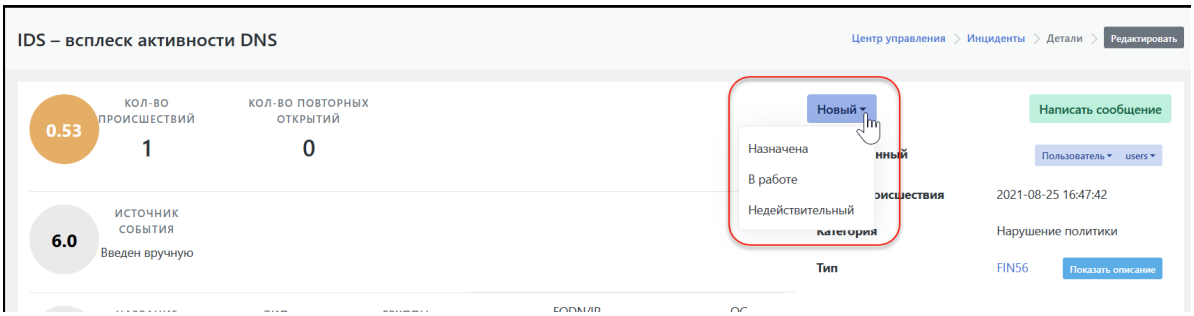


Рисунок 59 - Функция смены статуса на карточке инцидента

- "**Время происшествия**" -- время создания инцидента;
- "**Ответственный**" -- представляет собой два раскрывающихся списка: список пользователей и список групп пользователей (см. Рисунок 60). 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.

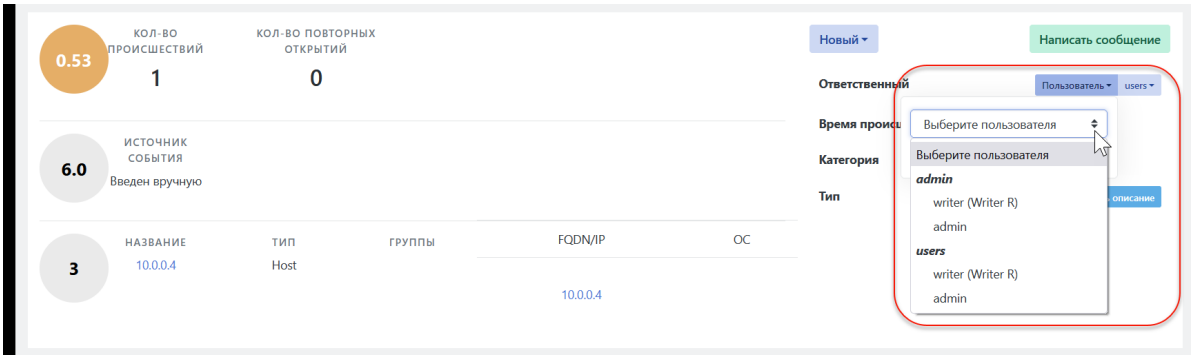


Рисунок 60 - Функция переназначения инцидента другому ответственному пользователю или группе пользователей на карточке инцидента

- **"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 детализации типа инцидента. Карточка типа"*
- В блоке сводной информации присутствует три типа оценок. Подробное описание работы с оценками приведено в отдельном 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 *"Расследование инцидента. Редактирование параметров инцидента"*.

- "**Написать сообщение**" -- при нажатии на кнопку открывается стандартное окно Платформы для создания и отправки сообщения. Подробное описание отправки сообщений с карточки инцидента приведено в разделе документа *"Расследование инцидента. Создание и отправка сообщения со ссылкой на инцидент"*.
- "**Показать описание**" -- при нажатии на кнопку отрывается информационное окно, содержащее описание инцидента (см. Рисунок 61). Описание содержит следующую информацию:
  - "Сводка "-- описание действия, вызвавшего инцидент;
  - "Описание угрозы";
  - "Последствия реализованной угрозы";
  - "Рекомендации по устранению угрозы";
  - "Рекомендации по уменьшению риска".

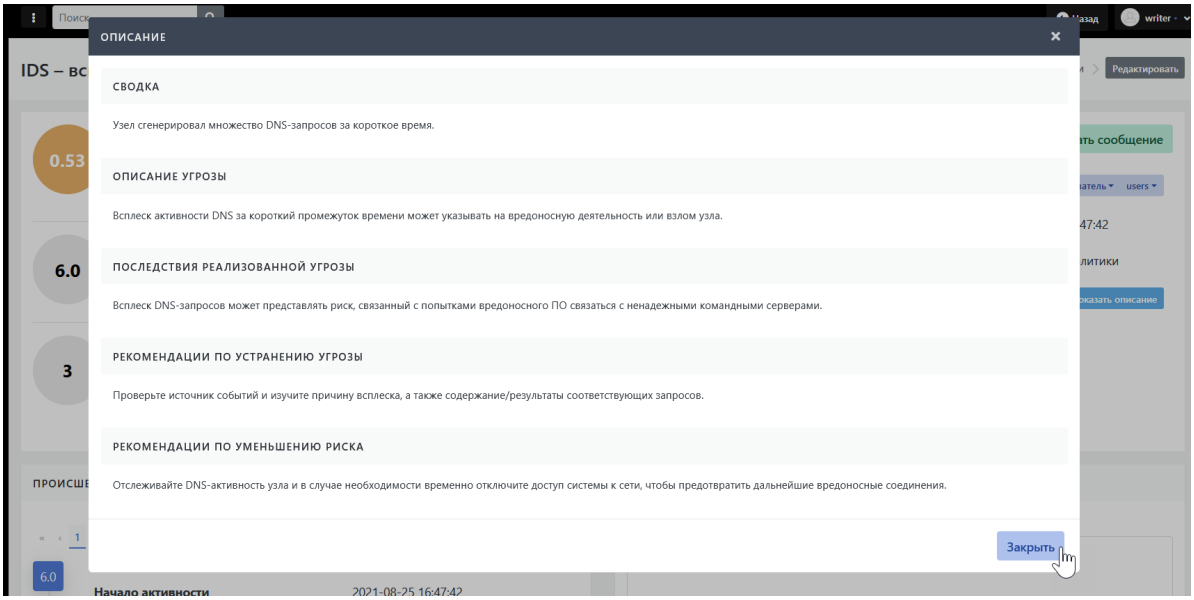


Рисунок 61 - Описание инцидента

10.4.2.3. Детализация оценок инцидента

На карточке инцидента указаны три типа оценок:

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

Оценка срочности -- верхний кружок с оценкой. 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 на кружок курсора мыши открывается список параметров, формирующих оценку срочности (см. Рисунок 62).

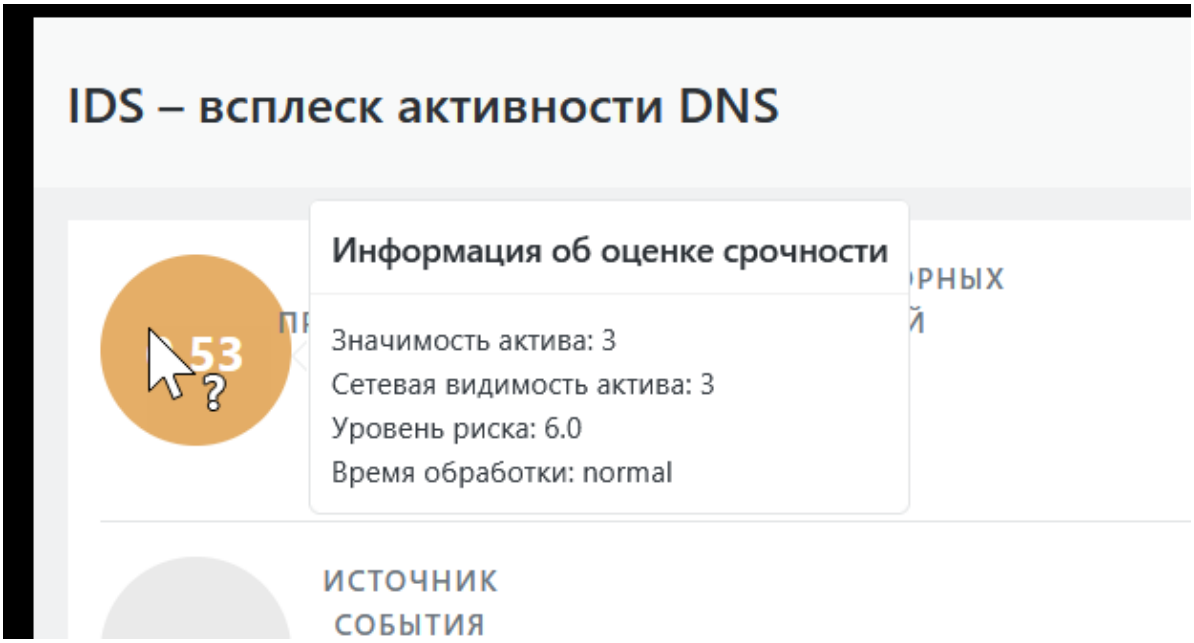


Рисунок 62 - Просмотр параметров, формирующих оценку срочности

Уровень риска (уровень значимости инцидента) -- второй кружок сверху (см. Рисунок 63). Определяет степень опасности данного типа инцидента для инфраструктуры. Значение уровня риска задается при создании типа инцидента на Платформе. Оценивается по шкале от 0 до 10.

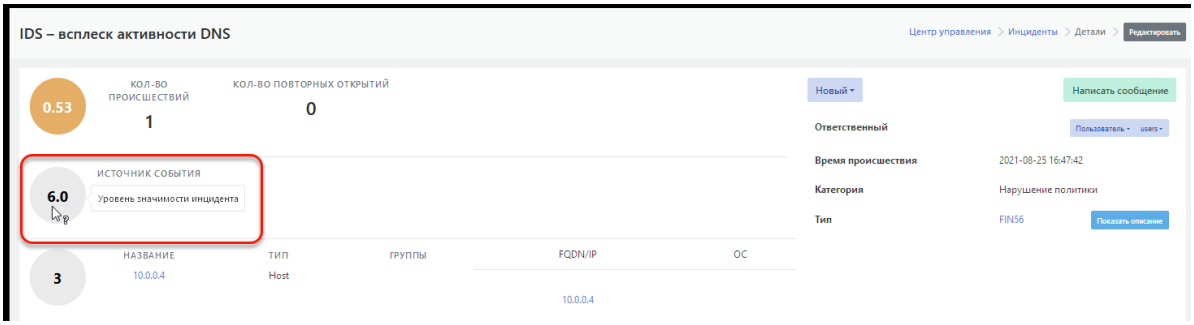


Рисунок 63 - Уровень риска для инцидента

Уровень значимости актива -- значимость актива, на котором произошел инцидент, рамках бизнес-процессов (см. Рисунок 64). Оценивается числовыми значениями от 1 до 5. Подробное описание значений приведено в приложении *"Статусы активов"*.

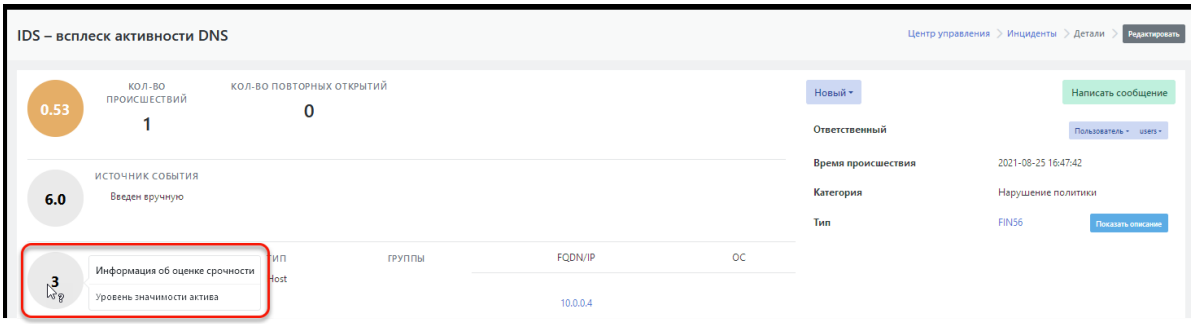


Рисунок 64 - Уровень значимости актива, на котором произошел инцидент

10.4.2.4. Блок информации "Происшествия". Общая информация

В данном блоке отображается текущий перечень происшествий, произошедших в рамках данного инцидента. 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/ неотправлено.

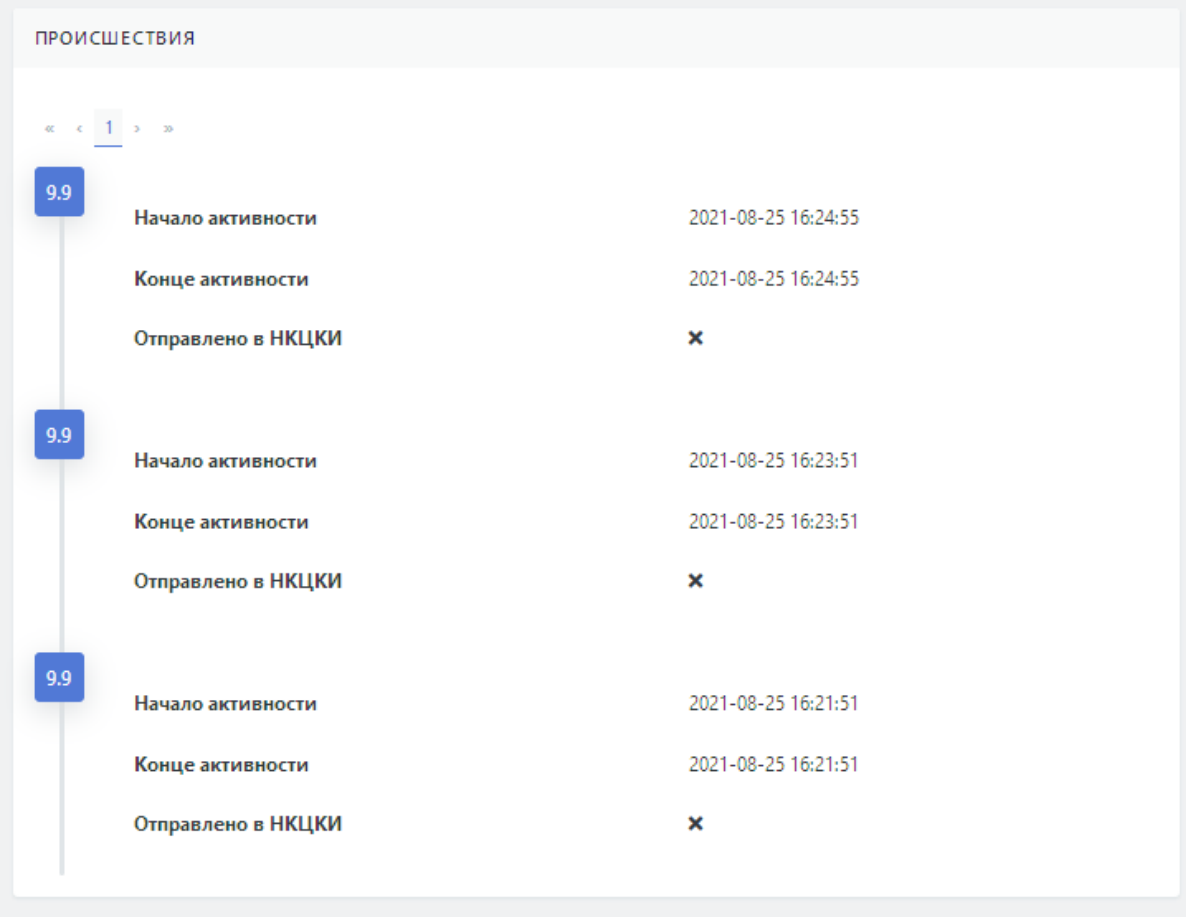


Рисунок 65 - Информация о происшествиях на карточке инцидента

10.4.2.5. Особенности просмотра 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 (по кнопке **Показать детали**, см. Рисунок 66);
  корреляции;
- уровень риска;
- правило корреляции, обнаружившее данное происшествие (по кнопке **Перейти к правилу корреляции**, см. Рисунок 66);
- идентификатор, предаваемый из правила корреляции.

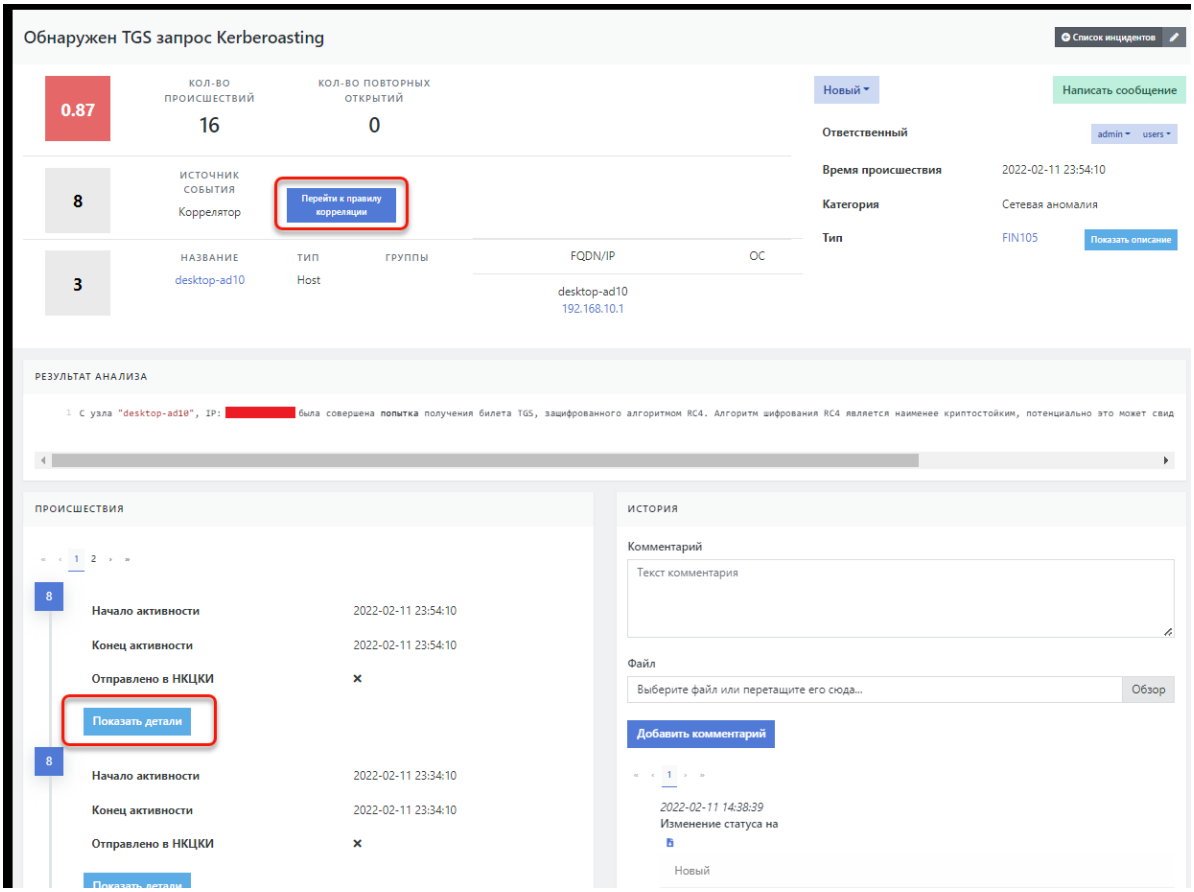


Рисунок 66 - Информация о происшествиях на карточке инцидента, обнаруженного правилами корреляции

Для происшествий, обнаруженных правилами корреляции, доступен просмотр деталей события. При нажатии кнопки **Показать детали** откроется просмотр "сырого" события в котором можно уточнить детали происшествия (см. Рисунок 67).

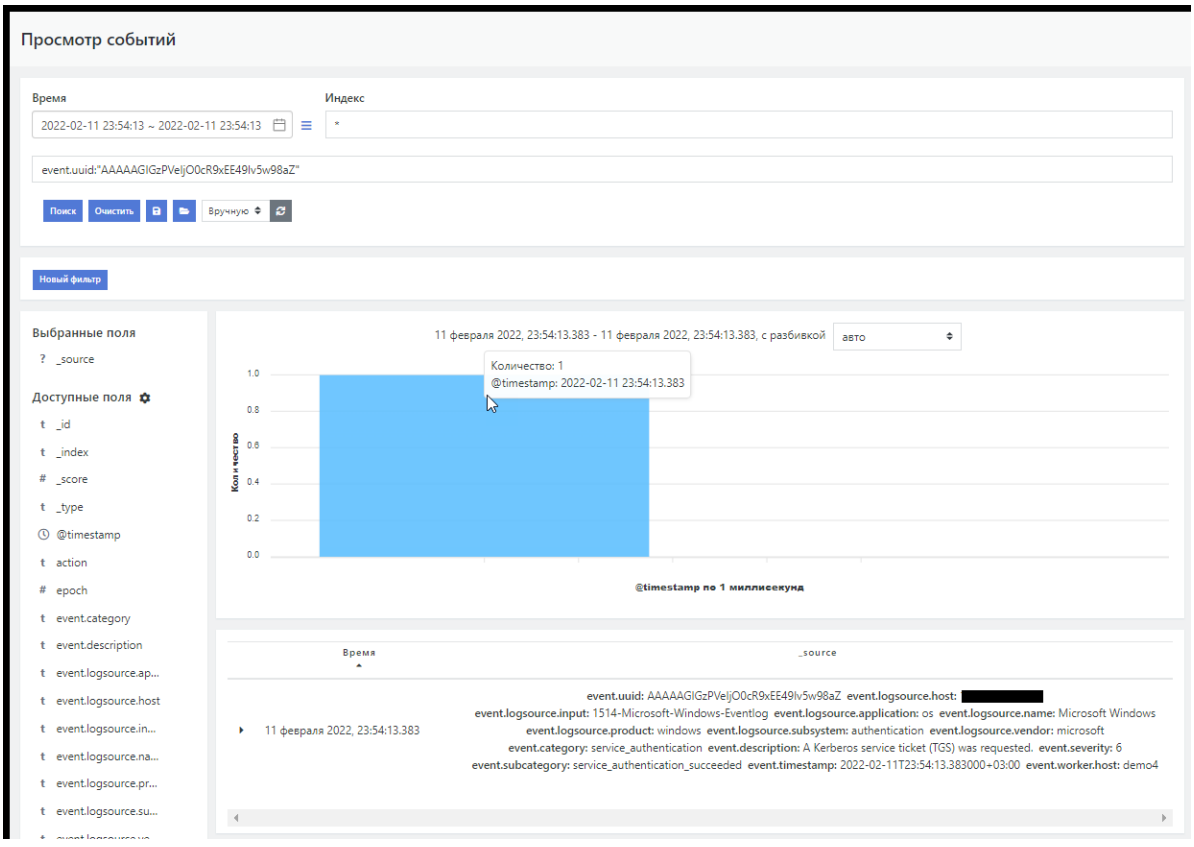


Рисунок 67 - Просмотр сырого события

10.4.2.6. Особенности просмотра происшествий, обнаруженных по результатам анализа данных сканера 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.

10.4.2.7. Блок информации "История"

В данном блоке отображается история изменения статуса данного инцидента. Для каждой смены статуса отображается (см. Рисунок 68):

- 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.

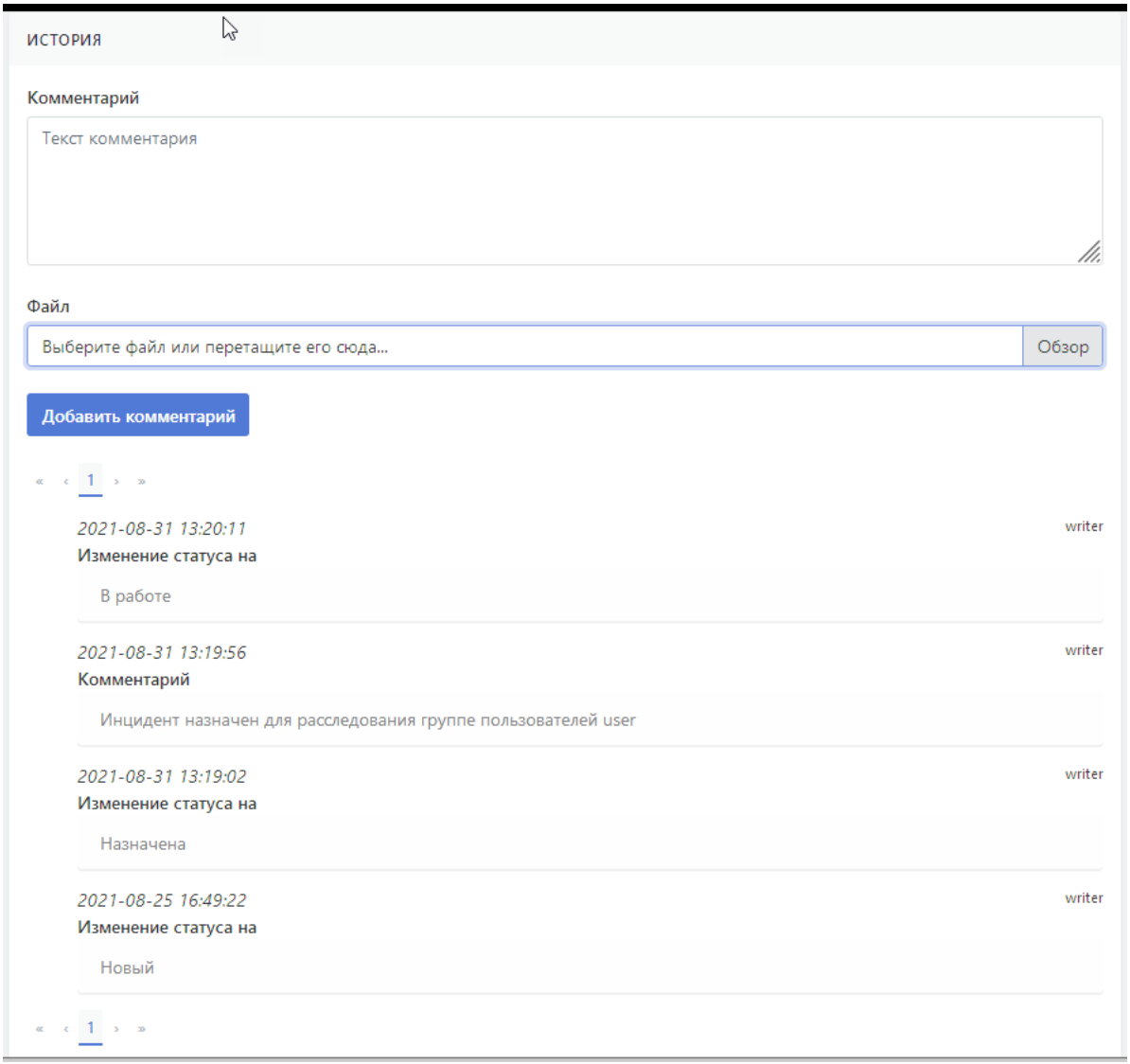


Рисунок 68 - История изменений статуса инцидента

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 69). Если к комментарию был добавлен файл, то в комментарии перед текстом комментария отобразится гиперссылка с именем файла.

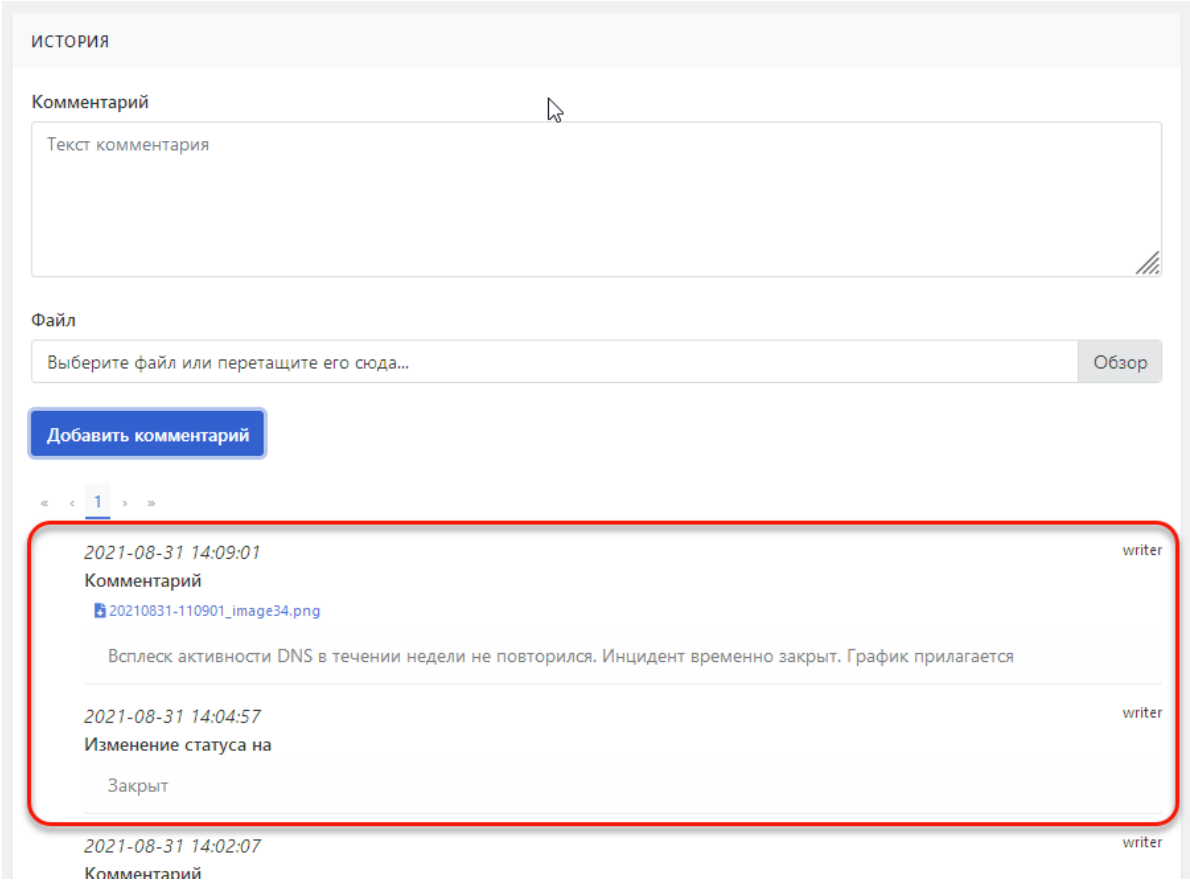


Рисунок 69 - Комментарий с добавленным файлом

10.5. Расследование инцидента

10.5.1. Алгоритм смены статусов при расследовании инцидента

В ходе расследования инцидент проходит ряд статусов, 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.

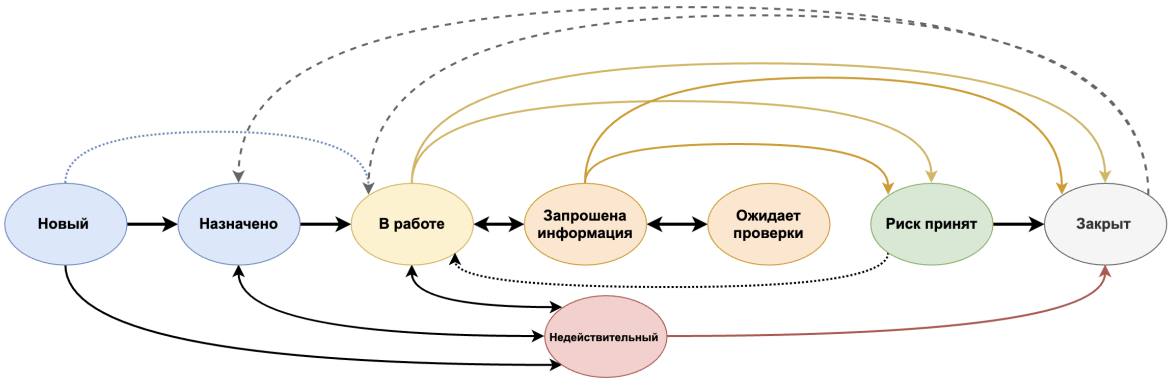


Рисунок 70 - Алгоритм смены статусов при расследовании инцидентов

В ходе расследования пользователь Платформы выполняет следующие действия над инцидентом:

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

10.5.2. Изменение статуса инцидента

10.5.2.1. 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/**.

10.5.2.2. 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 71).
3. Раскрыть список статусов и выбрать в нем новый статус (см. Рисунок 71).

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

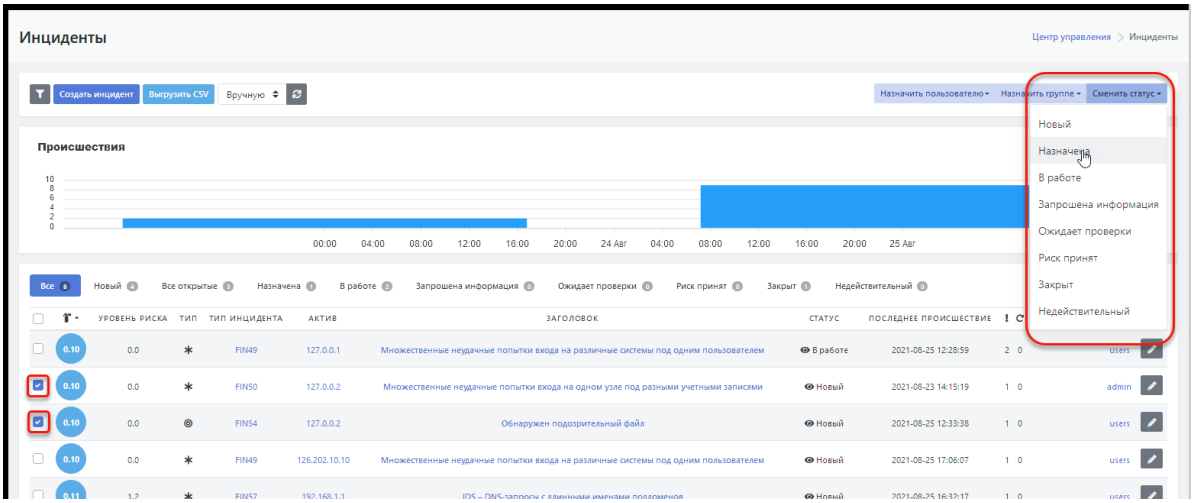


Рисунок 71 - Смена статуса инцидентов на странице списка инцидентов

10.5.2.3. 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 72).

   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 детализации инцидента. Карточка инцидента. Блок информации "История""*.

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 картинку с графиком или таблицу с данными, которые повлияли на смену статуса.

Подробное описание работы с комментариями к смене статуса приведено в разделе *"Просмотр детализации инцидента. Карточка инцидента. Блок информации "История""*.

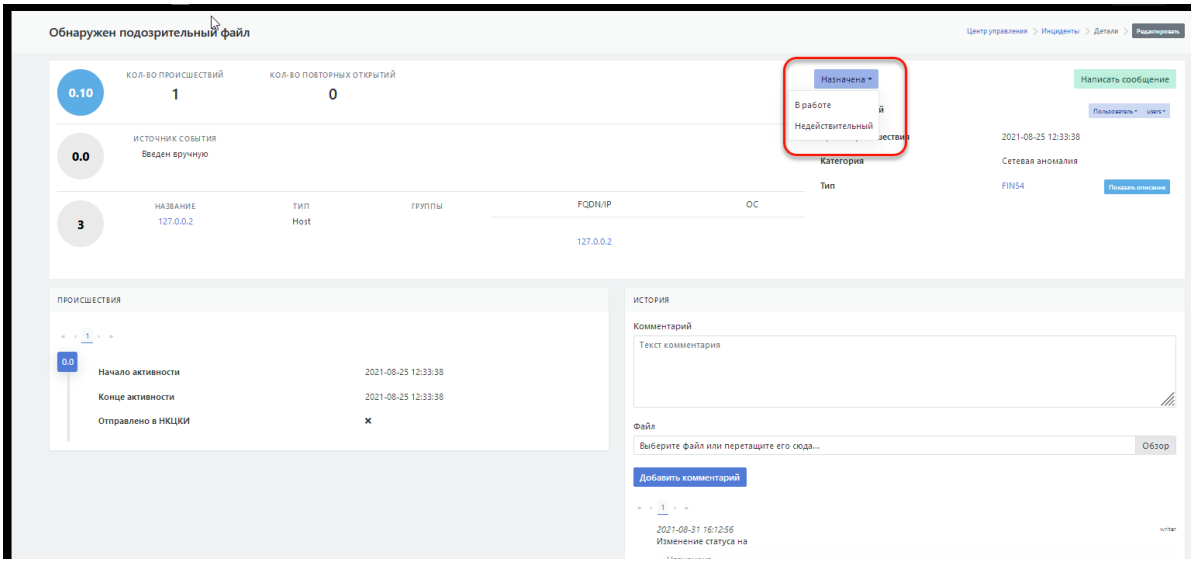


Рисунок 72 - Смена статуса на карточке инцидента

10.5.3. Назначение инцидента ответственным

10.5.3.1. 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/**..

10.5.3.2. 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 73).
3. Для назначения инцидента новому ответственному выбрать на экране функцию **"Назначить пользователю"** -- станет доступным раскрывающийся список пользователей и кнопка "**Назначить**" (см. Рисунок 66).
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 (см. выше). 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**" ().

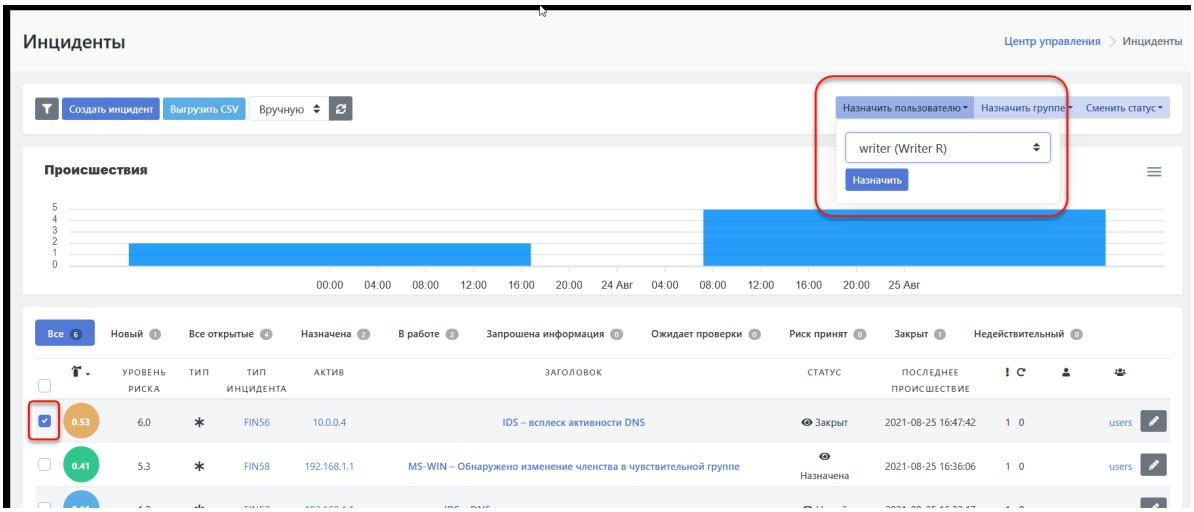


Рисунок 73 - Выбор пользователя, ответственного за инцидент

10.5.3.3. 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 74).

2. Для назначения инцидента новому пользователю выбрать функцию (слева) с именем текущего ответственного пользователя -- станет доступным раскрывающийся список пользователей и кнопка "**Назначить**" (см. Рисунок 67).
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 (см. выше). Выбирается функция с названием текущей ответственной группы. Раскрывающийся список будет содержать текущий список групп.

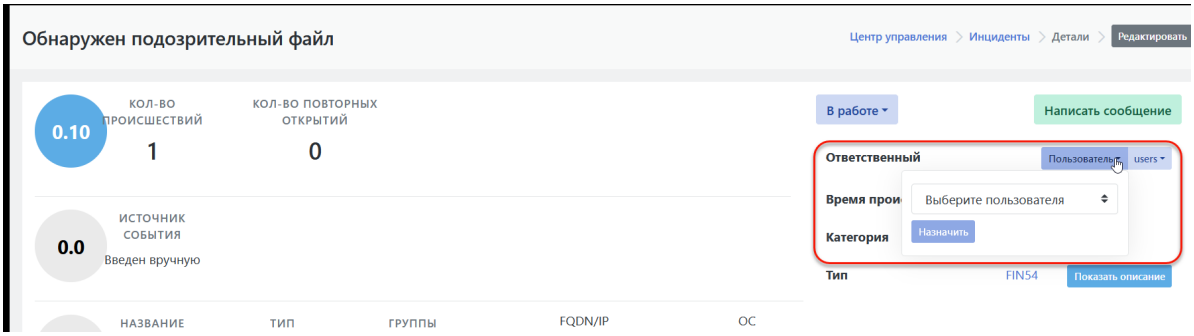


Рисунок 74 - Назначение ответственного или группы ответственных на карточке инцидента

10.5.4. Создание и отправка сообщения со ссылкой на инцидент

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

1. Открыть карточку инцидента: **"Инциденты"-> "Инциденты" -> /щелкнуть по заголовку интересующего инцидента в списке/**.
2. Нажать на кнопку **"Написать сообщение"** (см. Рисунок 67).
3. В открывшейся форме сообщения заполнить следующие поля:
    - "**Получатель**" -- выбрать адресата из раскрывающегося списка пользователей Платформы;
    - "**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 документации *"Работа с сообщениями"*.

10.5.5. Редактирование параметров инцидента

10.5.5.1. 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/**.

10.5.5.2. Перечень редактируемых параметров

В случае необходимости можно отредактировать такие параметры инцидента как:

- значение уровня риска (уровень значимости) инцидента;
- имя инцидента на Платформе;
- 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".

10.5.5.3. Проведение редактирования

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.

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. В открывшейся форме редактирования параметров инцидента внести необходимые изменения (см. Рисунок 75).
3. Для сохранения изменений нажать на кнопку "**Сохранить**".

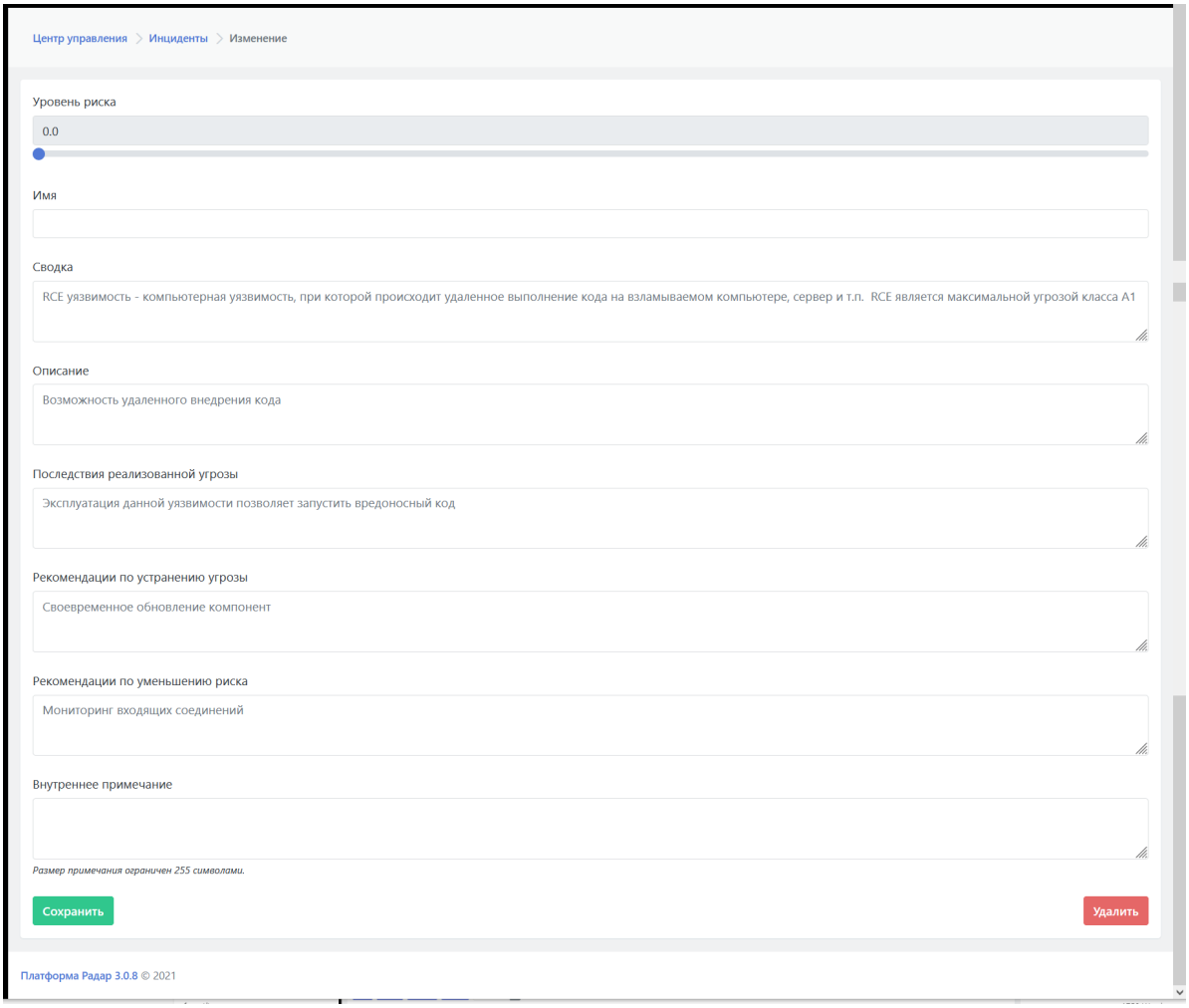


Рисунок 75 - Окно редактирования параметров

10.5.6. 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 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 75).
3. В открывшемся окне подтверждения удаления нажать на кнопку "**Ок**".

Произойдет автоматический переход к обновленному списку инцидентов.

10.5.7. Группировка инцидента

При формировании инцидента, платформа позволяет поместить инцидент в группу.
При этом система позволяет

- Поместить инцидент в уже имеющуся группу инцидентов
- Создать новую группу, из правила корреляции
- Поместить инцидент в группу в ручную

10.5.7.1. Группировка с использованием корреляций

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 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")
```

10.5.7.2. Ручное добавление в группу

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

Для создания группы инцидентов переходим в раздел **Инциденты** - **Группы инцидентов** и нажимаем кнопку "Создать"

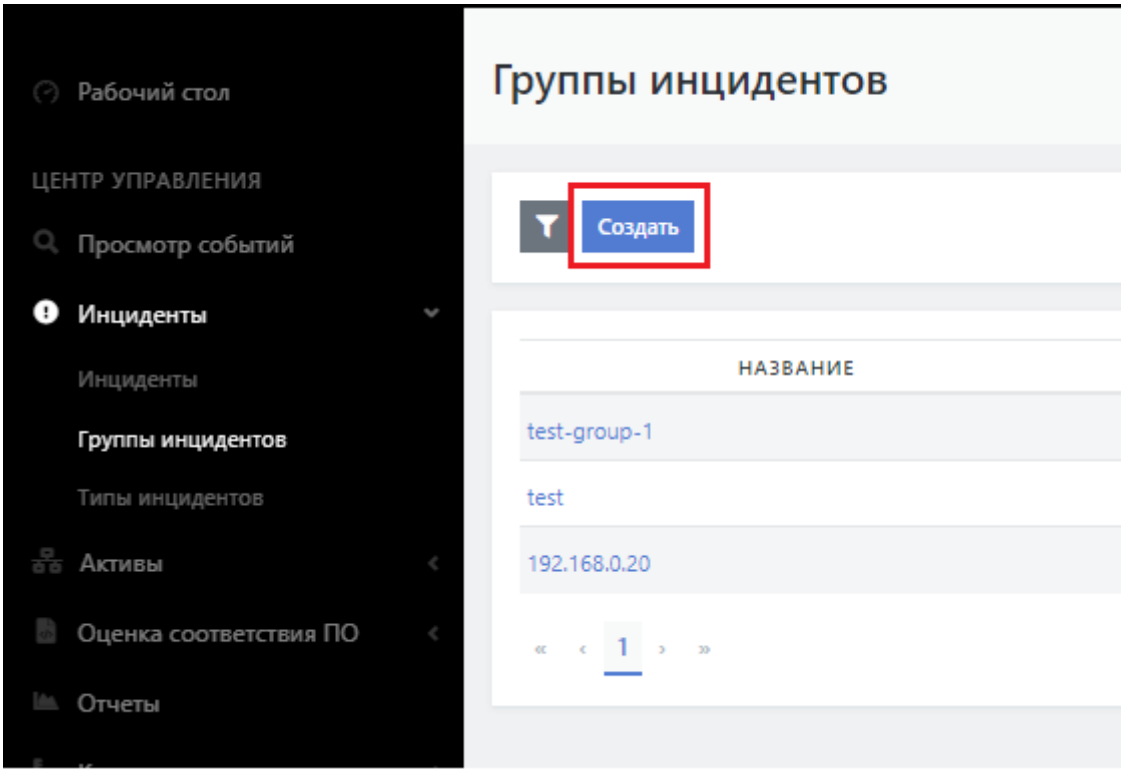


Рисунок 76

В появившейся форме указываем **Название** группы
При необходимости, указываем ОПисание, Пользователя по умолчанию или Группу пользователей по умолчанию.

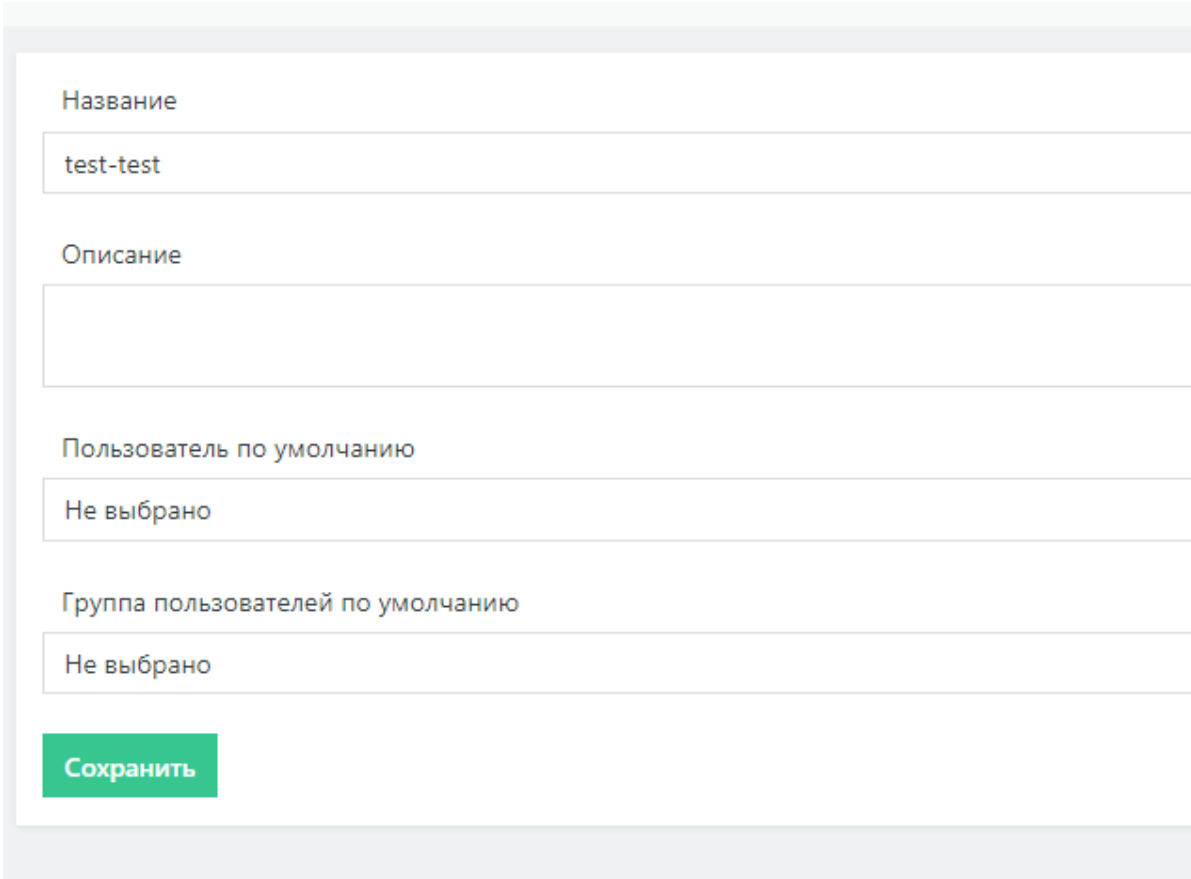


Рисунок 77

Для добавления инцидентов в группу, переходим в раздел **Инциденты** - **Инциденты**

Устанавливаем чек бокс, напротив инцидентов, которые необходимо объединить в группу.
В правом верхнем угру, нажимаем на "Объединить в группу".
В выпадающем списке выбираем необходимую группу
Нажимаем **"Назначить группу"**

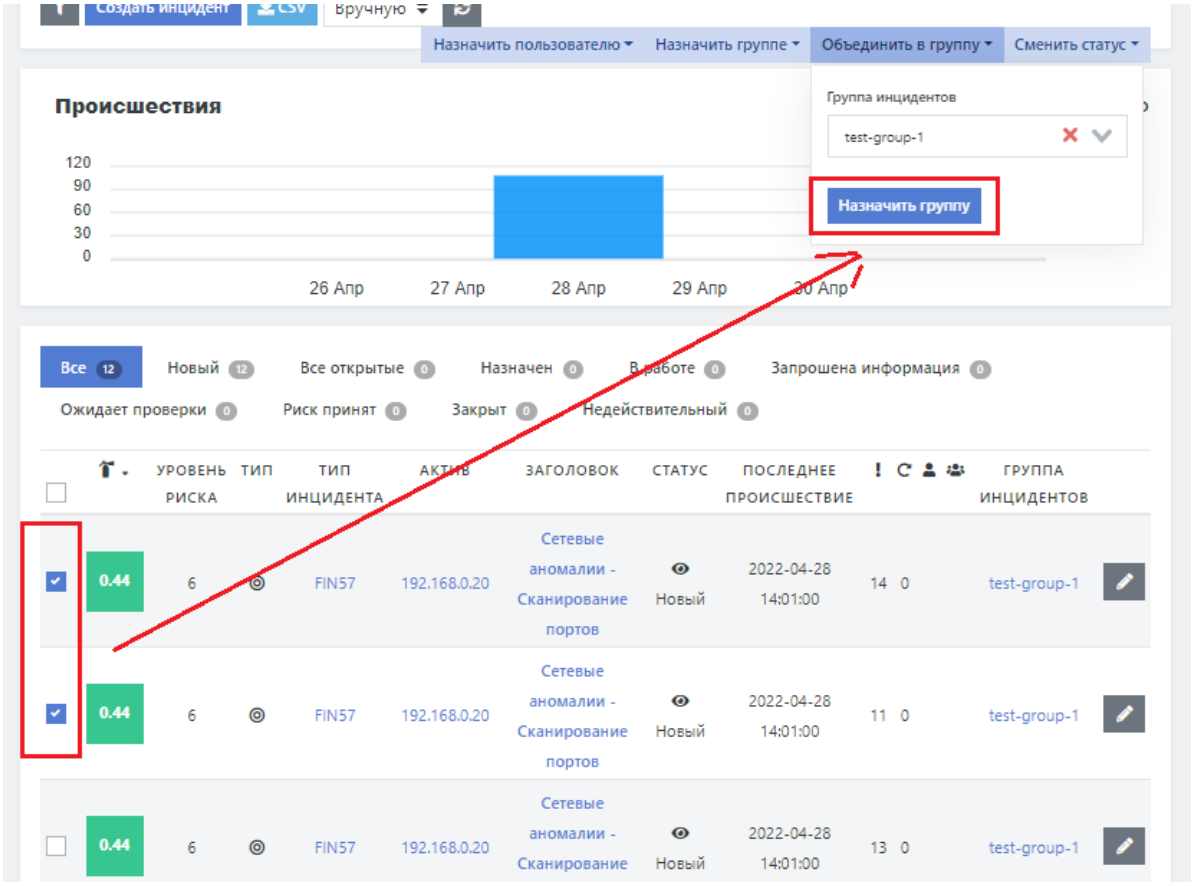


Рисунок 78

Для добавления инцидента в группу из инцидента.
Открываем инцидента на редактирование

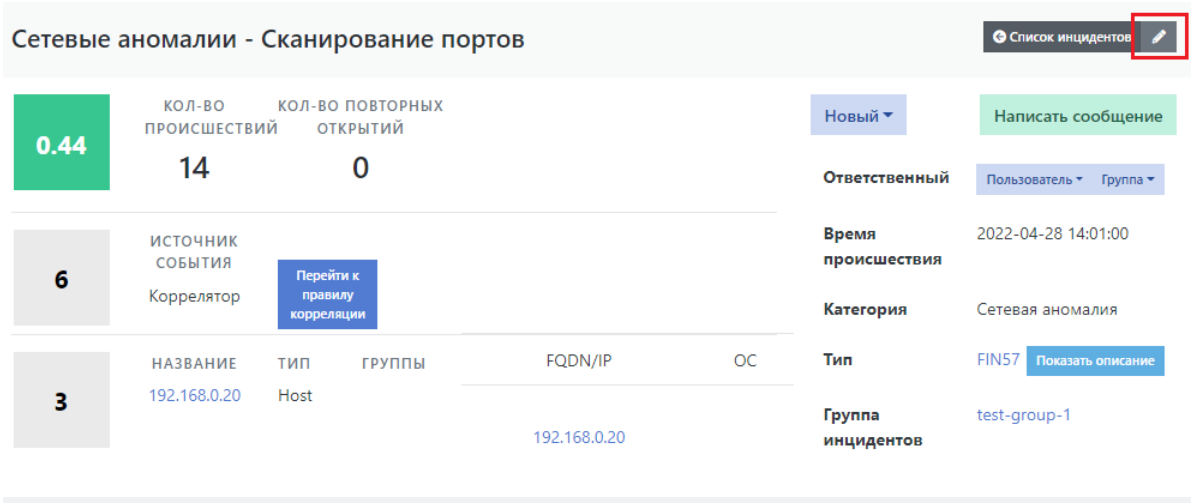


Рисунок 79

В разделе группа инцидентов выбираем необходимую группу из списка.
Нажимаем "**Сохранить**"

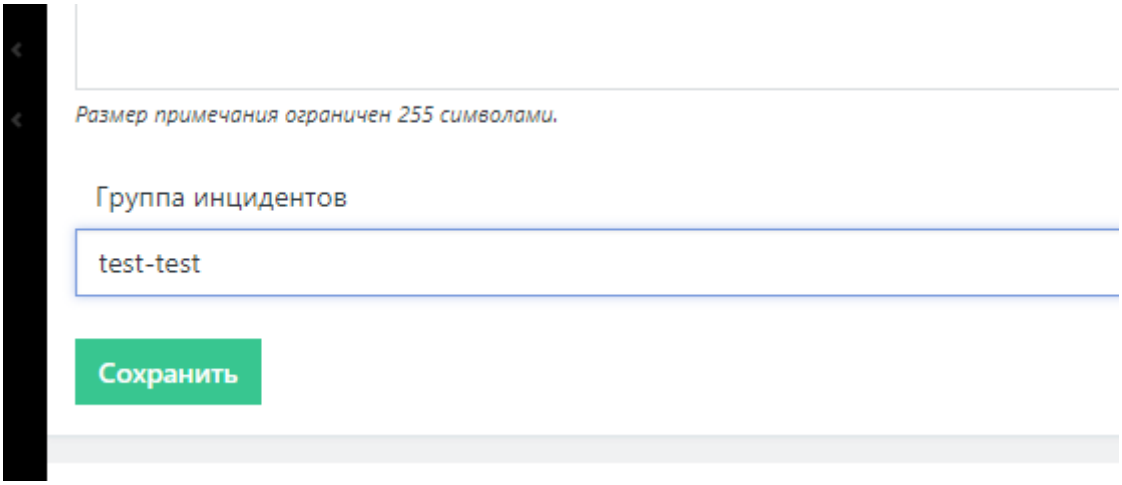


Рисунок 80

===Снимки экрана===

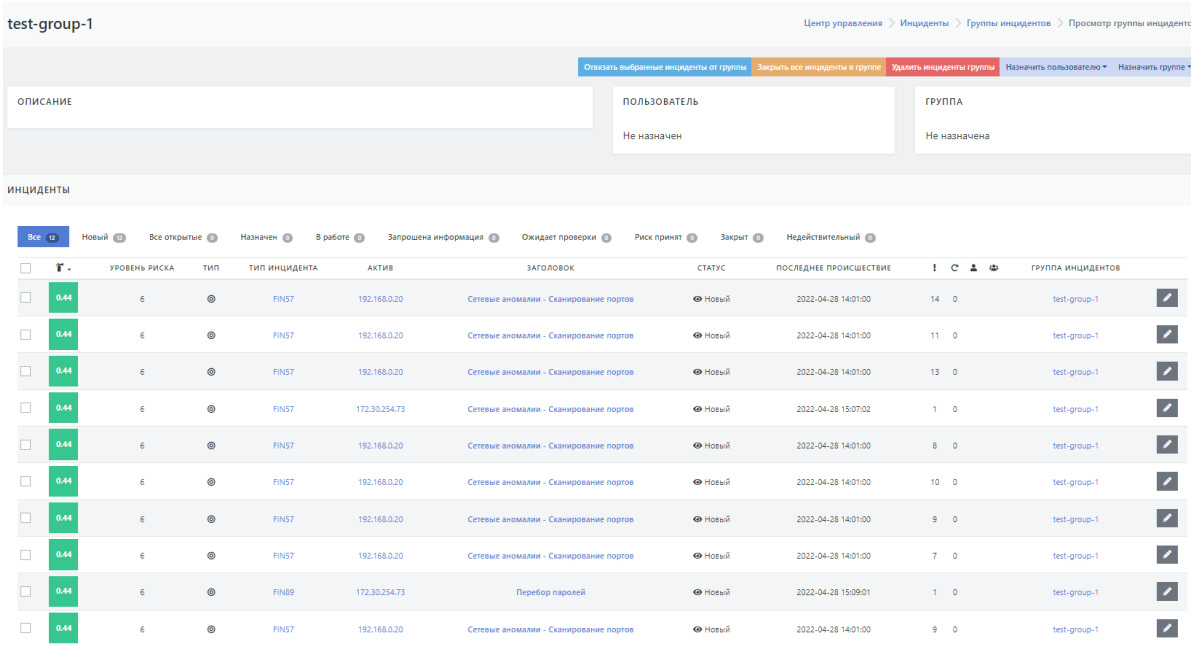


Рисунок 81

11. Поиск и фильтрация событий

Просмотрщик событий позволяет вам быстро искать и фильтровать данные и получать информацию о структуре полей. Вы можете настроить и сохранить результаты поиска и вернуться к ним позже или передать их другому пользователю.

Поиск и фильтрация осуществляется по всем полям в событиях, в том числе и по полям, добавленным пользователями.

11.1. Поиск

Сообщите Просмотрщику событий, где найти данные (выберите индекс), которые вы хотите исследовать, а затем укажите временной диапазон, в котором эти данные следует просмотреть.

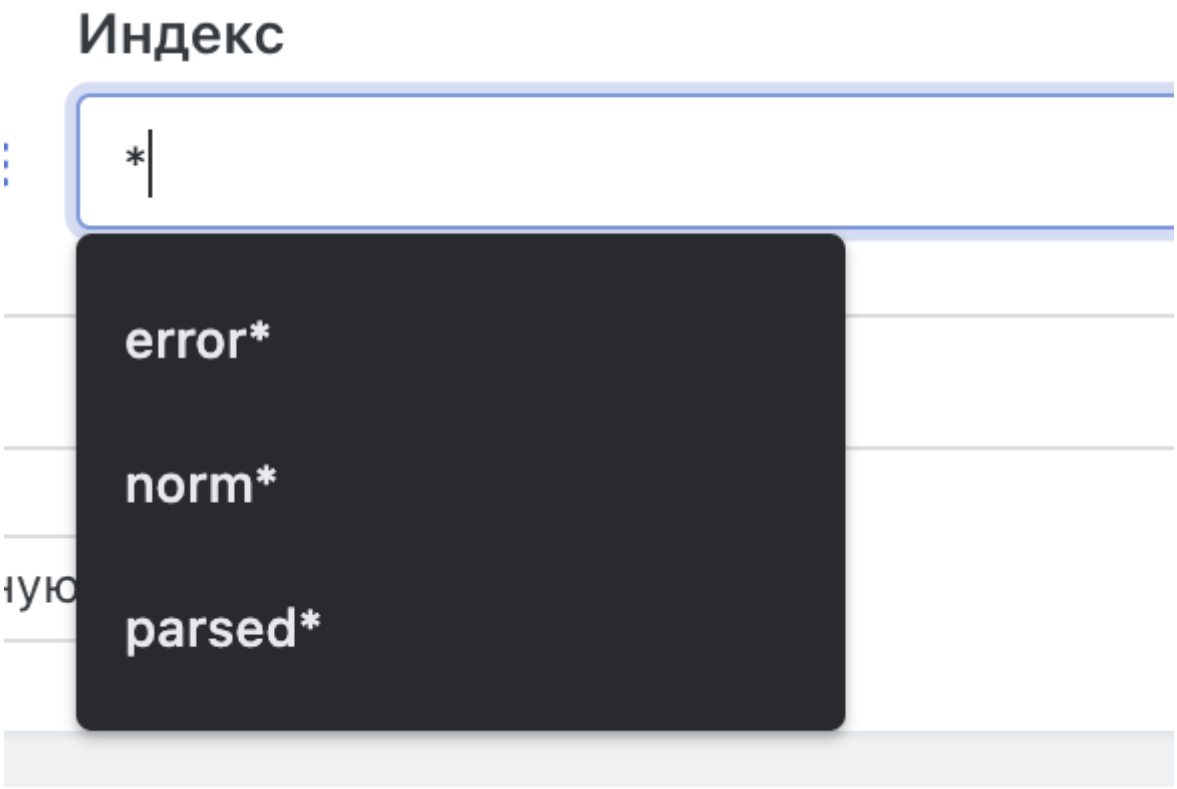


Рисунок 82

1. Откройте главное меню и выберите Инцидны/ **Просмотрщик событий**.
2. Выберите данные, с которыми хотите работать.
3. Просмотрщик событий использует шаблон индекса, чтобы указать ему, где найти данные Elasticsearch.
4. Настройте временной диапазон.

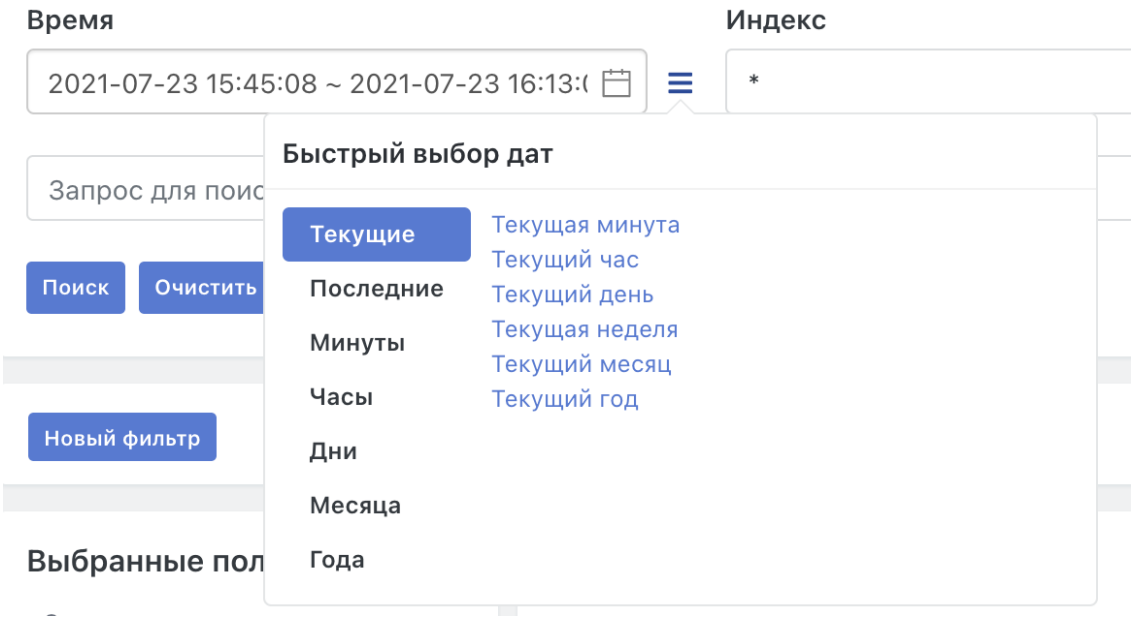


Рисунок 83

1. Выбор диапазона основан на поле времени по умолчанию в ваших данных - `@timestamp`.
2. Чтобы просмотреть количество документов за определенный период времени в указанном диапазоне, щелкните и перетащите указатель мыши на гистограмму.

Поле поиска поддерживает [стандартный синтаксис строкового поиска ElasticSearch]

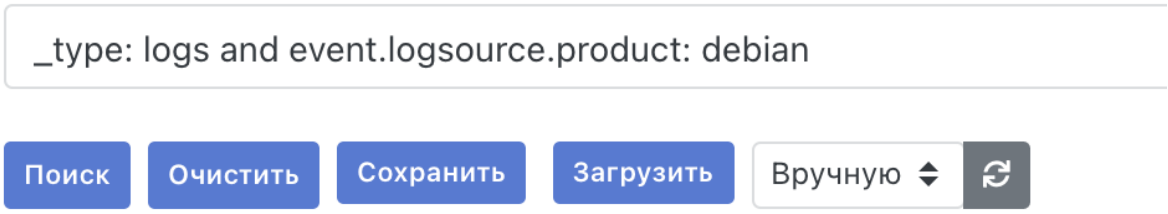


Рисунок 84

После набора запроса нажмите Enter на клавиатуре или на кнопку "Поиск" для выполнения запроса.

11.2. Представление данных

Просмотрщик событий показывает таблицу, в которой представлены все документы, соответствующие вашему запросу. По умолчанию таблица включает столбцы для поля времени и краткой сводки документа `_source`, что может быть неудобным для восприятия.

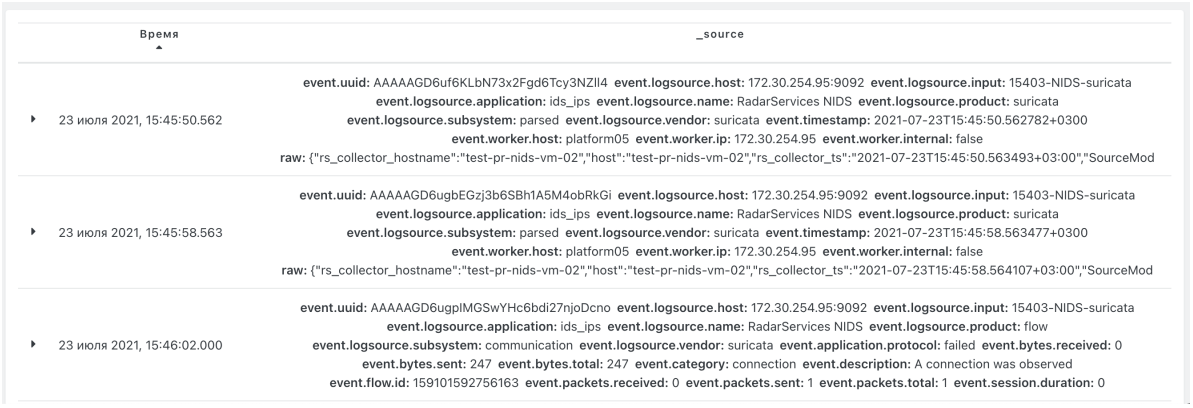


Рисунок 85

Вы можете изменить эту представление таблицы, чтобы отображались только интересующие вас поля.

1. Просмотрите список **Доступных полей**, пока не найдете интересующее поле.

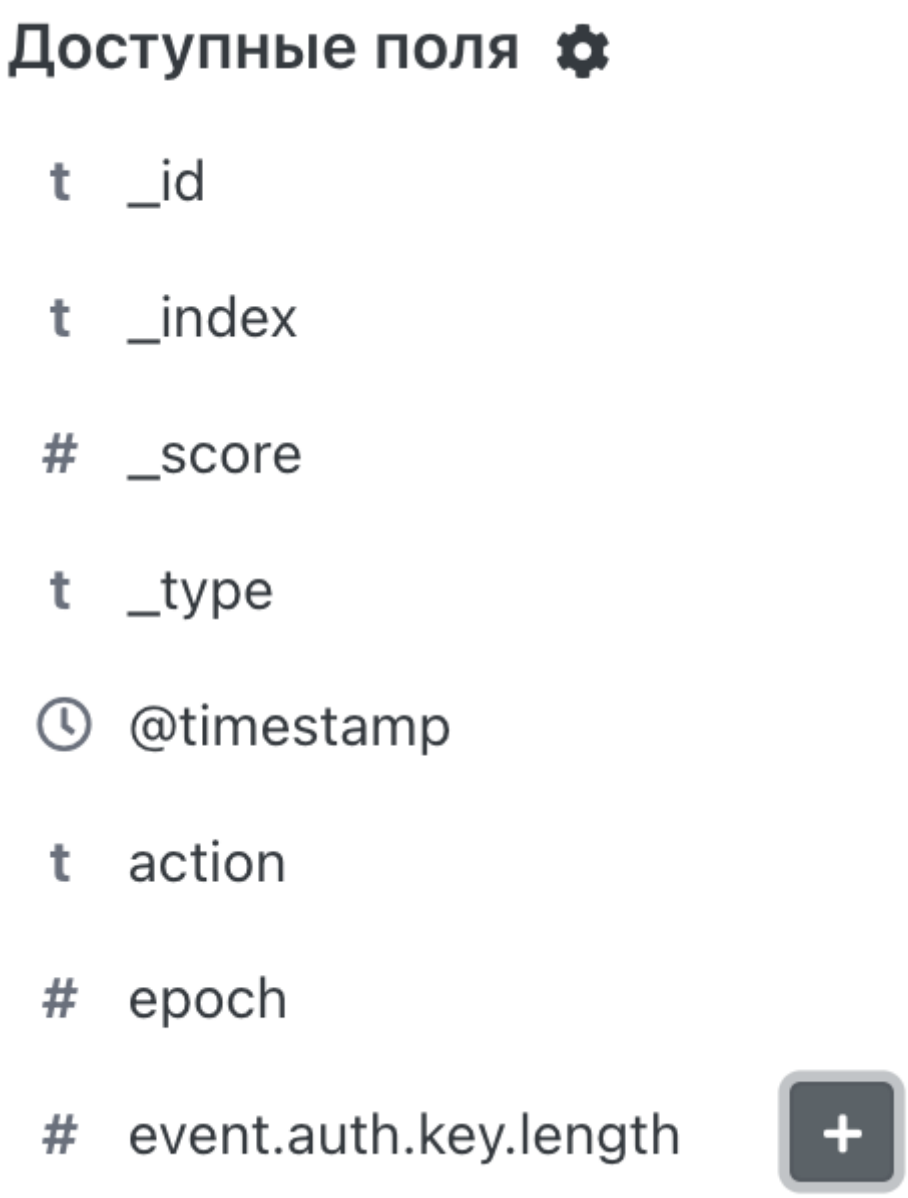


Рисунок 86

Вы также можете искать поле по имени открым раширенный поиск при клике на иконку рядом с заголовком "Доступные поля".

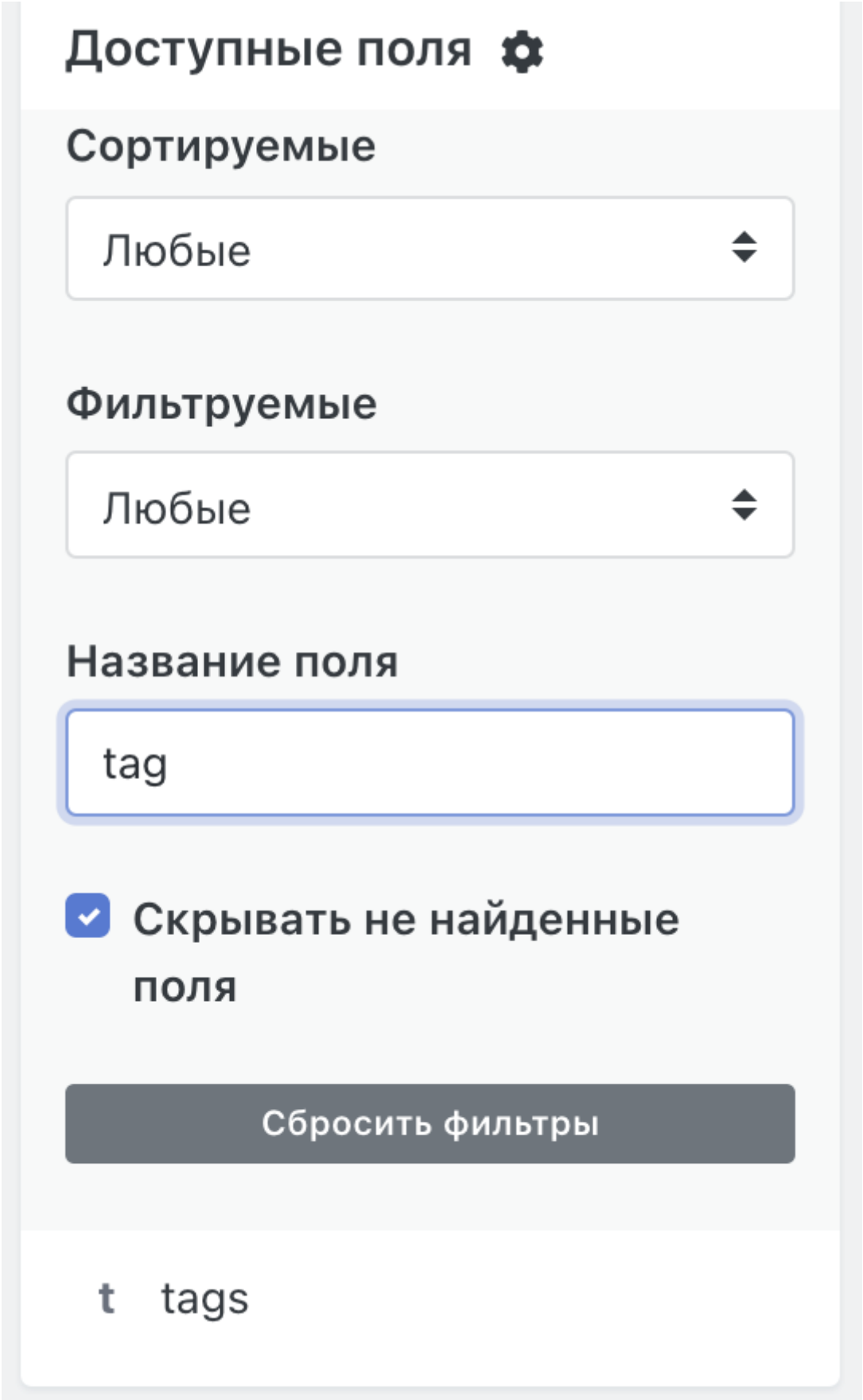


Рисунок 87

1. Щелкните на иконку с плюсом, чтобы переключить поле в таблицу документа.

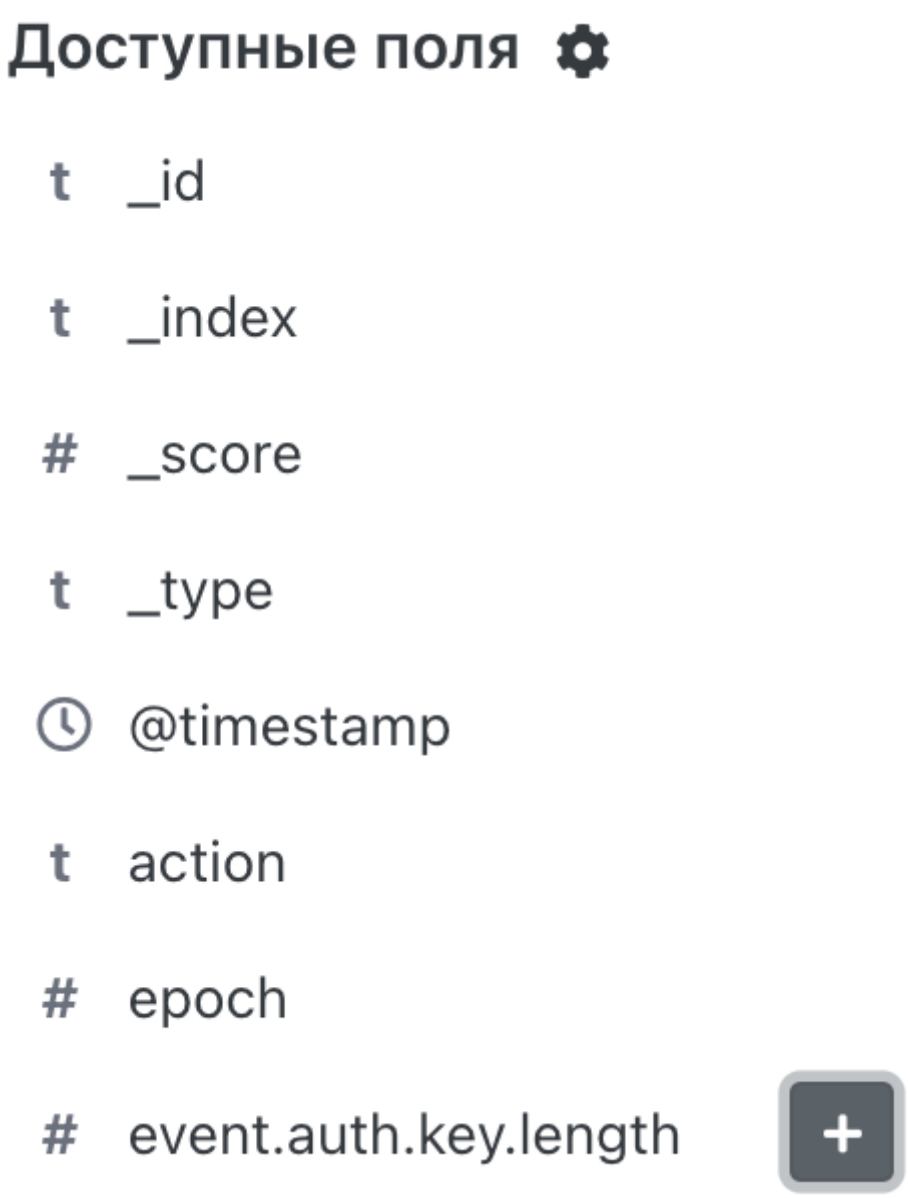


Рисунок 86

1. Чтобы изменить порядок столбцов таблицы, наведите указатель мыши на заголовок столбца и используйте элементы управления перемещением.

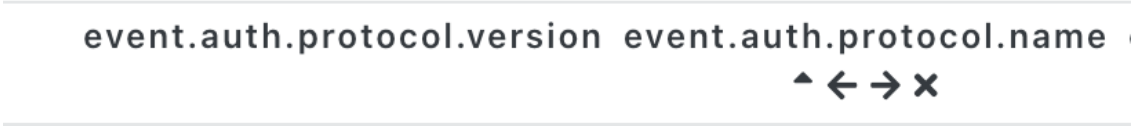


Рисунок 88

11.3. Просмотр документа

В табличном предсталении результатов поиска внезависимости от набранного кол-ва колонок или дефолтного представления доступна опция раскрытия строки с докуемнтов для его детального просмотра. Кликните на стрелочку вначале строки для открытия документа.

	Время	event.application.protocol	event.category	event.flow.id
▸	23 июля 2021, 15:45:10.559			
▸	23 июля 2021, 15:45:18.559			
▸	23 июля 2021, 15:45:26.560			
▸	23 июля 2021, 15:45:31.000	failed	connection	383625301127226
▸	23 июля 2021, 15:45:33.290		host_authentication	
▸	23 июля 2021, 15:45:33.290		privileges	
▸	23 июля 2021, 15:45:34.561			
▸	23 июля 2021, 15:45:36.461		host_authentication	
▸	23 июля 2021, 15:45:36.461		privileges	
▸	23 июля 2021, 15:45:36.462			

Рисунок 89

Внутри карточки документа доступны вкладки просмотра ввиде табличного представления

Найти инциденты

Таблица | JSON

@timestamp	2021-07-23T15:45:50.562782+03:00
_id	AAAAAGD6uf6KLbN73x2Fgd6Tcy3NZIl4
_index	parsed_suricata.suricata.ids_ips.parsed-3.14.0-3.11.0-2021.07.23
_score	
_type	logs
epoch	1627044350.562782
event.logsource.application	ids_ips
event.logsource.host	172.30.254.95:9092
event.logsource.input	15403-NIDS-suricata
event.logsource.name	RadarServices NIDS
event.logsource.product	suricata
event.logsource.subsystem	parsed
event.logsource.vendor	suricata
event.timestamp	2021-07-23T15:45:50.562782+0300
event.uuid	AAAAAGD6uf6KLbN73x2Fgd6Tcy3NZIl4
event.worker.host	platform05
event.worker.internal	false
event.worker.ip	172.30.254.95

Рисунок 90

и ввиде json документа


```
{
    "event": {
        "uuid": "AAAAAGD6uf6KLbN73x2Fgd6Tcy3NZll4",
        "logsource": {
            "host": "172.30.254.95:9092",
            "input": "15403-NIDS-suricata",
            "application": "ids_ips",
            "name": "RadarServices NIDS",
            "product": "suricata",
            "subsystem": "parsed",
            "vendor": "suricata"
        },
        "timestamp": "2021-07-23T15:45:50.562782+0300",
        "worker": {
            "host": "platform05",
            "ip": "172.30.254.95",
            "internal": false
        },
        "blacklist": {}
    },
    "raw": "{\"rs_collector_hostname\":\"test-pr-nids-vm-02\",\"host\":\"test-pr-nids-vm-02\",\"rs_collector_ts\":\"2021-07-23T15:45:50.563493+03:00\"
        ,\"SourceModuleName\":\"imfile\",\"message\":\"{\\\"timestamp\\\":\\\"2021-07-23T15:45:50.562782+0300\\\",\\\"event_type\\\":\\\"stats\\\",\\\"stats\\\"
        :{\\\"uptime\\\":1541474,\\\"capture\\\":{\\\"kernel_packets\\\":6554738,\\\"kernel_packets_delta\\\":24,\\\"kernel_drops\\\":0,\\\"kernel_drops_delta\\\":0
        ,\\\"errors\\\":0,\\\"errors_delta\\\":0},\\\"decoder\\\":{\\\"pkts\\\":6554732,\\\"pkts_delta\\\":24,\\\"bytes\\\":1978221000,\\\"bytes_delta\\\":13701
        ,\\\"invalid\\\":0,\\\"invalid_delta\\\":0,\\\"ipv4\\\":3429296,\\\"ipv4_delta\\\":24,\\\"ipv6\\\":431,\\\"ipv6_delta\\\":0,\\\"ethernet\\\":6554732
        ,\\\"ethernet_delta\\\":24,\\\"raw\\\":0,\\\"raw_delta\\\":0,\\\"null\\\":0,\\\"null_delta\\\":0,\\\"sll\\\":0,\\\"sll_delta\\\":0,\\\"tcp\\\":2338788
        ,\\\"tcp_delta\\\":18,\\\"udp\\\":1073497,\\\"udp_delta\\\":6,\\\"sctp\\\":0,\\\"sctp_delta\\\":0,\\\"icmpv4\\\":905,\\\"icmpv4_delta\\\":0,\\\"icmpv6\\\":431
        ,\\\"icmpv6_delta\\\":0,\\\"ppp\\\":0,\\\"ppp_delta\\\":0,\\\"pppoe\\\":0,\\\"pppoe_delta\\\":0,\\\"gre\\\":0,\\\"gre_delta\\\":0,\\\"vlan\\\":0
        ,\\\"vlan_delta\\\":0,\\\"vlan_qinq\\\":0,\\\"vlan_qinq_delta\\\":0,\\\"vxlan\\\":0,\\\"vxlan_delta\\\":0,\\\"ieee8021ah\\\":0,\\\"ieee8021ah_delta\\\":0
        ,\\\"teredo\\\":0,\\\"teredo_delta\\\":0,\\\"ipv4_in_ipv6\\\":0,\\\"ipv4_in_ipv6_delta\\\":0,\\\"ipv6_in_ipv6\\\":0,\\\"ipv6_in_ipv6_delta\\\":0,\\\"mpls\\\":0
        ,\\\"mpls_delta\\\":0,\\\"avg_pkt_size\\\":301,\\\"avg_pkt_size_delta\\\":0,\\\"max_pkt_size\\\":1514,\\\"max_pkt_size_delta\\\":0,\\\"erspan\\\":0
        ,\\\"erspan_delta\\\":0,\\\"event\\\":{\\\"ipv4\\\":{\\\"pkt_too_small\\\":0,\\\"pkt_too_small_delta\\\":0,\\\"hlen_too_small\\\":0,\\\"hlen_too_small_delta\\\":0
        ,\\\"iplen_smaller_than_hlen\\\":0,\\\"iplen_smaller_than_hlen_delta\\\":0,\\\"trunc_pkt\\\":0,\\\"trunc_pkt_delta\\\":0,\\\"opt_invalid\\\":0
        ,\\\"opt_invalid_delta\\\":0,\\\"opt_invalid_len\\\":0,\\\"opt_invalid_len_delta\\\":0,\\\"opt_malformed\\\":0,\\\"opt_malformed_delta\\\":0
        ,\\\"opt_pad_required\\\":15,\\\"opt_pad_required_delta\\\":0,\\\"opt_eol_required\\\":0,\\\"opt_eol_required_delta\\\":0,\\\"opt_duplicate\\\":0
        ,\\\"opt_duplicate_delta\\\":0,\\\"opt_unknown\\\":0,\\\"opt_unknown_delta\\\":0,\\\"wrong_ip_version\\\":0,\\\"wrong_ip_version_delta\\\":0,\\\"icmpv6\\\":0
        ,\\\"icmpv6_delta\\\":0,\\\"frag_pkt_too_large\\\":0,\\\"frag_pkt_too_large_delta\\\":0,\\\"frag_overlap\\\":0,\\\"frag_overlap_delta\\\":0,\\\"frag_ignored\\\":0
        ,\\\"frag_ignored_delta\\\":0},\\\"icmpv4\\\":{\\\"pkt_too_small\\\":0,\\\"pkt_too_small_delta\\\":0,\\\"unknown_type\\\":0,\\\"unknown_type_delta\\\":0
        ,\\\"unknown_code\\\":0,\\\"unknown_code_delta\\\":0,\\\"ipv4_trunc_pkt\\\":0,\\\"ipv4_trunc_pkt_delta\\\":0,\\\"ipv4_unknown_ver\\\":0
        ,\\\"ipv4_unknown_ver_delta\\\":0},\\\"icmpv6\\\":{\\\"unknown_type\\\":0,\\\"unknown_type_delta\\\":0,\\\"unknown_code\\\":0,\\\"unknown_code_delta\\\":0
        ,\\\"pkt_too_small\\\":0,\\\"pkt_too_small_delta\\\":0,\\\"ipv6_unknown_version\\\":0,\\\"ipv6_unknown_version_delta\\\":0,\\\"ipv6_trunc_pkt\\\":0
```


Рисунок 91

Платформа отображает информацию о значениях всех полей события, в том числе полей, добавленных пользователем.

11.4. Фильтрация

Для создания фильтра можно воспользоваться функционалом создания фильтра расположенного ниже строки поиска, либо добавить к фильтрации значение поля напрямую из карточки представления документа.

Время	event.application.protocol	event.category	event.flow.id
23 июля 2021, 15:45:10.559			
23 июля 2021, 15:45:18.559			
23 июля 2021, 15:45:26.560			
23 июля 2021, 15:45:31.000	failed	connection	383625301127226
23 июля 2021, 15:45:33.290		host_authentication	
23 июля 2021, 15:45:33.290		privileges	
23 июля 2021, 15:45:34.561			
23 июля 2021, 15:45:36.461		host_authentication	
23 июля 2021, 15:45:36.461		privileges	
23 июля 2021, 15:45:36.462			

Рисунок 89

11.4.1. Создание фильтра

1. Нажмите на кнопку "Новый фильтр"
2. В открывшемся окне выберите поле, вид фильтрации и значение, укажите ниже заголовок фильтра и нажмите кнопку "Добавить"

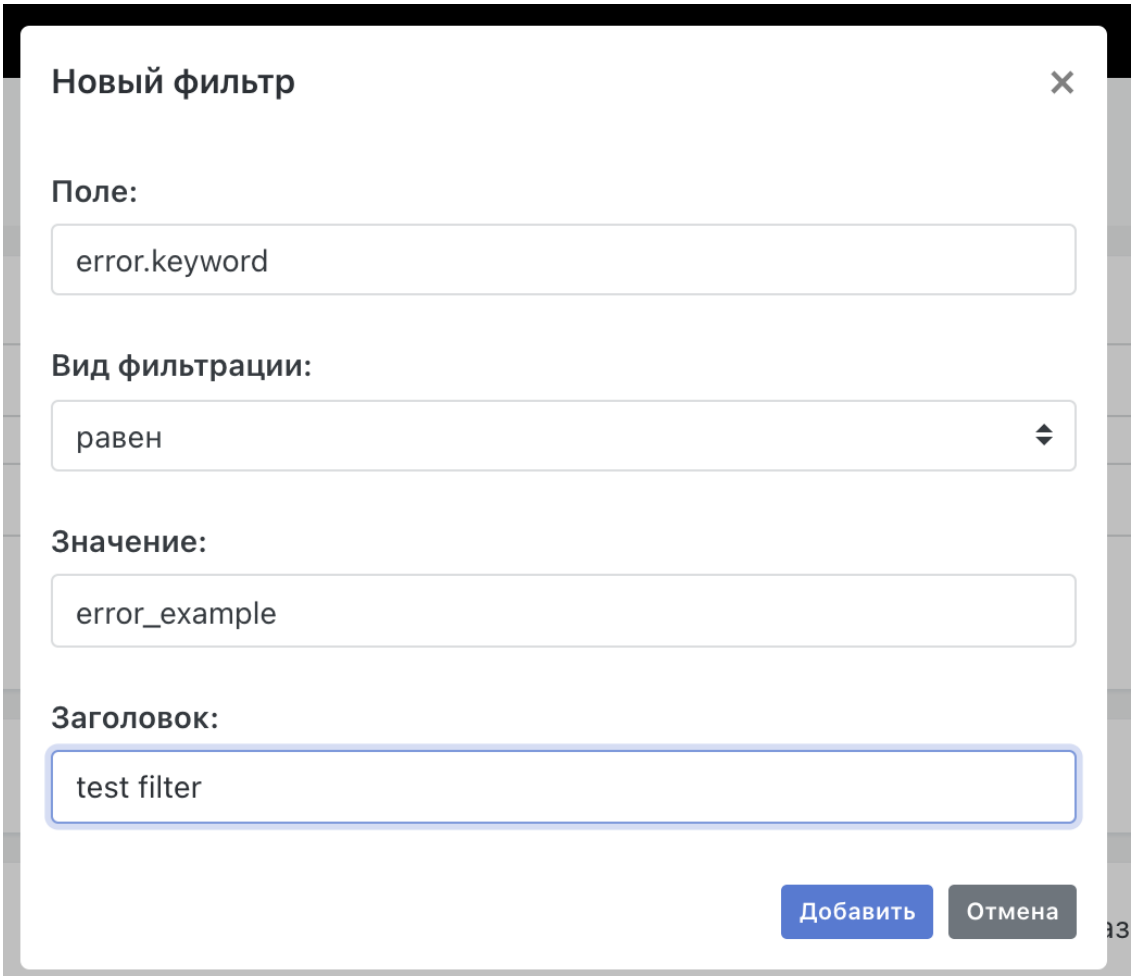


Рисунок 92

3. После добавления фильтра станет доступна опция работы с фильтром

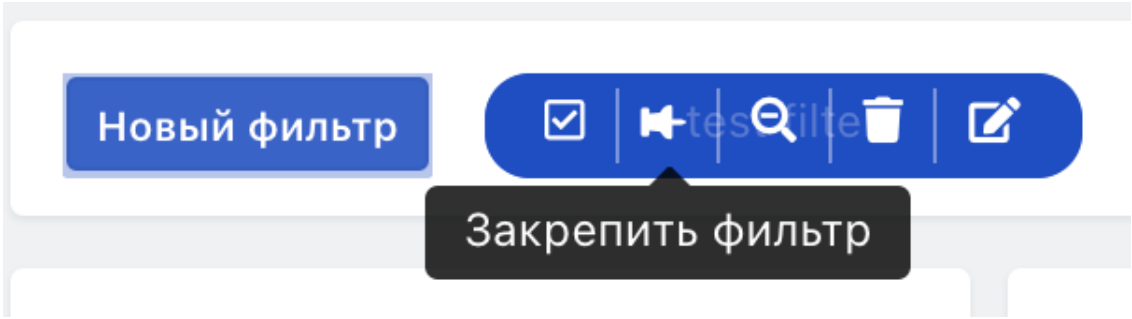
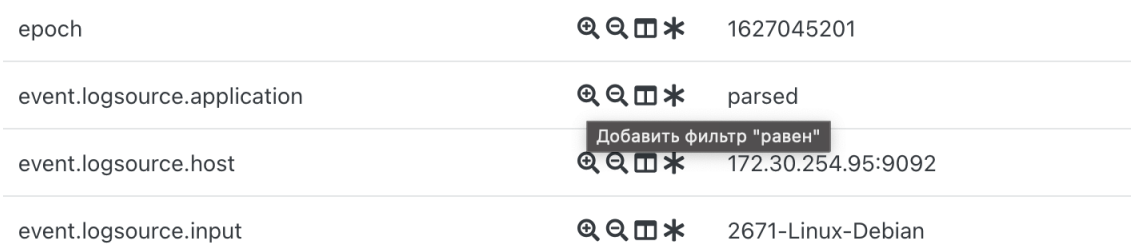


Рисунок 93

- Быстрое включение/выключение фильтра
- Закрепление фильтра
- Исключение фильтра
- Удаление фильтра
- Изменение фильтра

11.4.2. Создание быстрого фильтра

1. В карточке просмотра документа кликните на иконку с лупой и знаком плюс для добавления фильтра с равенством значения выбранного поля значению в просматриваемом документе



2. Лупа со знаком минус создает фильтр на выбранное поле с не равенством значения выбранного значения просматриваемого документа
3. После нажатия на иконку будет создан фильтр также как и при ручном создании

12. Работа с просмотрщиком событий

12.1. Общие данные

Внимание! Подраздел **"Инциденты"**-> "**Просмотр событий**" доступен только пользователям с соответствующими правами на просмотр событий.

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

12.2. Первичная настройка вывода событий на экран

12.2.1. 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 раздел *"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 94). Так же на экране отобразится список описаний по каждому найденному событию.

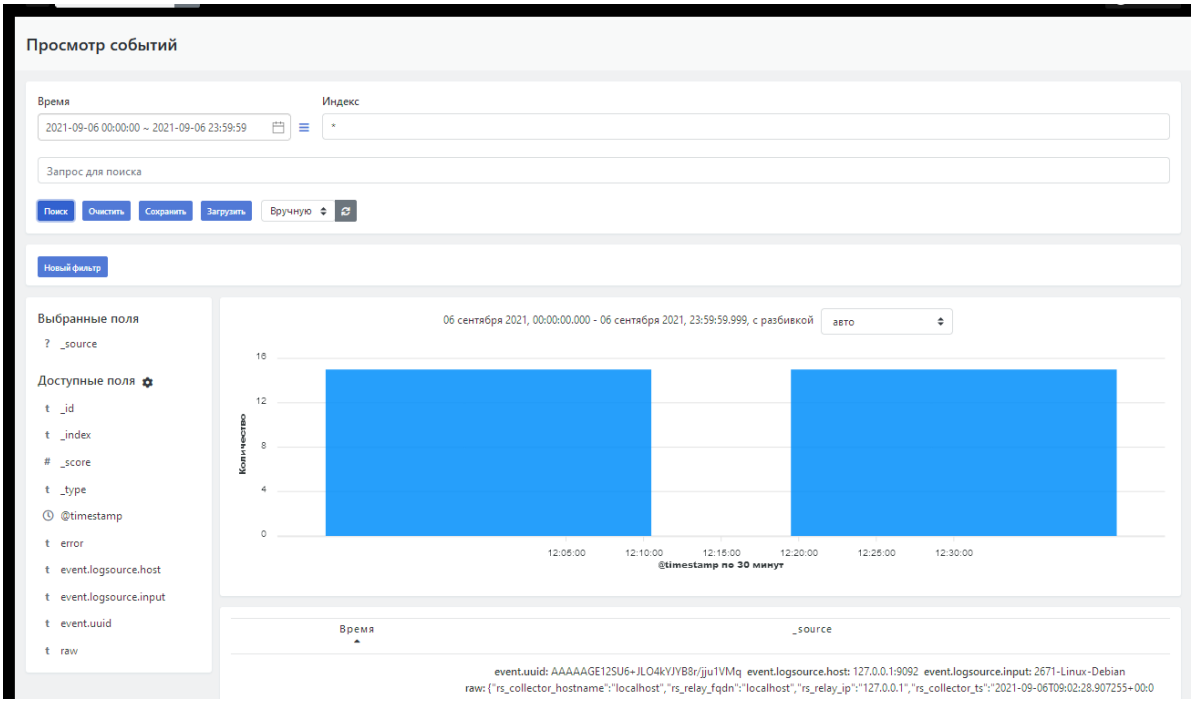


Рисунок 94 - Результат поиска событий по заданным параметрам

12.2.2. Сброс, сохранение, загрузка фильтров 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**".

12.2.3. 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 95).

Рисунок 95 - Настройка обновления данных

12.2.4. Особенности выбора временного интервала

12.2.4.1. Быстрый выбор дат

Просмотрщик 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 96):

- "**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 временных интервалов*").
- "**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.

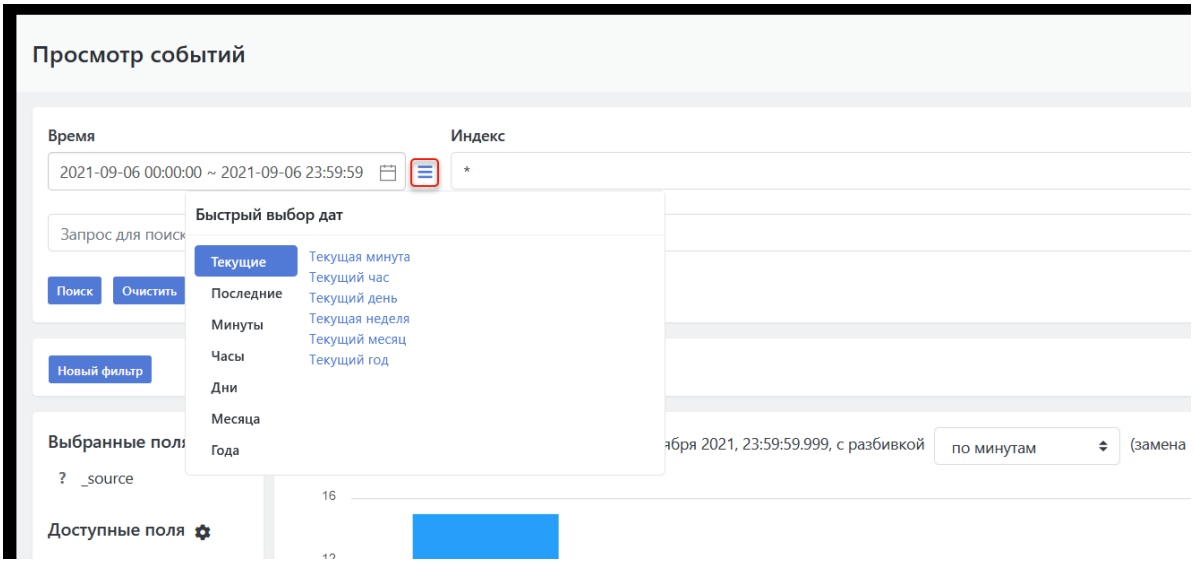


Рисунок 96 - Выбор предустановленного временного интервала для поиска событий

12.2.4.2. 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 начал и дату конца временного диапазона (см. Рисунок 97). Если необходимо указать один день, то два раза щелкнуть по нужному дню.

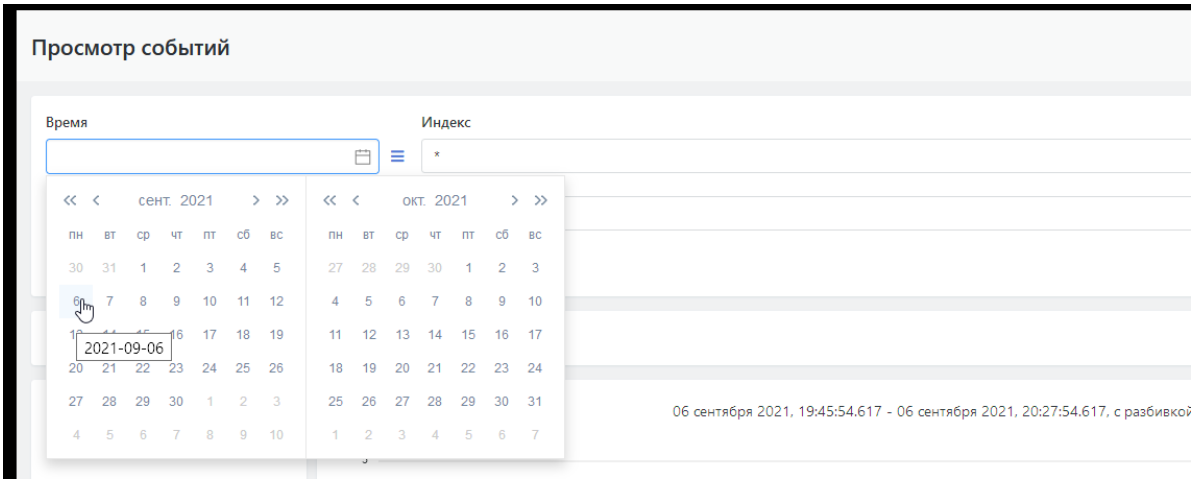


Рисунок 97 - Установка дат начала и конца временного интервала для поиска событий

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 98).

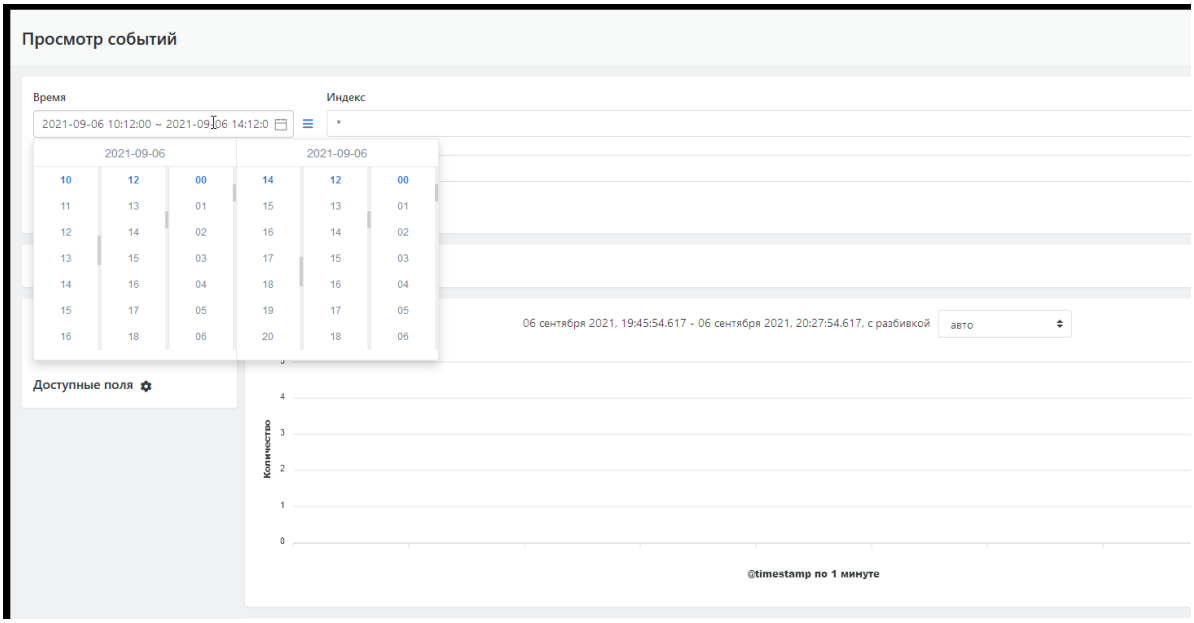


Рисунок 98 - Установка времени для дат начала и конца временного интервала для поиска событий

12.3. Анализ событий

12.3.1. 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 течении 1 часа (см. Рисунок 99).

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 100).

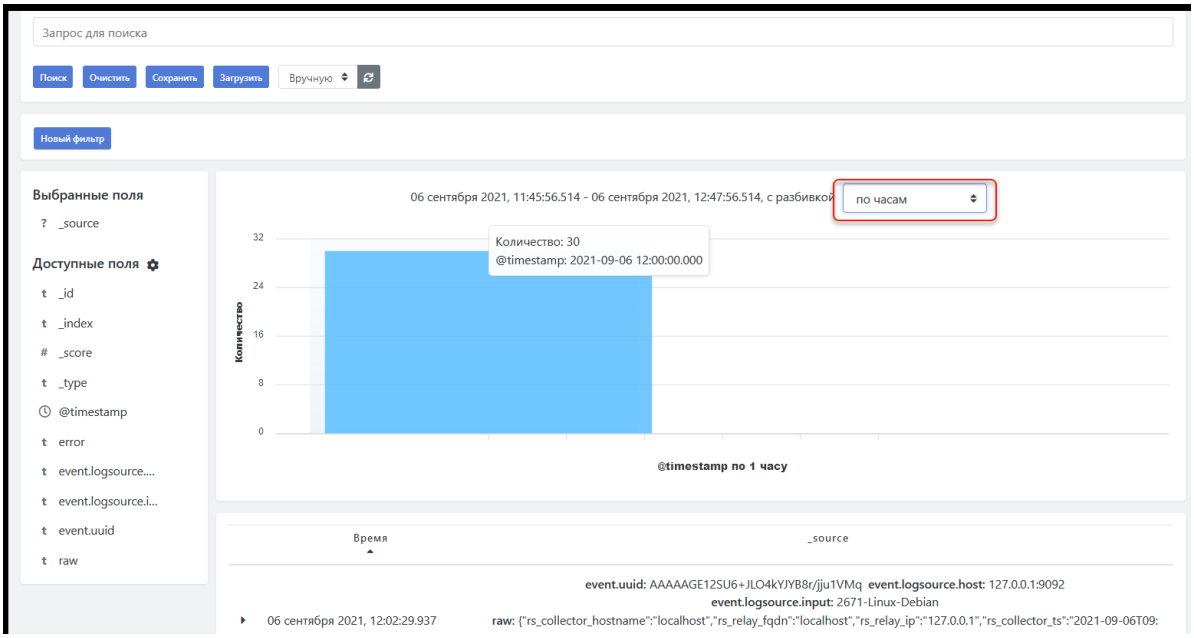


Рисунок 99 - Пример вывода данных о событиях с разбивкой по часам

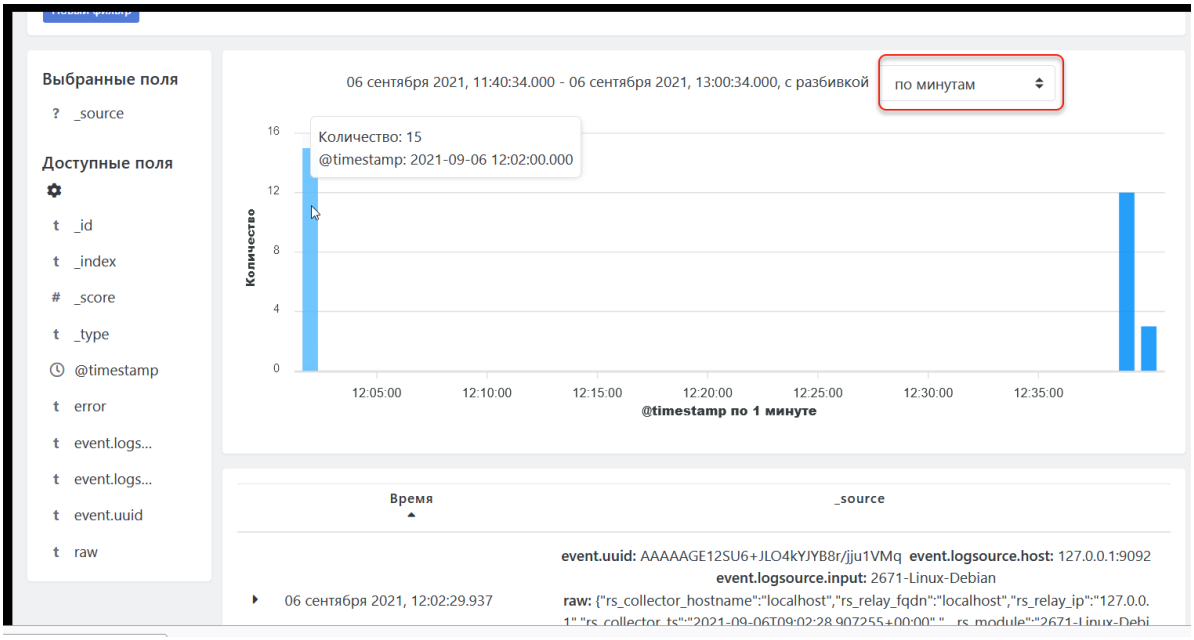


Рисунок 100 - Пример вывода данных о событиях с разбивкой по минутам

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. Рисунок 99):

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

12.3.2. Настройка полей табличного списка событий

12.3.2.1. Список событий по умолчанию

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

По умолчанию данный список содержит следующие поля (см. Рисунок 98):

- 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 101).

Рисунок 101 - Список событий по умолчанию

12.3.2.2. 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 102).

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

Так же данный параметр отобразится слева от диаграммы в области **"Выбранные поля"** (см. Рисунок 102).

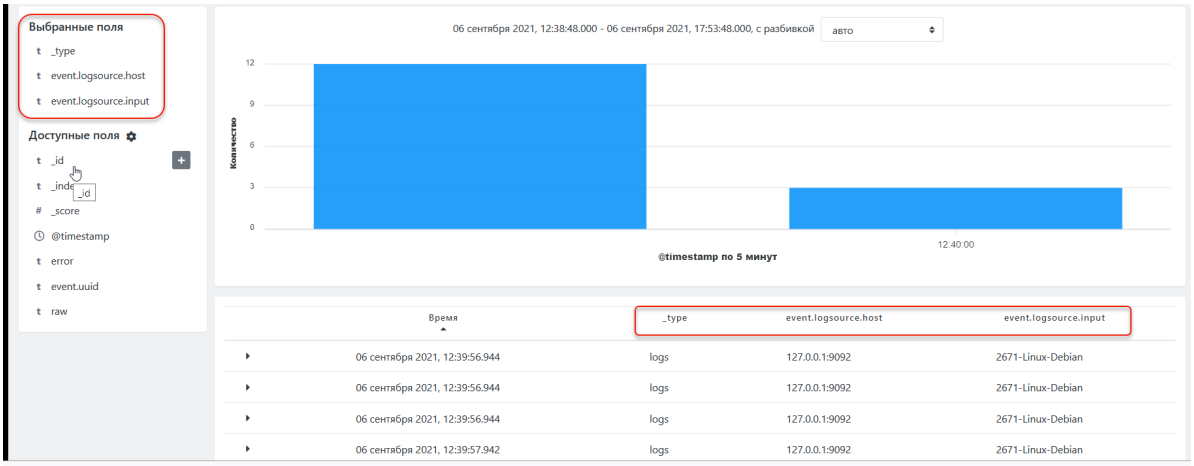


Рисунок 102 - Настройка полей табличного списка событий

12.3.2.3. 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.

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

Так же 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 103).

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

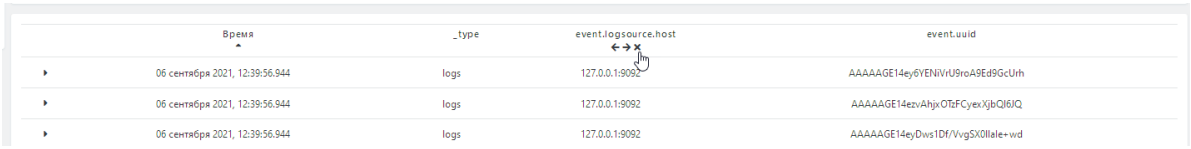


Рисунок 103 - Удаление поля из списка событий

12.3.3. Фильтрация списка событий

12.3.3.1. 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.

12.3.3.2. 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 104):

-  -- 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 104).
-  -- вывести на экран только те сообщения, у которых значение в данном поле не совпадает с указанным ("не равен").

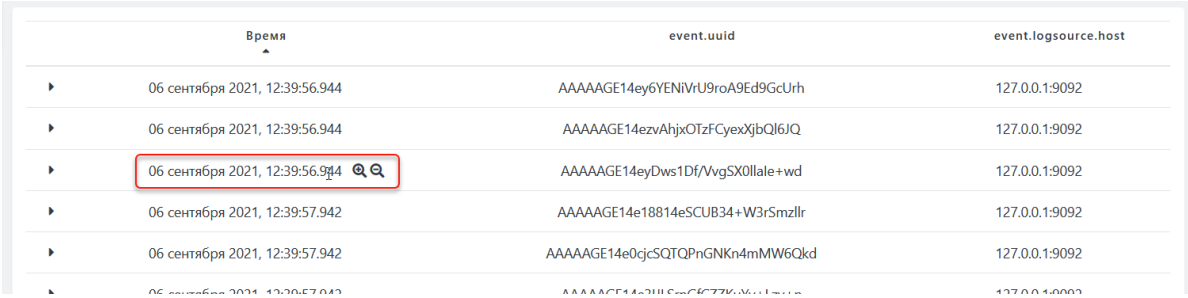


Рисунок 104 - Встроенные средства фильтрации табличного списка по значению поля

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 105).

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 105).

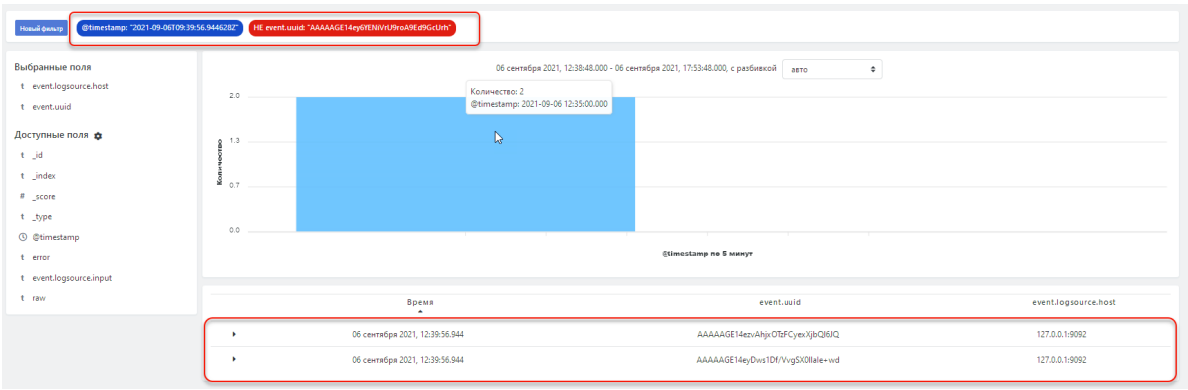


Рисунок 105 - Пример отфильтрованного по двум условиям списка сообщений

12.3.3.3. Снятие фильтра

Для снятия фильтра необходимо:

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

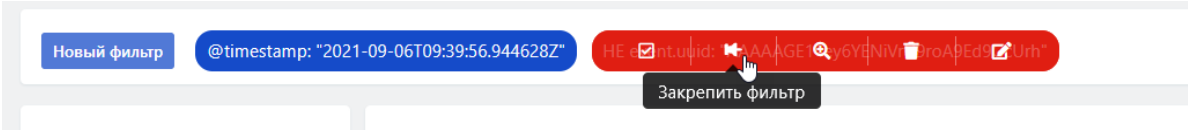


Рисунок 106 - Управление фильтром

12.3.3.4. Панель управления фильтром

Панель управления фильтром содержит следующие функции (см. Рисунок 106):

- **"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.

12.3.3.5. 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 107):
   - 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 раздел *"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.

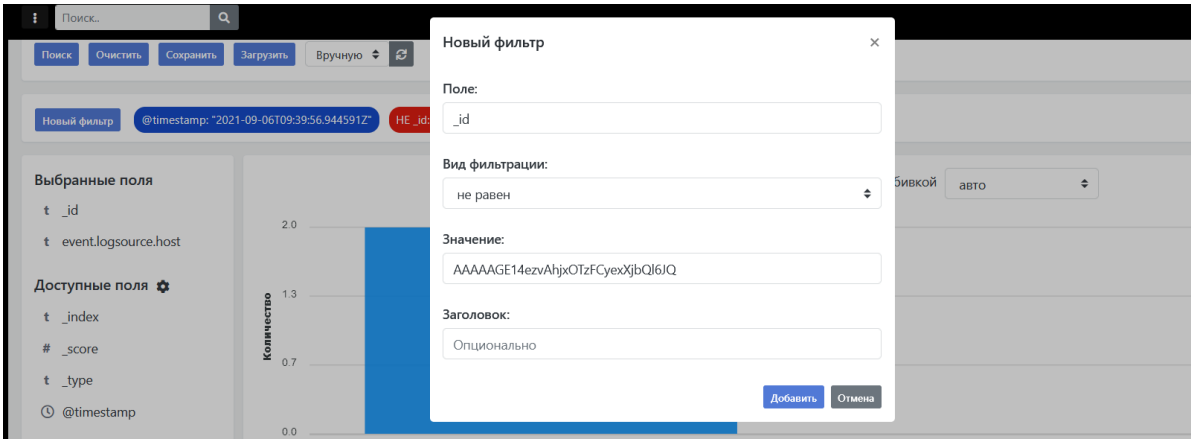


Рисунок 107 - Создание нового фильтра вручную, редактирование фильтра

При выборе вида фильтрации

12.3.3.6. Редактирование фильтра

При необходимости 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 107) .

3. Внести необходимые изменения в параметры фильтра.
4. Для сохранения изменений нажать на кнопку "**Добавить**".

12.3.4. Просмотр детализации события

12.3.4.1. 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 108) и состоит из двух вкладок: "**Таблица**" (по умолчанию) и "**JSON**". Так же в детализации доступна функция **"Найти инциденты"**.

12.3.4.2. Детализация события на вкладке "Таблица"

Вкладка "**Таблица**" содержит (см. Рисунок 108):

- 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.

Встроенные средства настройки таблицы включают следующие функции:

- -- добавить колонку с данным параметром в табличный список событий.

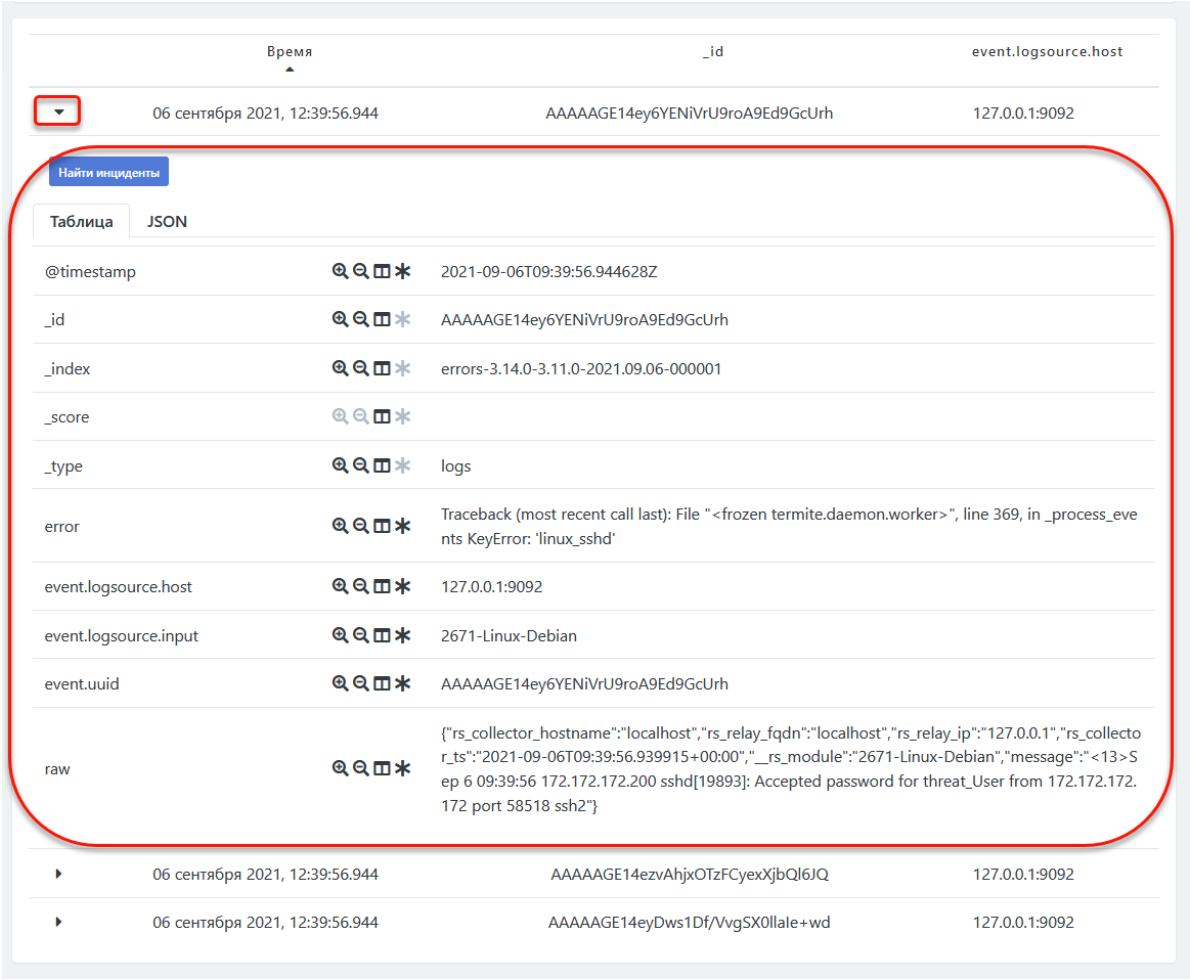


Рисунок 108 - Область детализации события, вкладка "Таблица"

12.3.4.3. Детализация события на вкладке "JSON"

Вкладка "**JSON**" содержит "сырые" данные события в формате JSON (см. Рисунок 109).

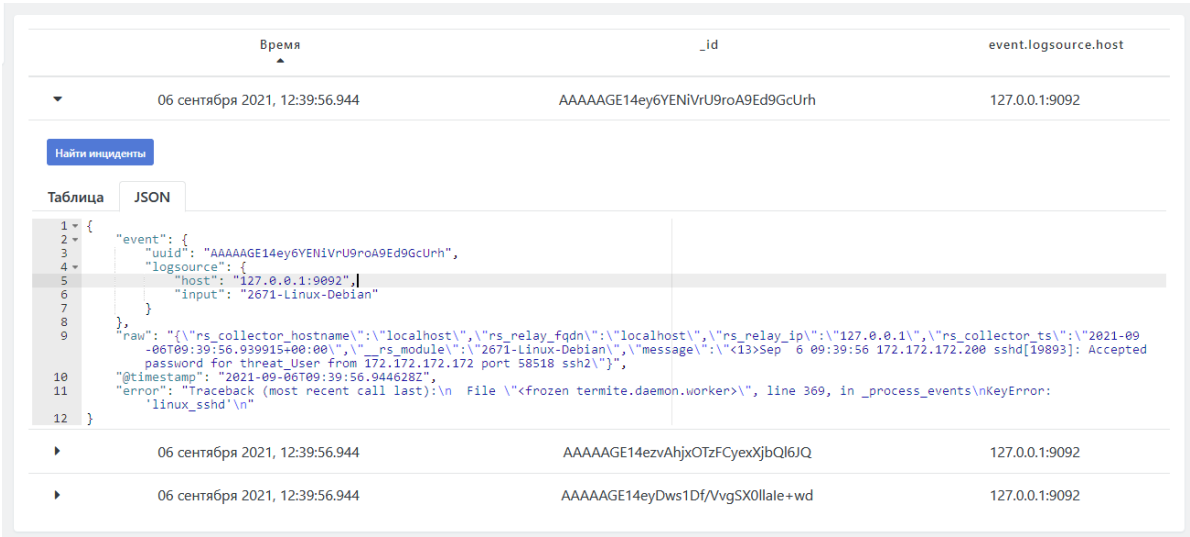


Рисунок 109 - Просмотр данных события в формате JSON

12.3.4.4. Функция "Найти инциденты"

12.3.5. 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 97):
    - Перейти к просмотру инцидента;
    - Создание нового инцидента.

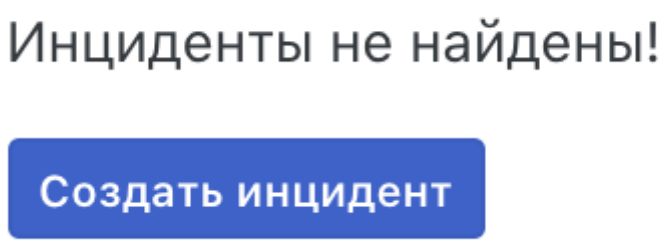


Рисунок 110 - Создание инцидента из результатов поиска события

3. Нажать на кнопки **"Создать инцидент"** (см. Рисунок 97).

   Откроется форма создания инцидента (см. Рисунок 98),

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"**.

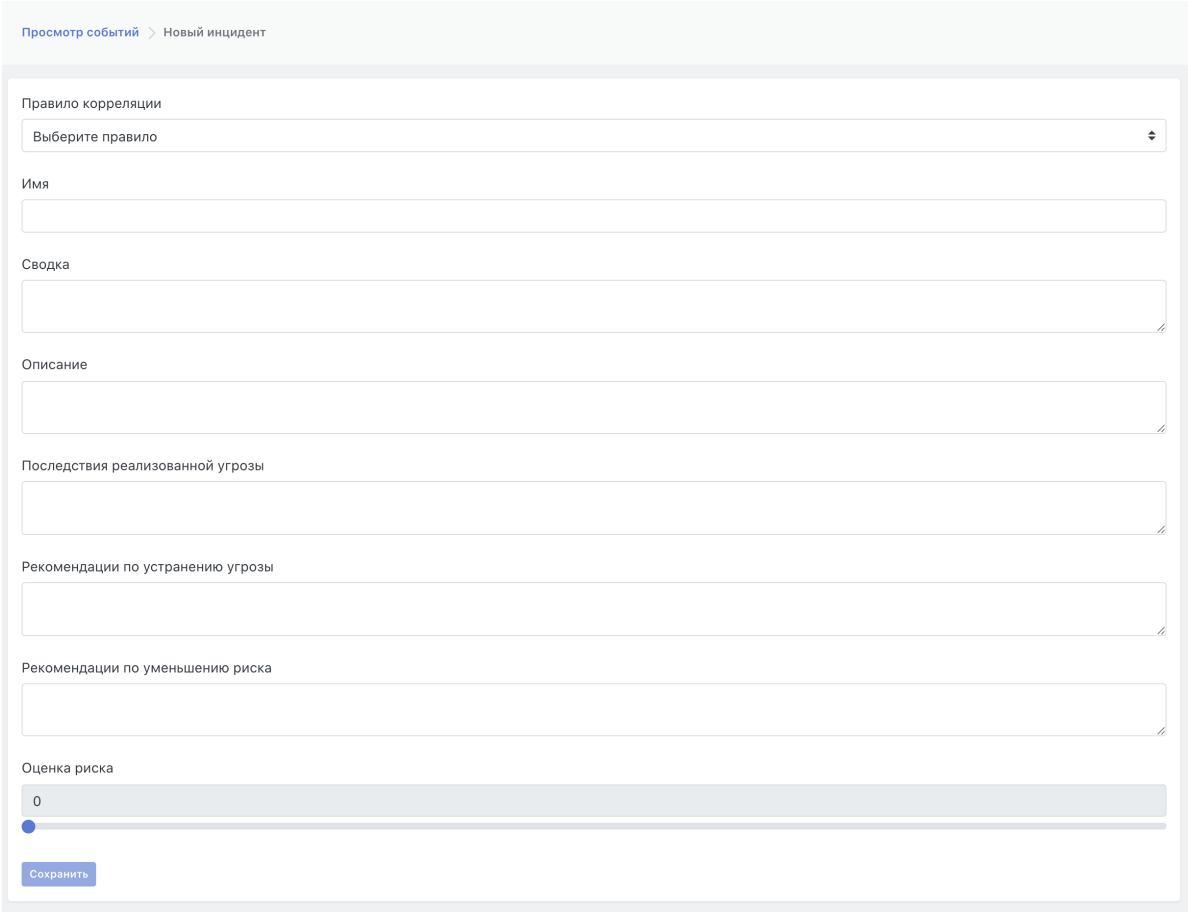


Рисунок 111 - Форма создания инцидента из результатов поиска события

13. Работа с активами

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

Атрибуты актива:

- Название -- произвольная текстовая строка.
- Value -- ценность 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.
- Network exposure -- 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.

13.1. Обнаружение активов

Существует несколько путей появления активов в системе:

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

13.1.1. 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, посвященном интеграции со сканерами уязвимостей.

13.1.2. 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, посвященном работе с сетевым сканером и инвентаризацией.

13.1.3. Создание активов вручную {#manual_create}

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

Для создания нового актива необходимо:

- Перейти в раздел «Активы», вкладка «Активы».

- Нажать кнопку «Создать».
- Заполнить атрибуты актива (Рисунок 50).
- Добавить сетевые интерфейсы из списка в системе. Если сетевой интерфейс актива отсутствует в списке его необходимо добавить.
- Добавить перечень ответственных за данный актив.
- Нажать «Создать».

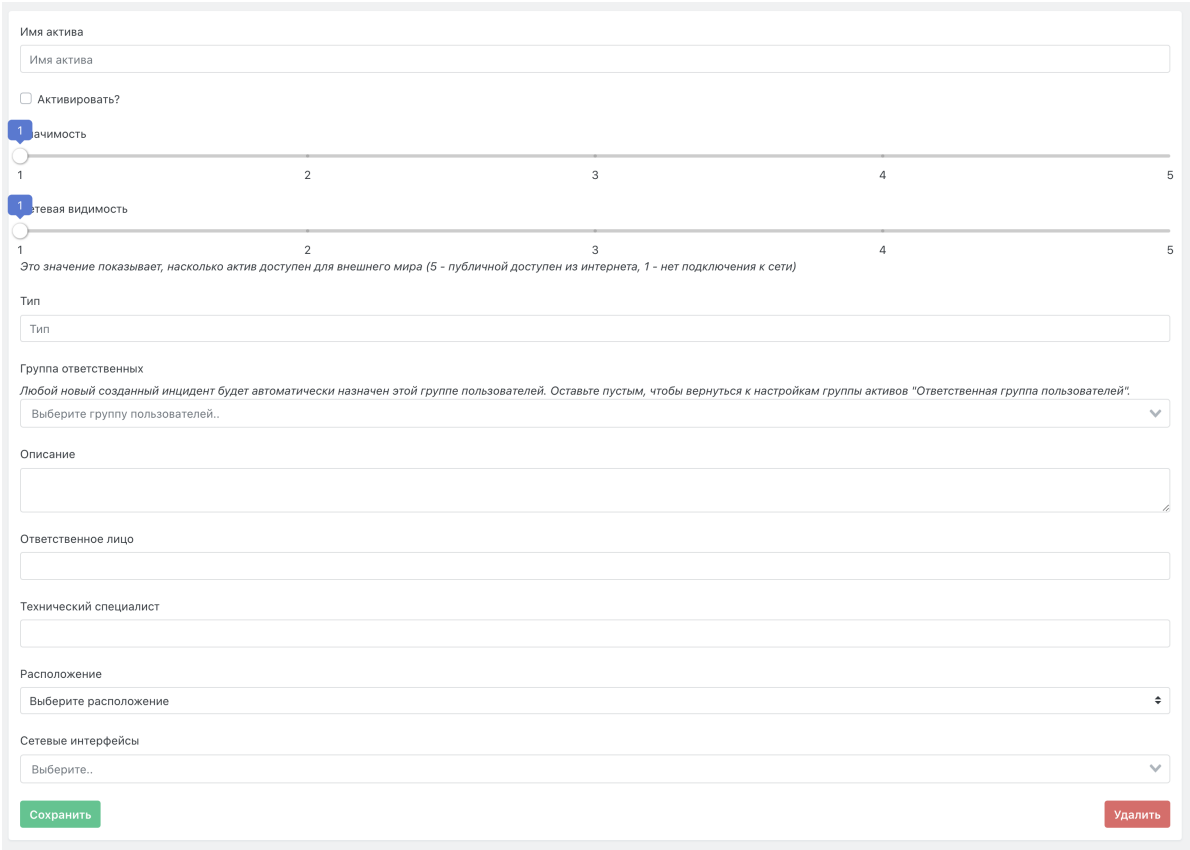


Рисунок 112 - Окно создания активов вручную

13.1.4. 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».**

13.1.5. 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

13.1.5.1. Создание новой политики идентификации

Для создания новой политики идентификации необходимо:

- Перейти в раздел «Активы», вкладка «Настройка идентификации активов»
- Нажать кнопку «Создать».
- Заполнить атрибуты политики идентификации (Рисунок 51):
    - 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 «Создать».

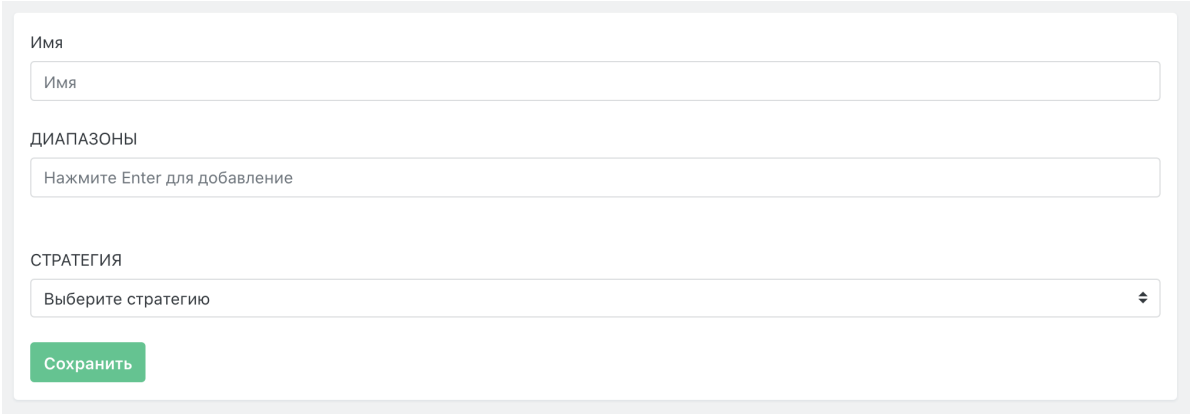


Рисунок 113 - Окно создания новой политики идентификации

13.1.5.2. 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 (Рисунок 52):
    - Name -- название политики.
    - Ranges -- Область действия политики. Адреса подсетей в CIDR-нотации, для который будет применяться выбранная стратегия идентификации.
    - Strategy -- Стратегия идентификации. Атрибут, который будет использоваться для идентификации актива (FQDN, IP-адрес или MAC-адрес).
- Нажать кнопку «Обновить Настройка обнаружения активов».

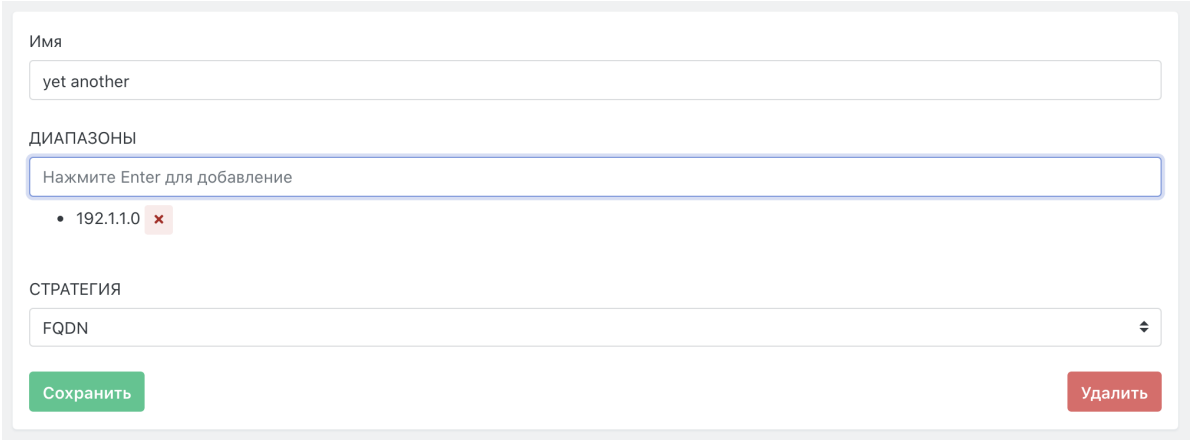


Рисунок 114 - Окно «Редактирование Настройка обнаружения активов»

13.1.5.3. Удаление политики идентификации

Для удаления политики идентификации необходимо:

- Перейти в раздел «Настройка обнаружения активов».
- Перейти в необходимую политику идентификации.
- Нажать кнопку «Удалить».

13.2. Аналитика по активам

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

13.2.1. Фильтрация активов

Для применения фильтра в списке активов необходимо (Рисунок 53):

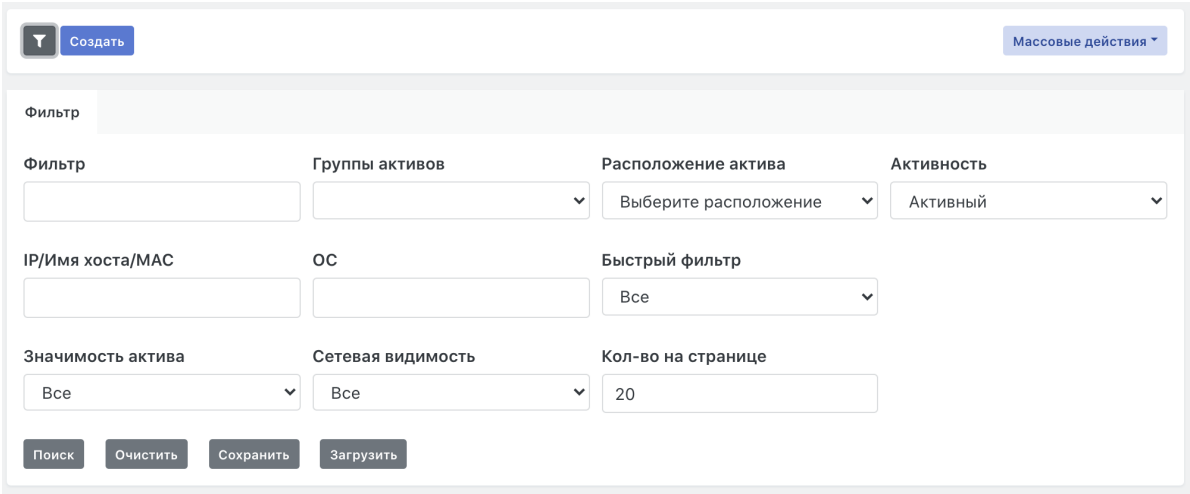


Рисунок 115 - Фильтр активов

- 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».

13.2.2. Просмотр данных по активу

В составе данных по активу доступны следующие блоки

- сводная информация;
- инциденты;
- данные о портах;
- изменения портов;
- соответствие ПО;
- установленное ПО;
- перечень сообщений, созданных в контексте данного актива.

13.2.2.1. Сводная информация

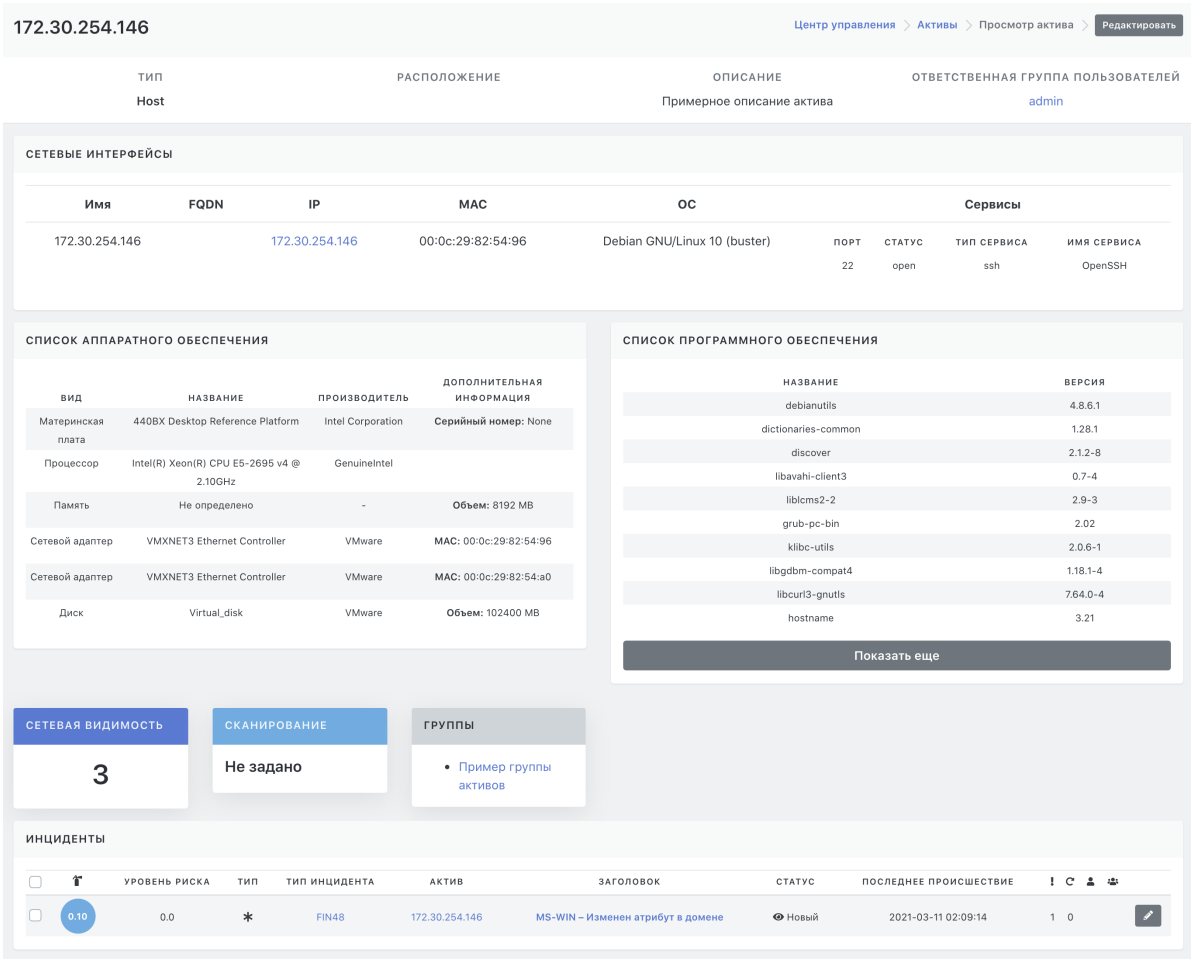


Рисунок 116 - Окно отображения сводной информации по активу

В сводной информации отображаются (Рисунок 54):

- Название актива.
- Тип.
- Описание.
- Географическое расположение.
- Группы активов, в которых состоит актив. По клику возможен переход в интерфейс просмотра группы активов.
- Группа ответственных за данный актив. По клику возможен переход в интерфейс просмотра группы пользователей.

- Дата последнего сканирования (при интеграции со сканером уязвимостей).
- Перечень сетевых интерфейсов.
- 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.
- Внутренний комментарий доступный только в интерфейсе администратора.
- Перечень инцидентов
  Данный раздел отображает перечень инцидентов, обнаруженный на выбранном активе (Рисунок 55).
  Работа с инцидентами описана в соответствующем разделе.

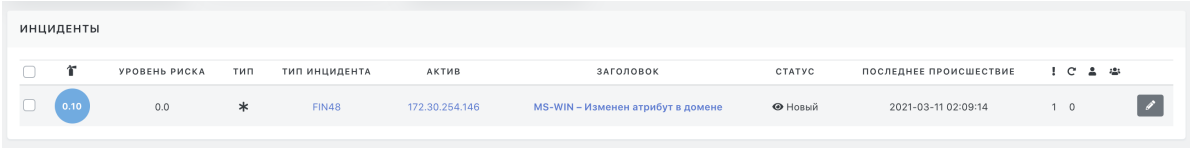


Рисунок 117 - Перечень инцидентов, обнаруженных при выбранном активе

13.2.2.2. Соответствие ПО

В разделе «Оценка соответствия ПО», вкладка «Результаты соответствия ПО» отображаются детали по проверке соответствия программного обеспечения политикам контроля.

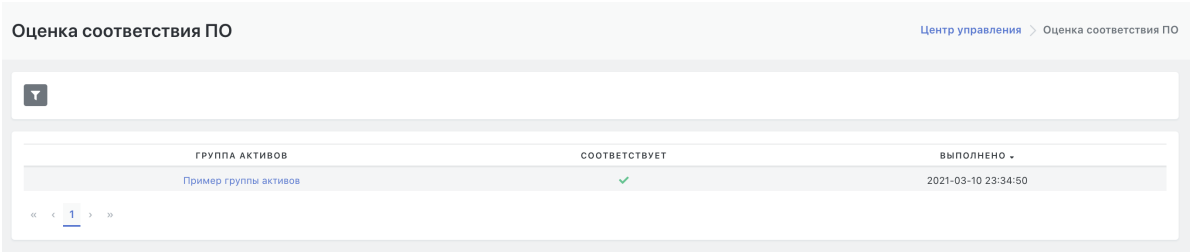


Рисунок 118 - Вкладка «Результаты соответствия ПО»

В таблице отображаются следующие колонки (Рисунок 56):

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

13.3. Работа с группами активов

Группы активов упрощают процесс управления активами.

13.3.1. Создание группы активов {#create_group}

Для создания группы активов необходимо:

- Перейти в раздел «Активы», вкладка «Группы активов».
- Нажать кнопку «Создать».
- Заполнить атрибуты группы активов (Рисунок 60).
    - 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.
    - Внутреннее примечание.
    - Описание.
    - ИД Системы.
    - Ответственное лицо.
    - Технический специалист.
- Указать наборы правил контроля соответствия установленного программного обеспечения.
- Нажать кнопку «Создать».

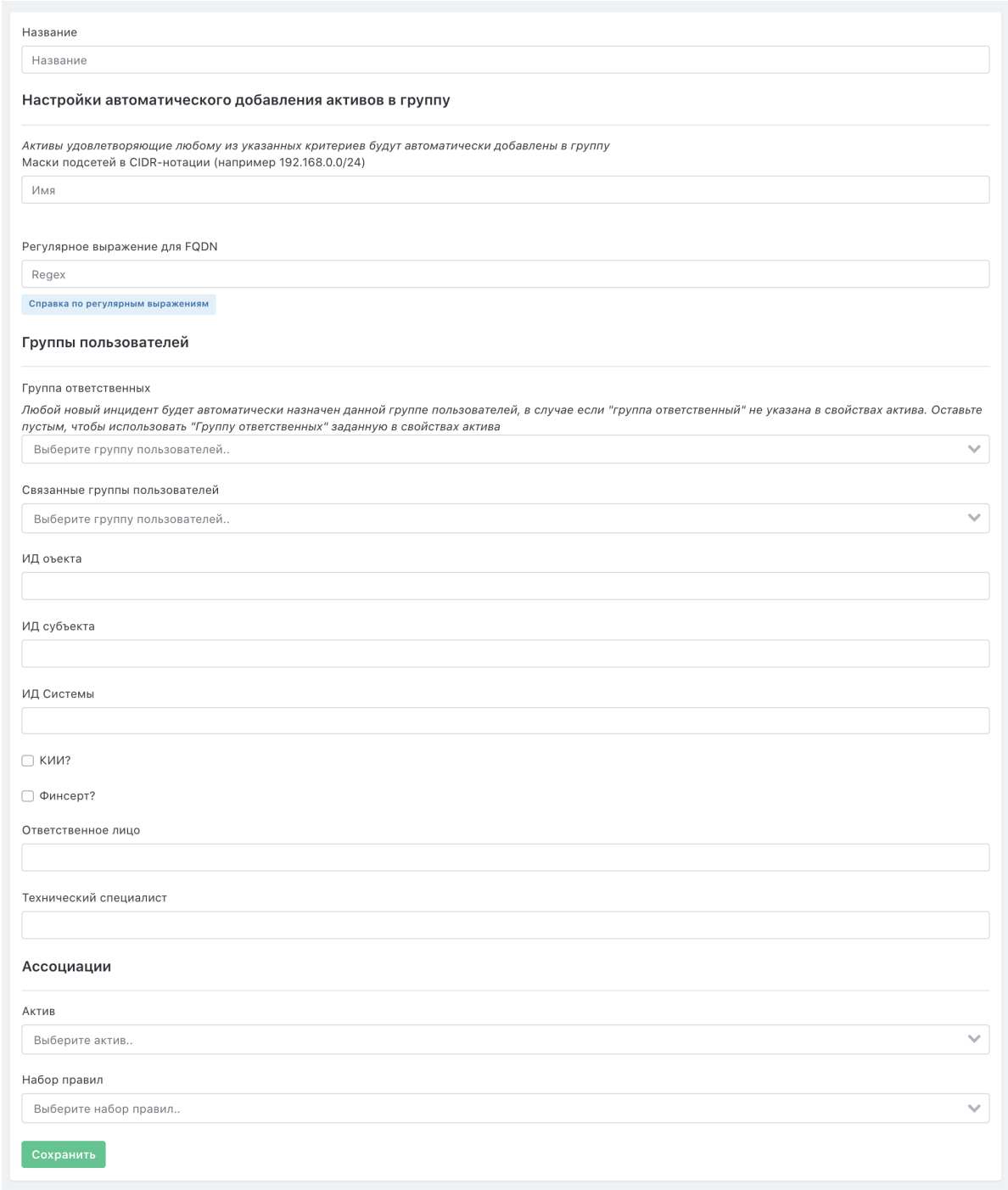


Рисунок 119 - Окно создания группы активов

13.3.2. Просмотр информации по группе активов

Для просмотра информации по группе активов необходимо:

- Перейти в раздел «Группы активов».
- Кликнуть на название группы, по которой требуется просмотреть информацию.

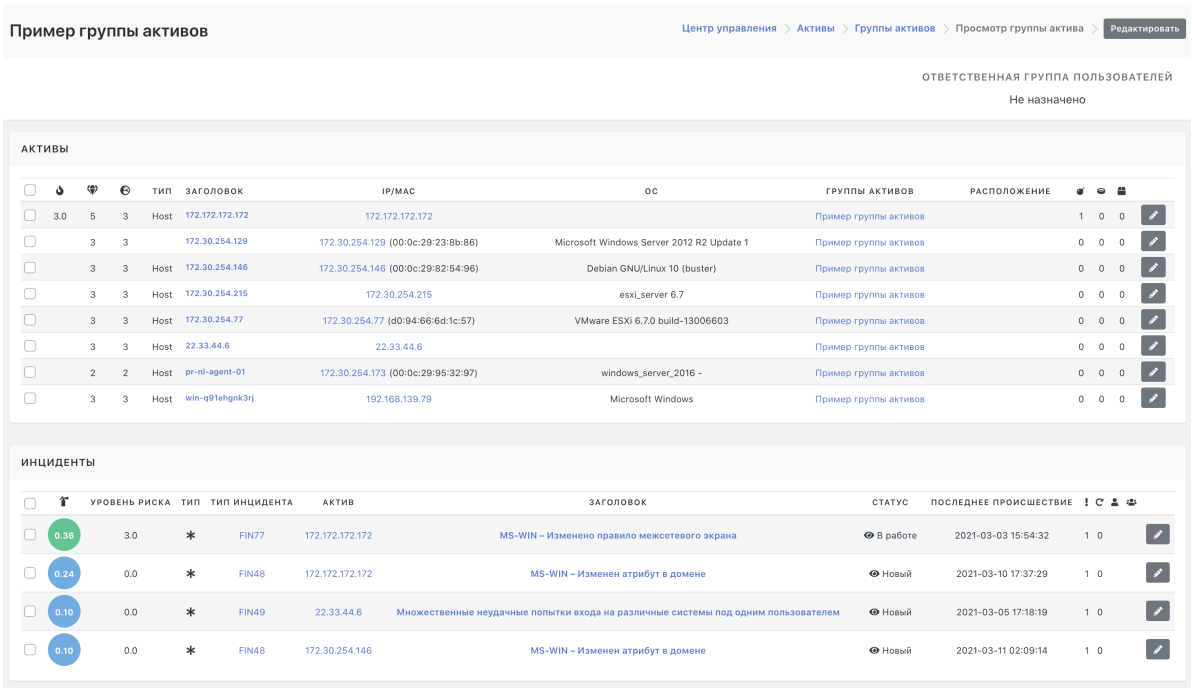


Рисунок 120 - Информация по группе активов

В форме просмотра отображаются (Рисунок 61):

- Название группы.
- Сетевые диапазоны для автоматической привязки актива к группе.
- Список связанных активов.
- Связанные группы пользователей -- перечень групп пользователей, ответственных за данную группу активов.
- Перечень связанных инцидентов

Кнопка «Редактировать» - открывать форму редактирования атрибутов группы.

13.3.3. Редактирование группы активов {#edit_group}

Для редактирования группы активов необходимо:

- Перейти в раздел «Активы», вкладка «Группы активов».
- Нажать кнопку «Edit».
- Заполнить атрибуты группы активов (Рисунок 62):
    - 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.
    - Внутреннее примечание.
    - Описание.
    - ИД Системы.
    - Ответственное лицо.
    - Технический специалист.
    - Включить активы в группу/Исключить активы из группы.

- Указать наборы правил контроля соответствия установленного программного обеспечения.

- Нажать кнопку «Сохранить».

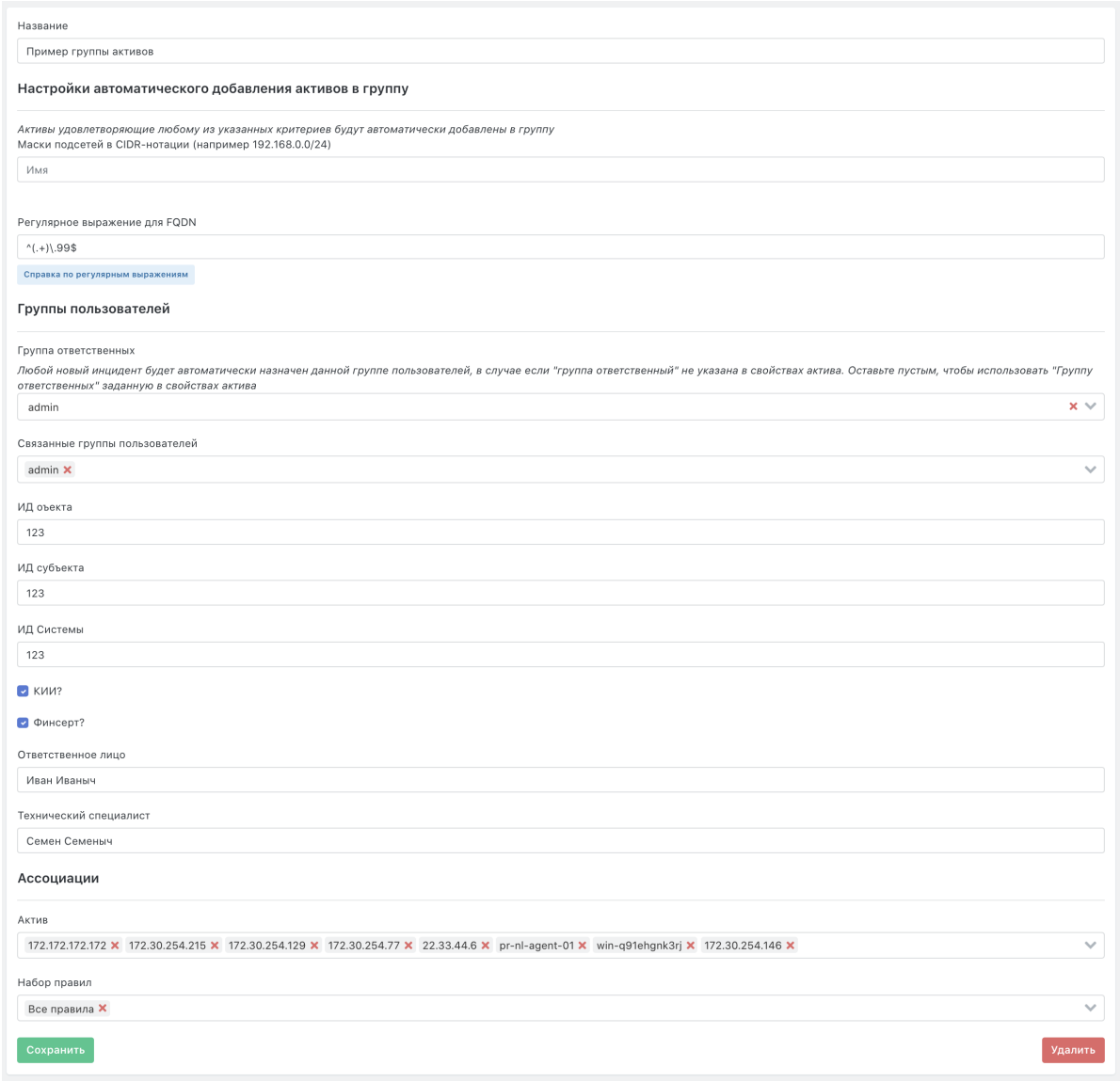


Рисунок 121 - Окно «Редактирование Группа активов»

13.3.4. Включение активов в группу активов

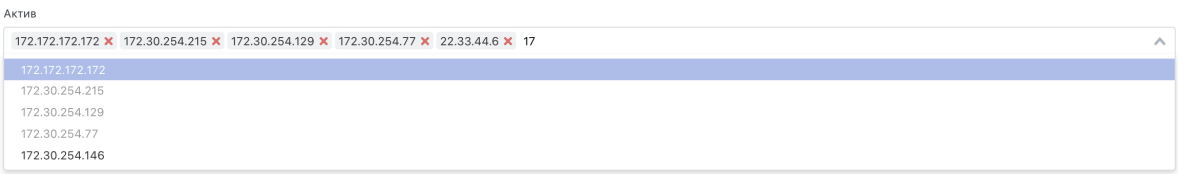


Рисунок 122 - Форма включения активов в группу

Включение активов в группу производится в форме редактирования атрибутов активов.

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

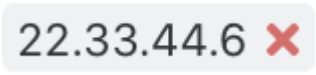
Для включения активов в группу необходимо выбрать один или несколько активов в списке.

После проделанных манипуляций необходимо сохранить изменения в группе активов. Данная операция также доступна из контекста списка активов (см. п.4.4.2).

13.3.5. Исключение активов из группы

Исключение активов из группы производится в форме редактирования атрибутов активов.

Рисунок 123 - Форма исключения активов из группы

Исключить актив из группы возможно нажатием на кнопку «x» рядом с именем актива 

После проделанных манипуляций необходимо сохранить изменения в группе активов. Данная операция также доступна из контекста списка активов (см. п.5.4.2).

13.4. Актуализация данных об активах

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

13.4.1. Редактирование данных по активу

Для редактирования информации необходимо:

- Перейти в раздел «Активы», вкладка «Активы».
- Кликнуть по заголовку актива, в который необходимо внести коррективы.
- Нажать кнопку «Редактировать».
- Внести коррективы в данные об активе.
- Нажать кнопку «Сохранить».

13.4.2. Классификация новых активов

Для поиска активов, которые некорректно классифицировались автоматически, предусмотрены специализированные фильтры 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.

13.4.3. 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», вкладка «Активы».
- Выбрать несколько активов с помощью чекбоксов.
- 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.

13.5. 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

13.5.1. Связывание интерфейса с активом

Форма связывания актива с сетевыми интерфейсами доступна при создании актива вручную и при редактировании актива.

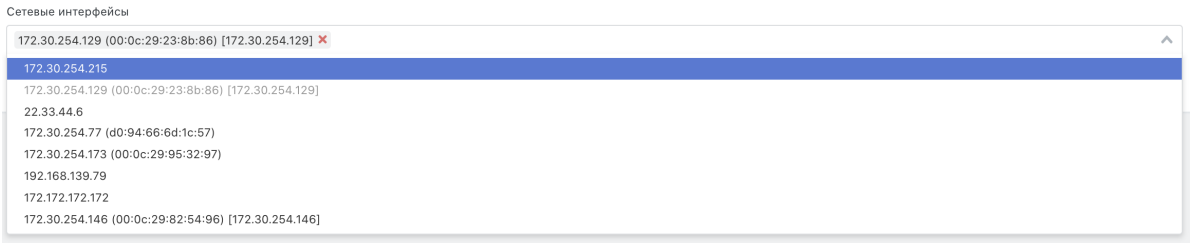


Рисунок 124 - исунок 71 --Форма связывания интерфейса с активом

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 связывания интерфейса.

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

Для отвязывания сетевых интерфейсов от актива необходимо нажать на кнопку «x» рядом с именем интерфейса

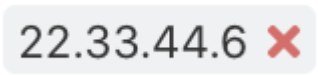


Рисунок 125

После указанных изменений необходимо сохранить изменения в активе.

13.5.2. Создание сетевых интерфейсов вручную {#create_net}

Для создания нового сетевого интерфейса вручную необходимо:

- Перейти в раздел «Активы», вкладка «Сетевые интерфейсы».
- Нажать кнопку «Создать».
- Заполнить атрибуты сетевого интерфейса (Рисунок 72):
    - Имя -- имя интерфейса для удобства поиска.
    - IP -- IP-адрес, заданный на интерфейсе.
    - MAC -- MAC-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 «Создать».

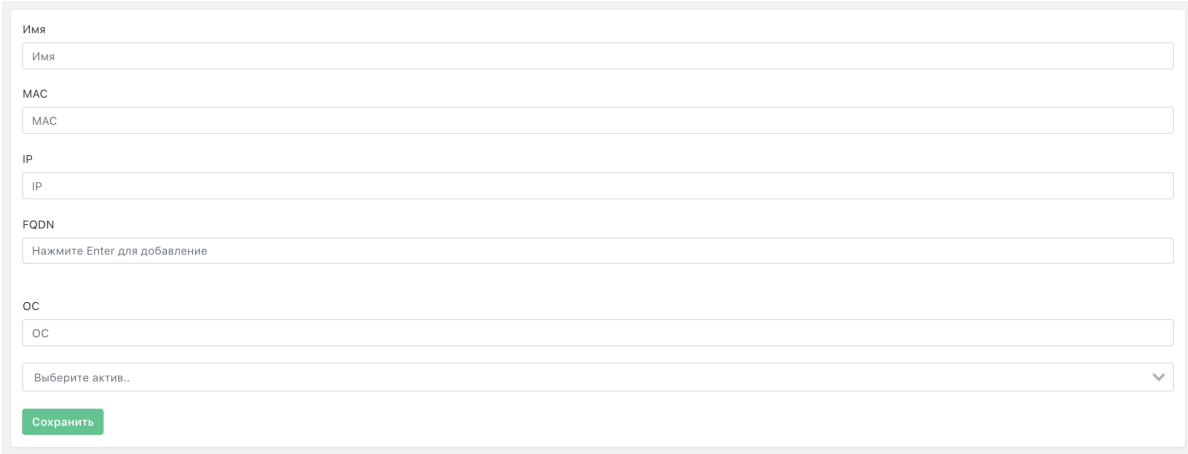


Рисунок 126 - Создание сетевых интерфейсов вручную

13.5.3. Редактирование сетевого интерфейса {#edit_net}

Для редактирования сетевого интерфейса необходимо:

- Перейти в раздел «Активы», вкладка «Сетевые интерфейсы».
- Нажать кнопку «Редактировать» напротив сетевого интерфейса, в который необходимо внести изменения.
- Внести изменения в атрибуты сетевого интерфейса (Рисунок 73):
    - Имя -- имя интерфейса для удобства поиска.
    - IP -- IP-адрес, заданный на интерфейсе.
    - MAC -- MAC-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».

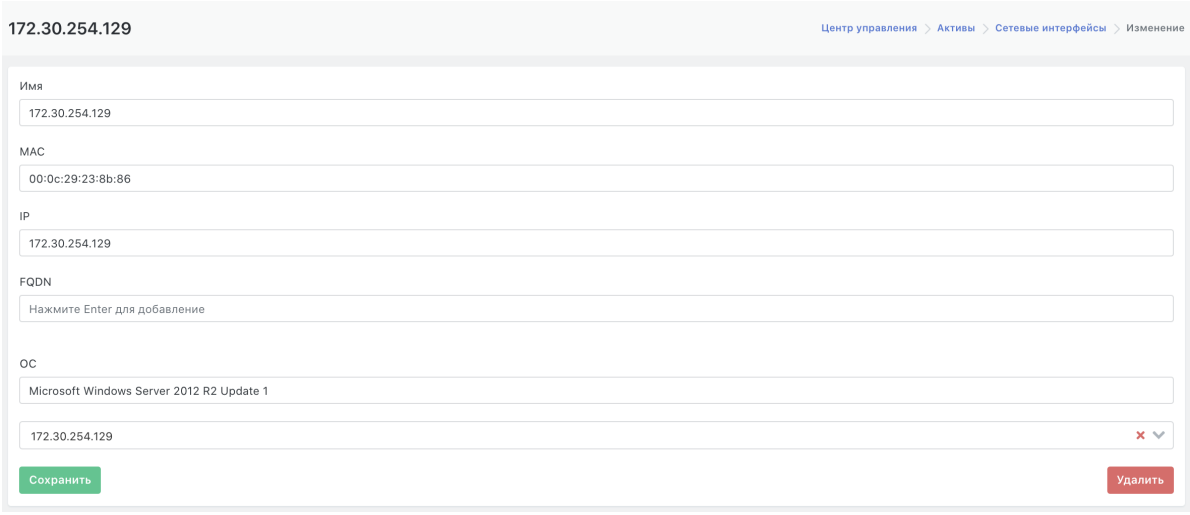


Рисунок 127 - Окно «Редактирование Сетевой интерфейс»

13.5.4. Удаление сетевого интерфейса

Для удаления сетевого интерфейса необходимо:

- Перейти в раздел «Активы», вкладка «Сетевые интерфейсы».
- Перейти в режим редактирования необходимого сетевого интерфейса
- Нажать кнопку «Удалить».

14. 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;

14.1. Поиск активов в компьютерной сети

Для обнаружения новых активов и актуализации старых необходимо:

- Перейти в раздел «Активы» во подраздел «Инвентаризация» и выбрать вкладку «Обнаружение хостов»
- Далее указать в поле IP адрес подсети которую необходимо просканировать
- В поле подсеть выбрать глубину сканирования сети (по умолчанию выбрана 24ая 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»

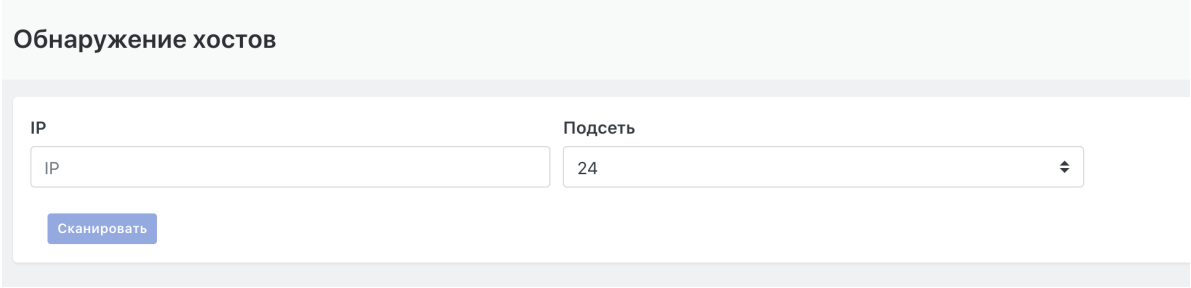


Рисунок 128 - форма обнаружения хостов

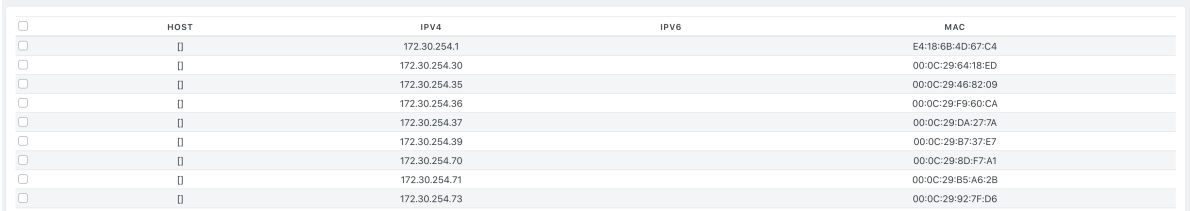
После запуска сканирования появится индикатор процесса сканирования

Рисунок 129

И после завершения сканирования будут доступен результат сканирования в виде таблицы с аттрибутами (Рисунок 97):

- 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 130 - 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 (Рисунок 98)

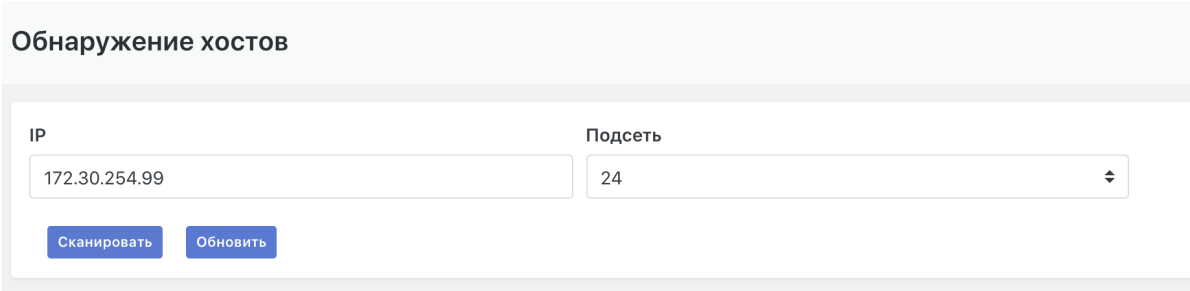


Рисунок 131 - форма обнаружения хостов после завершения сканирования

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» на вкладке «Активы»

14.2. Поиск сетевых сервисов на хосте без авторизации

Для запуска сканирования сетевых сервисов необходимо:

- Перейти на вкладку «Обнаружение сервисов» подраздела «Инвентаризация» раздела «Активы»
- Отметить чекбоксами нужны для сканирования активы (при необходимости воспользоваться поиском и фильтрацией)
- Нажать на кнопку «Сканировать сервисы»

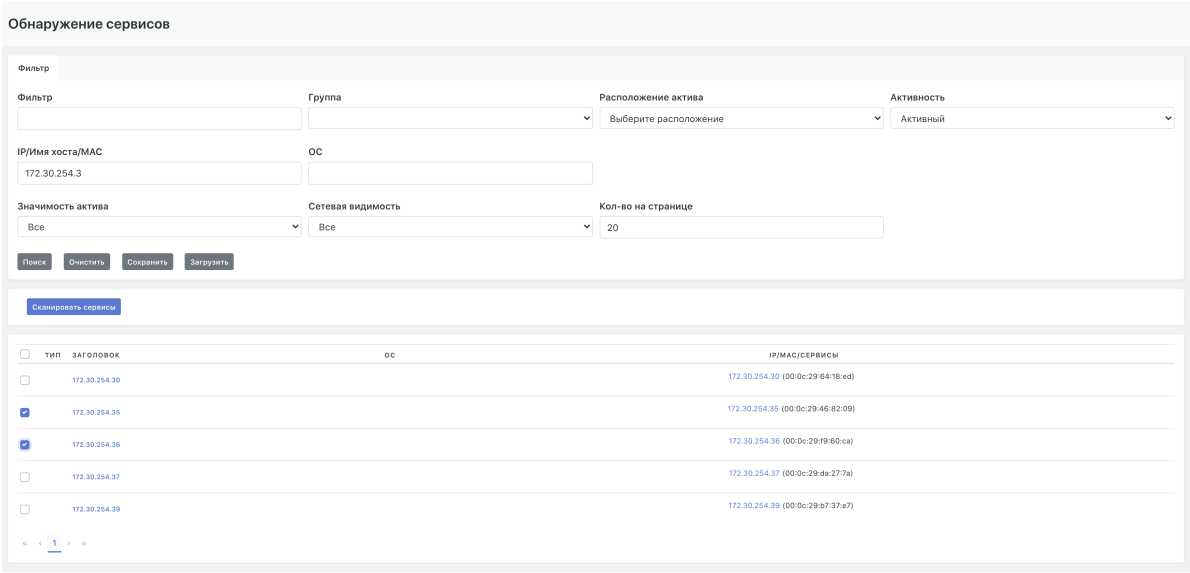


Рисунок 132 - экран сканирования сетевых сервисов

После нажатия на кнопку «Сканировать сервисы» появится индикатор прогресса сканирования.

Процедура занимает длительное время, в процессе её выполнения данные на странице будут обновляться (Рисунок 99)

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.

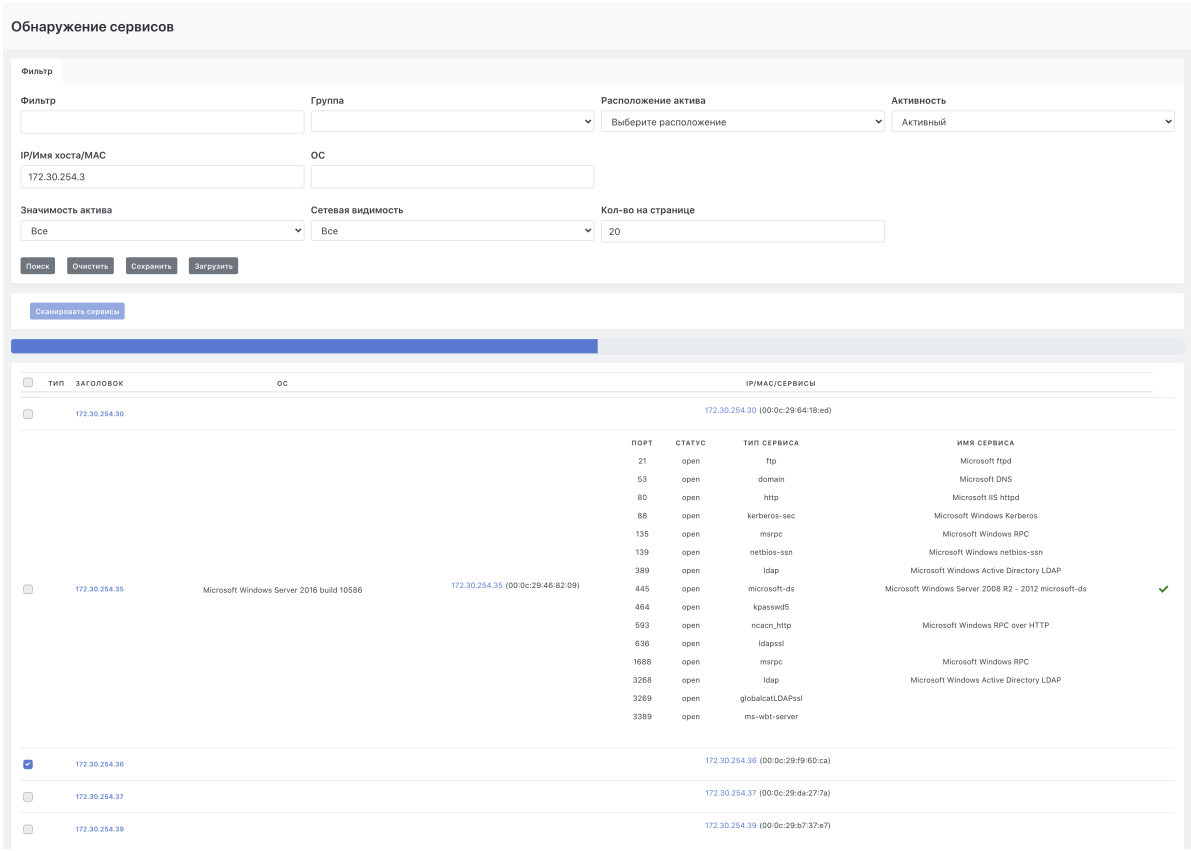


Рисунок 133 - экран сканирования сетевых сервисов в процессе сканирования

14.3. Обнаружение ПО на хосте с авторизацией

Для запуска сканирования сбора данных о ПО необходимо:

- Перейти на вкладку «Сбор данных» подраздела «Инвентаризация» раздела «Активы»
- Отметить чекбоксами нужны для сканирования активы (при необходимости воспользоваться поиском и фильтрацией)
- Выбрать протокол сканирования, учетную запись и тип сбора данных в форме сбора данных (Рисунок 100.1)
- Нажать на кнопку «Собрать»

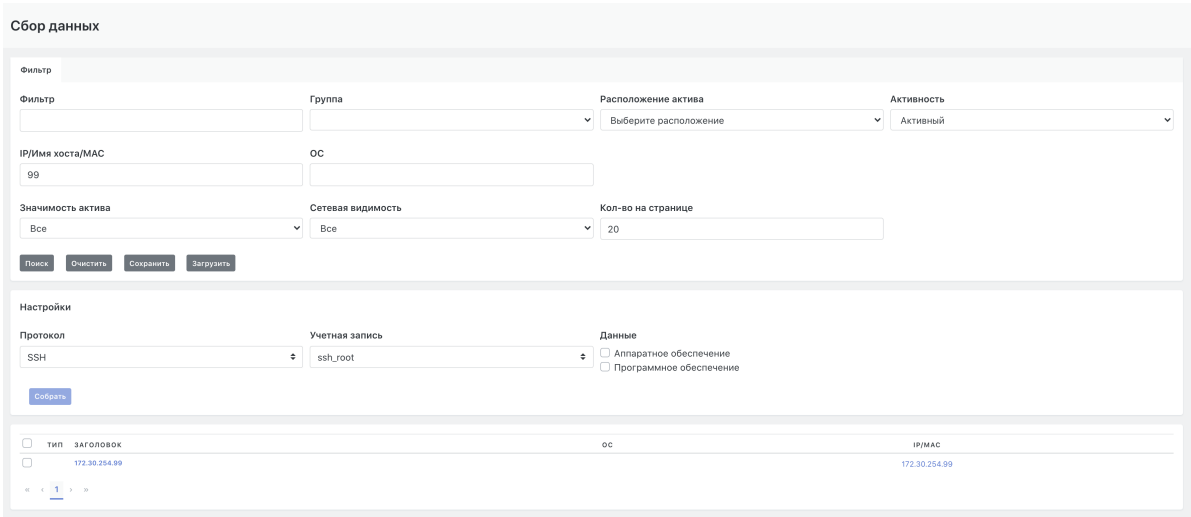


Рисунок 134 - экран сбора данных на хосте с авторизацией

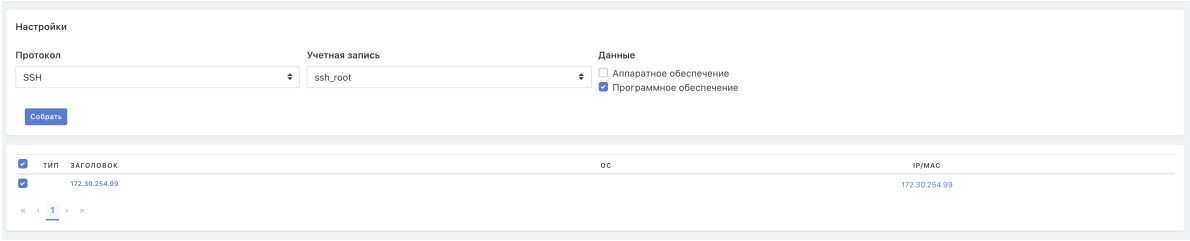


Рисунок 135 - форма сбора данных о Программном обеспечении на хосте с авторизацией

После завершения сбора данных в деталях актива появится информационный блок с списком программного обеспечения (Рисунок 100.3)

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

Рисунок 136 - список найденного программного обеспечения

14.4. Обнаружение аппаратной конфигурации на хосте с авторизацией

Для запуска сканирования сбора данных о ПО необходимо:

- Перейти на вкладку «Сбор данных» подраздела «Инвентаризация» раздела «Активы»
- Отметить чекбоксами нужны для сканирования активы (при необходимости воспользоваться поиском и фильтрацией)
- Выбрать протокол сканирования, учетную запись и тип сбора данных в форме сбора данных (Рисунок 100.2)
- Нажать на кнопку «Собрать»

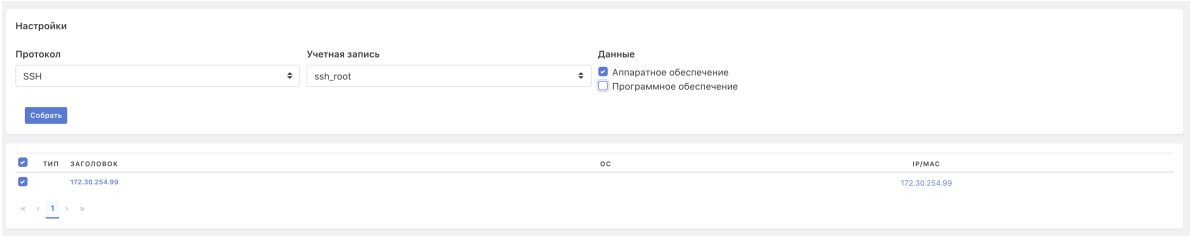
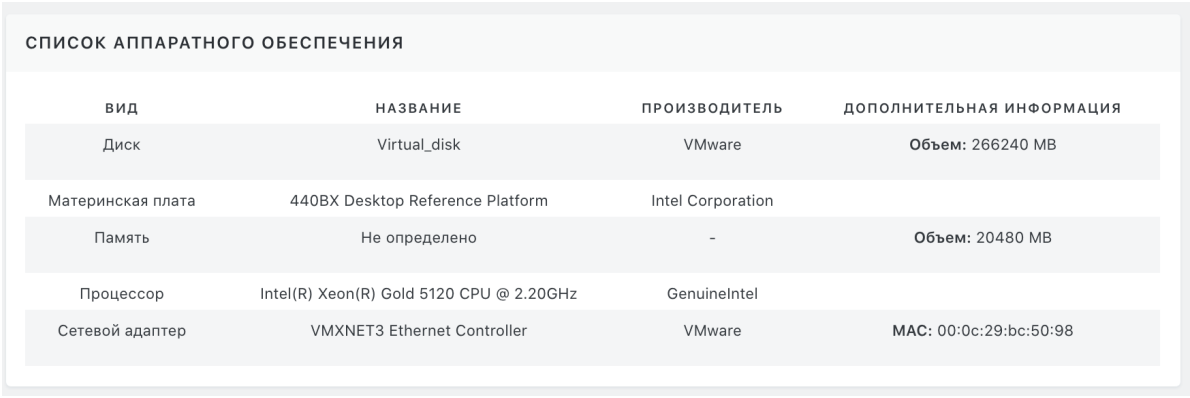


Рисунок 137 - форма сбора данных о Аппаратном обеспечении на хосте с авторизацией

После завершения сбора данных в деталях актива появится информационный блок с списком аппаратного обеспечения (Рисунок 100.4)



СПИСОК АППАРАТНОГО ОБЕСПЕЧЕНИЯ

ВИД	НАЗВАНИЕ	ПРОИЗВОДИТЕЛЬ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ
Диск	Virtual_disk	VMware	**Объем:** 266240 MB
Материнская плата	440BX Desktop Reference Platform	Intel Corporation	
Память	Не определено	-	**Объем:** 20480 MB
Процессор	Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz	GenuineIntel	
Сетевой адаптер	VMXNET3 Ethernet Controller	VMware	**MAC:** 00:0c:29:bc:50:98

Рисунок 138 - список найденного аппаратного обеспечения

14.5. Настройка учетных записей для авторизации на хостах

Данный функционал находится в разделе «Администрирования», подразделе «Кластер» и доступен только администраторам системы. Детальная документация по работе с учетными записями описана в документе -- Руководство Администратора.

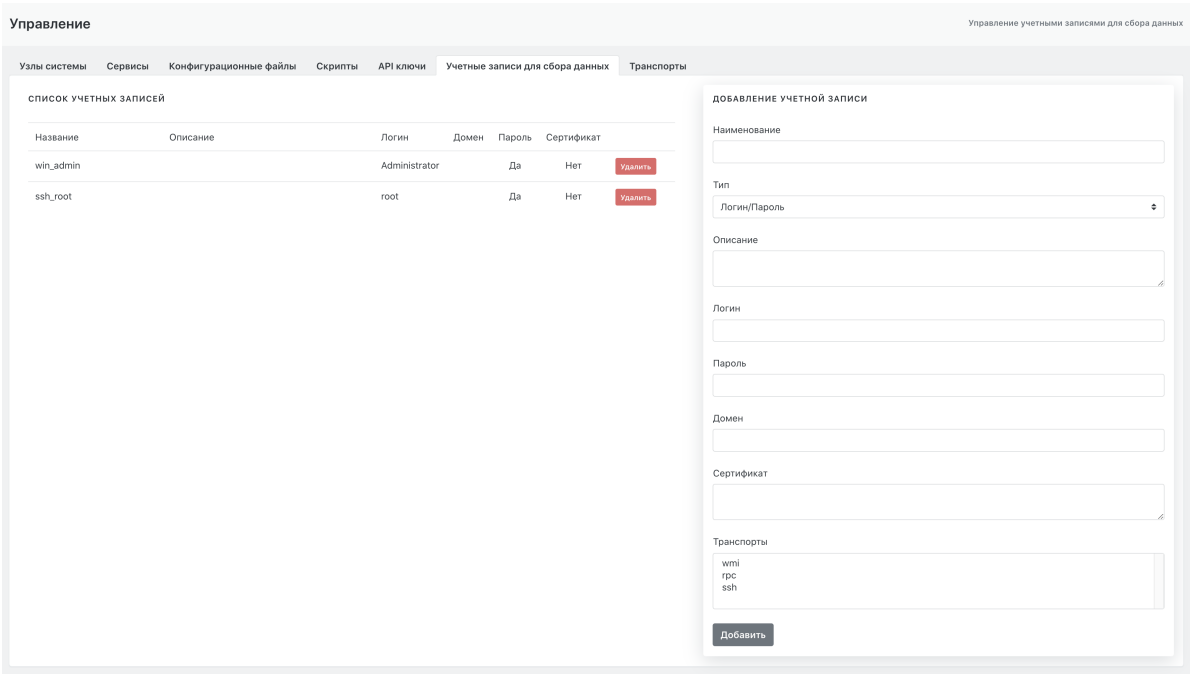


Рисунок 139 - Экран управления учетными записями для сбора данных

15. Настройка контроля установленного программного обеспечения

15.1. Общие положения

В Платформе 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. Правило контроля может контролировать:

- 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.

15.2. Анализ программного обеспечения на активах

15.2.1. 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 140).

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

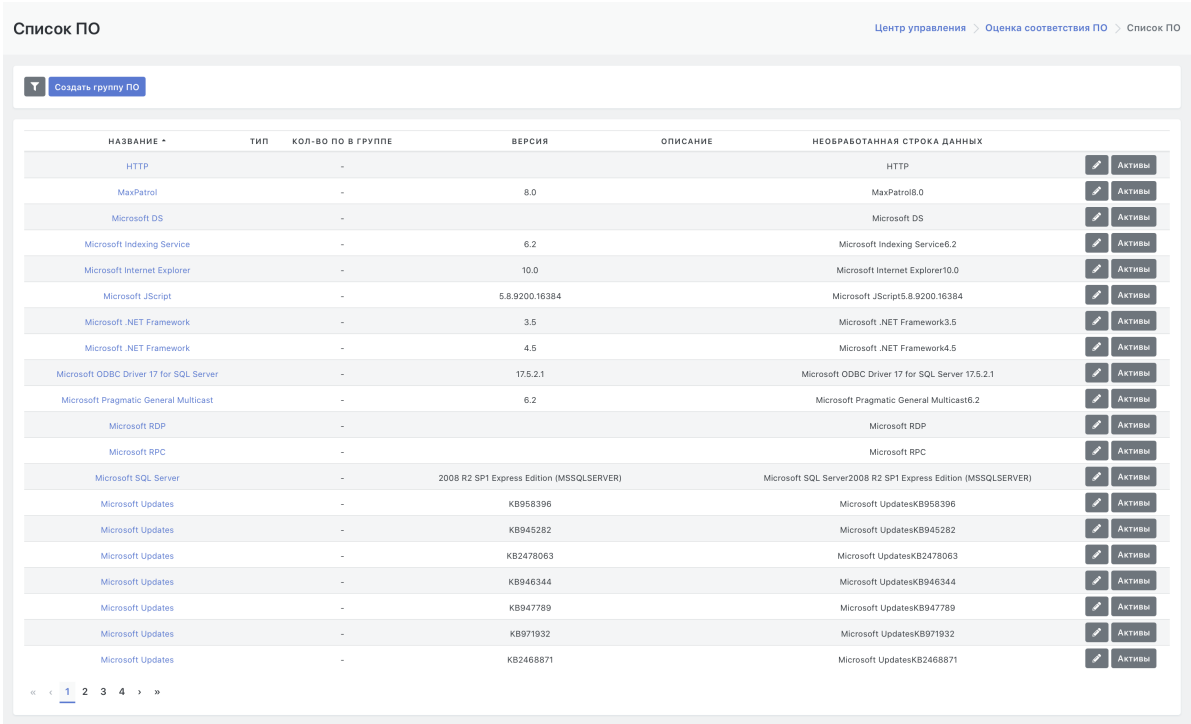


Рисунок 140 - Окно вкладки «Список ПО»

Для просмотра детализации по записи о программном обеспечении нужно щелкнуть на название программного обеспечения в поле **"Название"** (см. Рисунок 140). На экране откроется форма детализации информации о ПО (см. Рисунок 141).

Форма отображает следующие данные:

- "**Название клиента**" -- уникальное название ПО на Платформе.
- "**Описание**" -- описание программного обеспечения, написанное пользователем Платформы.
- "**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.

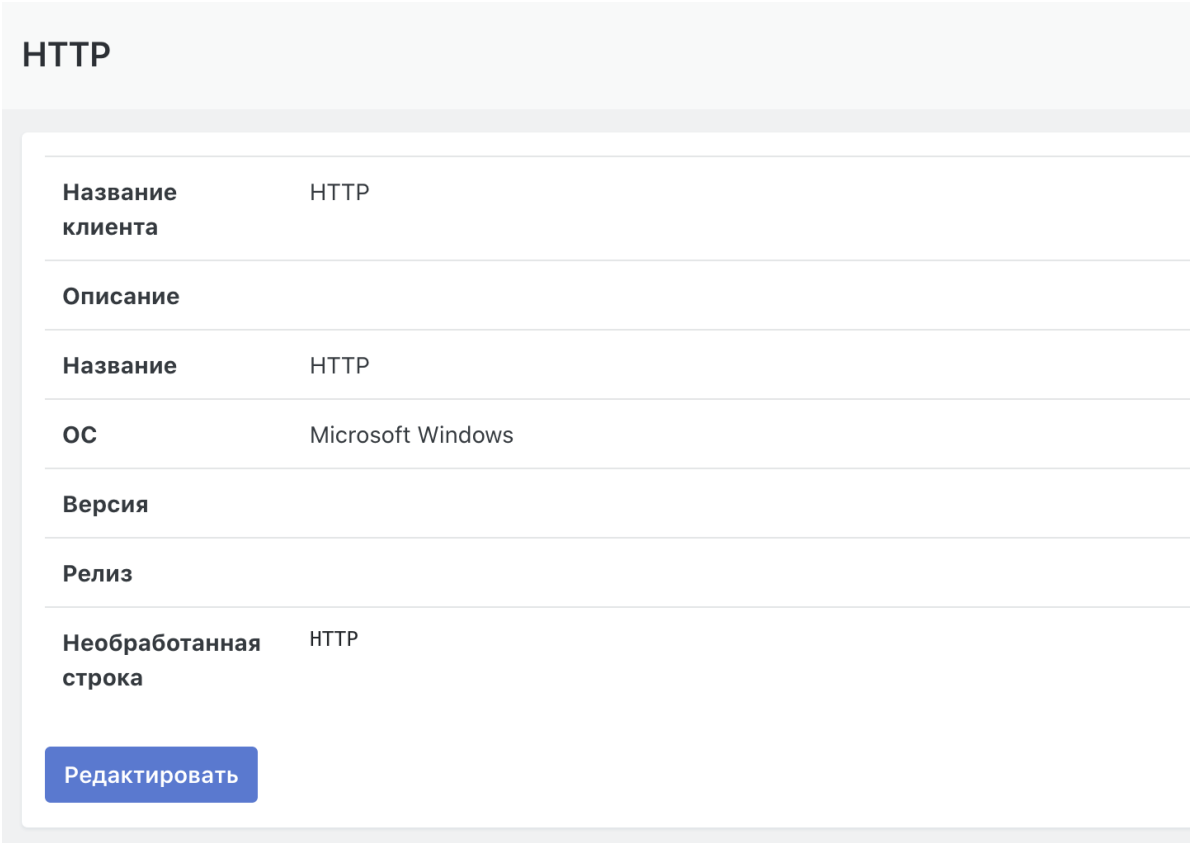


Рисунок 141 - Форма просмотра деталей записи о программном обеспечении.

15.2.2. 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 142). Данный перечень представляет собой стандартный для Платформы табличный список активов.

Полное описание табличного списка активов приведено в разделе *"Активы. Активы"*.

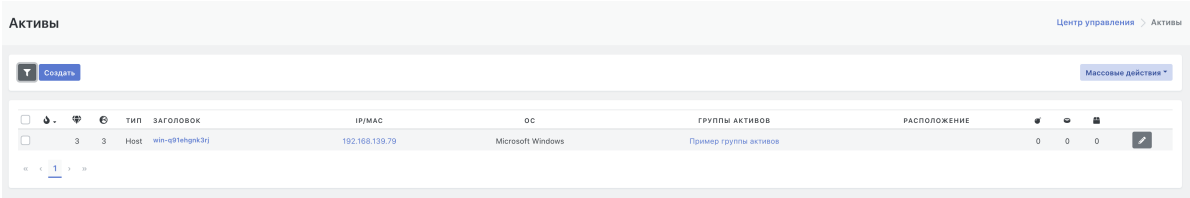


Рисунок 142 - Перечень активов, на которых найдено при сканировании данное программное обеспечение

15.2.3. 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 143):
    - **"Название клиента"** -- название ПО, которое будет отображаться в деталях инцидента.
    - **"Описание"** -- описание ПО, созданное пользователем Платформы. Например: назначение ПО.
4. Для сохранения внесенных изменений нажать на кнопку «Сохранить».

15.2.4. 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 143).

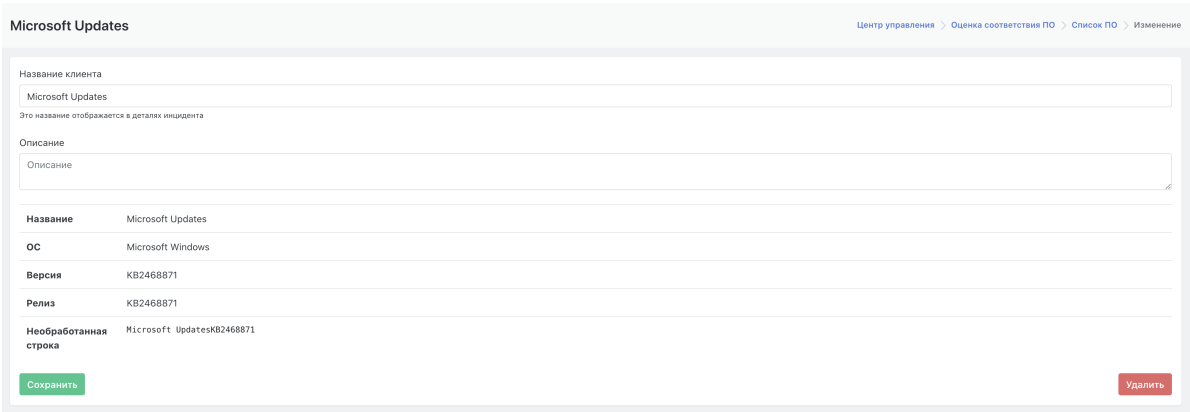


Рисунок 143 - Окно редактирования программного обеспечения

15.2.5. Создание группы ПО

...

15.3. 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 144).
    - 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**".

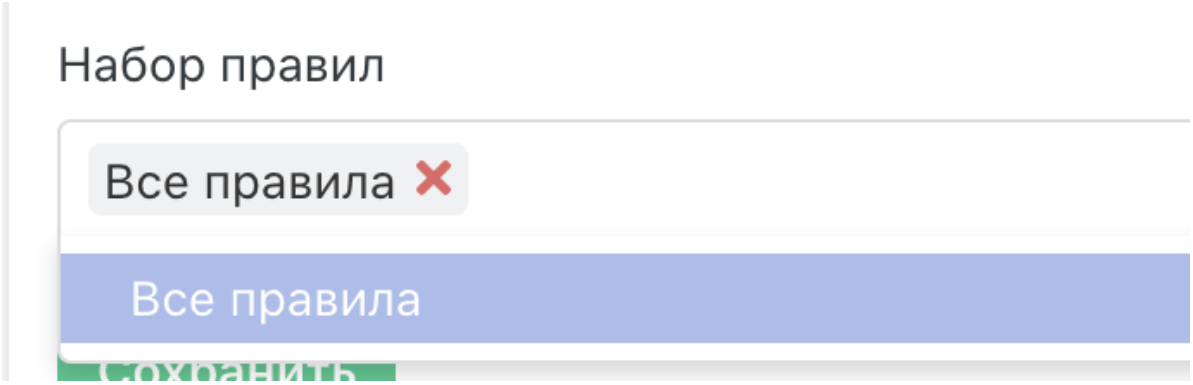


Рисунок 144 - Назначение политики контроля группе активов

15.4. Запуск процесса проверки соответствия

Процесс проверки соответствия ПО запускается пользователем Платформы 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.

15.5. Анализ результатов проверок соответствия ПО

15.5.1. Просмотр сводных результатов проверок соответствия ПО

Сводные результаты всех текущих проверок соответствия ПО расположены в разделе: **"Оценка соответствия ПО"-> "Результаты соответствия ПО"** (см. Рисунок 145).

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

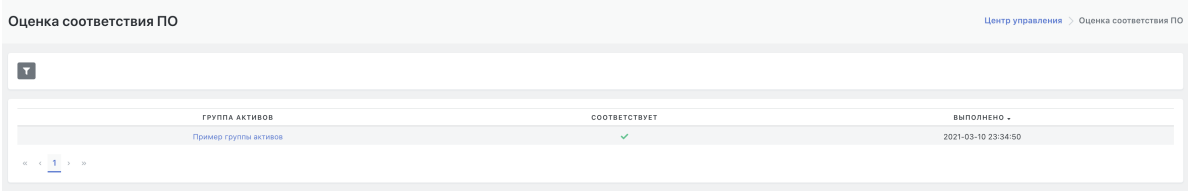


Рисунок 145 - Окно вкладки «Результаты соответствия ПО»

15.5.2. 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 146):

- "**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 на Платформе.
    - **"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 146 - Просмотр результатов контроля соответствия по группе активов

15.6. Управление политиками проверки соответствия ПО

15.6.1. Просмотр текущего списка политик

Текущий список политик расположен в разделе: **"Оценка соответствия ПО"-> "Наборы правил"** (см. Рисунок 147).

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

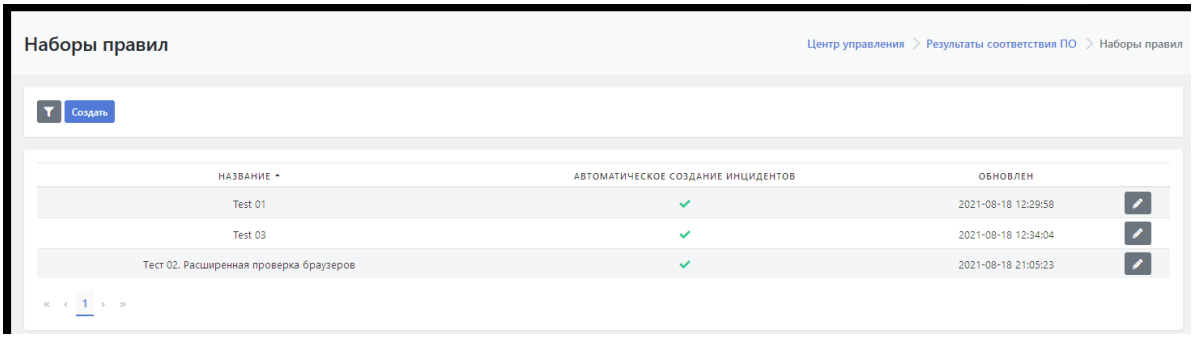


Рисунок 147 - Список политик проверки соответствия ПО (набор правил)

15.6.2. Создание новой политики

Для создания политики проверки соответствия ПО необходимо:

1. Перейти в раздел **"Оценка соответствия ПО"-> "Наборы правил"** (см. Рисунок 147).
2. Нажать на кнопку "**Создать**".
3. Заполнить форму создания политики проверки (см. Рисунок 148):
    - **"Название клиента"**– название политики в Платформе;
    - 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.

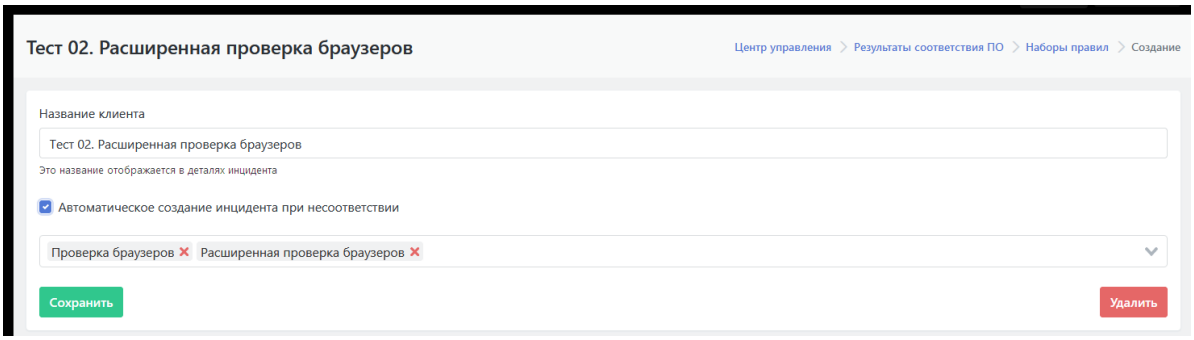


Рисунок 148 - Создание новой политики (набора правил)

15.6.3. 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 148).

15.6.4. 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 148).

15.7. Управление правилами

15.7.1. Просмотр текущего списка правил

Текущий список правил расположен в разделе: **"Оценка соответствия ПО"-> "Правила"** (см. Рисунок 149).

Полное описание табличного списка политик приведено в разделе "*Подраздел "Правила"* ".

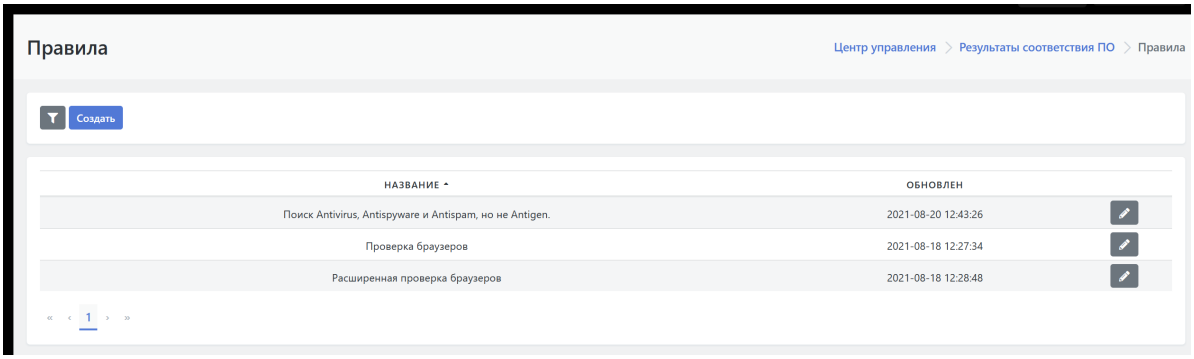


Рисунок 149 - Текущий список правил проверки

15.7.2. Создание нового правила

Для создания нового правила проверки соответствия ПО необходимо:

1. Перейти в раздел **"Оценка соответствия ПО"-> "Правила"** (см. Рисунок 149).
2. Нажать на кнопку "**Создать**".
3. Заполнить форму создания правила (см. Рисунок 150):
    - **"Название клиента"**– название правила в Платформе;
    - 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**".

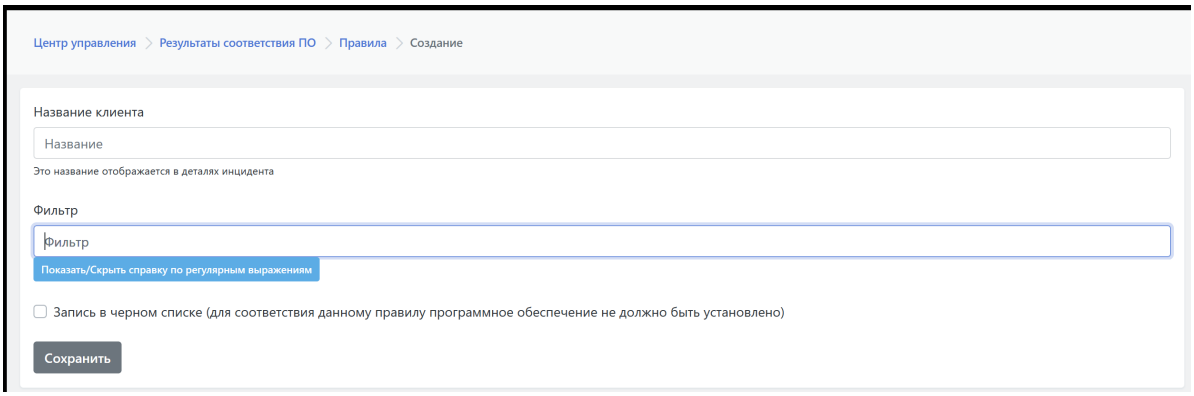


Рисунок 150 - Создание нового правила

15.7.3. 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 151).

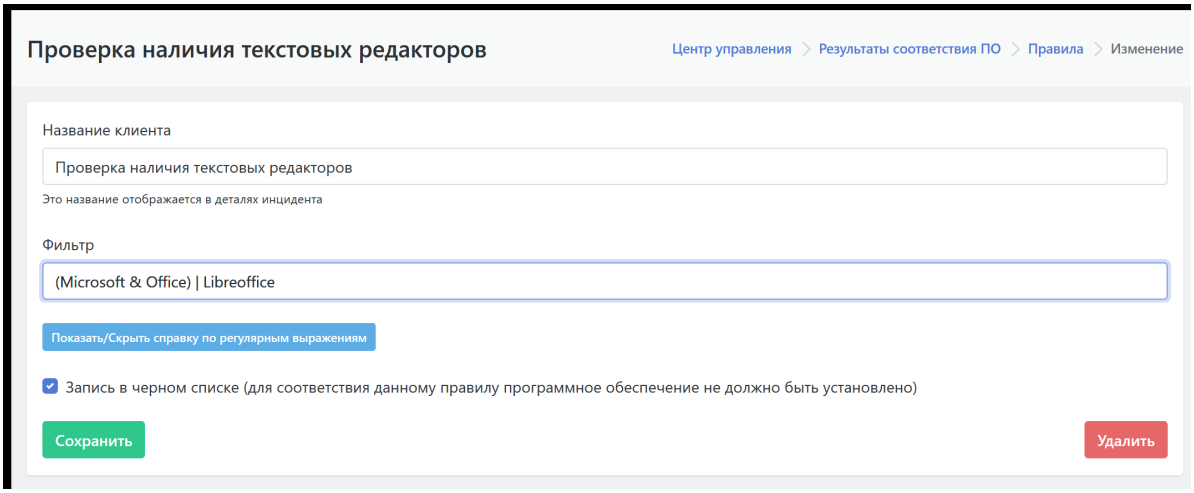


Рисунок 151 - Редактирование правила

15.7.4. 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 150).
4. В открывшейся форме подтвердить удаление нажав на кнопку **"Ok"**.

16. Интеграция со сканерами уязвимостей

Для наглядности наши специалисты подготовили видео фрагмент для работы с сканерами уязвимостей SIEM "Платформа Радар"

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.

16.1. Загрузка результатов сканирования

Для импорта результатов сканирования необходимо:

- Перейти в раздел «Активы» на вкладку «Результаты сканирования»
- Нажать кнопку «Создать»
- Выбрать тип сканера из выпадающего списка (Рисунок 1)
- Загрузить через появившуюся форму файл с результатами сканирования (Рисунок 2)
- В появившемся файле нажать на пиктограмму

  () (Рисунок 3)

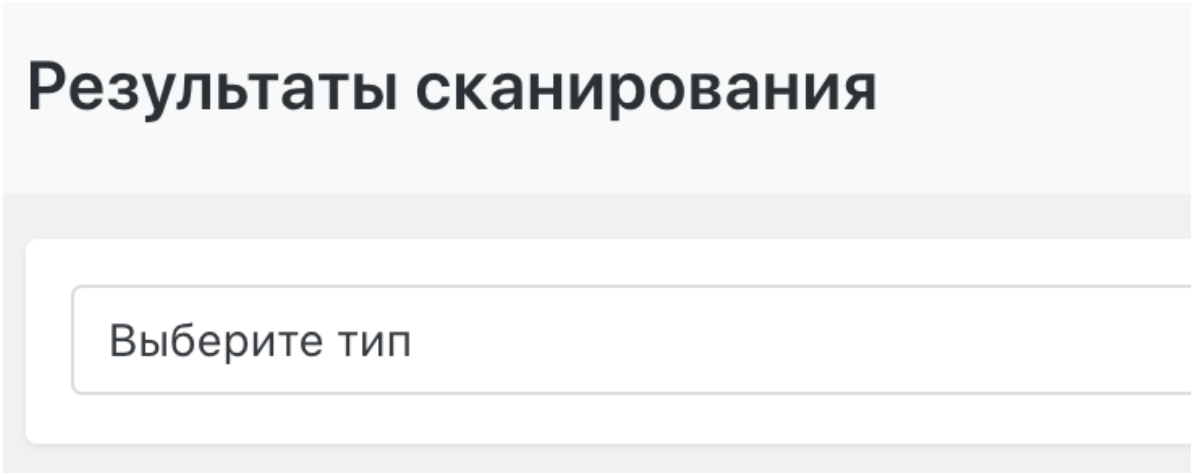


Рисунок 153 - форма выбора типа сканера

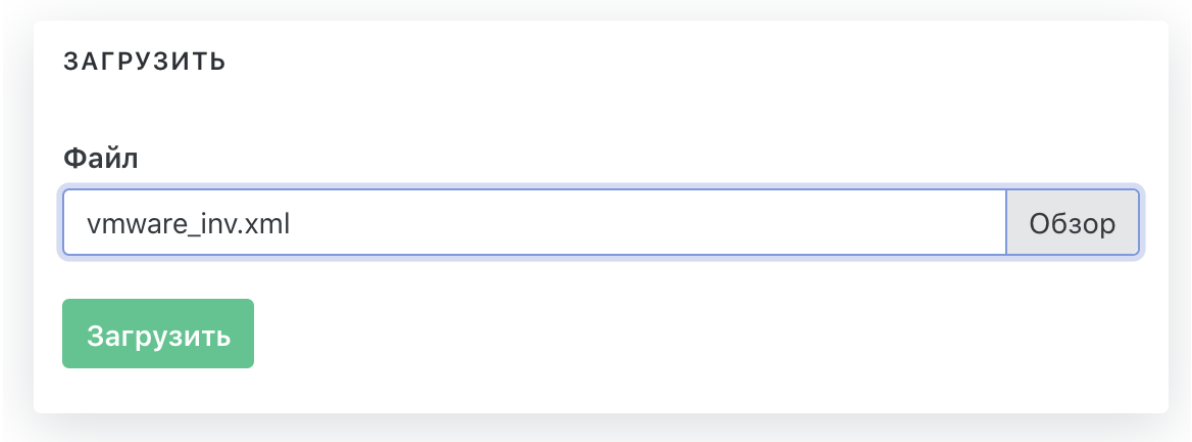


Рисунок 154 - форма загрузки файла результата сканирования

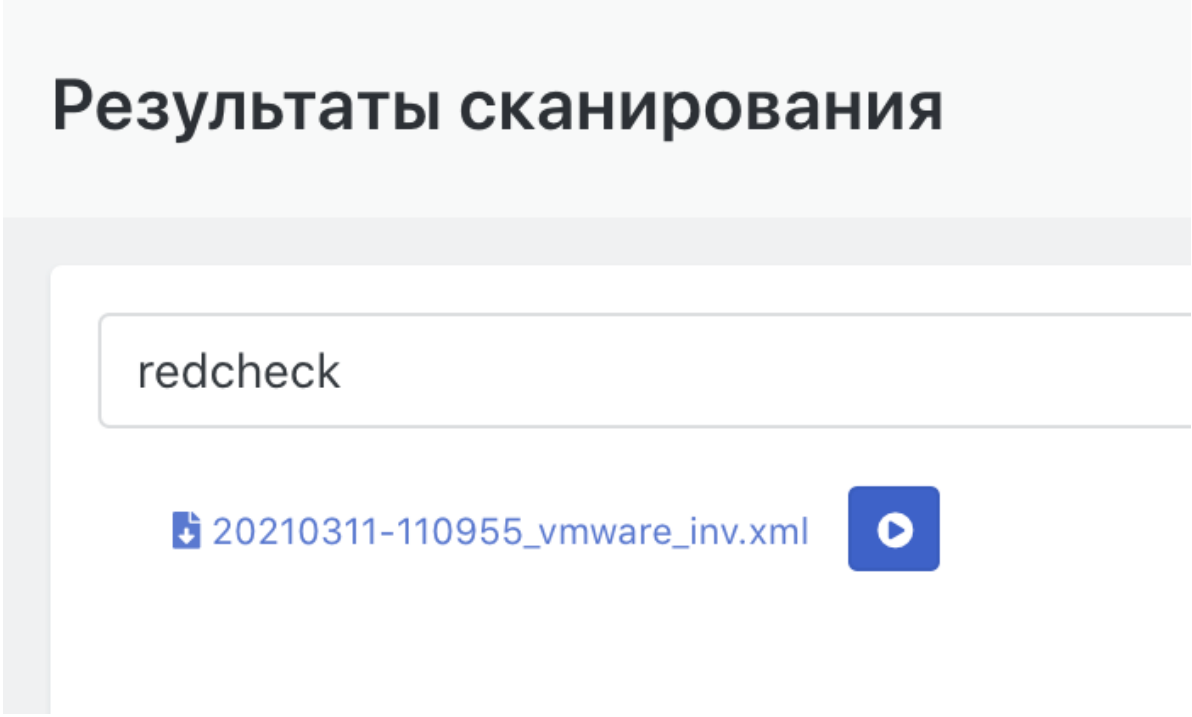


Рисунок 155 - Список загруженных файлов для старта запуска обработки отчета

16.2. Просмотр результатов сканирования

Для просмотра деталей импортированного сканирования необходимо:

- Перейти в раздел «Активы», вкладка «Результаты сканирования».
- Кликнуть на название импортированной задачи.

В форме отображаются количественные результаты найденных уязвимостей, разделенные на группы важности по цвету согласно оценке CVSS (Рисунок 4):

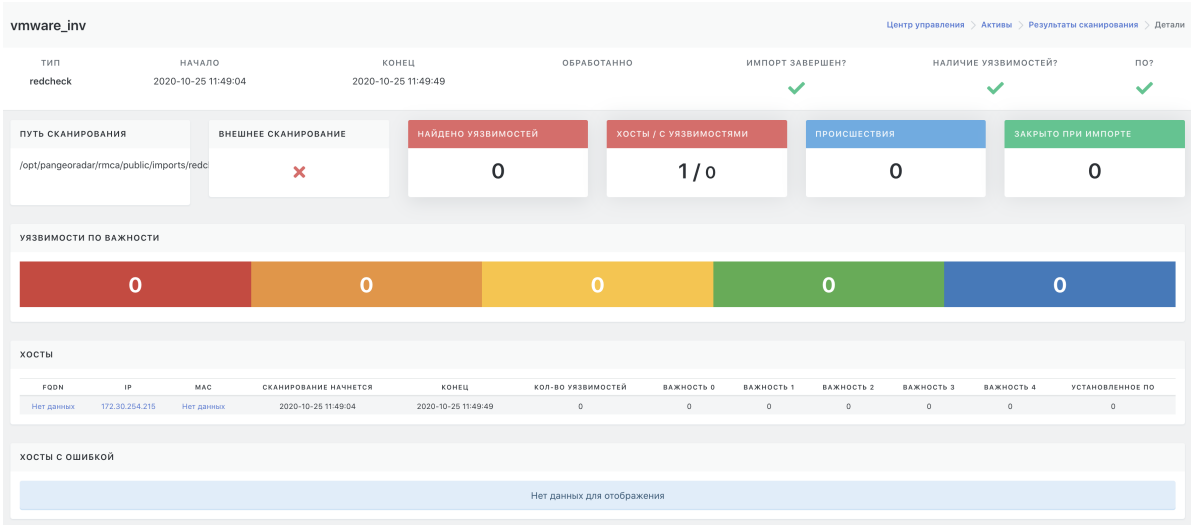


Рисунок 156 - Окно просмотра результатов сканирования

17. Работа с отчетами

Система позволяет выполнять все работы с отчетами и дашбордами в пользовательском веб-интерфейсе

17.1. 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 содержит два типа предустановленных отчетов: **"Главная"** и **"Для печати"**.

17.2. Просмотр отчетов

17.2.1. Вывод отчета на экран

Для просмотра отчетов необходимо выполнить следующие действия (см. Рисунок 157):

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"*).

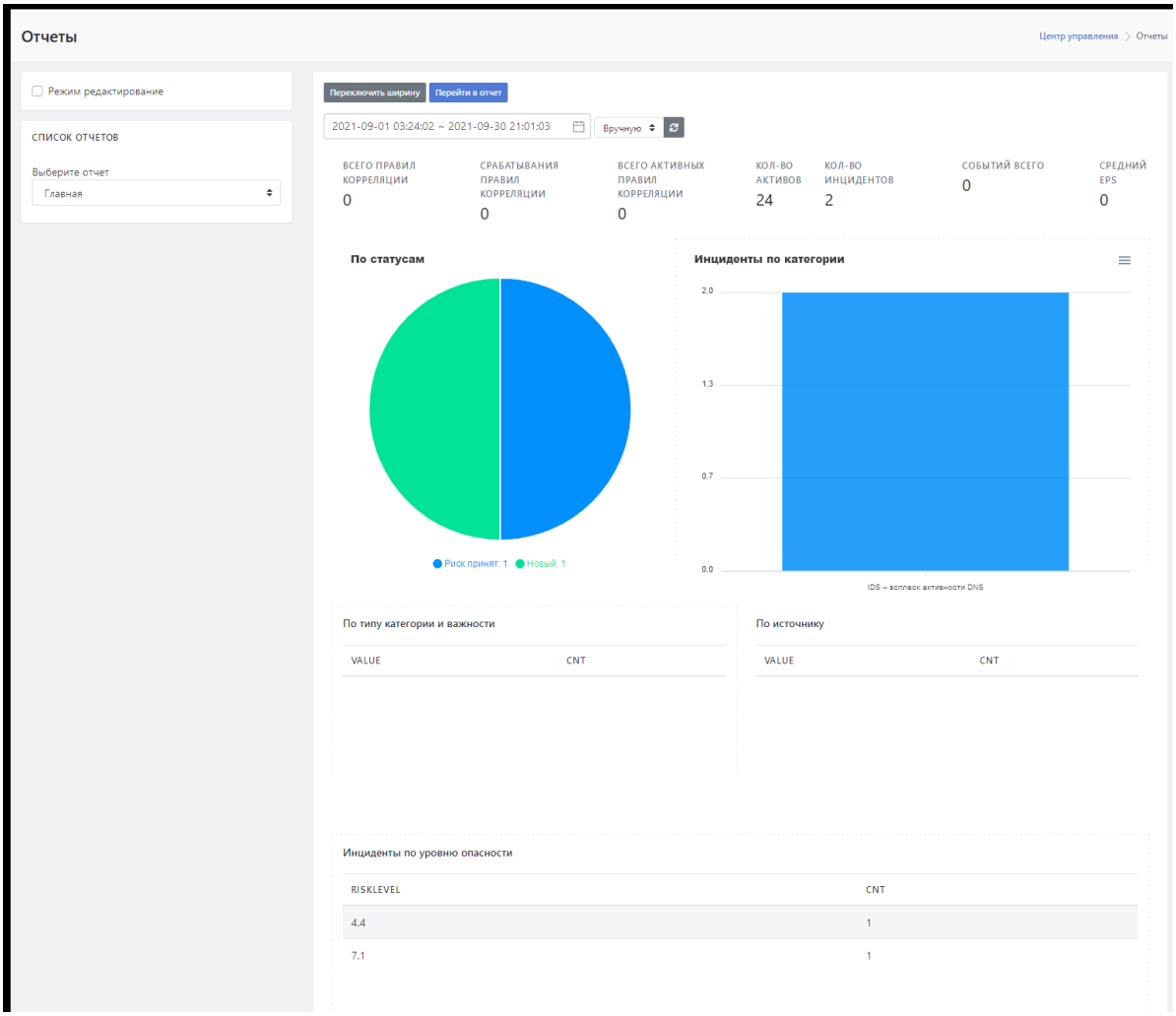


Рисунок 157 - Просмотр отчета

17.2.2. Настройка временного интервала для отчета {#set_time_report}

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 158). Если необходимо указать один день, то два раза щелкнуть по нужному дню.

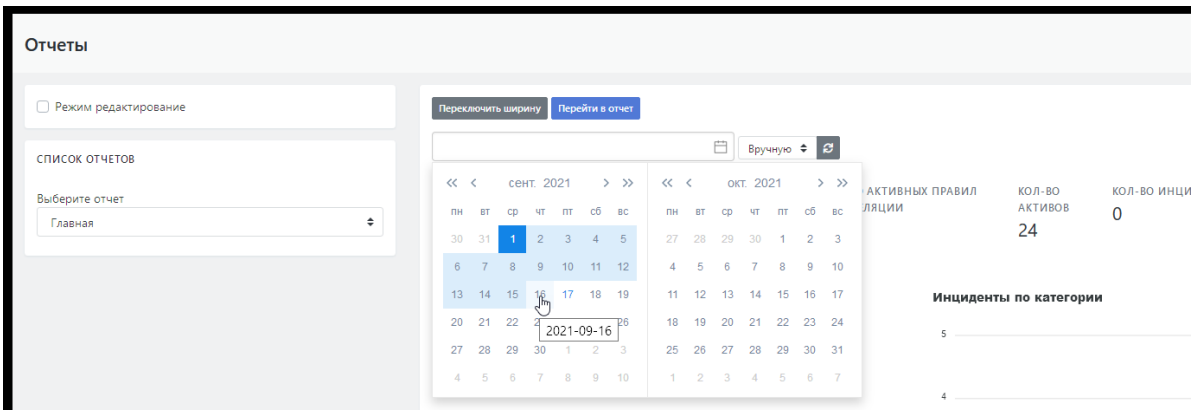


Рисунок 158 - Установка дат начала и конца временного интервала выборки данных для отчета

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 161).

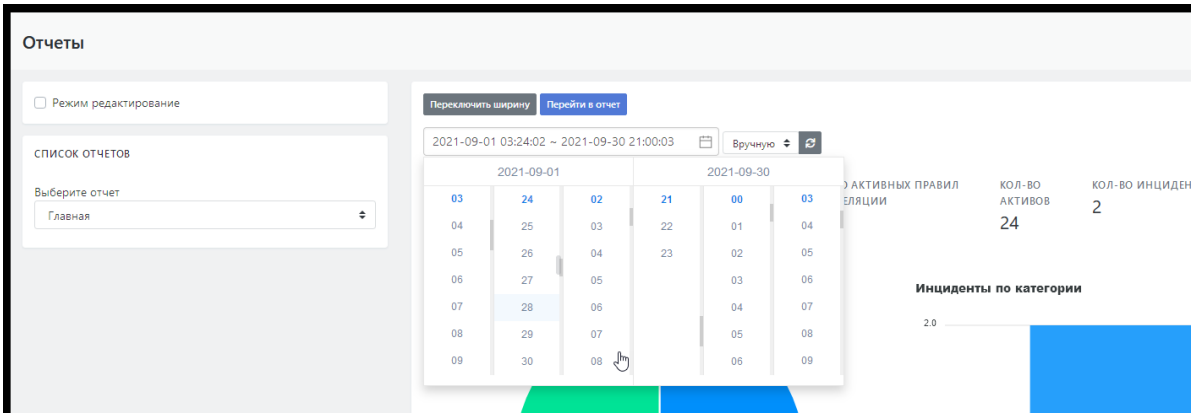


Рисунок 159 - Установка времени для дат начала и конца временного интервала выборки данных для отчета

После установки временного интервала в отчете отобразятся данные за указанный интервал.

17.2.3. Настройка обновления данных отчета {#set_dataupdate_report}

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.

17.2.4. Настройка отчета для печати {#set_print_report}

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 160).

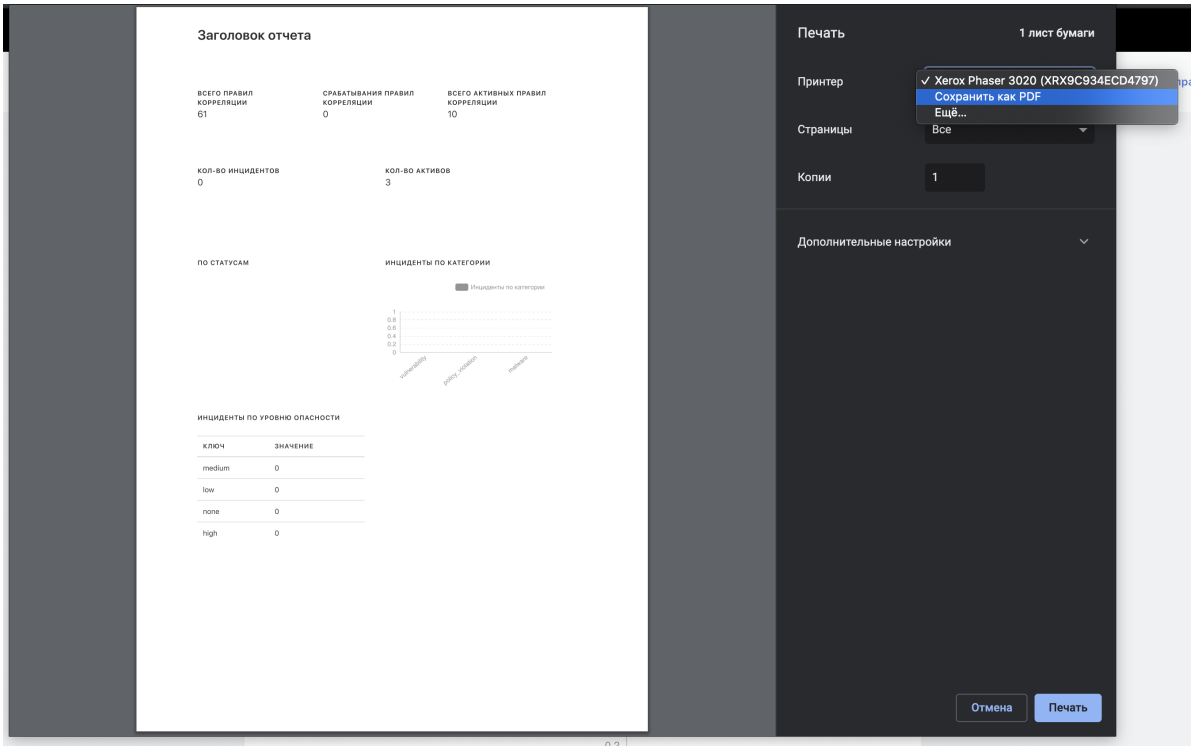


Рисунок 160 - Печать отчета и сохранение его в PDF

17.2.5. Назначение и описание предустановленных отчетов

Платформа 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 (см. раздел *"Описание интерфейса. Рабочий стол"*). Предустановленная форма отчета включает в себя стандартный набор основных данных по инцидентам (см. Рисунок 161):

- **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.

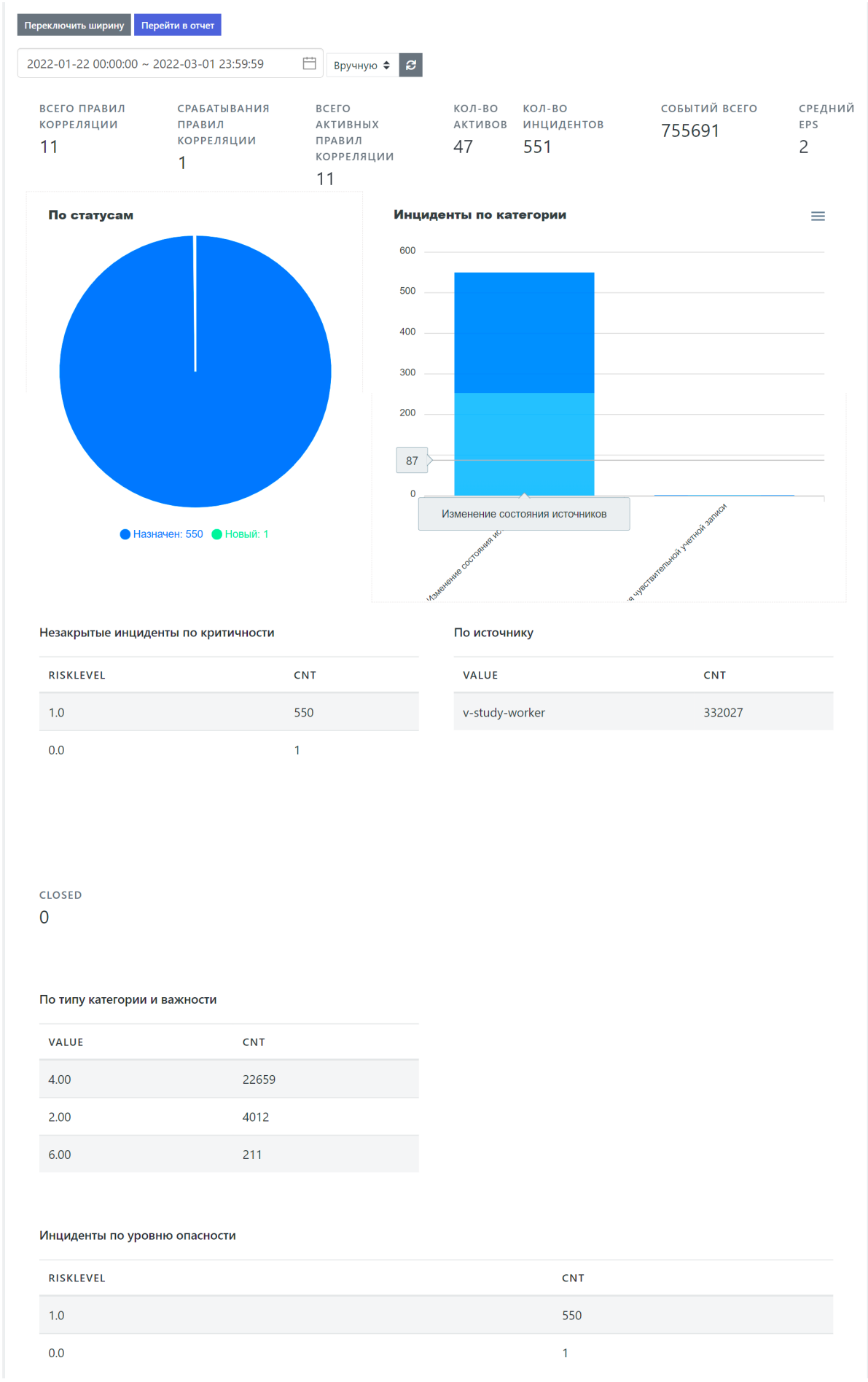


Рисунок 161 - Отчет "**Главная**", предустановленный состав полей отчета

Отчет **"Для печати"** - это отчет, в котором набор данных скомпонован для условий вывода на печать или просмотра в виде PDF-файла (под формат A4). 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 162):

- **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.

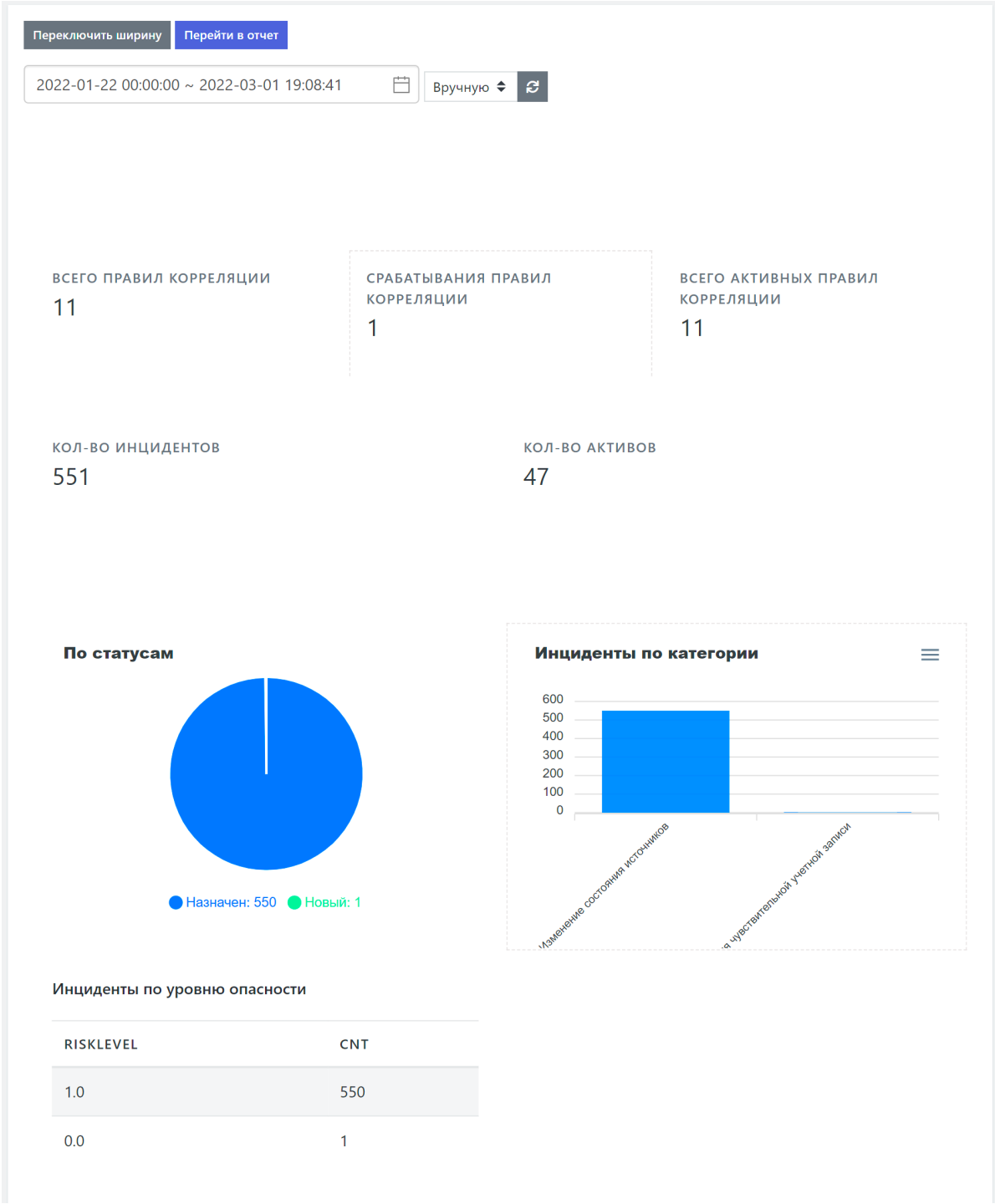


Рисунок 162 - Отчет "**Для печати**", предустановленный состав полей отчета

17.3. Управление отчетами

17.3.1. Закрепление отчета на рабочем столе

Для закрепления отчета на рабочем столе как отчета "по умолчанию" необходимо выполнить следующие действия (см. Рисунок 161):

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.

5. Вернуться в раздел **"Отчеты"** и убедится что в рабочей области раздела отображается заданный отчет.

Функция установки отчета "по умолчанию" - кнопка **"Поставить на главную"**:

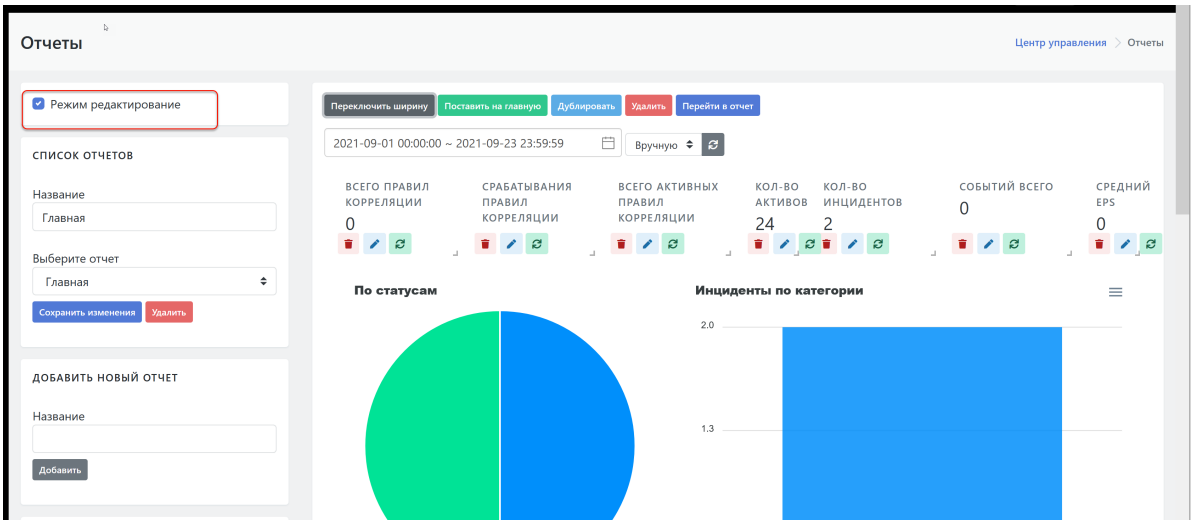


Рисунок 163 - Работа с отчетами в режиме редактирования

17.3.2. 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 162).

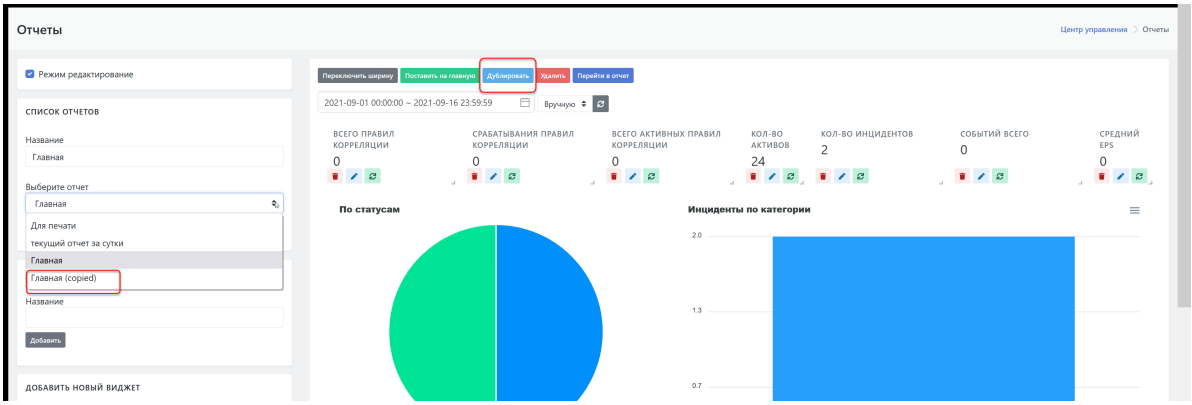


Рисунок 164 - Дублирование отчета

17.3.3. 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"*.

17.3.4. Редактирование отчета

Для редактирования отчета необходимо выполнить следующие действия:

1. Перейти в режим редактирования, установив флажок в поле **"Режим редактирования"**.
2. Выбрать интересующий отчет в списке отчетов.
3. 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.
4. Нажать на кнопку **"Сохранить изменения"**, расположенную под списком отчетов.

Работа с виджетами подробно приведена в разделе *"Управление виджетами"*.

17.3.5. Удаление отчета

Для удаления отчета с Платформы 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.

17.4. Управление виджетами {#vidgets}

Внимание! Все действия по управлению виджетами в отчетах совершаются в режиме редактирования. Для этого необходимо установить флажок в поле **"Режим редактирования"**.

17.4.1. Добавление нового виджета {#add_vidget}

Добавление в отчет нового виджета приведено ниже в разделе *"Создание виджетов на основе сохраненных фильтров/запросов. Провайдеры"*.

17.4.2. 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"**.

17.4.3. 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 165).
4. Для сохранения нового размера виджета в отчете нажать на кнопку **"Сохранить изменения"**.

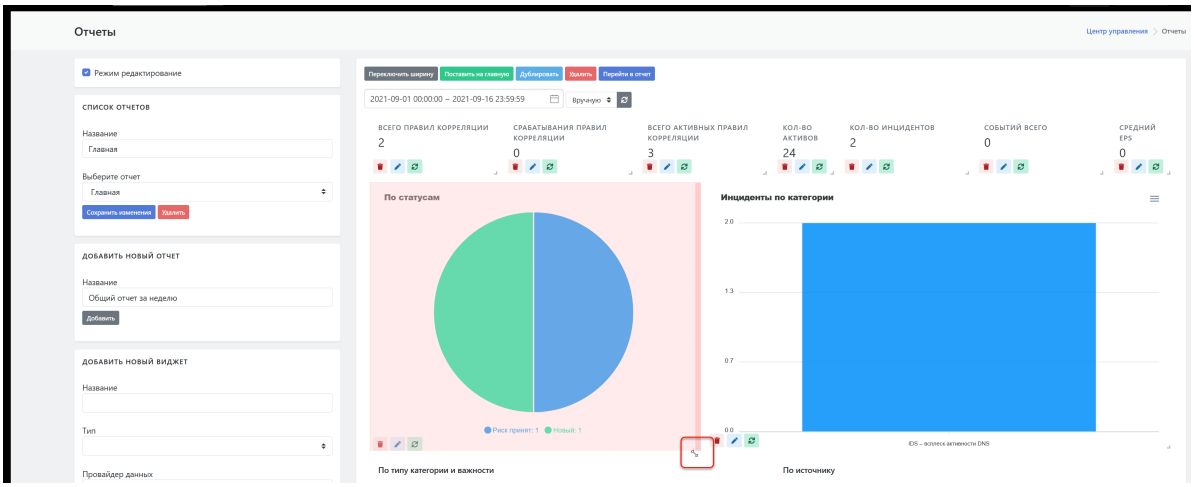


Рисунок 165 - Изменение размера виджета

17.4.4. Редактирование параметров существующего 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.

17.4.5. 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"**.

17.4.6. Типы виджетов

17.4.6.1. Перечень типов виджетов

Перечень типов виджетов представлен в раскрывающемся списке **"Тип"** (см. Рисунок 166).

Платформа 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".

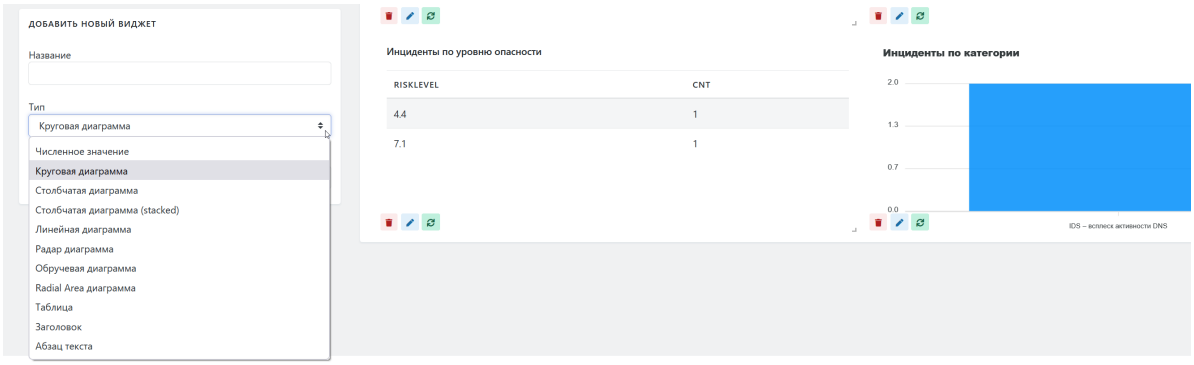


Рисунок 166 - Типы виджетов

17.4.6.2. Численное значение

Данный виджет содержит в себе целое число из результата запроса к базе данных (см. Рисунок 167).

Поддерживается провайдерами:

- SIEM;
- Коррелятор;
- События;
- Сохраненные фильтры;

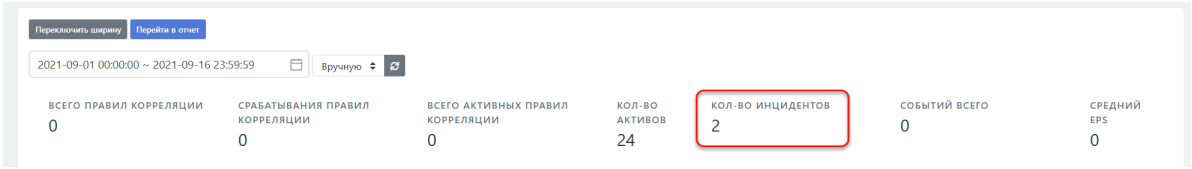


Рисунок 167 - Пример виджетов типа «Численное значение»

17.4.6.3. Круговая диаграмма

Тит виджета "Круговая диаграмма" (см. Рисунок 168) поддерживается провайдерами:

- SIEM;
- Коррелятор;
- События.

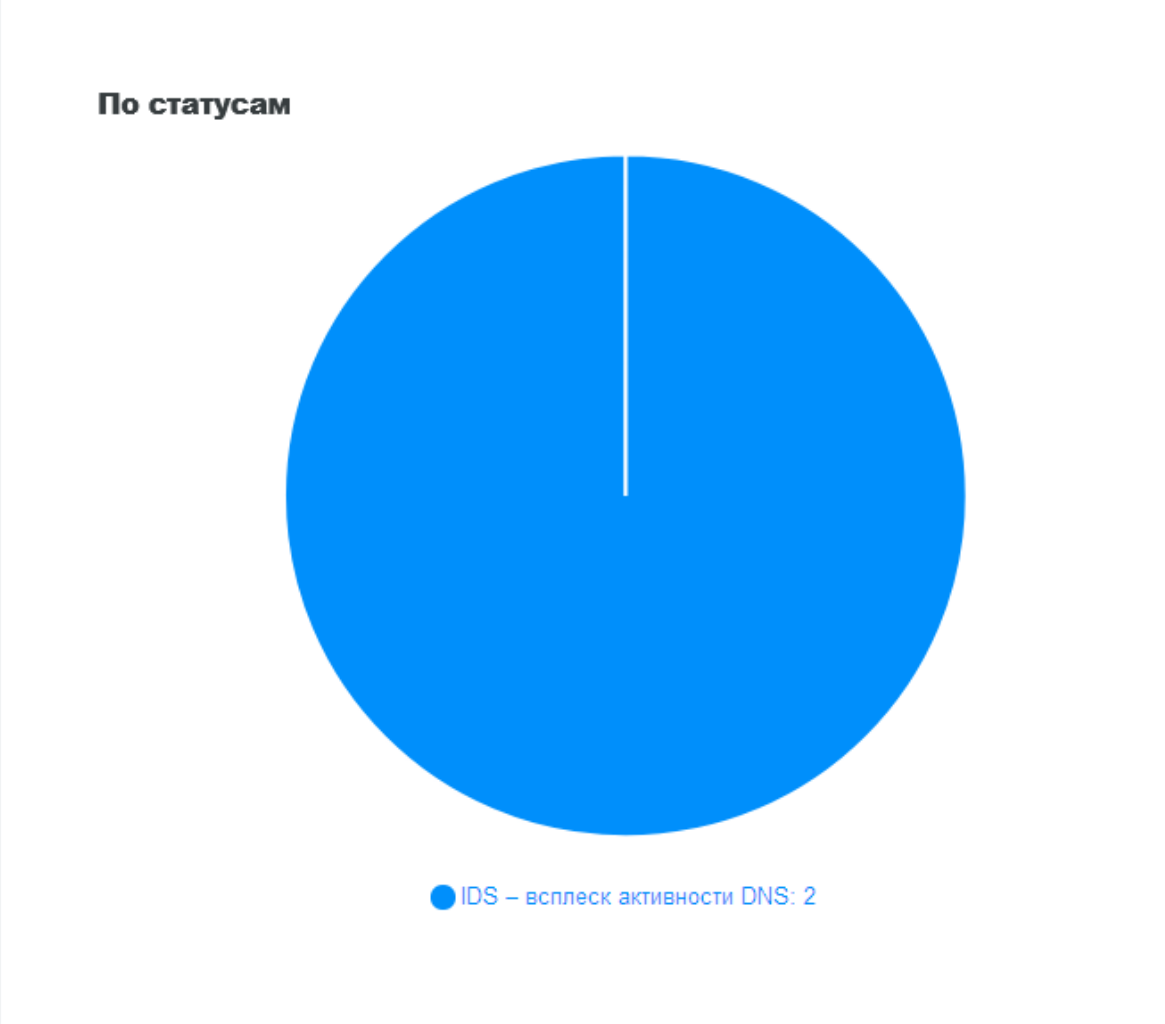


Рисунок 168 - Пример виджета типа «Круговая диаграмма»

17.4.6.4. Столбчатая диаграмма

Тит виджета "Столбчатая диаграмма" (см. Рисунок 169) поддерживается провайдерами:

- SIEM;
- Коррелятор;
- События.

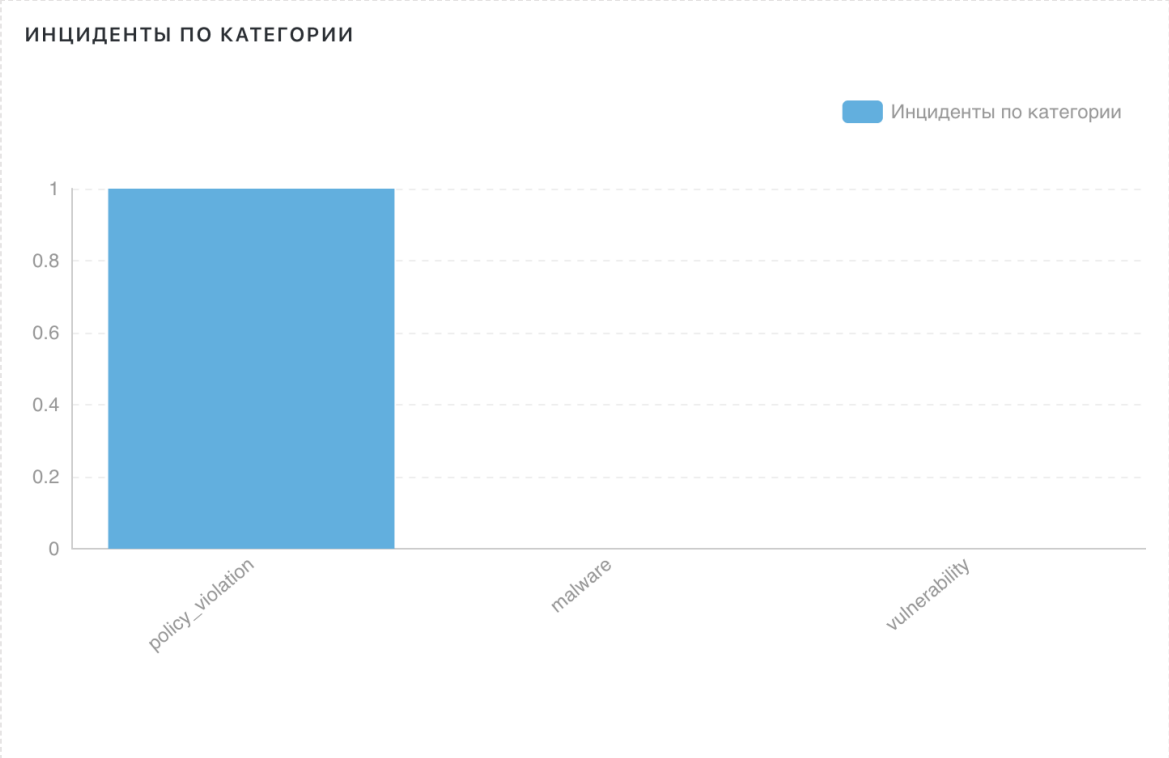


Рисунок 169 - Пример виджета типа «Столбчатая диаграмма»

17.4.6.5. Таблица

Тит виджета "Таблица" (см. Рисунок 170) поддерживается провайдерами: :

- SIEM;
- Коррелятор.

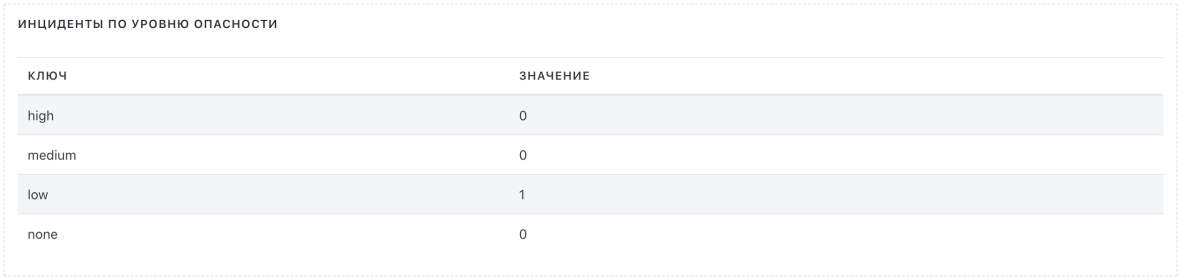


Рисунок 170 - Пример виджета типа «Таблица»

17.4.6.6. Заголовок

Информационный виджет - отображает заранее сохраненный текст в настройках виджета (см. Рисунок 171).

Рисунок 171 - Пример виджета типа «Заголовок»

17.5. Создание виджетов на основе сохраненных фильтров/запросов. Провайдеры {#vidgets_providers}

17.5.1. Провайдеры. Общее описание

Платформа 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);

17.5.2. Добавление в отчет нового виджета {#add_vidget_report}

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 171).
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.

Общий отчет

Сохранить изменения | Удалить

ДОБАВИТЬ НОВЫЙ ОТЧЕТ

Название

Общий отчет за неделю

Добавить

ДОБАВИТЬ НОВЫЙ ВИДЖЕТ

Название

Количество инцидентов

Тип

Круговая диаграмма

Провайдер данных

Готовые запросы

Запрос

Поле

total

```
groupField - поле первого уровня группировки
groupType - тип группировки (terms, cardinality, value_count, tim
subGroupField - второй уровень группировки (включается только есл
subGroupType - тип группировки (terms, cardinality, value_count)
esIndex - индекс поиска, по умолчанию normal*
whereFieldsMap - json для фильтрафии формата ключ: значение (всег,
whereFieldsMapNot - json для фильтрафии формата ключ: значение (в
esSort - правила сортировки { "name" : "desc" }
```

Параметры

Ключ	Тип	Значение

Добавить поле

page	1	
per_page	1	
order_value	updated_at	
order_direction		

```
{
  "page": 1,
  "per_page": 1,
  "order_value": "updated_at",
  "order_direction": false
}
```

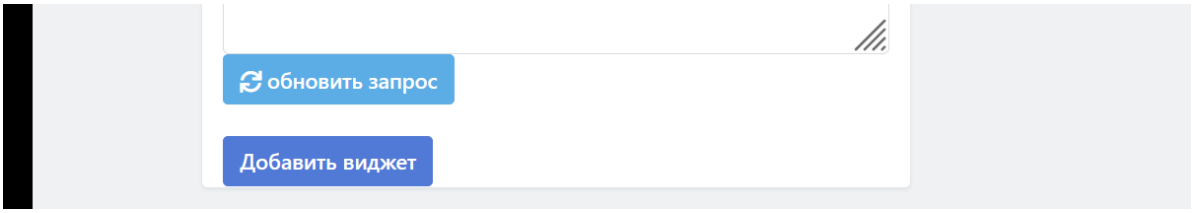


Рисунок 172 - Добавление нового виджета

18. Работа с правилами корреляции

Раздел содержит описание процессов, связанных с настройкой и обслуживанием правил корреляции.

18.1. Предустановленные правила корреляции. Разработка правил корреляции

Платформа 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. Процесс разработки правил корреляции приведен в отдельном документе Описание специальных функций для правил корреляции.

18.2. Управление правилами корреляции

18.2.1. Включение правил корреляции

Для включения правил корреляции необходимо:

1. Зайти в раздел **"Коррелятор"->"Правила"**.
2. В табличном списке правил найти интересующее выключенное правило.
3. В строке правила нажать на пиктограмму ✖ статуса активности (см. Рисунок 173).

Статус правила сменится на Активное, в поле отобразится пиктограмма ✔ .

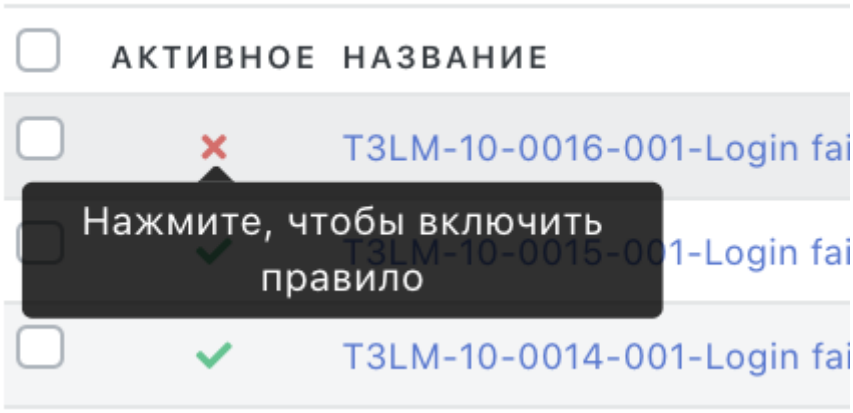


Рисунок 173 - Включение правил корреляции в списке правил в разделе "Корреляторы"->"Правила"

18.2.2. Выключение правил корреляции

Для выключения правил корреляции необходимо:

1. Зайти в раздел **"Коррелятор"->"Правила"**.
2. В табличном списке правил найти интересующее включенное правило.
3. В строке правила нажать на пиктограмму ✔ статуса активности (см. Рисунок 174).

Статус правила сменится на Неактивное, в поле отобразится пиктограмма ✖ .

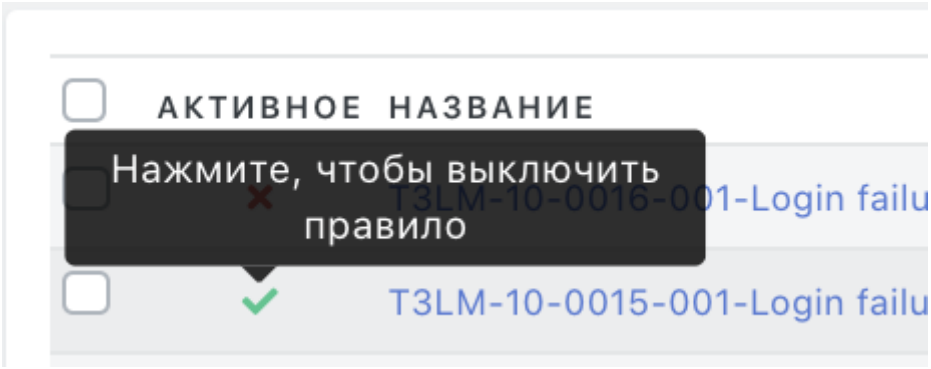


Рисунок 174 - Выключение правил корреляции в списке правил в разделе "Корреляторы"->"Правила"

18.3. Обработка результатов работы правил корреляции

18.3.1. Источник результатов работы правил корреляции

Результаты работы правил корреляции создаются при вызове функции alert в правиле корреляции. Подробное описание приведено в отдельном документе Описание специальных функций для правил корреляции.

18.3.2. Просмотр деталей инцидента, созданного по результатам работы правил корреляции

Для перехода к просмотру результата работы правила корреляции необходимо выполнить следующие действия:

1. Зайти в раздел **"Коррелятор"->"Результаты"**.
2. В табличном списке найти интересующий инцидент и щелкнуть по заголовку результата (поле "Заголовок результата").

Откроется форма с детализацией инцидента, созданного по результатам работы правил корреляции. Детализированная информация состоит из нескольких блоков.

Блок сводной информации (см. Рисунок 175) содержит следующие параметры:

- Заголовок - заголовок инцидента;
- Произошло - время определения инцидента правилами корреляции;
- Время создания - время "ручного" оформления инцидента в системе;
- Время последнего изменения - время последнего изменения параметров инцидента.

Заголовок	nono
Произошло	2021-02-18 15:24:15
Время создания	2021-02-20 14:05:49
Время последнего изменения	2021-02-20 14:05:50

Рисунок 175 - Форма детализации инцидента. Блок сводной информации

Блок описания правила корреляции (см. Рисунок 176) одержит следующие параметры:

- "**Оценка риска**";
- "**Правило**" - название используемого при обнаружении инцидента правила корреляции.
- **"Ключ из правил"**;
- **"Тип инцидента"**;
- **"Актив"** - адрес актива, на котором был зафиксирован инцидент.
- **"Инцидент"**.

Оценка риска	5.5
Правило	T3LM-10-0009-001-MS-WIN-Local authentication: account brutforce followed by success login
Ключ из правила	
Тип инцидента	MS-WIN-Local authentication Атака методом подбора завершилась успешным входом в систему
Актив	172.30.254.146
Инцидент	

Рисунок 176 - Форма детализации инцидента. Блок описания правила

Так же в форме детализации инцидента отображаются детали анализа события, передаваемые из правила в инцидент. Детали события, по которому создан инцидент, приведены ниже (см. Рисунок 177).

СОБЫТИЕ


```
{
    "event": {
        "uuid": "AAAAAGAuXG+Q42xaECx0ZrejFUCzrt8b",
        "logsource": {
            "host": "172.30.254.146:9092",
            "input": "1514-Microsoft-Windows-Eventlog",
            "application": "os",
            "name": "Microsoft Windows",
            "product": "windows",
            "subsystem": "authentication",
            "vendor": "microsoft"
        },
```


Рисунок 177 - Детали анализа события, по которому был создан инцидент

18.3.3. Конвертирование результатов работы правил корреляции в инцидент

Решение о необходимости конвертирования результатов работы правила в инцидент принимается пользователем после анализа результатов работы правила корреляции.

Для конвертирования в инцидент одного результата необходимо выполнить следующие действия:

1. Зайти в раздел **"Коррелятор"->"Результаты"**.
2. Нажать на кнопку **Инцидент** напротив результата, который нужно конвертировать в инцидент.

Выбранный результат будет преобразован в инцидент (см. Рисунок 177).

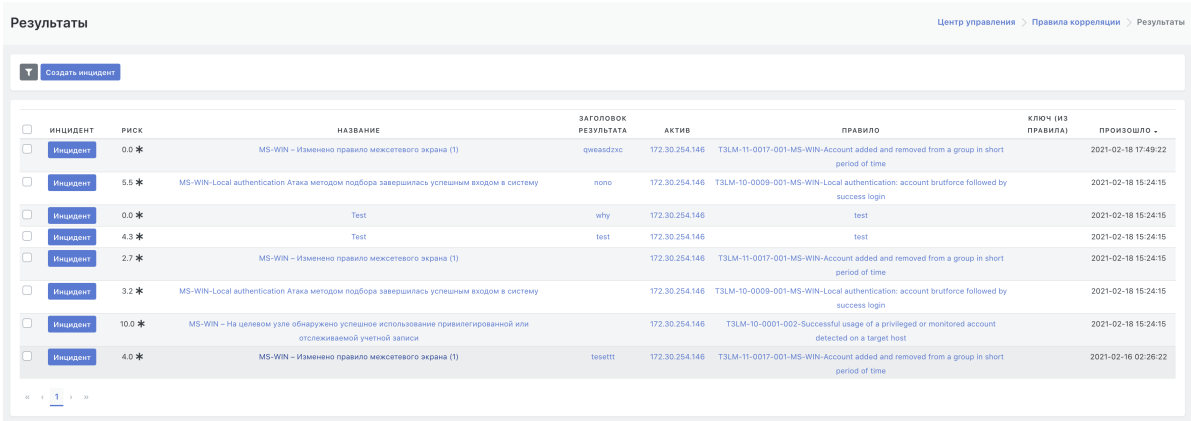


Рисунок 178 - Окно конвертирования результатов в инцидент

Для просмотра созданного инцидента нужно нажать на кнопку **Инцидент**.

18.4. Основные возможности применения правил корреляции

18.4.1. Настройка корреляции по количественному признаку {#cor_set_count}

В правилах корреляции присутствуют переменные, позволяющие настроить правило по количественным признакам. Это такие переменные, как:

- временное окно детектирования - стандартное имя переменной в Платформе: **detection_windows**.
- пороговые значения количества событий или объектов - рекомендуется при создании пороговых переменных, присваивать им имена, которые содержат слово **threshold**. Например, переменная **files_threshold** - порог срабатывания по количеству обнаруженных файлов для правила корреляции "Обнаружение загрузки вредоносного файла".

Для правил корреляции, использующих данные переменные, можно настраивать значения переменных под текущие требования использования правила.

Для настройки существующего правила корреляции по количественному признаку необходимо:

1. В веб-интерфейсе Платформы перейти в раздел **"Коррелятор"->"Правила"**.
2. Выбрать в списке правил корреляции интересующее правило и открыть его на редактирование нажав  .
3. Отредактировать правило в части временного окна и порогового значения (см. Рисунок 179).
4. Нажать кнопку **Сохранить**.

Согласно правилу корреляции, происшествие будет сформировано в Платформе при превышении событиями (объектами) заданного порога в рамках заданного временного окна.

Каточка Инцидента в веб-интерфейсе должна содержать Происшествия, связанные с инцидентом. При просмотре деталей происшествия, должны отображаться события спровоцировавшие происшествие.

Подробное описание работы с правилами корреляции и описание основных стандартных правил корреляции приведены в документе *"Руководство разработчика правил корреляции"*.

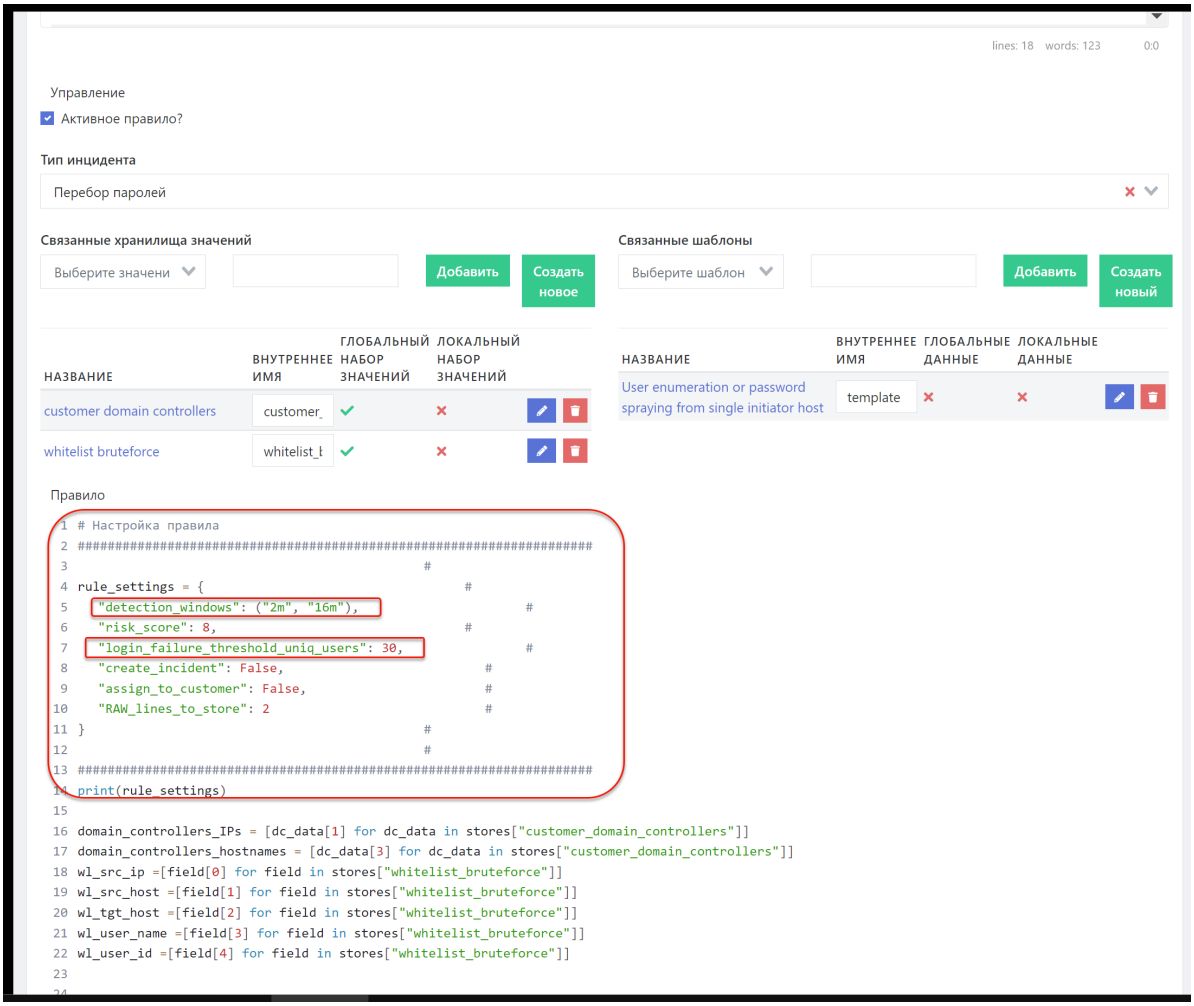


Рисунок 179 - Настройка правила корреляции по количественным параметрам

18.4.2. Формирование корреляции по последовательности событий

В Платформе предусмотрена возможность создания правила корреляции, работающего по последовательности событий. Например, правила типа: «Многочисленные неудачные попытки входа, с последующим успешным входом на узел».

Для таких правил устанавливаются пороговые переменные на каждый тип события из последовательности событий (описание количественных переменных и редактирование правила см. выше в раздел *"Настройка корреляции по количественному признаку"*). Например, для правила «Многочисленные неудачные попытки входа, с последующим успешным входом на узел»:

1. Должны быть установлены:
    - пороговая переменная на событие "неудачный вход" - устанавливается порог на допустимое количество неудачных входов;
    - пороговая переменная на событие "удачный вход" - устанавливается значение "1".
2. В правиле настраивается соответствующая цепочка событий.

Если в разделе **"Инциденты"** выбрать в списке инцидентов инцидент по последовательности событий и открыть его карточку, то в карточке инцидента должны отображаться данные по каждому происшествию в последовательности и по каждому событию, спровоцировавшему последовательность происшествий.

Подробное описание работы с правилами корреляции и описание основных стандартных правил корреляции приведены в документе *"Руководство разработчика правил корреляции"*.

18.4.3. Поддержка операций выделения фрагментов события в правилах корреляции

Подробнее в разделе **Фильтрация событий**

18.4.4. Настройка автоматического оповещения пользователя при срабатывании правила корреляции

При необходимости в Платформе можно настроить систему автоматического оповещения пользователя на электронную почту, ответственного за инцидент, при срабатывании правила корреляции.

Подробнее в разделе **Toller**

18.4.5. Особенности многоуровневого применения правил корреляции

Возможно использование сработок одного правила на обход другого правила.

18.4.6. 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 скопировать его нажатием иконки 

Добавить префикс в имени правила `retro_` и изменить в правиле ключ, который будет использоваться для подписки на очередь с историческими данными.

Для изменения ключа необходимо на странице редактирования правила найти строку с функцией `@log_connection.fetch` и указать в ней ключ, который далее планируется использовать в задаче по ретроспективному анализу. Наименование ключа может быть любым. Наименование в примере `#.retro-event-clear.#`

> При создании нового правила, для тестирования его на исторических данных, нужно сразу указать необходимый ключ в функции подписи на очередь событий и указать в префиксе названия правила `retro_`.

Вид измененной функции:
%%(python)
@log_connection.fetch('#.retro-event-clear.#')
%%

После внесения изменений в правило нажать кнопку **Клонировать**.

Далее необходимо создать задачу по ретроспективному анализу. Для этого нужно перейти в раздел **Коррелятор** - **Ретроспективная корреляция**.

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.
Ключ в правиле - указать ключ, который был задан в правиле корреляции, подготовленном для ретроспективного анализа.
Индекс - указать индексы, по которым необходимо произвести анализ (поддерживается wildcard символ "*").

После настройки параметров необходимо нажать **Создать задачу**.

После выполнения вышеописанных действий система запустит созданную задачу с указанными параметрами.

19. Работа с сообщениями

19.1. Общие данные об используемых на Платформе сообщениях

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.

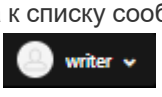
Сообщение может быть отправлено с дополнительной контекстной информацией.

В качестве контекста сообщений могут выступать следующие сущности:

- Тип инцидента.
- Инцидент.
- Актив.

В случае наличия контекста в сообщение добавляется ссылка на соответствующий объект.

19.2. 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 180).

Подробное описание интерфейса раздела "**Сообщения**" приведено в отдельном разделе документации *"Пользовательские настройки. Профиль -Сообщения"*.

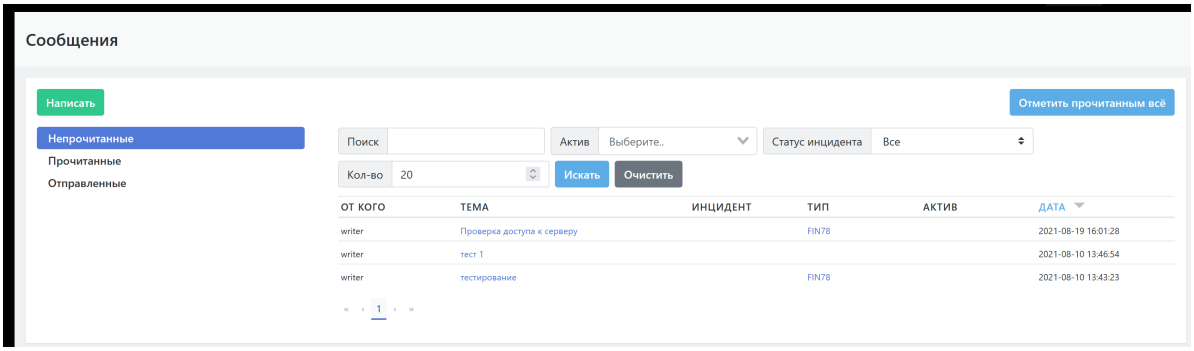


Рисунок 180 - Список сообщений в профиле пользователя

19.3. Просмотр деталей сообщения

19.3.0.1. 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 181):

- "**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 -- 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 документации *"Создание и отправка сообщений"*.

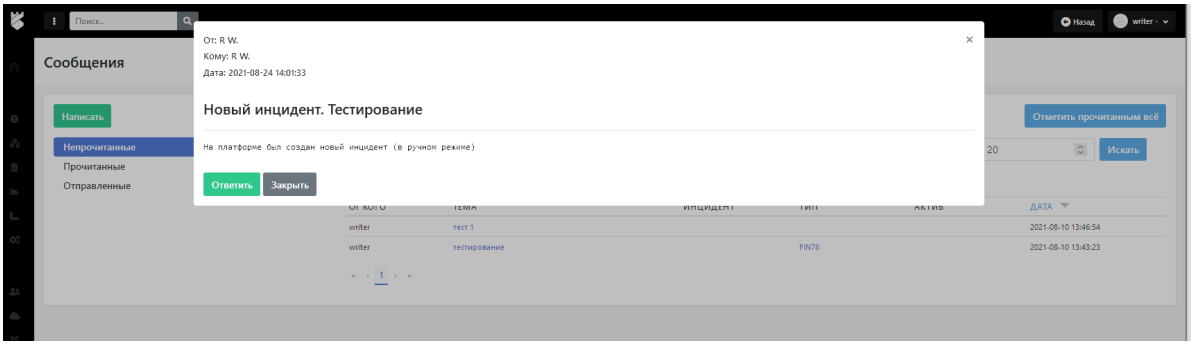


Рисунок 181 - Окно просмотра сообщения

19.3.0.2. 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 182):

- Поле "**Инцидент**" -- содержит название инцидента, с которым связано данное сообщение. Гиперссылка ведет на страницу описания данного инцидента.
- Поле "**Тип**" -- содержит идентификатор типа инцидента, с которым связано данное сообщение. Гиперссылка ведет на страницу описания данного типа инцидента.
- Поле "**Актив**" -- содержит идентификатор (например IP-адрес) актива, с которым связано данное сообщение. Гиперссылка ведет на страницу описания данного актива.

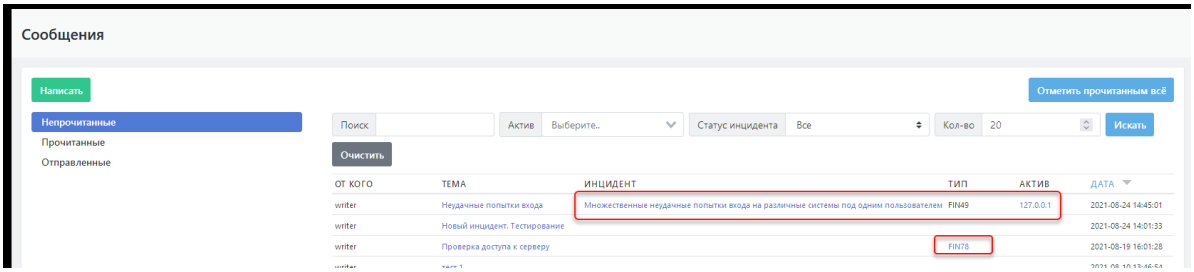


Рисунок 182 - Гиперссылки сообщений с контекстной информацией

19.4. Создание и отправка сообщений {#create_message}

19.4.1. Отправка сообщения без контекстной информации {#message_send_nocontext}

Для отправки сообщения без ссылки на объект (без контекстной информации) необходимо:

1. Перейти в раздел «**Сообщения**» -- в профиле пользователя 

выбрать пункт "Сообщения".
2. Нажать кнопку «**Написать**».
3. В открывшейся форме сообщения заполнить следующие поля (см. Рисунок 183):
    - "**Получатель**" -- выбрать адресата из раскрывающегося списка пользователей Платформы;
    - "**Заголовок**" -- ввести заголовок сообщения;
    - "**Сообщение**" -- ввести текст сообщения.
4. Нажать на кнопку "**Отправить**".

Данное сообщение должно появится в списке отправленных сообщений пользователя.

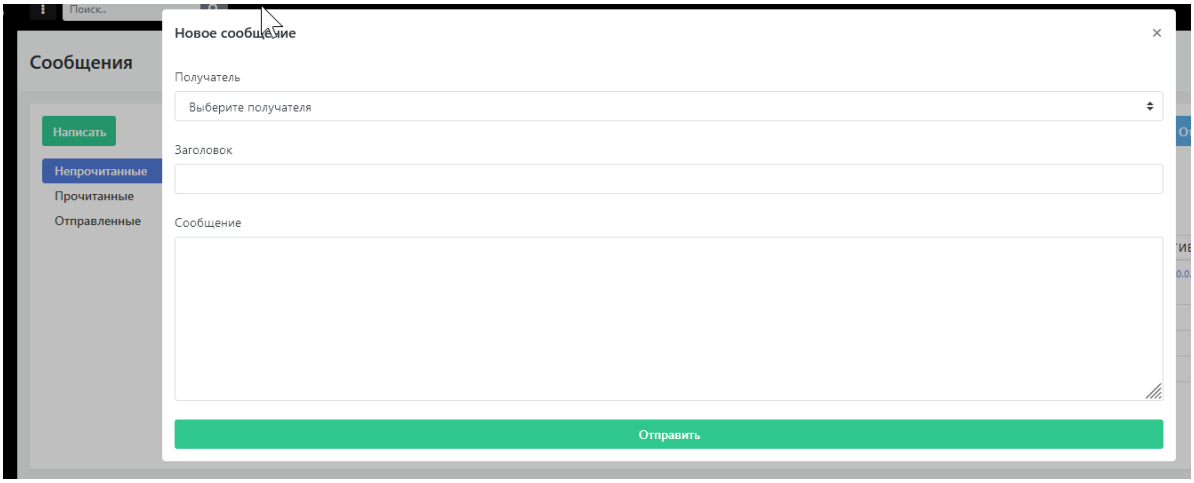


Рисунок 183 - Отправка сообщения без ссылки на объект

19.4.2. 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 подразделе документации *"Отправка сообщения без контекстной информации"*.

20. НКЦКИ

20.1. Общая информация

Для создания карточки инцедента в ГосСОПКА необходимо учитывать поля:

`objectid` - "Объекты ГосСОПКА"

Представляет собой объект сопки, фактически адрес, по которому объект находится. С соответствующими вытекающими. Адреса задаются едиными идентификаторами, отмечается статус объекта (активен/не активен) и тд. На сегодняшний день мы не реализуем на своей стороне создание таких объектов. Поэтому при первичной настройке сопки у клиента необходимо зайти на портал сопки и зарегистрировать объект и записать его ID. Он понадобится в будущем.

`subjectid` - "Субъекты ГосСОПКА"

Субъект СОПКА. Проще говоря Юр лицо. На это указывают все поля которые нужно будет заполнять: Код из справочника ОКОПФ, Название бренда, ИНН, ОГРН и прочее.Наравне с объектом, создаем в интерфейсе сопки и сохраняем ID.

`systemid` - "Системы(ИТС) ГосСОПКА"

`description` : "Название системы" Под системой понимается некоторая совокупность железа/софта, выполняющих определенную роль.

Характеризуется такими значениями:

- Категория значимости

```
enum:
  - 5  # "СВТ/АРМ",
  - 4  # "ИСПДн",
  - 3  # "АСУ ТП",
  - 2  # "АС (автоматизированная система)",
  - 1  # "ИС/ИТС/ГИС/МИС/ГеоИС",
  - 0  # "Другое"
```

- Тип секретной информации
- Тип Конфиденциальности

20.2. Как зарегистрировать актив в ГосСОПКе

1. Создаем группу активов. В группе указываем `objectid` и `subjectid` Эти данные, в большинстве случаев, будут портироваться на все активы одной группы. Если в компании будет несколько разных юр лиц, или физически объектов, в которых есть КИИ, то создаем под каждый свою группу.
2. Отмечаем в свойствах группу галочку "КИИ". Т.t. мы указываем, что актив, который принадлежит этой группе может быть отправлен в ГосСОПКу. Важно – актив может принадлежать только одной группе с категорией КИИ. Это связано с ограничением как раз, на те самые `objectid` и `subjectid`. Один актив не может быть привязан сразу к нескольким объектам. Целостность проверяется на уровне системы.
3. Установить `system_id` для каждого актив. В настройках активов есть `systemid`. Т.к. это достаточно уникальное значение, мы приняли решение указывать его для каждого актива вручную. Если рабочий кейс покажет, что это очень неудобно и есть реальная необходимость часто указывать один и тот же системный идентификатор в разных активах, то необходимо добавить такую фичу:
4. Добавить в группы новый параметр `systemid`. Все активы КИИ привязывать к двум группам, первая это группа с флаком КИИ, как написано выше, вторая группа, это группа из которой будут унаследованы systemid.Придется проверять уникальность групп с `systemid`

(один актив не может принадлежать к более чем одной группе с `systemid`)если в актив уже прописан `systemid`, брать его приоритетным.

5. Записать в группу или в каждый актив "Технический специалист" и "Технический специалист". Также можно указать в актив, данные указанные напрямую в актив имеют приоритет.
6. Указать в инцинденте корректным тип инцидента. Список "тип инцидента" используется Платформой для идентификации какие данные мы отправляем в ГосСОПКу. Т.е. если пришел индцидент, где мы описываем вредоносное ПО, то указываем malware и будет применен соответствующий маппинг.
7. Наконец получив инцидент, если все условия выше выполнены, то в его описании появится кнопка "синхронизировать", по этой кнопке мы перейдем в интерфейс синхронизации где можем гранулярно выбрать что и куда синхронищировать.