Платформа Радар

Руководство оператора

Версия 4.1.0

ООО «Пангео Радар»

Оглавление

1. Общие сведения о «Платформе Радар» ... 11
2. Требования ... 12
3. Вход в платформу ... 13
4. Интерфейс платформы ... 14
   - 4.1 Шапка сайта ... 15
   - 4.2 Панель разделов ... 15
   - 4.3 Универсальные таблицы ... 18
     - 4.3.1 Настройка сортировки и фильтрации записей таблицы ... 19
     - 4.3.2 Настройки отображения полей ... 20
   - 4.4 Боковая панель ... 21
     - 4.4.1 Поиск объектов в списке ... 22
     - 4.4.2 Сортировка и фильтрация объектов в списке ... 22
     - 4.4.3 Массовые действия ... 22
   - 4.5 Папки контента ... 24
   - 4.6 Формы работы с объектами ... 25
     - 4.6.1 Шаблоны объектов ... 26
     - 4.6.2 Визуализации ... 27
5. События ... 28
   - 5.1 Общие данные ... 28
     - 5.1.1 График "Поток событий" ... 29
     - 5.1.2 Топ-10 значений по выделенной области потока событий ... 30
       - 5.1.2.1 Масштабирование графика потока событий ... 32
     - 5.1.3 Список событий ... 33
   - 5.2 Работа с фильтрами ... 36
     - 5.2.1 Настройка запросов ... 38
       - 5.2.1.1 Добавление запроса в условия фильтра ... 38
       - 5.2.1.2 Сохранение конфигурации запроса ... 41
     - 5.2.2 Настройка агрегации ... 42
       - 5.2.2.1 Добавление агрегации ... 43
       - 5.2.2.2 Добавление подагрегации ... 45
       - 5.2.2.3 Сохранение агрегации ... 45
     - 5.2.3 Работа с пресетами ... 46
       - 5.2.3.1 Создание пресета ... 47
       - 5.2.3.2 Применение пресета ... 48
       - 5.2.3.3 Удаление пресета ... 48
     - 5.2.4 История поиска ... 48
   - 5.3 Работа с событиями ... 49
     - 5.3.1 Создание инцидента ... 50
     - 5.3.2 Добавление события в инцидент ... 52

5.3.3 Поиск инцидента ... 52
5.3.4 Экспорт списка событий ... 53
5.3.5 Вспомогательные инструменты для анализа событий ... 54
5.3.5.1 Поиск событий ... 54
5.3.5.2 Просмотр событий по сформированной агрегации ... 56
5.3.5.3 Настройка плотности отрисовки потока событий ... 56
5.3.5.4 Сортировка событий ... 57
5.3.5.5 Настройка набора полей для табличного вида ... 58
6. Инциденты ИБ ... 60
6.1 Инциденты ... 60
6.1.1 Общие данные ... 60
6.1.2 Создание инцидента ... 63
6.1.3 Просмотр инцидента ... 65
6.1.3.1 Общая информация об инциденте ... 66
6.1.3.2 Информация об активе ... 68
6.1.3.3 Информация о происшествиях ... 68
6.1.3.4 История коммуникации ... 70
6.1.4 Назначение инцидента ... 71
6.1.5 Изменение статуса инцидента ... 71
6.1.6 Добавление комментария к инциденту ... 71
6.1.7 Редактирование инцидента ... 72
6.1.8 Просмотр истории изменения инцидента ... 72
6.1.9 Удаление инцидента ... 73
6.2 Типы инцидентов ... 73
6.2.1 Общие сведения ... 73
6.2.2 Просмотр и анализ типа инцидента ... 75
6.2.3 Создание типа инцидента ... 76
6.2.4 Редактирование типа инцидента ... 77
6.2.5 Написать ответственному ... 77
6.2.6 Дублирование типа инцидента ... 78
6.2.7 Импорт типов инцидентов ... 78
6.2.8 Экспорт типов инцидентов ... 78
6.2.9 Экспорт типов инцидентов в CSV ... 78
6.2.10 Удаление типа инцидента ... 78
6.3 Группы инцидентов ... 78
6.3.1 Просмотр группы инцидентов ... 80
6.3.2 Создание группы инцидентов ... 81
6.3.3 Редактирование группы инцидентов ... 82
6.3.4 Назначение группы инцидентов пользователю ... 82
6.3.5 Назначение группы инцидентов группе пользователей ... 82
6.3.6 Добавление инцидентов в группу ... 82
6.3.7 Массовое закрытие инцидентов через группу ... 82
6.3.8 Откреплление инцидентов от группы ... 82

6.3.9 Удаление группы инцидентов ... 83
6.4 Происшествия на отправку ... 83
6.5 Дополнительные поля ... 83
6.5.1 Создание дополнительного поля ... 84
6.5.2 Редактирование дополнительного поля ... 85
6.5.3 Добавление дополнительного поля в инцидент ... 85
6.5.4 Просмотр значений дополнительного поля ... 86
6.5.5 Удаление дополнительного поля ... 86
7. Активы ... 87
7.1 Активы ... 87
7.1.1 Общие данные ... 87
7.1.2 Просмотр и анализ актива ... 89
7.1.3 Создание актива ... 90
7.1.4 Редактирование актива ... 92
7.1.5 Добавление актива в группу ... 92
7.1.6 Написать ответственному ... 92
7.1.7 Удаление актива ... 93
7.2 Группы активов ... 93
7.2.1 Создание группы активов ... 94
7.2.2 Просмотр группы активов ... 96
7.2.3 Редактирование группы активов ... 97
7.2.4 Настройка автоматического добавления актива в группу ... 97
7.2.5 Написать ответственному ... 98
7.2.6 Удаление группы активов ... 98
7.3 Настройки идентификации активов ... 99
7.3.1 Создание стратегии идентификации активов ... 100
7.3.2 Редактирование стратегии идентификации активов ... 100
7.3.3 Удаление стратегии идентификации активов ... 100
7.4 Сетевые интерфейсы ... 100
7.4.1 Просмотр сетевого интерфейса ... 101
7.4.2 Создание сетевого интерфейса ... 102
7.4.3 Редактирование сетевого интерфейса ... 103
7.4.4 Удаление сетевого интерфейса ... 103
7.5 Результаты сканирования ... 104
7.5.1 Импорт результатов сканирования ... 104
7.5.2 Просмотр списка результатов сканирования ... 105
7.5.3 Просмотр результата сканирования ... 106
7.5.3.1 Основная информация о результате сканирования ... 106
7.5.3.2 Информация о просканированных хостах ... 107
7.5.4 Сравнение результатов сканирования ... 108
7.5.4.1 Создание инцидентов по результатам сравнения ... 110
7.5.4.2 Закрытие инцидентов по результатам сравнения ... 110
7.5.5 Изменение статуса результата сканирования ... 110
7.6 Обнаружение хостов ... 111

7.7 Обнаружение сервисов ... 112
7.8 Сбор данных ... 113
8. Соответствие ПО ... 115
8.1 Общие сведения ... 115
8.2 Результаты соответствия ПО ... 115
8.2.1 Запуск процесса проверки соответствия ПО ... 116
8.2.2 Просмотр информации о результате соответствия ПО ... 117
8.2.3 Удаление результатов соответствия ПО ... 117
8.3 Список ПО ... 118
8.3.1 Просмотр информации о ПО ... 119
8.3.2 Просмотр информации об активах, на которых установлено ПО ... 120
8.3.3 Редактирование записи о ПО ... 120
8.3.4 Удаление записи о ПО из платформы ... 120
8.4 Список групп ПО ... 121
8.4.1 Создание группы ПО ... 122
8.4.2 Просмотр группы ПО ... 123
8.4.3 Редактирование группы ПО ... 123
8.4.4 Удаление группы ПО ... 123
8.5 Правила соответствия ПО ... 124
8.5.1 Создание правила соответствия ПО ... 125
8.5.2 Просмотр правила соответствия ПО ... 126
8.5.3 Редактирование правила соответствия ПО ... 126
8.5.4 Удаление правила соответствия ПО ... 126
8.6 Наборы правил соответствия ПО ... 127
8.6.1 Создание политики соответствия ПО ... 128
8.6.2 Просмотр политики соответствия ПО ... 128
8.6.3 Редактирование политики соответствия ПО ... 129
8.6.4 Удаление политики соответствия ПО ... 129
9. Коррелятор ... 131
9.1 Общие данные ... 131
9.2 Правила корреляции ... 131
9.2.1 Просмотр статистики работы правил ... 133
9.2.1.1 Вкладка "Инциденты" ... 133
9.2.1.2 Вкладка "Результаты" ... 135
9.2.1.3 Вкладка "Лог изменений" ... 135
9.2.1.4 Вкладка "Лог правила" ... 136
9.2.1.5 Вкладка "Метрики" ... 136
9.2.2 Создание и настройка правила ... 138
9.2.2.1 Создание правила с помощью визуального конструктора ... 138
9.2.2.2 Создание правила с помощью скриптового языка Lua ... 151
9.2.3 Редактирование правила ... 156
9.2.4 Активация правила ... 156
9.2.5 Перезапуск правила ... 156

9.2.6 Дублирование правила ... 157
9.2.7 Конвертирование правила в код Lua ... 157
9.2.8 Импорт правил ... 157
9.2.9 Экспорт правил ... 157
9.2.10 Удаление правила ... 157
9.2.11 Массовые действия над правилами ... 158
9.2.12 Действия над результатами сработок правила ... 159
9.2.12.1 Создание инцидента ... 159
9.2.12.2 Просмотр события ... 159
9.3 Пересылка событий ... 160
9.3.1 Общие данные ... 160
9.3.2 Включение пересылки событий ... 161
9.3.3 Просмотр фильтра для пересылки событий ... 162
9.3.4 Создание фильтра для пересылки событий ... 163
9.3.5 Редактирование фильтра для пересылки событий ... 164
9.3.6 Дублирование фильтра для пересылки событий ... 165
9.3.7 Импорт фильтров ... 165
9.3.8 Экспорт фильтров ... 165
9.3.9 Удаление фильтра ... 165
9.4 Фильтры потока событий ... 166
9.4.1 Общие данные ... 166
9.4.2 Просмотр фильтра потока событий ... 166
9.4.3 Создание фильтра потока событий ... 167
9.4.4 Редактирование фильтра потока событий ... 169
9.4.5 Дублирование фильтра потока событий ... 169
9.4.6 Импорт фильтров потока событий ... 169
9.4.7 Экспорт фильтров потока событий ... 170
9.4.8 Удаление фильтра потока событий ... 170
9.5 Макросы ... 170
9.5.1 Общие данные ... 170
9.5.2 Просмотр макроса ... 171
9.5.3 Создание макроса ... 171
9.5.4 Редактирование макроса ... 172
9.5.5 Дублирование макроса ... 172
9.5.6 Импорт макросов ... 172
9.5.7 Экспорт макросов ... 172
9.5.8 Удаление макроса ... 172
9.6 Шаблоны алертов ... 173
9.6.1 Общие данные ... 173
9.6.2 Просмотр шаблона "алерта" ... 173
9.6.3 Создание шаблона "алерта" ... 174
9.6.4 Редактирование шаблона "алерта" ... 175
9.6.5 Дублирование шаблона "алерта" ... 175
9.6.6 Удаление шаблона "алерта" ... 176

9.7 Шаблоны группировки ... 176
9.7.1 Общие данные ... 176
9.7.2 Просмотр шаблона группировки ... 177
9.7.3 Создание шаблона группировки ... 177
9.7.4 Редактирование шаблона группировки ... 179
9.7.5 Дублирование шаблона группировки ... 179
9.7.6 Удаление шаблона группировки ... 180
9.8 Табличные списки ... 180
9.8.1 Общие данные ... 180
9.8.2 Создание табличного списка ... 181
9.8.3 Работа с записями табличного списка ... 182
9.8.4 Редактирование табличного списка ... 183
9.8.5 Дублирование табличного списка ... 183
9.8.6 Импорт табличных списков ... 184
9.8.7 Экспорт табличных списков ... 184
9.8.8 Удаление табличного списка ... 184
9.8.9 Массовые действия над табличными списками ... 185
9.9 Ретроспективная корреляция ... 185
9.9.1 Общие данные ... 185
9.9.2 Добавление задачи для ретроспективной корреляции ... 186
9.9.3 Остановка задачи ... 187
9.9.4 Перезапуск задачи ... 187
9.9.5 Удаление задачи ... 187
9.9.6 Массовые действия над задачами ... 188
10. Параметры ... 189
10.1 Основные параметры ... 189
10.2 Оповещения по задержкам ... 191
10.3 Черный список ID плагинов ... 193
10.4 Фоновые задачи ... 194
10.5 Интеграции ... 195
10.6 Типы интеграций ... 196
10.7 Папки контента ... 196
10.8 Шаблоны ... 197
11. Рабочие столы ... 199
11.1 Общие данные ... 199
11.2 Создание рабочего стола ... 201
11.3 Редактирование рабочего стола ... 202
11.4 Управление виджетами ... 203
11.4.1 Установка периода и обновление данных виджетов ... 204
11.4.2 Добавление виджета на рабочий стол ... 204
11.4.3 Переход к табличному представлению данных ... 204
11.4.4 Редактирование виджета ... 204
11.4.5 Копирование настроек виджета ... 205
11.4.6 Изменение расположения виджета ... 205
11.4.7 Изменение размера виджета ... 205

11.4.8 Удаление виджета ... 205
11.5 Копирование рабочего стола ... 206
11.6 Создание отчета ... 206
11.7 Удаление рабочего стола ... 207
11.8 Grafana. Единицы измерения и временной диапазон ... 207
12. Конструктор виджетов ... 209
12.1 Особенности работы в конструкторе ... 213
12.2 Конструктор запросов ... 213
12.2.1 Добавление запроса ... 214
12.2.1.1 Шаг 1. Выбор источника данных и датасета ... 214
12.2.1.2 Шаг 2. Выбор периода формирования запроса ... 215
12.2.1.3 Шаг 3. Настройка набора полей ... 215
12.2.1.4 Шаг 4. Условия фильтрации ... 217
12.2.1.5 Шаг 5. Группировка и Сортировка ... 217
12.2.2 Копирование запроса ... 218
12.2.3 Дублирование запроса ... 219
12.2.4 Удаление запроса ... 219
12.3 Настройка внешнего вида виджета ... 219
12.3.1 Основные настройки виджета ... 219
12.3.2 Временной ряд ... 220
12.3.2.1 Шаг 1. Настройка осей ... 221
12.3.2.2 Шаг 2. Настройка визуализации ... 221
12.3.2.3 Шаг 3. Легенда ... 223
12.3.3 Круговая диаграмма ... 223
12.3.4 Таблица ... 226
12.3.5 Текст ... 227
12.3.6 Гистограмма ... 228
12.3.6.1 Шаг 1. Настройка осей ... 229
12.3.6.2 Шаг 2. Настройка визуализации ... 230
12.3.6.3 Шаг 3. Легенда ... 231
12.3.7 Метрика ... 231
12.3.8 Изображение ... 233
12.4 Копирование виджета ... 234
12.5 Предустановки ... 235
13. Отчеты ... 236
13.1 Общие данные ... 236
13.2 Создание отчета ... 237
13.3 Конструктор отчета ... 238
13.3.1 Добавление страницы ... 241
13.3.2 Выбор периода формирования данных виджетов ... 242
13.3.3 Настройка наименования отчета в момент генерации ... 242
13.3.4 Настройка страниц ... 243

13.3.4.1 Настройка верхнего колонтитула ... 243
13.3.4.2 Настройка нижнего колонтитула ... 244
13.3.4.3 Настройка стиля шрифта ... 245
13.3.5 Настройка виджетов ... 245
13.3.5.1 Добавление виджета ... 246
13.3.5.2 Редактирование виджета ... 246
13.3.5.3 Копирование настроек виджета ... 247
13.3.5.4 Изменение расположения виджета ... 247
13.3.5.5 Изменение размера виджета ... 247
13.3.5.6 Удаление виджета ... 247
13.3.6 Изменение порядка страниц ... 247
13.3.7 Удаление страницы ... 248
13.4 Настройка расписания генерации отчета ... 248
13.4.1 Просмотр истории генерации отчета ... 248
13.5 Настройка прав доступа к отчету ... 249
13.6 Импорт отчетов ... 250
13.7 Экспорт отчетов ... 250
13.8 Удаление отчета ... 250
13.9 Архив отчетов ... 251
14. Сообщения ... 252
14.1 Создание сообщения ... 253
14.2 Просмотр сообщения ... 253
14.3 Ответ на сообщение ... 254
14.4 Отметить сообщения прочитанными ... 254
14.5 Отметить прочитанные сообщения как непрочитанные ... 254
14.6 Экспорт сообщений ... 254
14.7 Удаление сообщений ... 255
15. Профиль пользователя ... 256
15.1 Изменение информации о своей учетной записи ... 257
15.2 Изменение пароля ... 257
15.3 Подключение аутентификатора ... 258
15.4 Выход из всех сессий ... 258
15.5 Просмотр журнала изменений учетной записи ... 259
15.6 Настройка оповещений ... 259
15.7 Просмотр истории действий в платформе ... 260
16. Интеграции ... 262
16.1 RT Protect EDR ... 262
16.1.1 Общие сведения ... 262
16.1.1.1 Характеристики системы ... 262
16.1.1.2 Активные действия ... 262
16.1.1.3 Синхронизация инцидентов и активов ... 263
16.1.1.4 Параметры типа интеграции RT Protect EDR ... 263

16.1.2 EDR действия ... 266
16.1.2.1 Создание EDR действия ... 267
16.1.2.2 Просмотр EDR действия ... 268
16.1.2.3 Редактирование EDR действия ... 270
16.1.2.4 Дублирование EDR действия ... 270
16.1.2.5 Изменение статуса EDR действия ... 270
16.1.2.6 Экспорт EDR действий ... 270
16.1.2.7 Импорт EDR действий ... 271
16.1.2.8 Удаление EDR действий ... 271
16.1.3 Настройка интеграции RT Protect EDR ... 271
16.1.3.1 Шаг 1. Создание экземпляра интеграции с RT Protect EDR ... 271
16.1.3.2 Шаг 2. Настройка задачи синхронизации активов ... 273
16.1.3.3 Шаг 3. Настройка активных действий для интеграции ... 274
16.1.3.4 Шаг 4. Активация интеграции ... 274
16.1.4 Работа с интеграцией RT Protect EDR ... 274
16.1.4.2 Работа с правилами корреляции ... 278
16.1.4.3 Работа с активами ... 281
16.1.4.4 Работа с инцидентами ... 282
16.1.4.5 Просмотр журнала выполнения действий по интеграции ... 283
16.2 Kaspersky Security Center ... 284
16.2.1 Характеристики системы ... 284
16.2.2 Настройка интеграции ... 285
16.2.2.1 Шаг 1. Создание экземпляра интеграции с KSC ... 285
16.2.2.2 Шаг 2. Создание задачи по синхронизации активов ... 286
16.2.2.3 Шаг 3. Активация экземпляра интеграции с KSC ... 287
16.2.3 Работа с интеграцией ... 287

1. Общие сведения о «Платформе Радар»

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

Платформа обеспечивает решение следующих задач:

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

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

2. Требования

Для работы с сервисом пользователю необходимы:

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

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

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

3. Вход в платформу

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

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

Где:

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

Откроется окно «Вход» (см. «Рис. 1»).

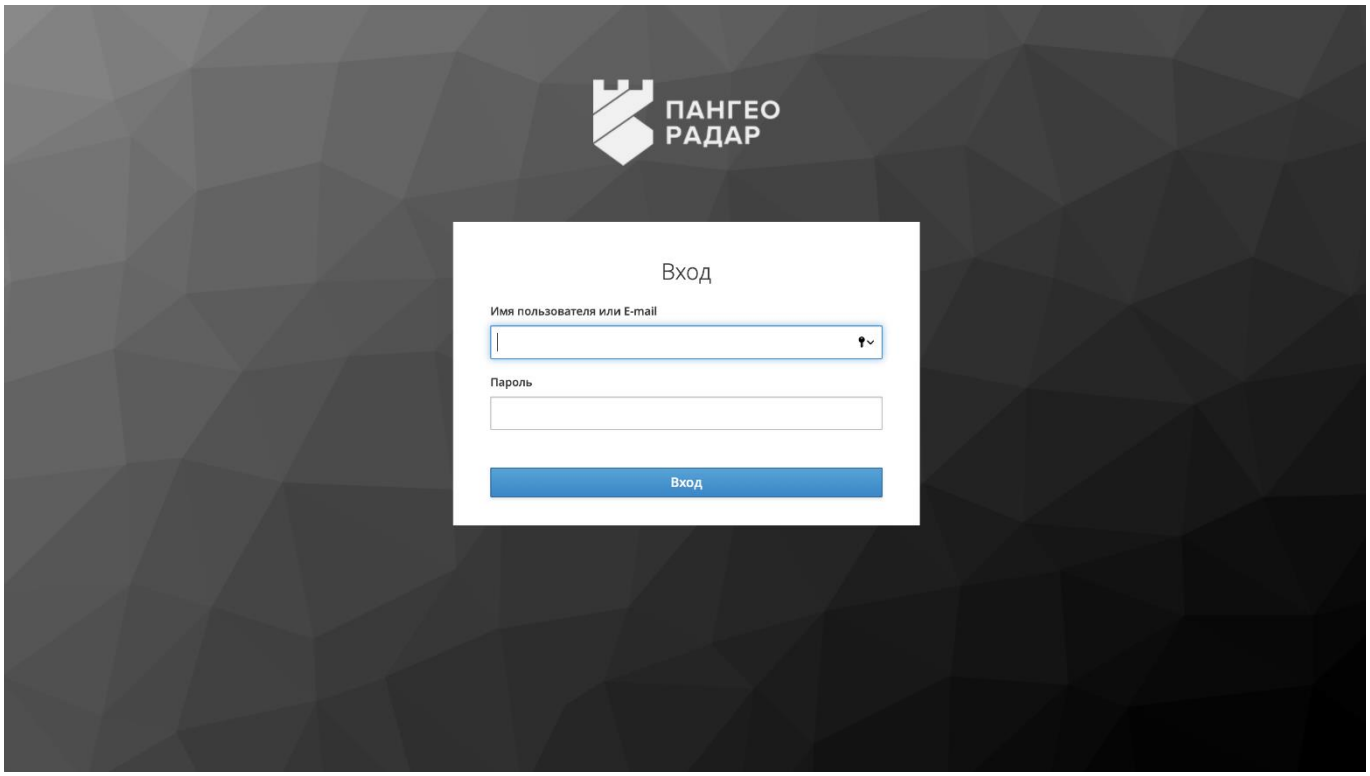


Рис. 1 – Окно входа в платформу

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

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

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

4. Интерфейс платформы

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

Рабочая область раздела имеет два варианта представления:

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

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

Рис. 2 – Интерфейс Платформы Радар. Табличное представление

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

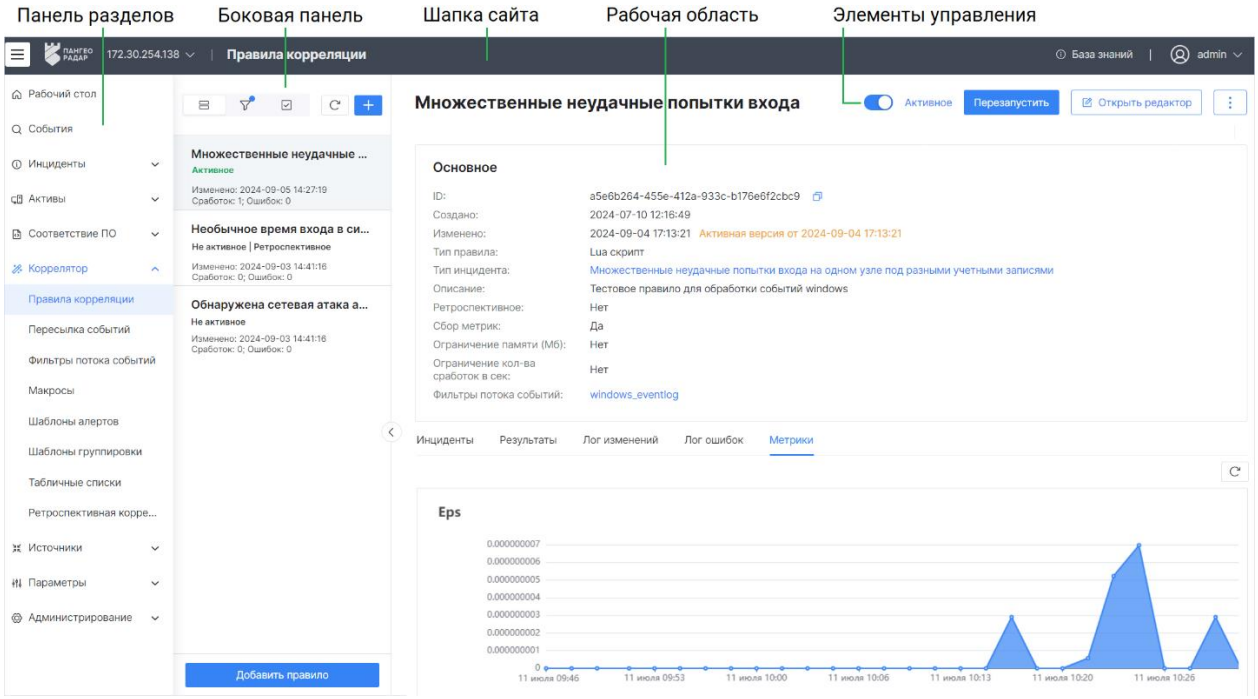
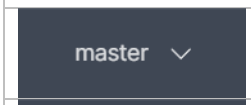
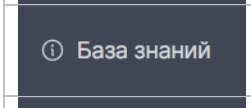
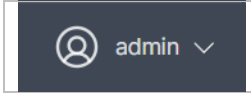


Рис. 3 – Интерфейс Платформы Радар. Представление через боковую панель и формы объектов

4.1 Шапка сайта

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

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

4.2 Панель разделов

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

В интерфейсе доступны следующие разделы:

- События. Раздел предназначен для просмотра и анализа событий информационной безопасности.
- Инциденты ИБ. Раздел содержит следующие подразделы:
    - «Инциденты» - расследование инцидентов информационной безопасности;

- «Типы инцидентов» - сведения о уязвимостях, нарушениях политики, аномальной сетевой активности которые могут послужить основой для возникновения инцидента;
- «Группы инцидентов» - управление группами инцидентов и массовые операции над инцидентами через группы;
- «Происшествия на отправку» - отправка происшествий, выявленных в критической информационной инфраструктуре (КИИ) Российской Федерации, в национальный координационный центр по компьютерным инцидентам;
- «Дополнительные поля» - настройка параметров дополнительной информации, которую можно добавить к инцидентам.

- Активы. Раздел содержит следующие подразделы:
  - «Активы» – управление и анализ состояния активов;
  - «Группы активов» – управление группами активов;
  - «Настройки идентификации активов» – настройка сравнения отдельных атрибутов актива (его идентификаторов) с атрибутами существующих активов, о которых есть записи в платформе;
  - «Сетевые интерфейсы» – сведения о сетевых интерфейсах, обнаруженных у активов;
  - «Результаты сканирования» – изучение данных по наличию уязвимостей, полученные сторонними сканерами уязвимости в ходе работы и импортированные в платформу;
  - «Обнаружение хостов» – сканирование подсети, в результате которого может быть получен набор данных, достаточный для идентификации актива;
  - «Обнаружение сервисов» – сбор данных о сервисах на выбранных активах;
  - «Сбор данных» – сбор общих данных на выбранных активах.
- Соответствие ПО. Раздел содержит следующие подразделы:
  - «Результаты соответствия ПО» – просмотр результатов всех текущих проверок соответствия ПО;
  - «Список ПО» – перечень всего программного обеспечения, обнаруженного сканерами уязвимостей при сканировании активов;
  - «Список групп ПО» – управление группами ПО;
  - «Наборы правил соответствия ПО» – настройка политик для выполнения проверки соответствия ПО;
  - «Правила соответствия ПО» – настройка регулярных выражений, по которым формируются политики для выполнения проверки соответствия ПО.
- Коррелятор. Раздел содержит следующие подразделы:
  - «Правила корреляции» - управление правилами корреляции;
  - «Пересылка событий» - управление фильтрами потока событий, которые применяются для отправки событий на другой экземпляр платформы;

- «Фильтры потока событий» - управление фильтрами потока событий, которые применяются в правилах корреляции;
- «Макросы» - управление модулями поведения для правил корреляции;
- «Шаблоны алертов» - управление шаблонами "алертов";
- «Шаблоны группировки» - управление шаблонами группировки событий;
- «Табличные списки» - управление справочниками;
- «Ретроспективная корреляция» - проведение ретроспективного анализа на основе данных хранимых в платформе

- Источники. Раздел содержит следующие подразделы:
  - «Источники» – подключение и настройка источников событий информационной безопасности;
  - «Отладка источника» – проверка работы правил разбора и обогащения для выбранного источника;
  - «Правила разбора» – управление правилами разбора поступающих событий;
  - «Обогащение» – управление правилами обогащения разобранных событий;
  - «Группы GROK» – управление группами пользовательских GROK паттернов;
  - «Паттерны GROK» – управление пользовательскими GROK паттернами;
  - «Поля события» – настройка маппинга полей события, используемых в процессах разбора и нормализации;
  - «Агенты сбора» – настройка агентов сбора событий от источников;
  - «Профили сбора» – управление профилями сбора событий ИБ на выбранных агентах сбора.

Примечание: *подробнее о работе с источниками событий ИБ, настройке лог-коллектора и правил разбора событий см. руководство «Работа с источниками событий ИБ»*.

- Параметры. Раздел содержит следующие подразделы:
  - «Основные параметры» – настройка основных параметром **Платформы Радар**;
  - «Оповещения по задержкам» – настройки автоматических оповещений по задержкам в обработке инцидентов операторами;
  - «Черный список ID плагинов» – настройка списка ID плагинов сканеров уязвимости, которые будут игнорироваться в процессе работы;
  - «Фоновые задачи» – просмотр информации о запущенных задачах ретроспективной корреляции, синхронизации и отчетов;
  - «Интеграции». Управление экземплярами интеграций со сторонними системами;
  - «Типы интеграций». Просмотр доступных классов систем, с которым можно настроить интеграцию, а также переключение платформы в режим работы с соответствующим типом интеграции;

    - «Папки контента». Управление папками для структурирования пользовательского контента;
    - «Шаблоны». Управление шаблонами форм пользовательского контента.
- Сообщения. Раздел предназначен для просмотра и управления личными сообщениями, создаваемые в рамках работы с платформой, а также для обмена сообщениями с другими пользователями платформы.
- Профиль. Раздел предназначен для просмотра и управления своей учетной записью, оповещениями, а также для просмотра истории действий в платформе.
- Рабочие столы. Раздел предназначен для оперативного отслеживания данных о состоянии информационной безопасности с помощью интерактивных информационных панелей.
- Отчеты. Раздел предназначен для формирования отчетов о состоянии информационной безопасности.

4.3 Универсальные таблицы

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

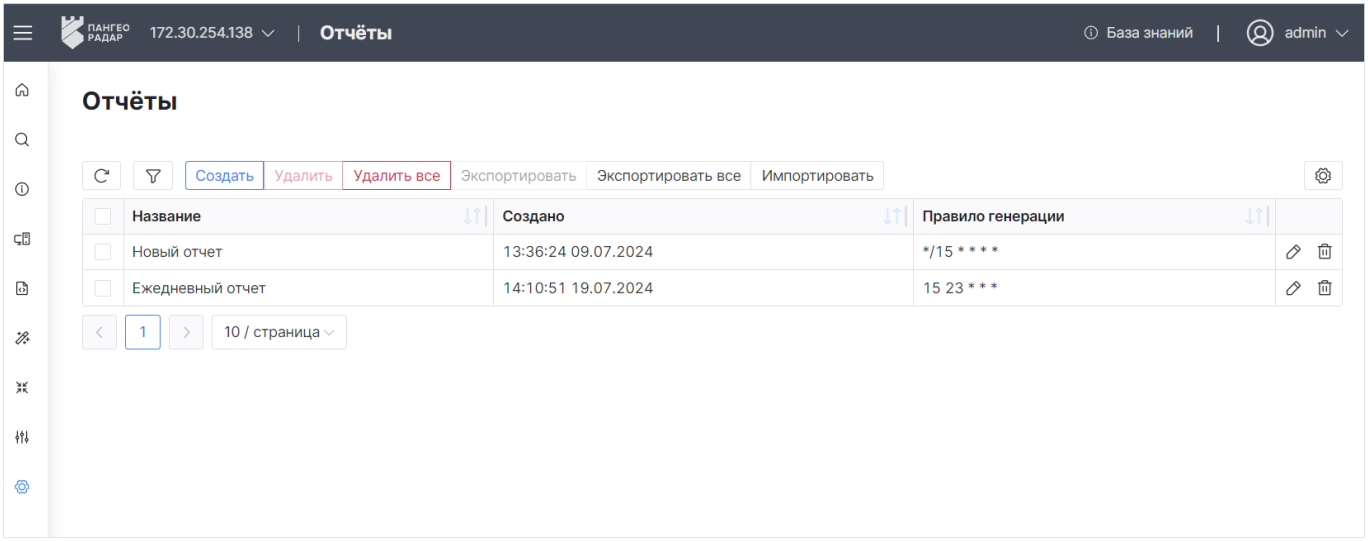


Рис. 4 -- Рабочая область. Таблицы

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

Кнопка	**Действие**
	обновление данных
	настройка сортировки и фильтрации записей таблицы
	если у кнопки есть специальный значок, то это означает что к таблице применяется фильтр
Создать	создание записи/объекта в таблице

Кнопка	Действие
Удалить	удаление выбранной записи/объекта из таблицы
Удалить все	удаление всех показанных записей/объектов. Будут удалены все записи/объекты, попавшие под параметры сортировки и фильтрации
Экспортировать	экспорт выбранной записи/объекта
Экспортировать все	экспорт всех показанных записей/объектов. Будут выгружены в архив все записи/объекты, попавшие под параметры сортировки и фильтрации
Экспортировать выбранные в csv	массовый экспорт выбранных записей/объектов в формат CSV
Экспортировать в csv	экспорт всех показанных записей/объектов в формат CSV. Будут выгружены в файлы формата CSV все записи/объекты, попавшие под параметры сортировки и фильтрации
Импортировать	импорт записей/объектов в таблицу
Переместить в папку	переместить выбранные объекты в папку
	настройка столбцов таблицы

В колонках таблицы могут располагаться следующие кнопки:

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

4.3.1 Настройка сортировки и фильтрации записей таблицы

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

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

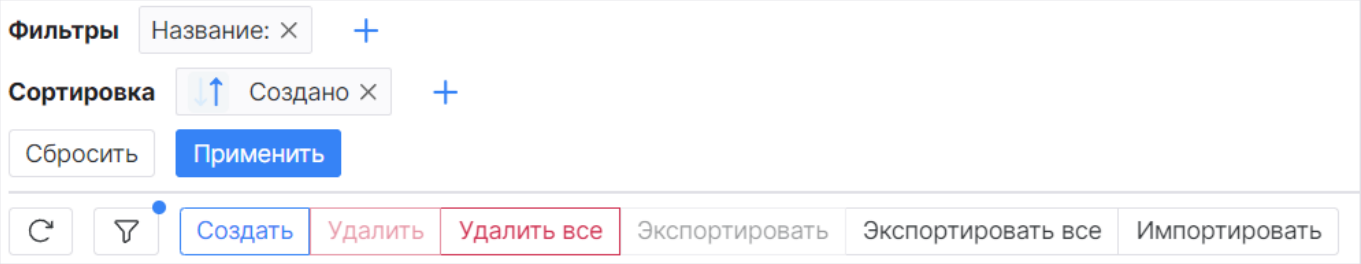


Рис. 5 – Таблица. Блоки для настройки фильтров и сортировки

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

4.3.2 Настройки отображения полей

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

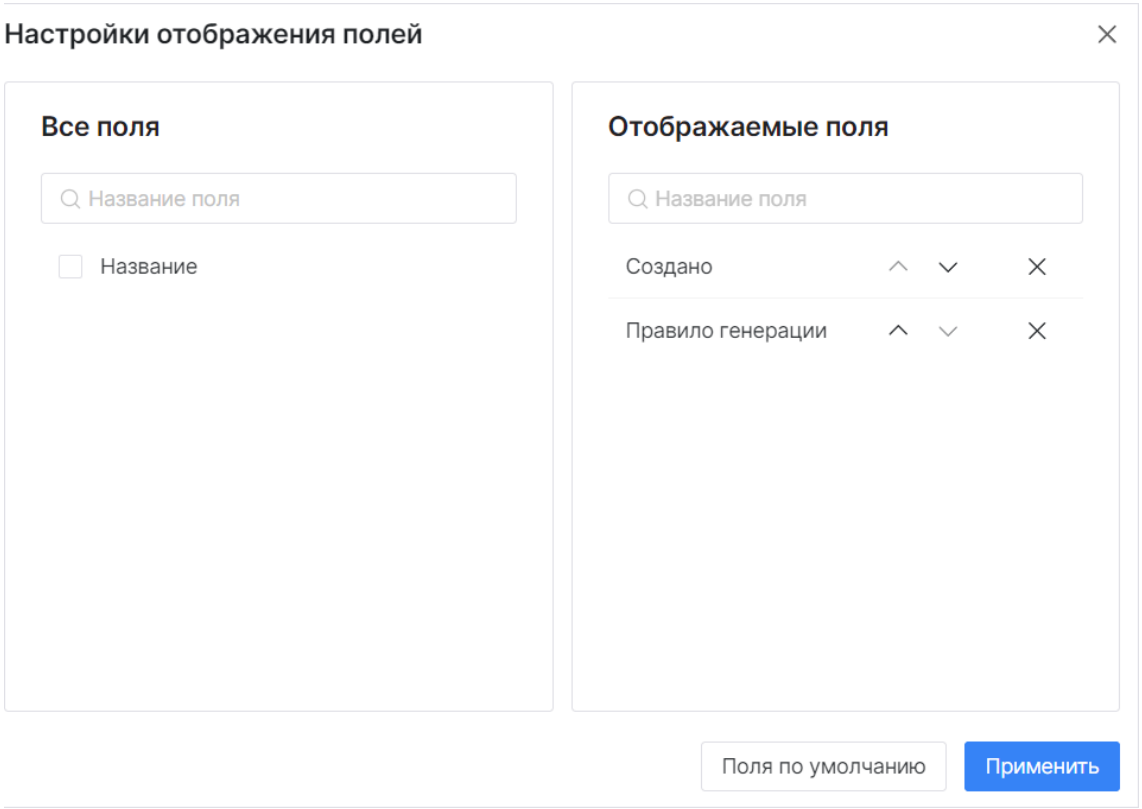


Рис. 6 – Настройки отображения полей

4.4 Боковая панель

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

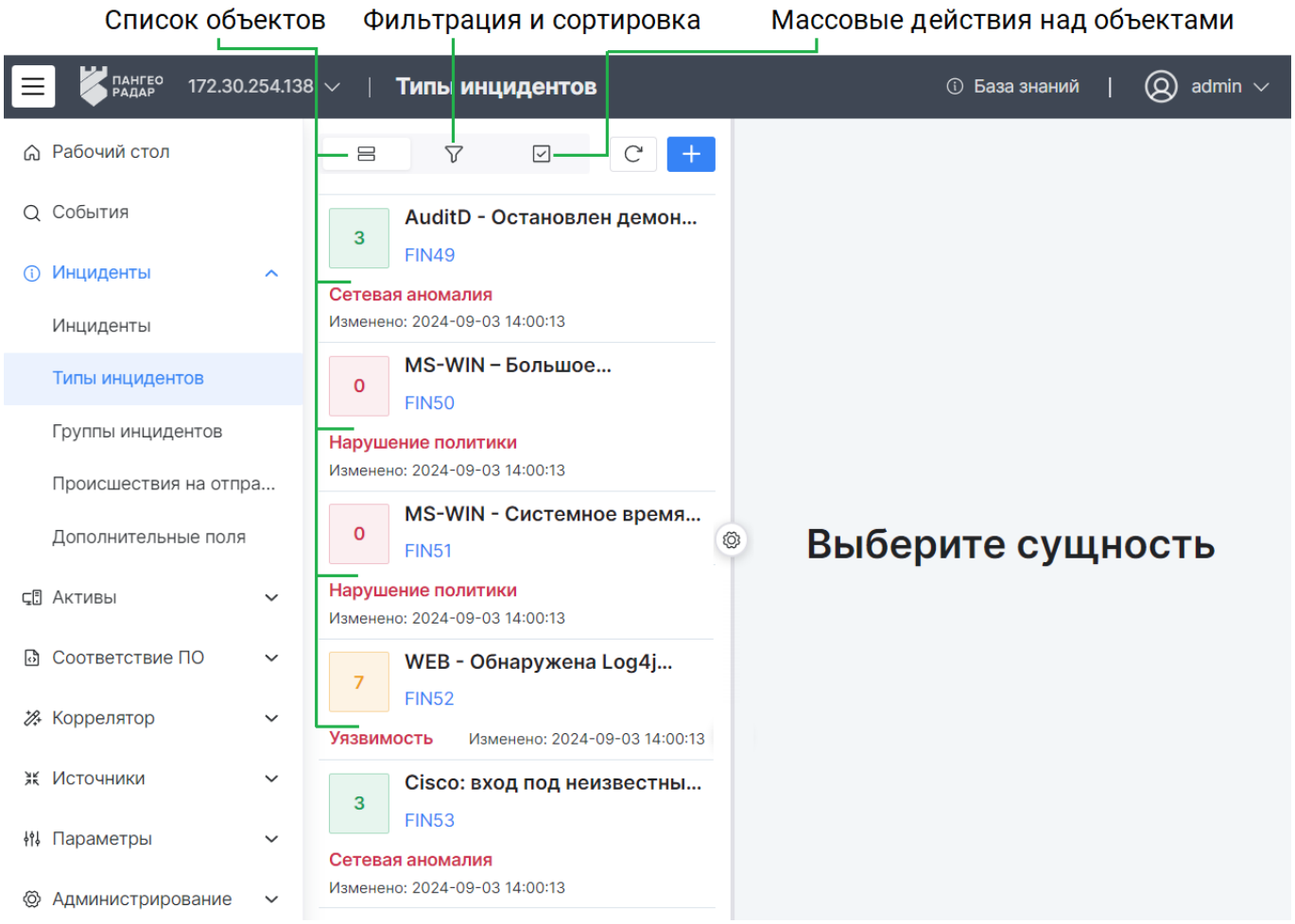


Рис. 7 – Боковая панель. Список объектов

На боковой панели доступны следующие элементы управления:

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

4.4.1 Поиск объектов в списке

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

4.4.2 Сортировка и фильтрация объектов в списке

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

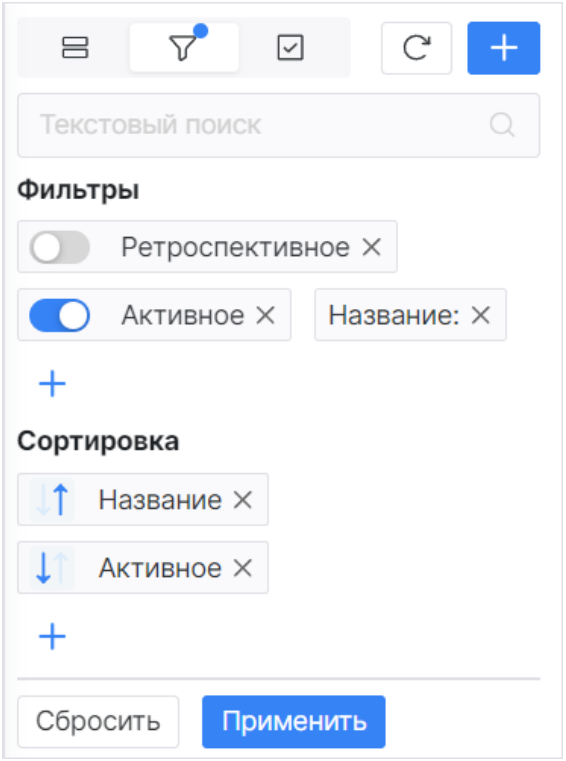


Рис. 8 – Боковая панель. Сортировка и фильтрация

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

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

4.4.3 Массовые действия

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

В общем случае над объектами доступны следующие массовые действия:

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

Для выполнения массового действия выполните следующие шаги:

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

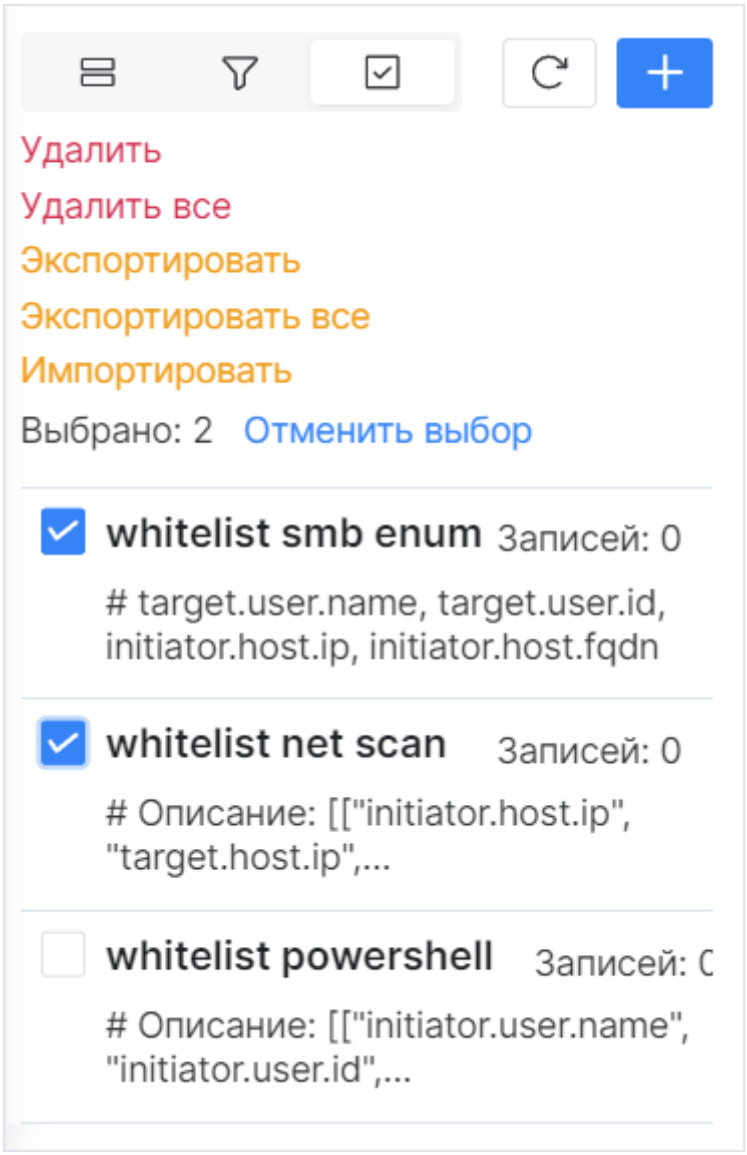


Рис. 9 – Массовые действия над табличными списками

2. Выберите объекты, установив соответствующие флаги.
3. Нажмите на соответствующую кнопку действия.

4. Завершите действие в открывшемся окне.

4.5 Папки контента

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

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

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

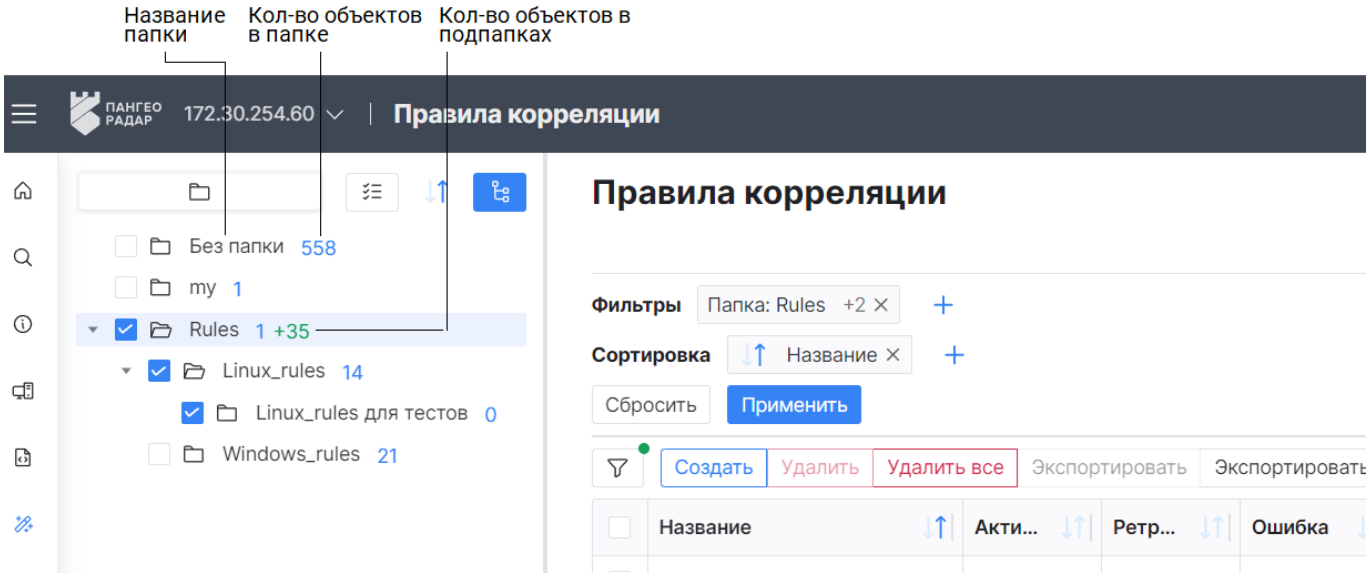


Рис. 10 – ***Боковая панель. Папки контента***

При просмотре содержимого папок доступны следующие элементы управления:

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

Отображение содержимого папок работает по следующему принципу:

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

Для создания пользовательского контента в папке выполните следующие действия:

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

Для переноса пользовательского контента в папку выполните следующие действия:

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

В версии 4.1.0 данный механизм доступен для следующего контента:

- Правила корреляции.

4.6 Формы работы с объектами

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

- Создание;
- Просмотр;
- Редактирование.

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

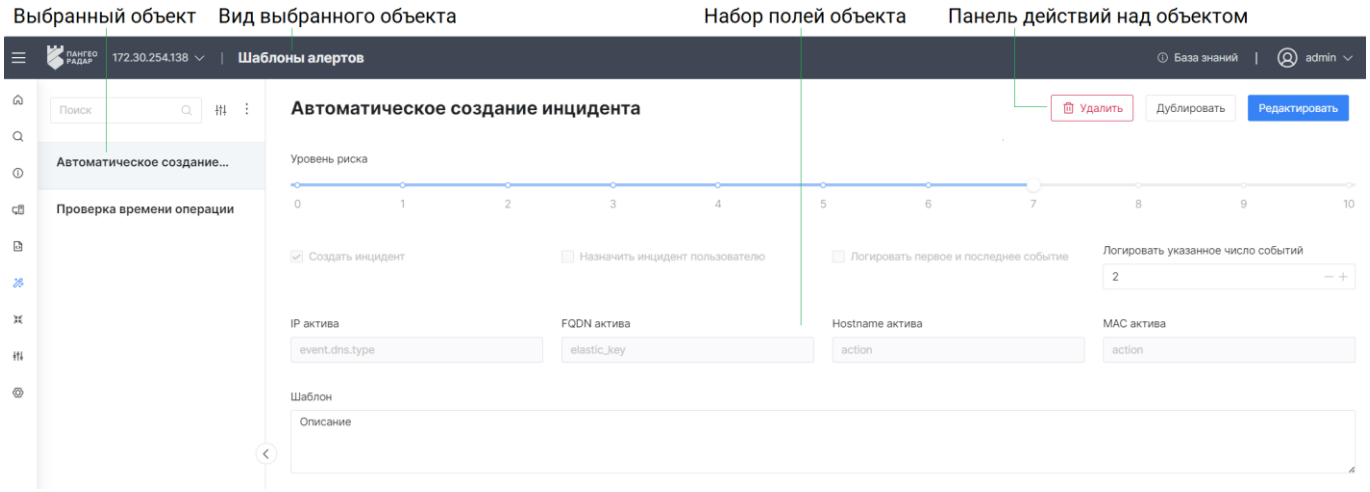


Рис. 11 – Рабочая область. Форма объекта

В общем случает страница состоит из следующих элементов:

- **Поля формы** – содержит поля для указания сведений и выполнения настроек объекта;
- **Панель действий** – содержит кнопки для работы с объектами. Кнопки, которые не помещаются на панели действий, будут помещены в выпадающее меню, доступное по кнопке  .

Панель действий может содержать следующие элементы управления:

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

4.6.1 Шаблоны объектов

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

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

Для создания шаблона выполните следующие действия:

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

Для использования шаблона выполните следующие действия:

1. Откройте форму необходимого объекта на создание или редактирование.
2. В поле **Использовать существующий шаблон** из выпадающего списка выберите заранее созданный шаблон.

3. Поля формы будут автоматически заполнены данными из шаблона.

В версии 4.1.0 данный механизм доступен для следующих объектов:

- Профили сбора.

4.6.2 Визуализации

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

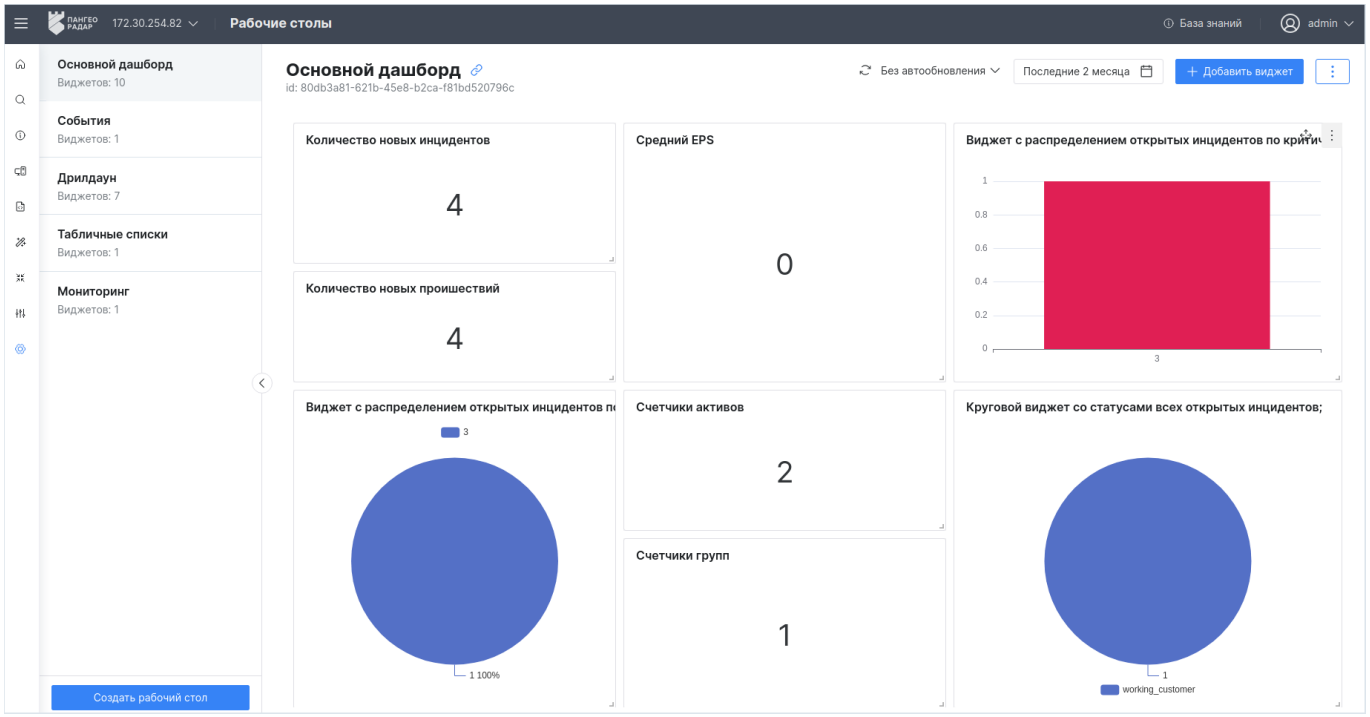


Рис. 12 – Рабочая область. Визуализации

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

5. События

5.1 Общие данные

Платформа Радар предоставляет большое количество информации о событиях информационной безопасности и удобные инструменты по их анализу:

- просмотр потока событий в виде графика;
- просмотр выделенного фрагмента потока событий в виде круговой диаграммы, таблицы или гистограммы;
- просмотр детальной информации по каждому событию.

При рассмотрении событий пользователю предоставляется следующая информация:

- id - уникальный идентификатор события;
- этап разбора события. Может принимать следующие значения: **Событие нормализовано**, **Событие разобрано**, **Событие не разобрано**;
- информация о полях события.

По результатам анализа событий платформа предоставляет следующие возможности:

- создание инцидента на основе анализа события;
- добавление события в существующий инцидент;
- быстрый переход к просмотру инцидента, в котором участвует событие.

Платформа предоставляет широкий набор инструментов для формирования списка событий:

- фильтрация по следующим параметрам: по периоду, по этапам разбора события, по запросам к конкретным полям события, по агрегациям;
- пресеты - вы можете сохранить часто используемые условия фильтрации как пресет;
- поиск по значениям полей события;
- фильтрация по выбранным полям просматриваемого события;
- просмотр истории поиска с возможностью повторного применения ранее используемых условий фильтрации.

Для работы с событиями перейдите раздел **События** (см. «Рис. 13»).

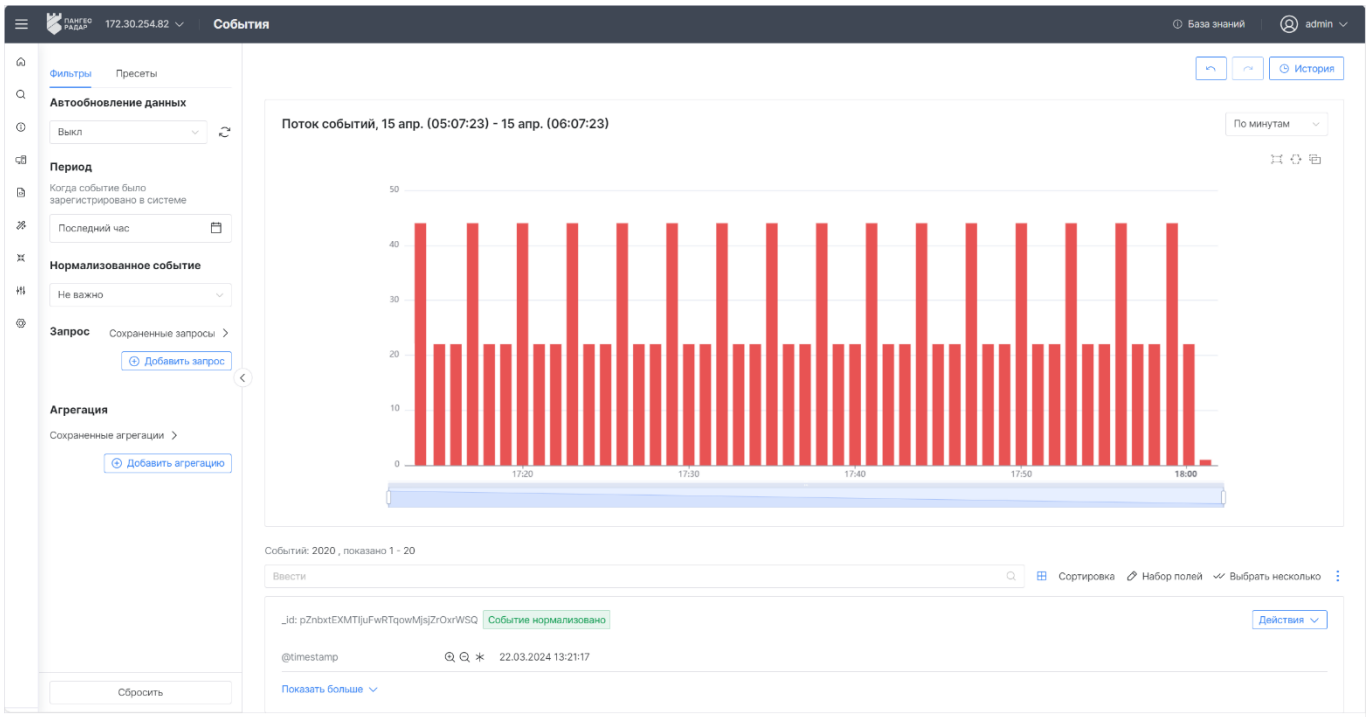


Рис. 13 – Страница "События"

Интерфейс раздела состоит из следующих блоков:

- график "Поток событий";
- топ-10 значений по выделенной области потока событий (опционально);
- список событий;
- фильтры - настройка условий фильтрации потока событий;
- пресеты - список сохраненных условий фильтрации.

5.1.1 График "Поток событий"

Блок представляет из себя график, в котором отображается плотность появления событий за период времени.

Пример потока событий приведен на «Рис. 14».

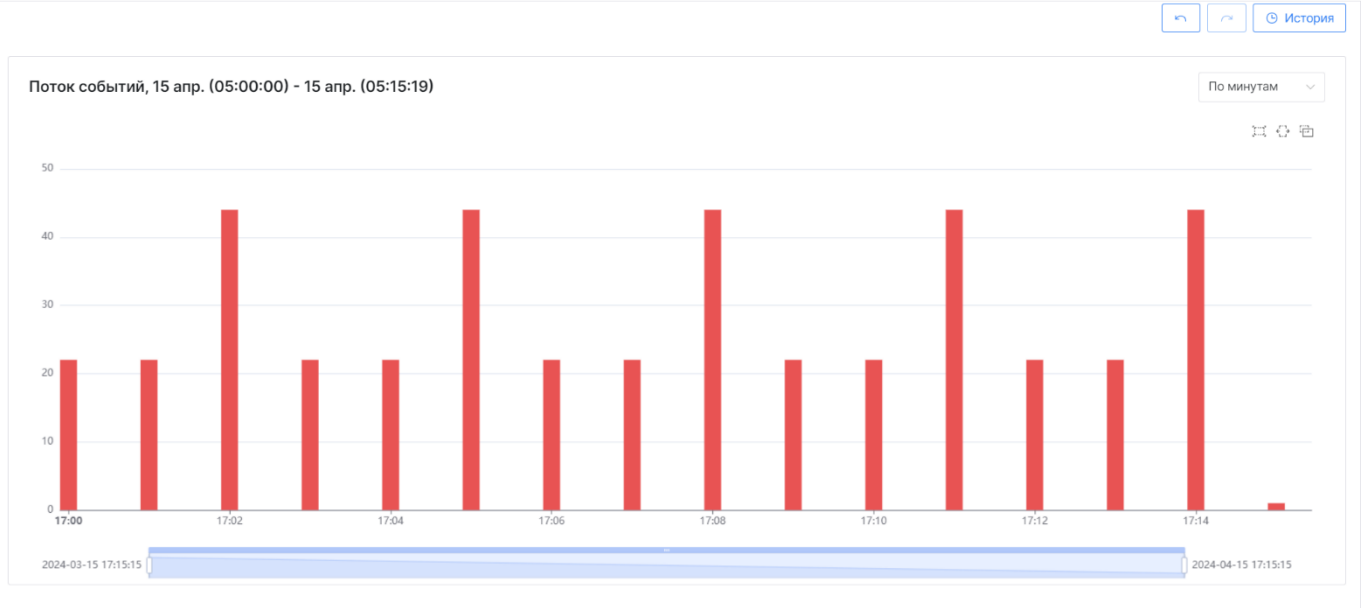


Рис. 14 – Страница "События". График "Поток событий"

В блоке доступны следующие элементы управления:

Кнопка	Действие
История	просмотр истории поиска событий
	просмотр предыдущего запроса из истории поиска событий
	просмотр следующего запроса из истории поиска событий
По дням	выбор плотности отрисовки значений графика "Поток событий"
	инструмент "Прямоугольное выделение" - создает прямоугольную рамку вокруг области на графике потока событий, ограничивая ее по горизонтальным и вертикальным сторонам
	инструмент "Выделение по горизонтали" - создает прямоугольную рамку вокруг области по оси X, при этом выделяя все значения по оси Y
	режим "Массовое выделение" - позволяет прямоугольному и горизонтальному выделению создать рамку вокруг нескольких областей на графике потока событий

5.1.2 Топ-10 значений по выделенной области потока событий

В блоке отображаются первые 10 запросов о регистрации событий в платформе за выбранный период.

Блок появляется после выделения области на графике "Поток событий". Для выделения области на графике выполните следующие действия:

1. Сформируйте график "Поток событий" (см. раздел «Работа с фильтрами»).
2. Выберите инструмент для выделения:
   - - прямоугольное выделение;
   - - выделение по горизонтали.
3. Нарисуйте выделение, перетаскивая инструмент по графику потока событий.

4. В блоке ниже будет отображаться статистика по выделенной области.
5. Для выделения нескольких областей на графике, включите режим "Массовое выделение" по кнопке .
6. Используйте инструмент «Масштабирование» для более точного выделения нужной области (см. раздел «Масштабирование графика потока событий»).

Пример блока приведен на «Рис. 15».

Рис. 15 – Страница "События". Блок "Топ-10"

В блоке отображается следующая информация:

- дата и время регистрации событий в платформе;
- количество событий в запросе о регистрации.

Информацию можно вывести следующими способами:

- столбчатая диаграмма (см. «Рис. 15»);
- таблица;
- круговая диаграмма (см. «Рис. 16»).

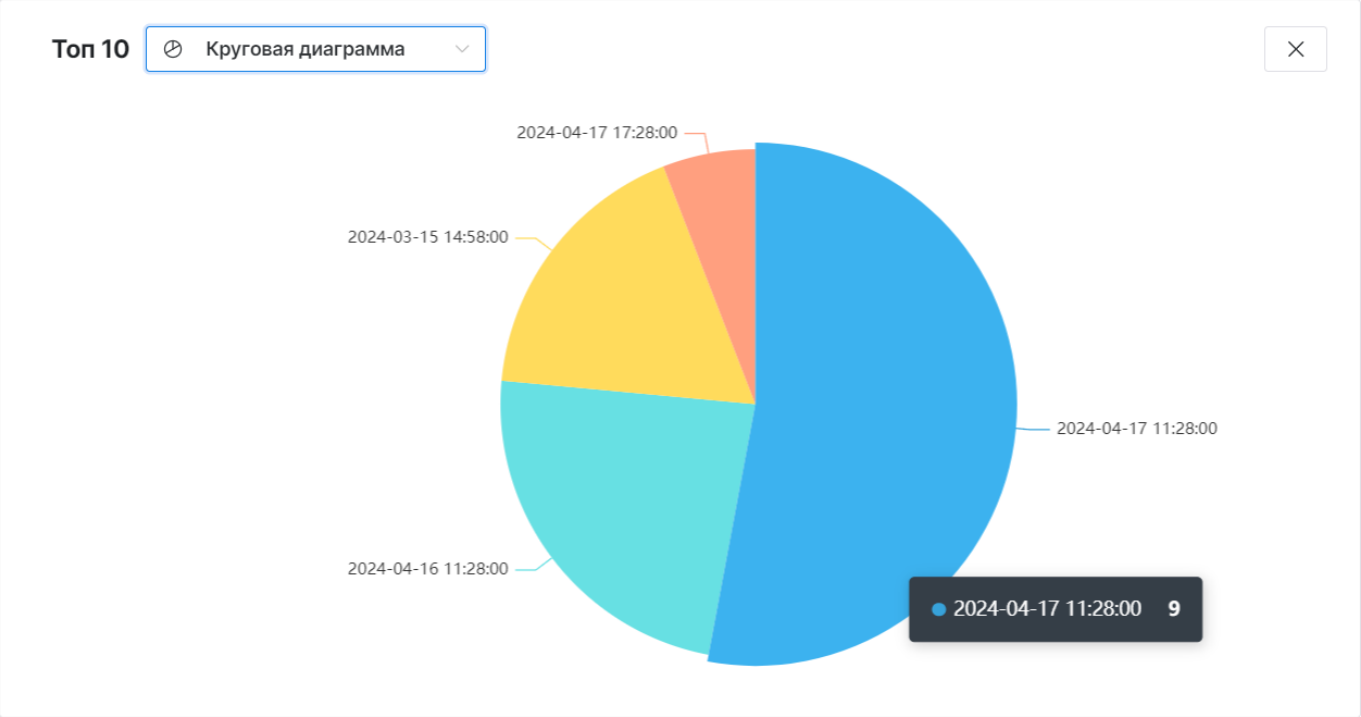


Рис. 16 – Блок "Топ-10". Круговая диаграмма

Для закрытия блока нажмите кнопку ✕.

5.1.2.1 Масштабирование графика потока событий

Для более подробной детализации графика потока событий используйте инструмент "Масштабирование" (см. «Рис. 17»).

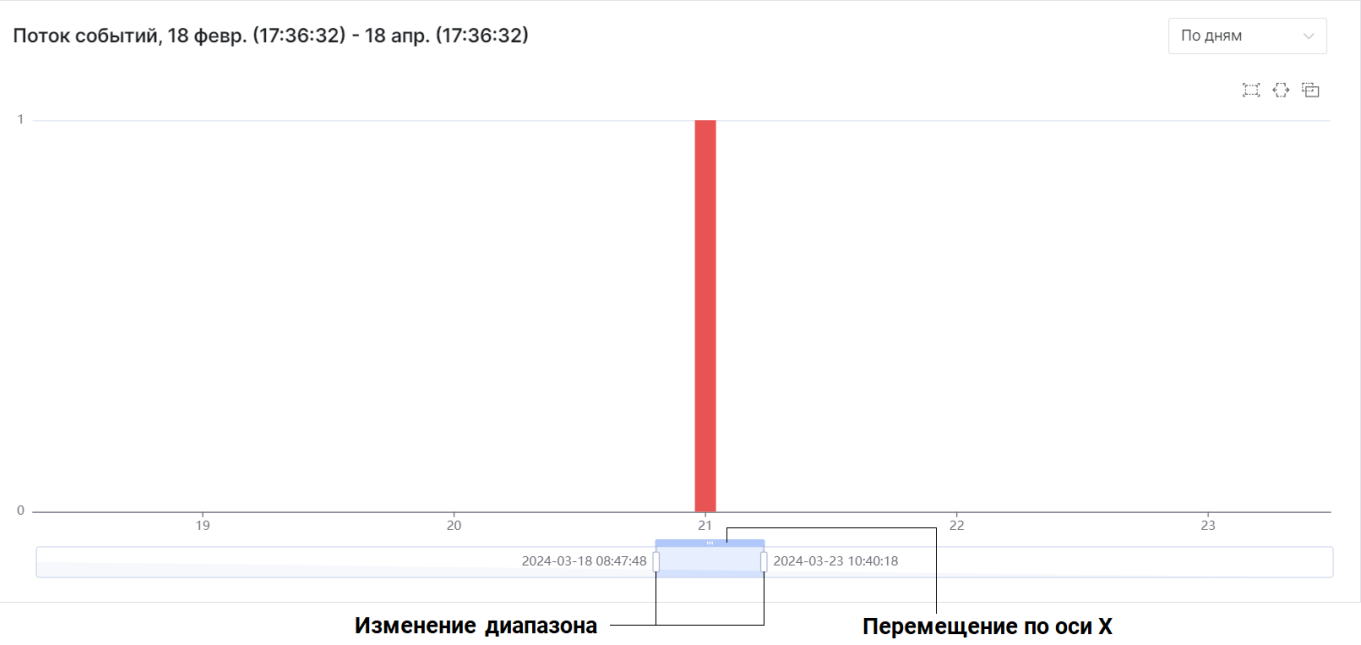


Рис. 17 – Элементы управления масштабом

Инструмент позволяет менять масштаб следующим образом:

- изменение диапазона отображаемой области по оси X;
- перемещение выбранного диапазона по оси X.

Для использования инструмента выполните следующие действия:

1. Наведите курсор на нужный элемент управления масштабом.
2. Зажмите ЛКМ.
3. Двигайте курсор в нужном направлении. Данные на графике будут автоматически изменяться.

5.1.3 Список событий

Блок располагается под графиком "Поток событий". В блоке отображается информация о событиях. Информация о событиях может отображаться двумя способами:

- в карточном виде (используется по умолчанию);
- в табличном виде.

Панель управления списком событий

Панель располагается над списком событий (см. «Рис. 18»).

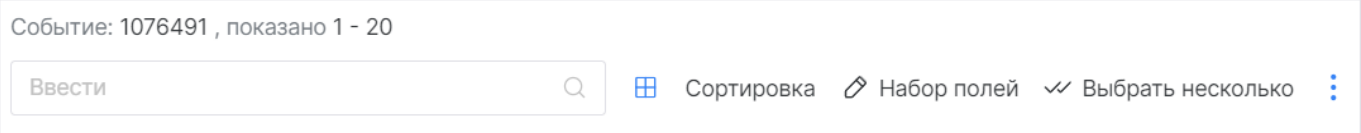


Рис. 18 – Панель управления списком событий

На панели доступны следующие элементы управления:

Кнопка	Действие
Поиск	поиск по значениям полей события
	включить табличный вид
	включить карточный вид
Сортировка	настроить параметры сортировки событий в списке
Набор полей	выбрать поля для отображения в таблице (только для табличного вида)
Выбрать несколько	включение режима для массовых операций над событиями
	доступ к следующим действиям над событиями: – создать инцидент; – добавить в инцидент; – экспорт в CSV.

Карточный вид

По умолчанию события отображаются в карточном виде (см. «Рис. 19»).

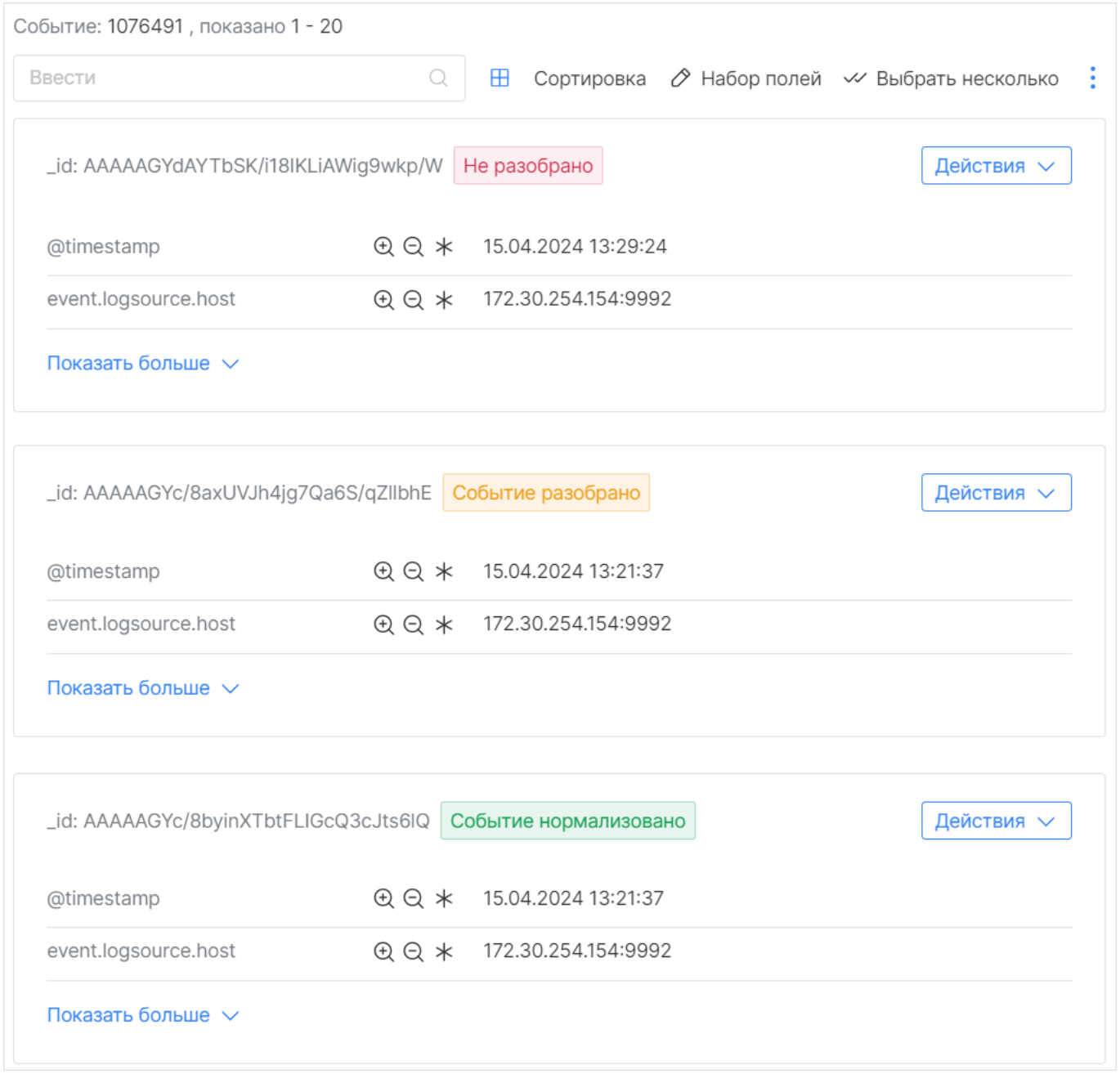


Рис. 19 – Список событий в карточном виде

По кнопкам **Показать больше** / **Показать меньше** можно открыть/скрыть отображение всех полей события (см. «Рис. 20»).

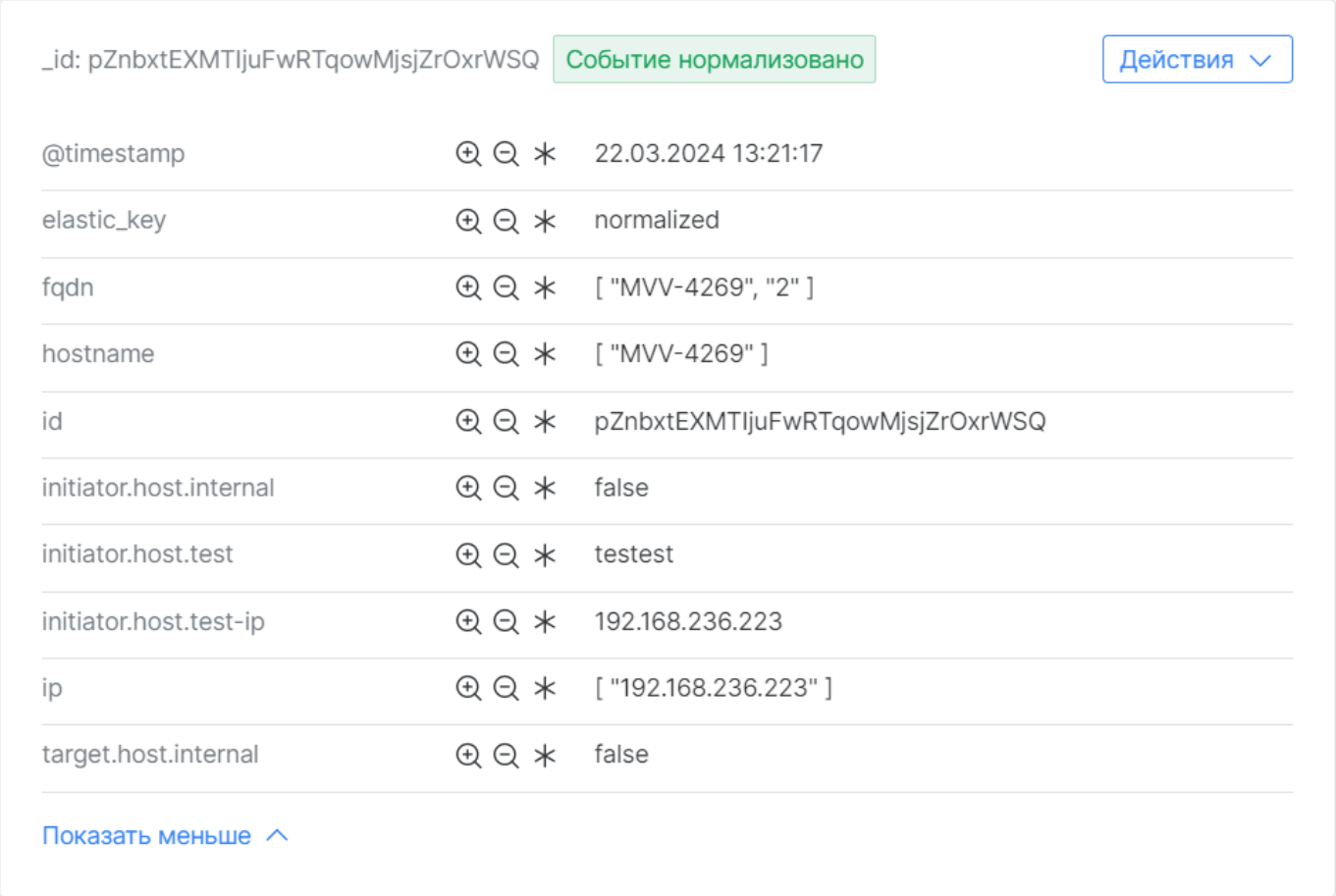


Рис. 20 – Просмотр карточки события

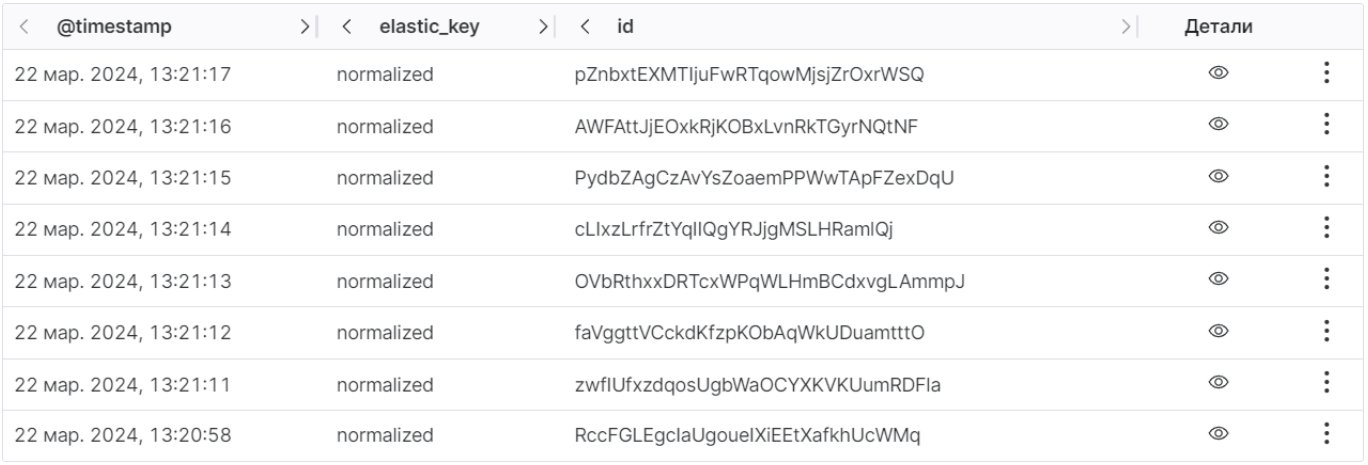
При просмотре событий в карточном виде доступны следующие элементы управления:

Кнопка	Действие
	установить фильтр "Равно". В параметры запроса фильтра добавится условие поиска событий по значению равным в указанном поле
	установить фильтр "Не равно". В параметры запроса фильтра добавится условие поиска событий по всем значениям, кроме того, что указано в поле
	установить фильтр "Существует". В параметры запроса фильтра добавится условие поиска событий по всем событиям, в которых существует выбранное поле
	доступ к действию "Найти инцидент", в котором присутствует событие

Табличный вид

Для переключения списка событий в табличный вид нажмите кнопку  .

Пример табличного представления данных приведен на «Рис. 21».



@timestamp	elastic_key	id	Детали
22 мар. 2024, 13:21:17	normalized	pZnbxtEXMTIjuFwRTqowMjsjZrOxrWSQ	
22 мар. 2024, 13:21:16	normalized	AWFAttJjEOxkRjKOBxLvnRkTGyrNQtNF	
22 мар. 2024, 13:21:15	normalized	PydbZAgCzAvYsZoaemPPWwTApFZexDqU	
22 мар. 2024, 13:21:14	normalized	cLIxzLrfrZtYqIlQgYRJjgMSLHRamlQj	
22 мар. 2024, 13:21:13	normalized	OVbRthxxDRTcxWPqWLHmBCdxvgLAmmpJ	
22 мар. 2024, 13:21:12	normalized	faVggttVCckdKfzpKObAqWkUDuamtttO	
22 мар. 2024, 13:21:11	normalized	zwflUfxzdqosUgbWaOCYXKVKUumRDFla	
22 мар. 2024, 13:20:58	normalized	RccFGLEgcIaUgouelXiEEtXafkhUcWMq	

Рис. 21 – *Список событий в табличном виде*

Кнопки > / <, которые располагаются в заголовке столбцов, позволяют изменить порядок столбцов.

Кнопка 👁, которая располагается в графе "Детали", позволяет посмотреть детали события в карточном виде (см. «Рис. 22»).

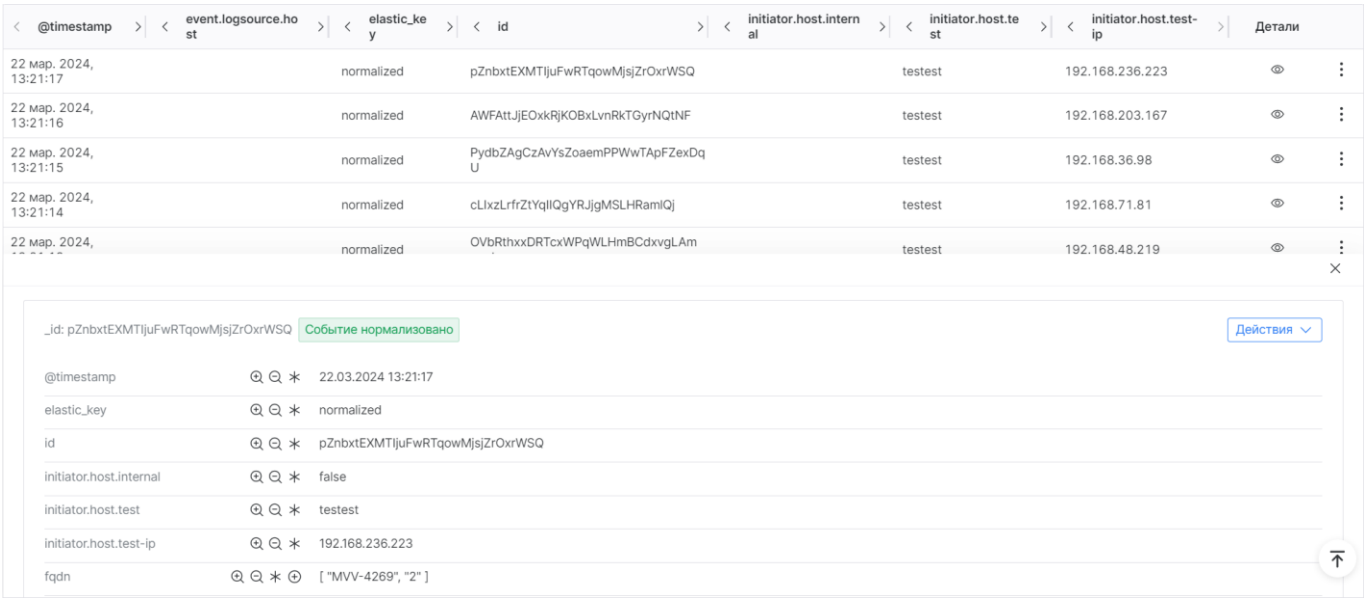


Рис. 22 – Список событий в табличном виде. Детали

Кнопка ⊕, которая располагается в блоке "Детали" (см. «Рис. 22»), позволяет добавить поле в набор столбцов таблицы.

Кнопка ⋮, которая располагается в конце строки, предоставляет доступ к действию "Найти инцидент" (подробнее см. раздел «Поиск инцидента»).

5.2 Работа с фильтрами

Настройка фильтра выполняется на вкладке "Фильтры" (см. «Рис. 23»).

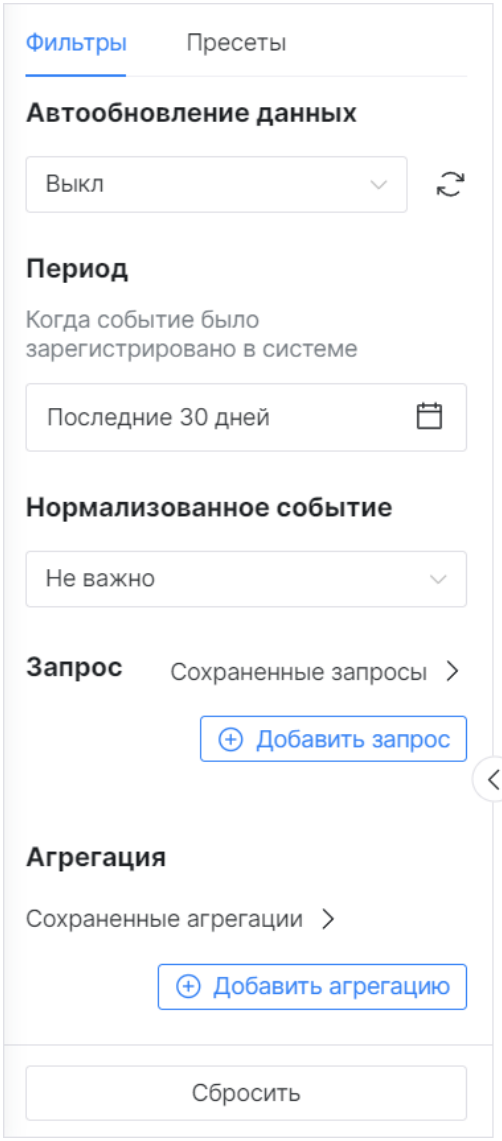


Рис. 23 – Страница "События". Вкладка "Фильтры"

При работе с фильтрами доступны следующие элементы управления:

Кнопка	Действие
	обновить список событий
	редактирование запроса/агрегации
Добавить запрос	добавление запроса в условия фильтра
Добавить агрегацию	добавление агрегаций в условия фильтра
	редактирование запроса/агрегации
	удаление запроса/агрегации
Сбросить	очистить условия фильтра

Для настройки условий фильтра выполните следующие действия:

1. В поле "Автообновление данных" из выпадающего списка выберите режим автоматического обновления данных. Доступные значения:
    - выключен;
    - по секундам: каждые 5, 10, 30 секунд;
    - по минутам: каждые 1, 5, 10, 30 минут.
2. В поле **Период** нажмите кнопку  . Откроется окно выбора временного диапазона.
3. В открывшемся окне выберите период и нажмите кнопку **Применить**. Доступные значения:
    - текущие: минута, час, день, месяц, год;
    - последние: минуты, часы, месяца, года;
    - период можно указать вручную в соответствующих полях. Поддерживается формат дат из **Grafana**.
4. В поле **Нормализованное событие** выберите этап разбора события:
    - событие нормализовано - будут показаны только нормализованные события;
    - событие разобрано - будут показаны только разобранные события;
    - событие не разобрано - будут показаны только неразобранные события;
    - не важно - будут показаны все события.
5. В поле **Запрос** добавьте необходимое количество запросов (см. раздел «Настройка запросов»).
6. В поле **Агрегация** добавьте необходимое количество агрегаций (см. раздел «Настройка агрегации»).
7. При необходимости вы можете сохранить условия фильтра как пресет (см. раздел «Работа с пресетами»).
8. Вы можете посмотреть журнал истории поиска и применить соответствующий фильтр из истории (см. раздел «История поиска»).

5.2.1 Настройка запросов

Настройка запросов включает в себя следующие процессы:

1. «Добавление запроса».
2. «Сохранение конфигурации запроса».

5.2.1.1 Добавление запроса в условия фильтра

Добавление запроса в условия фильтра можно выполнить тремя способами:

- **Способ 1**. Ручное добавление нового запроса.
- **Способ 2**. Добавление запроса из списка сохраненных.

- **Способ 3**. Добавление условий в запрос из полей события.

Все добавленные запросы отобразятся в соответствующем блоке (см. «Рис. 24»).

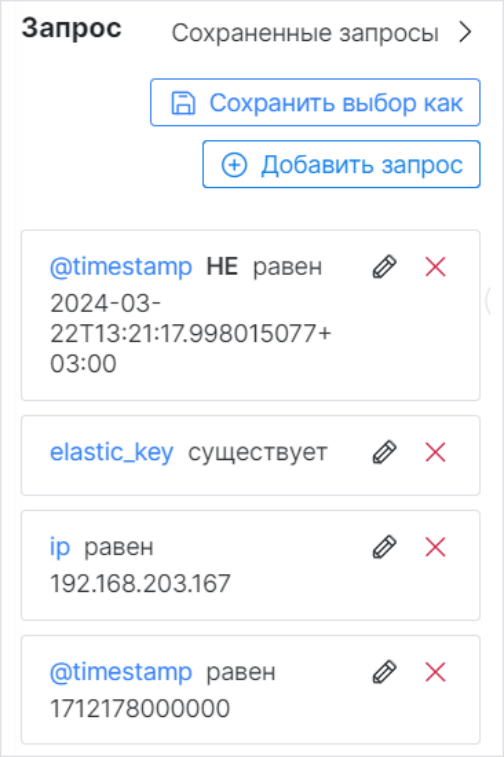


Рис. 24 – Вкладка "Фильтры". Список запросов

Способ 1. Ручное добавление нового запроса

1. На вкладке **Фильтры** в блоке **Запрос** нажмите кнопку **Добавить запрос**. Откроется окно "Добавить запрос" (см. «Рис. 25»).

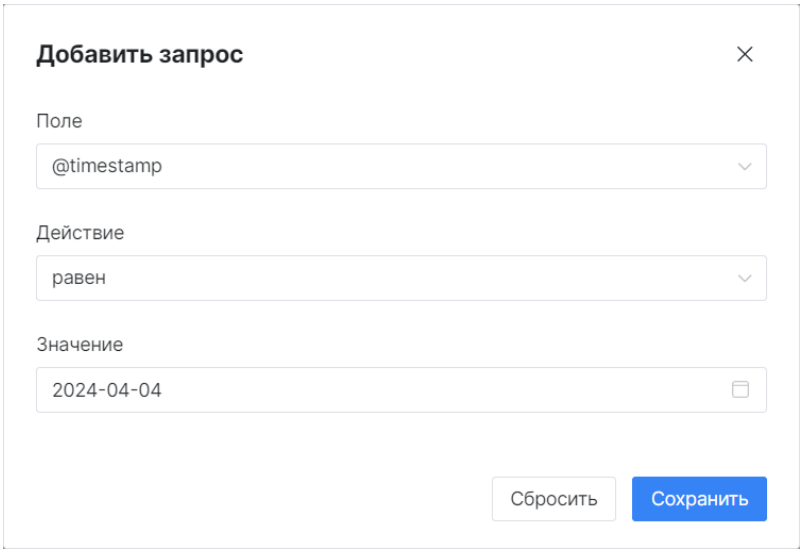


Рис. 25 – Окно "Добавить запрос"

2. Укажите следующие данные:
    - из выпадающего списка выберите поле, по которому будет выполняться запрос;
    - в поле "Действие" из выпадающего списка выберите логический оператор;
    - в поле "Значение" укажите значение логического оператора.

3. Нажмите кнопку **Сохранить**.
4. Добавьте необходимое количество запросов.

Способ 2. Добавление запроса из списка сохраненных

Примечание. Подробнее о сохранении запроса см. раздел «Сохранение конфигурации запроса».

1. На вкладке **Фильтры** в блоке **Запрос** нажмите кнопку **Сохраненные запросы**. Откроется окно "Сохраненные запросы" (см. «Рис. 26»).

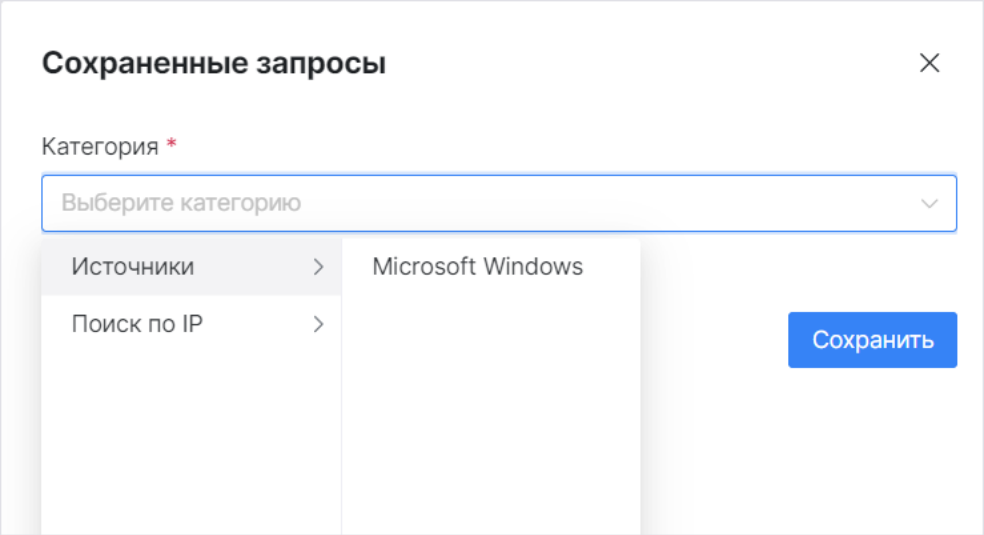


Рис. 26 – Окно "Сохраненные запросы"

2. В поле "Категория" выберите сохраненную категорию, а затем необходимый запрос. Отобразится структура запроса (см. «Рис. 27»).

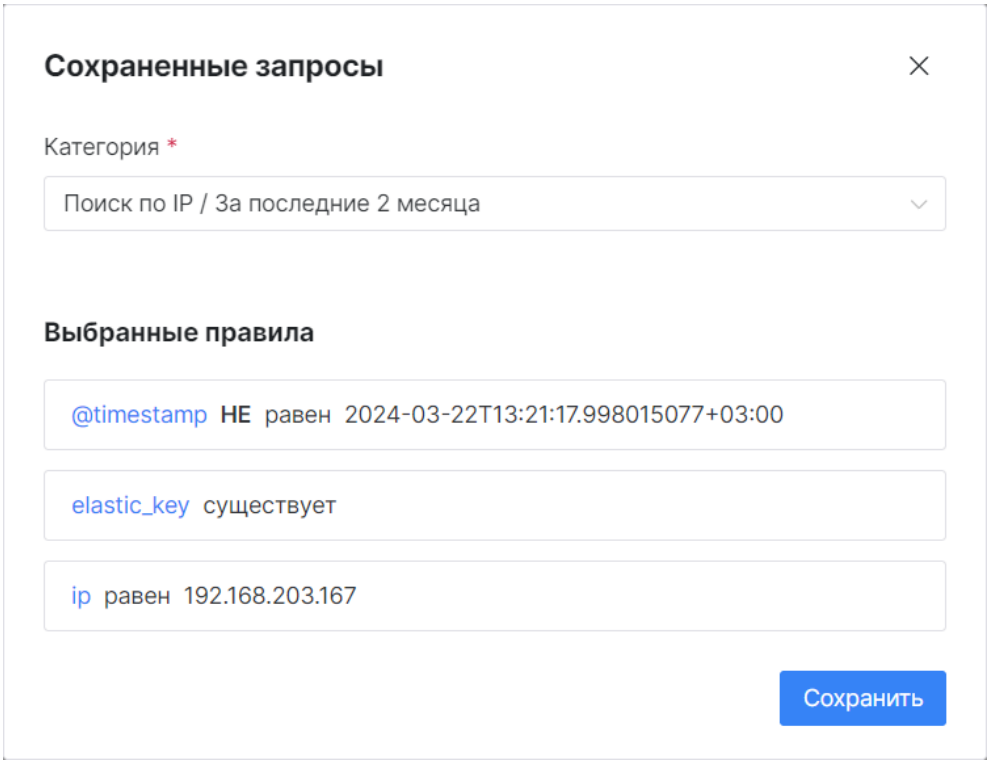


Рис. 27 – Окно "Сохраненные запросы". Структура запроса

3. Проверьте структуру запроса и нажмите кнопку **Сохранить**.

Способ 3. Добавление запросов по полям событий.

Если список событий уже сформирован, то вы можете добавить в запрос условия по выбранным полям конкретного события.

Для этого откройте карточку события и в соответствующем поле выберите нужное условие:

- для добавления в запрос условия "Равен" выберите поле и нажмите кнопку ⊕;
- для добавления в запрос условия "Не равен" выберите поле и нажмите кнопку ⊖;
- для добавления в запрос условия "Существует" выберите поле и нажмите кнопку ✳.

Пример, добавленных таких способом запросов, приведен на «Рис. 28».

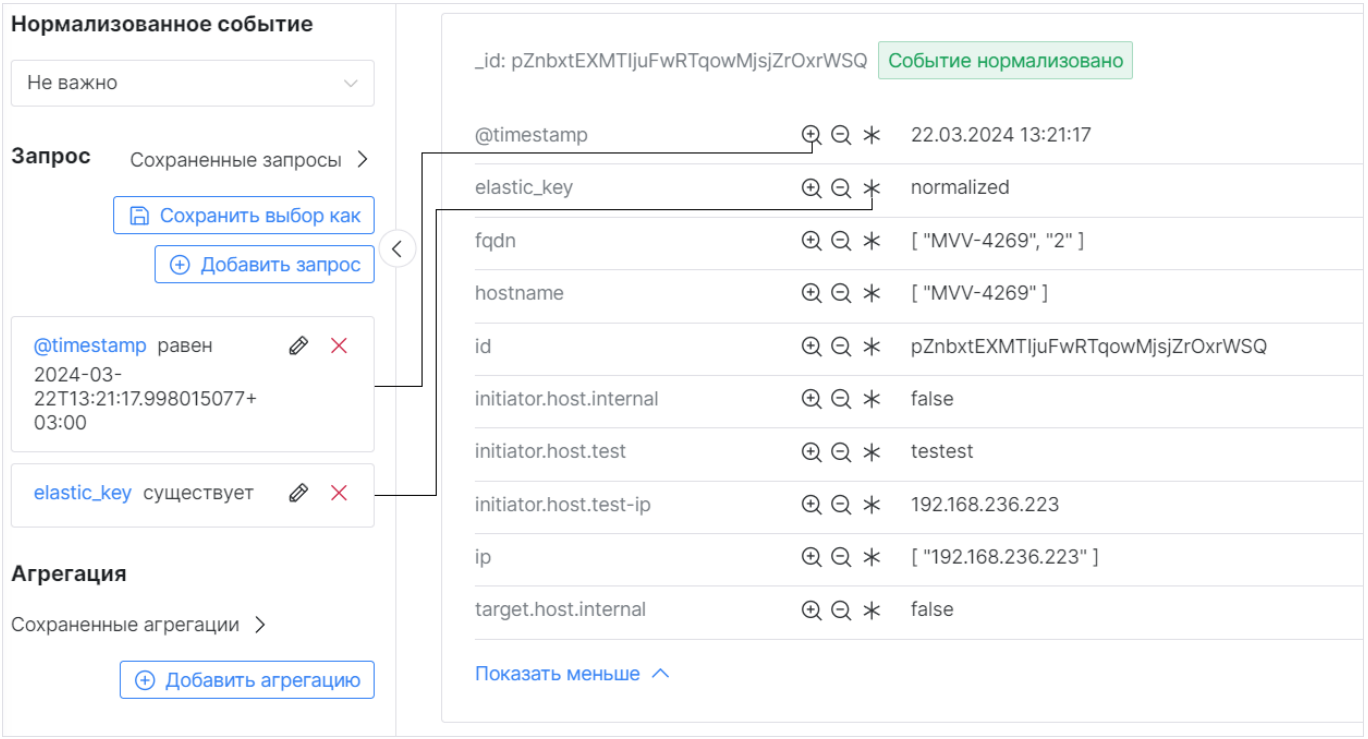


Рис. 28 – Добавление запросов по полям событий

5.2.1.2 Сохранение конфигурации запроса

Настроенную конфигурацию запросов можно сохранить для дальнейшего использования.

Для этого выполните следующие действия:

1. Добавьте необходимое количество условий в запрос.
2. Нажмите кнопку **Сохранить выбор как**. Откроется окно "Сохранить запрос" (см. «Рис. 29»).

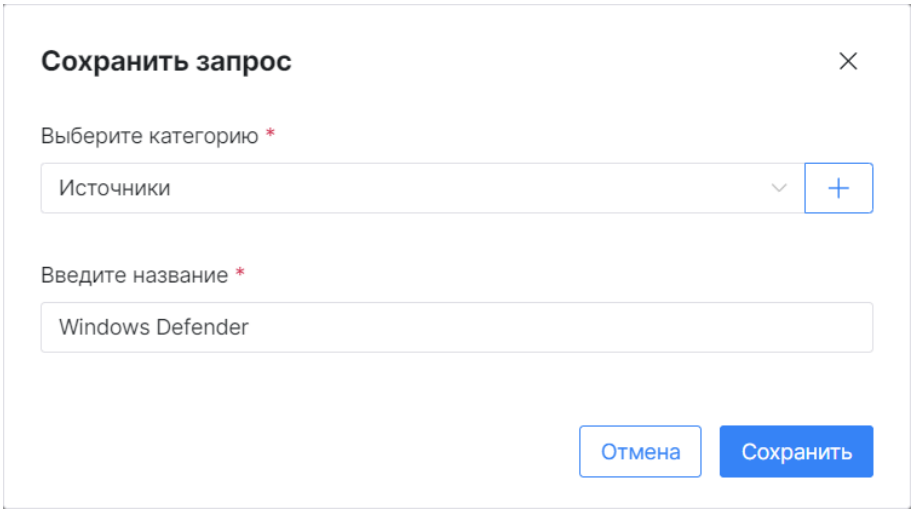


Рис. 29 – Окно "Сохранить запрос"

3. Укажите следующие данные:
    - в поле "Выберите категорию" из выпадающего списка выберите категорию, в которую будет сохранен запрос;
    - если вы еще не добавили ни одной категории, то нажмите кнопку «+», укажите название категории и сохраните изменения;
    - в поле "Введите название" укажите название запроса.
4. Нажмите кнопку **Сохранить**.

5.2.2 Настройка агрегации

Агрегация - функция группировки результатов поиска по выбранному полю.

Агрегацию можно выполнить по следующим функциям:

- `min` - по минимальным значениям;
- `max` - по максимальным значениям;
- `sum` - по сумме всех значений;
- `avg` - по среднему значению;
- `stats` - вывод по функциям `count`, `min`, `max`, `sum`, `avg`;
- `terms` - поиск нескольких значений в одном поле.

Для функции `terms` можно добавить подагрегации.

Результат поиска по агрегации будет выводиться в табличном виде вместо графика потока событий (см. «Рис. 30»).

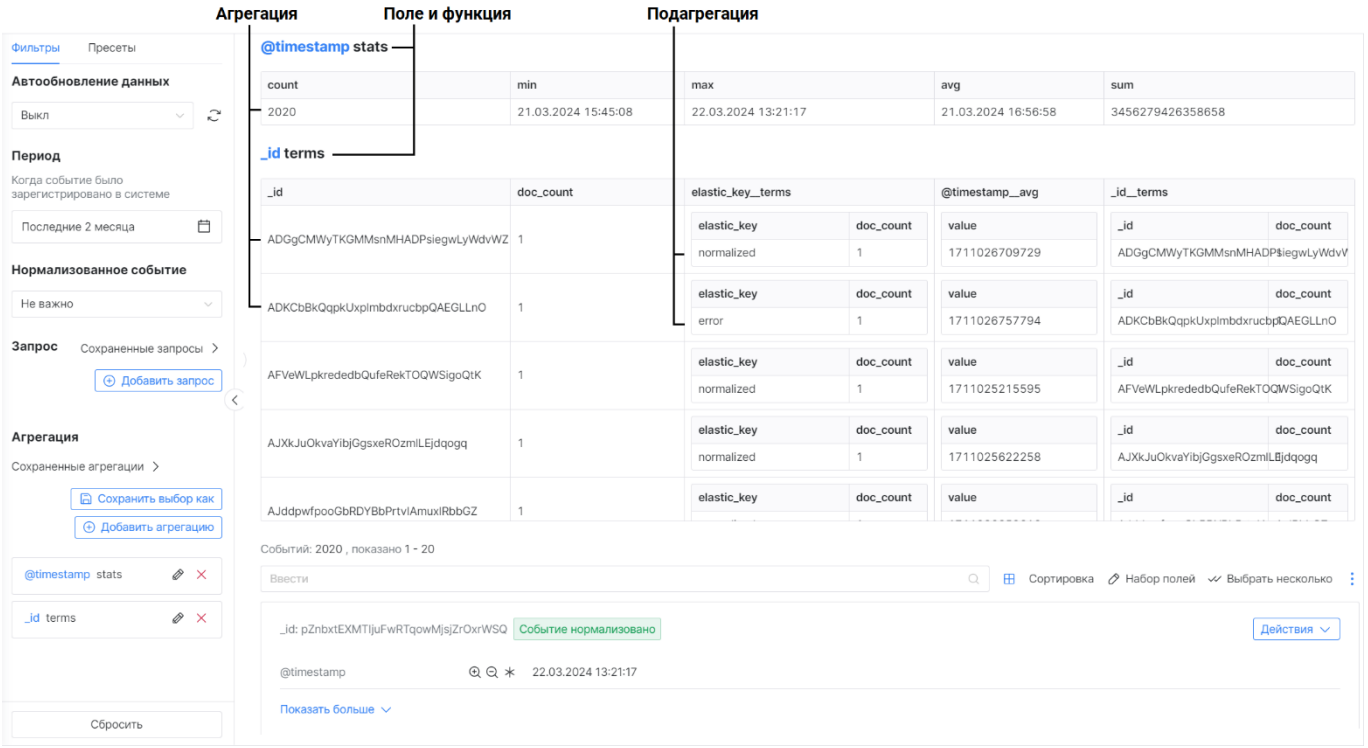


Рис. 30 – Страница "События". Просмотр агрегаций

Настройка агрегации включает в себя следующие процессы:

1. «Добавление агрегации».
2. «Добавление подагрегации».
3. «Сохранение агрегации».

5.2.2.1 Добавление агрегации

Способ 1. Ручное добавление агрегации.

1. На вкладке **Фильтры** в блоке **Агрегация** нажмите кнопку **Добавить агрегацию**. Откроется окно "Добавить агрегацию" (см. «Рис. 31»).

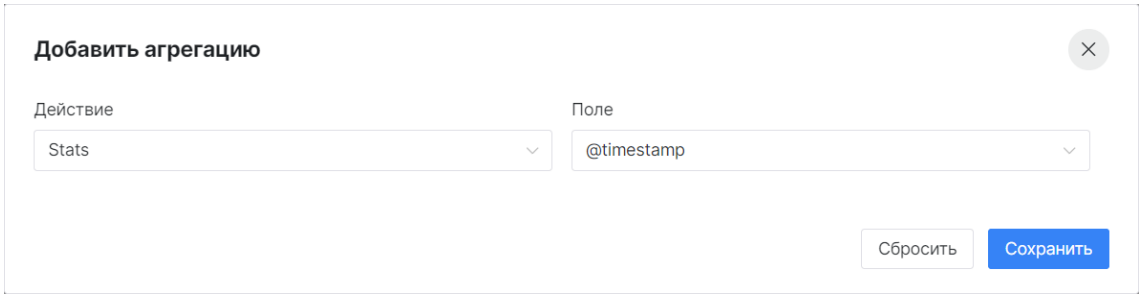


Рис. 31 – Окно "Добавить агрегацию"

2. Укажите следующие данные:
   - в поле "Действие" из выпадающего списка выберите функцию агрегации;
   - из выпадающего списка выберите поле, по которому будет выполняться функция агрегации.
3. Нажмите кнопку **Сохранить**.

4. Добавьте необходимое количество агрегаций.

Способ 2. Добавление агрегации из списка сохраненных

Примечание. Подробнее о сохранении агрегаций см. раздел «Сохранение агрегации».

1. На вкладке **Фильтры** в блоке **Агреграции** нажмите кнопку **Сохраненные агрегации**. Откроется окно "Сохраненные агрегации" (см. «Рис. 32»).

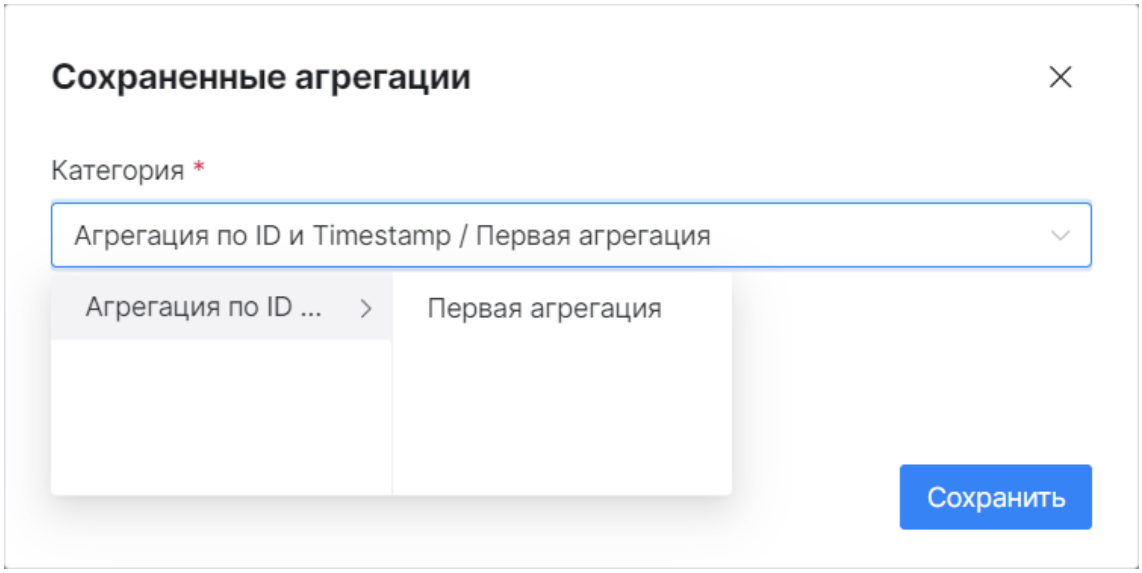


Рис. 32 – Окно "Сохраненные агрегации"

2. В поле "Категория" выберите сохраненную категорию, а затем необходимую агрегацию. Отобразятся параметры агрегации (см. «Рис. 33»).

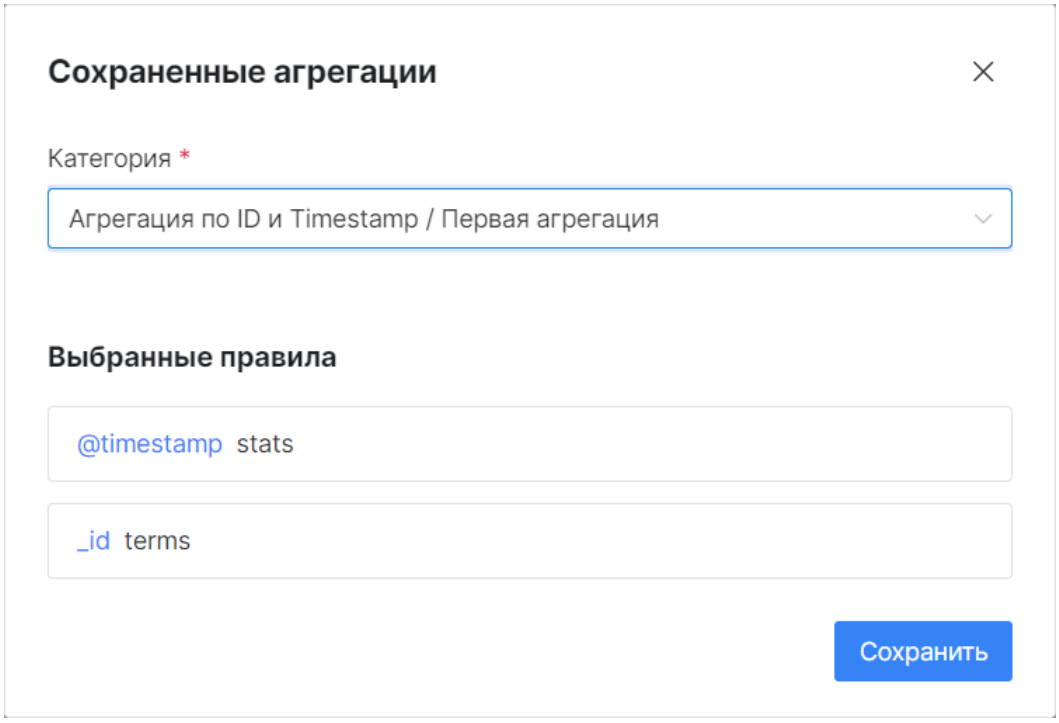


Рис. 33 – Окно "Сохраненные агрегации". Структура агрегации

3. Проверьте структуру агрегации и нажмите кнопку **Сохранить**.

5.2.2.2 Добавление подагрегации

Вы можете добавить в агрегацию необходимое количество подагрегаций.

Чтобы добавить подагрегацию необходимо при добавлении/редактировании агрегации в поле "Действие" из выпадающего списка выбрать функцию `terms`. Откроется блок для добавления подагрегаций (см. «Рис. 34»).

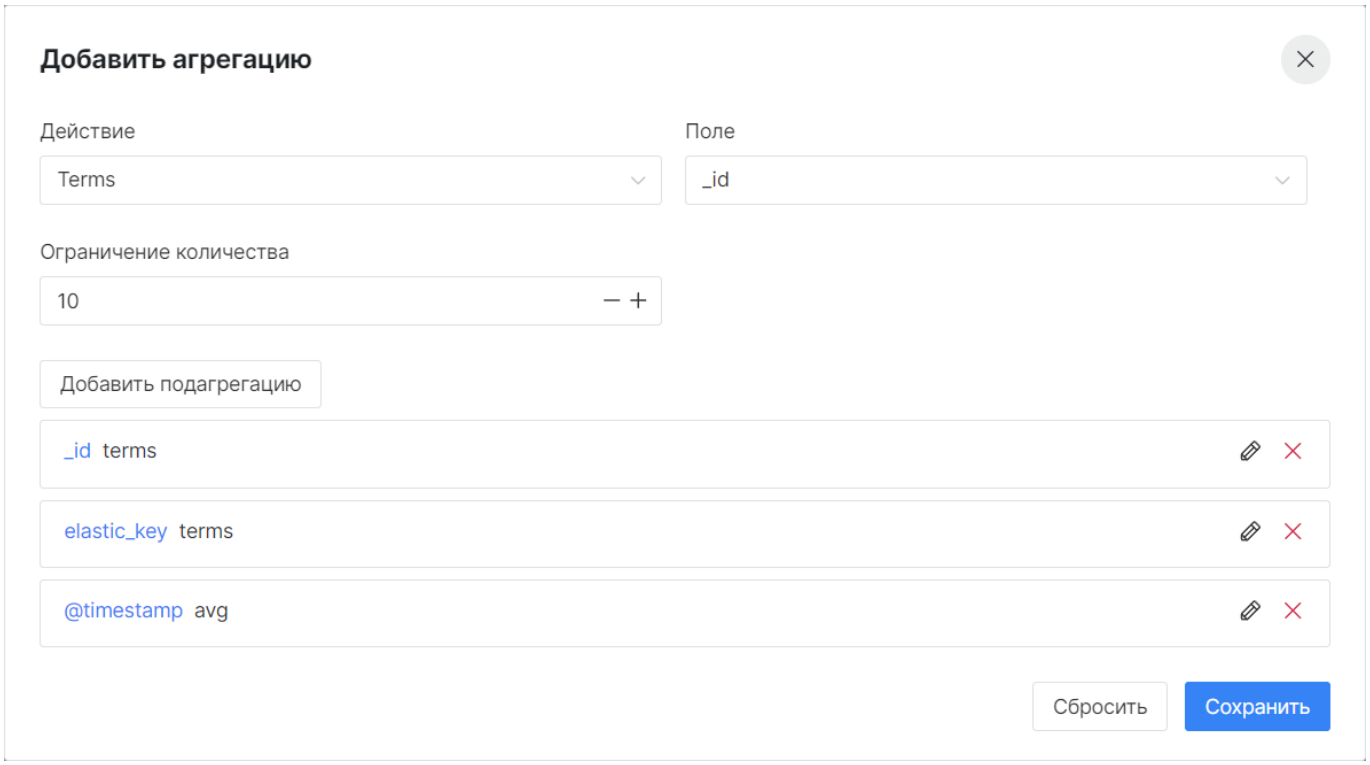


Рис. 34 – Окно "Добавить агрегацию". Блок "Подагрегации"

Нажмите кнопку **Добавить подагрегацию**. Действия по добавлению подагрегации аналогичны действиям при добавлении агрегации.

При необходимости вы можете сделать подагрегацию многоуровневой, также указав при ее добавлении в поле "Действие" функцию `terms`.

Добавьте необходимое количество подагрегаций и нажмите кнопку **Сохранить**.

5.2.2.3 Сохранение агрегации

Настроенную агрегацию можно сохранить для дальнейшего использования.

Для этого выполните следующие действия:

1. Добавьте необходимое количество условий в агрегацию.
2. Нажмите кнопку **Сохранить выбор как**. Откроется окно "Сохранить агрегацию" (см. «Рис. 35»).

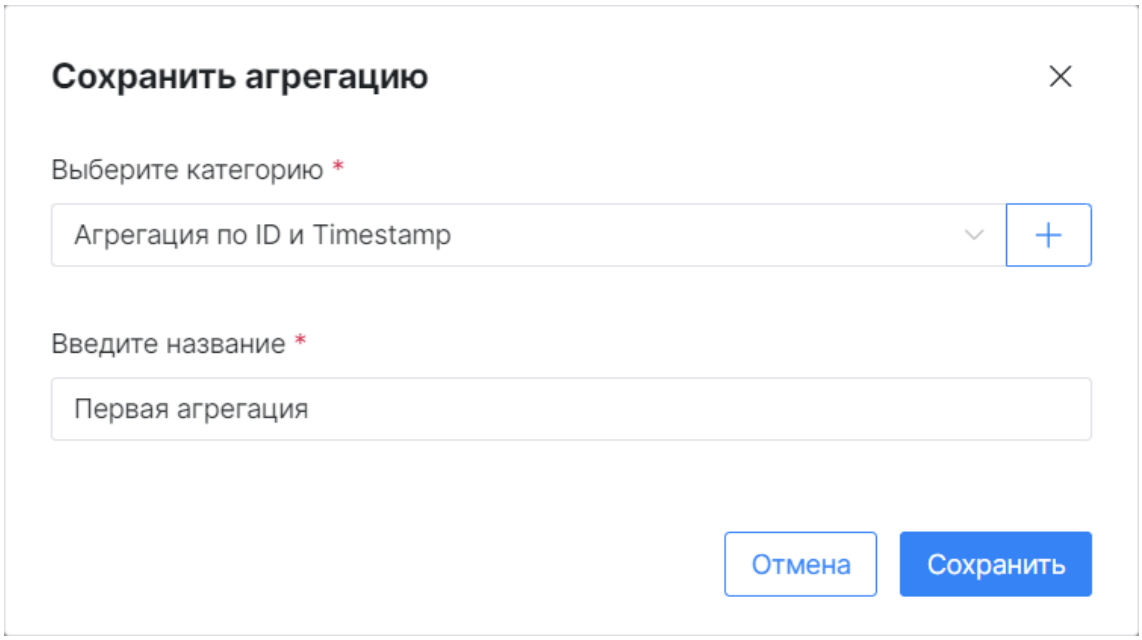


Рис. 35 – Окно "Сохранить агрегацию"

3. Укажите следующие данные:
    - в поле "Выберите категорию" из выпадающего списка выберите категорию, в которую будет сохранена агрегация;
    - если вы еще не добавили ни одной категории, то нажмите кнопку «+», укажите название категории и сохраните изменения;
    - в поле "Введите название" укажите название агрегации.
4. Нажмите кнопку **Сохранить**.

5.2.3 Работа с пресетами

Пресет – это сохраненные условия фильтрации, которые можно использовать как шаблон для формирования списка событий.

Работа с пресетами выполняется на вкладке "Пресеты" (см. «Рис. 37»).

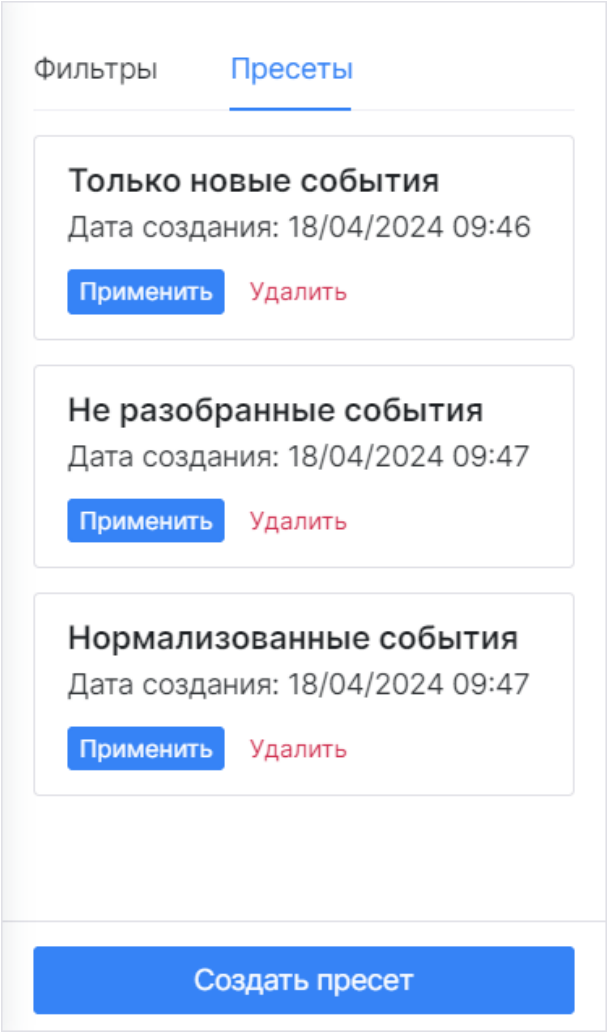


Рис. 36 – Страница "События". Вкладка "Пресеты"

На вкладке отображается следующая информация:

- название пресета;
- дата создания пресета.

Работа с пресетами включает в себя следующие процессы:

1. «Создание пресета».
2. «Применение пресета».
3. «Удаление пресета».

5.2.3.1 Создание пресета

1. Настройте условия фильтра для получения списка событий.
2. Перейдите на вкладку "Пресеты".
3. Нажмите кнопку **Создать пресет**. Откроется окно "Создание пресета" (см. «Рис. 37»).

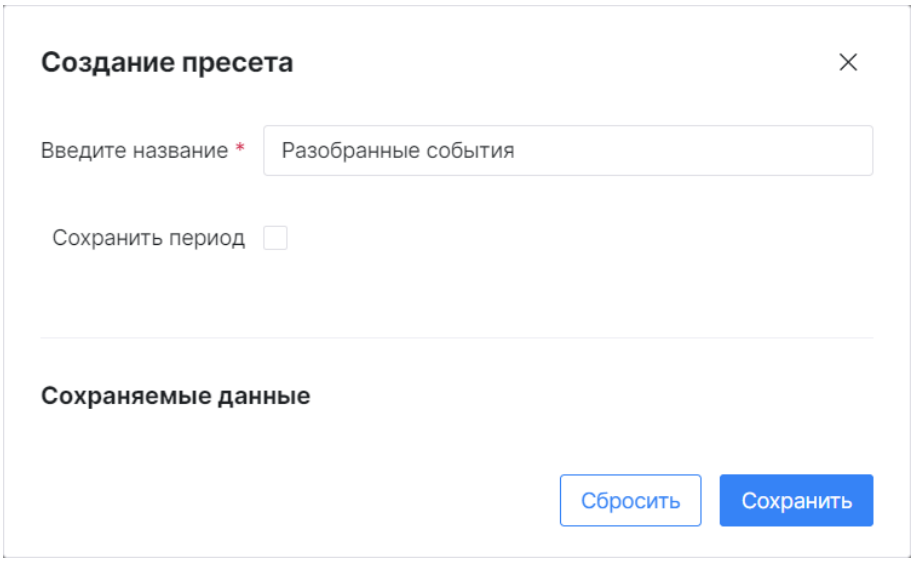


Рис. 37 – Окно "Создание пресета"

2. Укажите следующие данные:
    - в поле "Введите название" укажите название пресета;
    - установите флаг "Сохранить период" если необходимо сохранить данные о периоде формирования списка событий.
3. Нажмите кнопку **Сохранить**.

5.2.3.2 Применение пресета

1. Перейдите на вкладку "Пресеты".
2. Выберите пресет и нажмите кнопку **Применить**.
3. Будет сформирован список событий по сохраненному шаблону.

5.2.3.3 Удаление пресета

1. Перейдите на вкладку "Пресеты".
2. Выберите пресет и нажмите кнопку **Удалить**.
3. Пресет будет удален из списка.

5.2.4 История поиска

Платформа Радар ведет историю поиска событий.

Для ее просмотра нажмите кнопку 

. Отроется окно "История поиска" (см. «Рис. 38»).

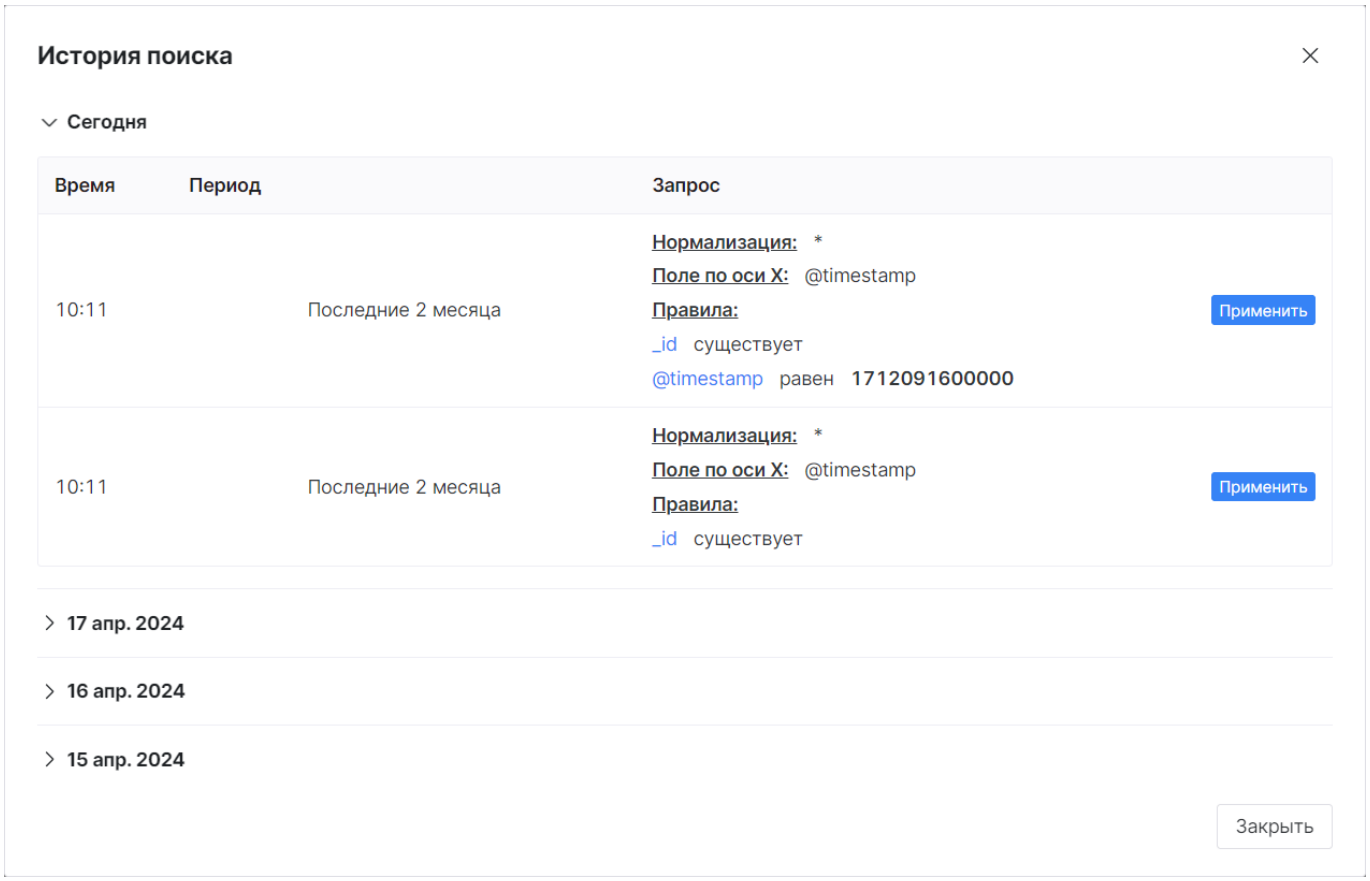


Рис. 38 – ***Окно "История поиска"***

В окне отображается следующая информация:

- день формирования списка событий;
- время создания списка событий;
- период, за который был сформирован список событий;
- условия запроса, по которым был сформирован список событий.

Вы можете сформировать список событий из истории поиска. Для этого в соответствующей строке нажмите кнопку **Применить**.

5.3 Работа с событиями

Перед началом работы с событиями:

1. Ознакомьтесь с общими данными и интерфейсом раздела (см. раздел «Общие данные»).
2. Сформируйте список событий (см. раздел «Работа с фильтрами»).

Пример сформированного списка событий приведен на «Рис. 39».

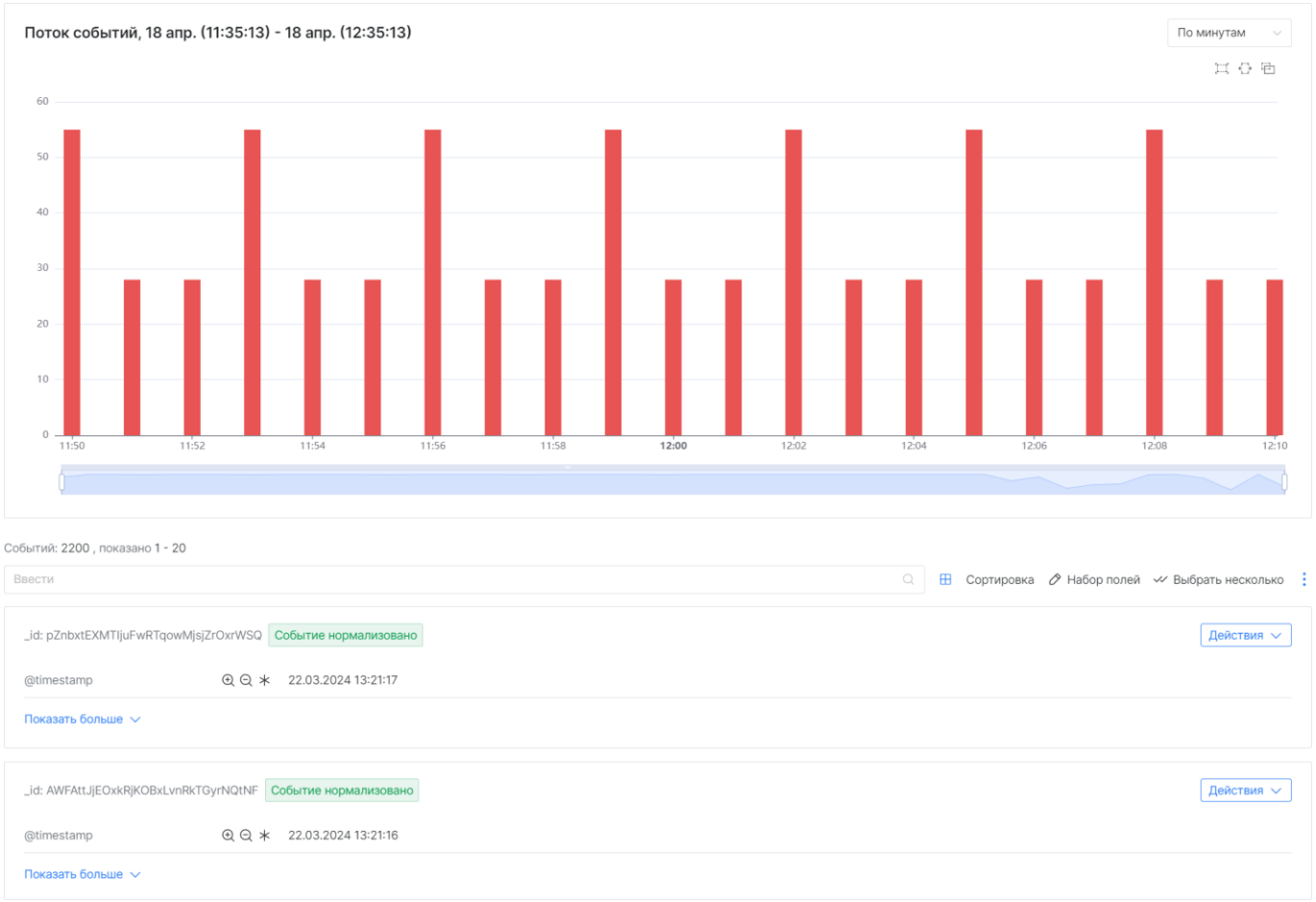


Рис. 39 – Страница "События". Сформированный список событий

Работа с событиями включает в себя следующие процессы:

1. «Создание инцидента».
2. «Добавление в инцидент».
3. «Поиск инцидент».
4. «Экспорт списка событий».

При работе с событиями можно воспользоваться вспомогательными инструментами для анализа событий:

- поиск событий;
- просмотр событий по сформированной агрегации;
- настройка плотности отрисовки значений графика;
- сортировка событий;
- настройка набора полей для табличного вида.

Подробнее см. раздел «Вспомогательные инструменты для анализа событий».

5.3.1 Создание инцидента

Примечание. *Подробнее об инцидентах см. раздел «Инциденты».*

Платформа Радар позволяет создать инцидент на основе подозрительного события.

Для этого выполните следующие действия:

1. Включите режим для массовых операций над событиями нажав кнопку **Выбрать несколько**.
2. Выберите одно или несколько событий установив флаг в соответствующей карточке/строке таблицы.
3. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт "Создать инцидент". Откроется окно "Быстрое создание инцидента".
4. В поле "Тип инцидента" из выпадающего списка выберите тип инцидента. В окне отобразится полный набор полей для заполнения сведений о выбранном типе инцидента (см. «Рис. 40»).

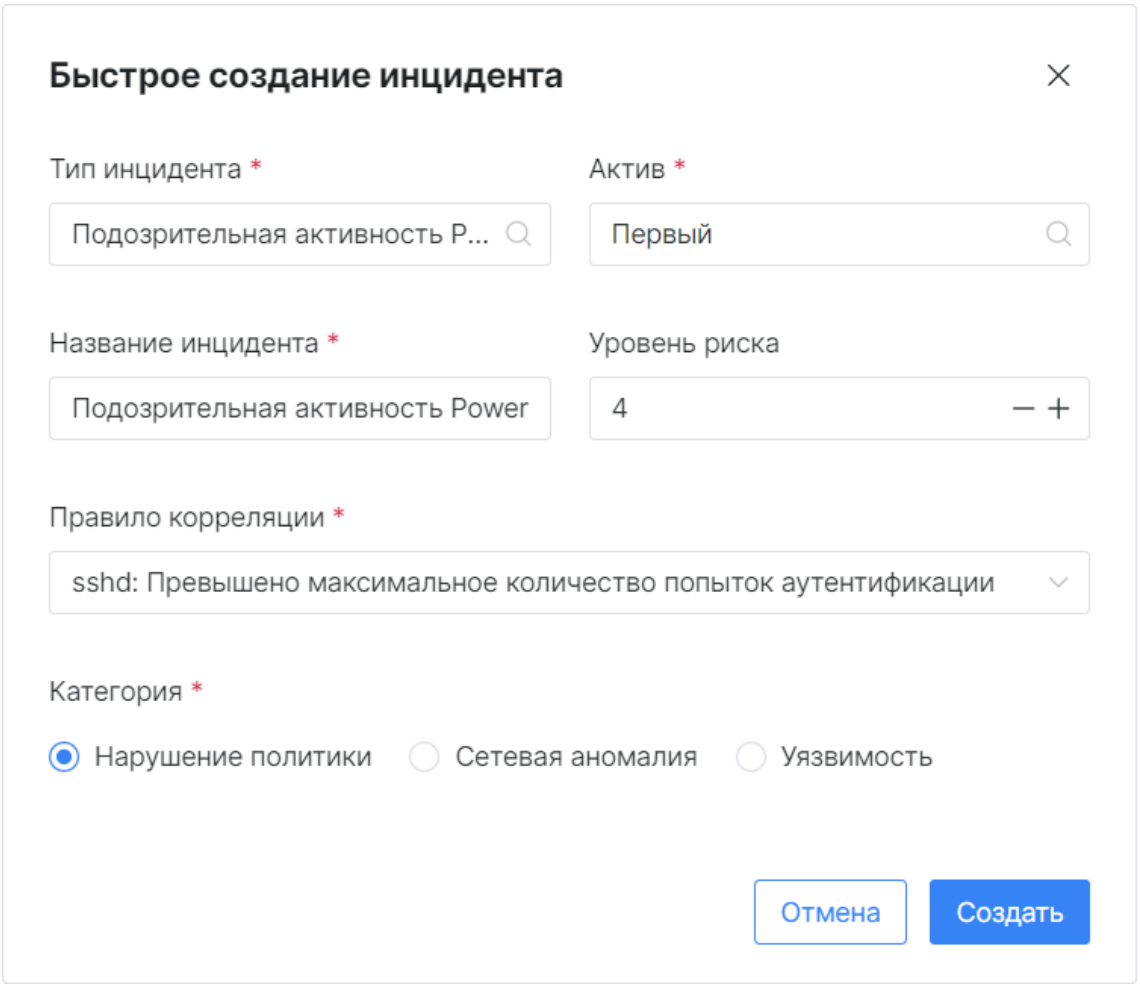


Рис. 40 – ***Окно "Быстрое создание инцидента"***

5. В зависимости от выбранного типа инцидента значения полей будут предзаполнены соответствующей информацией. При необходимости измените следующие данные:
   - в поле **Актив** из выпадающего списка выберите техническое средство информационной системы, на котором произошел инцидент;
   - в поле **Название инцидента** укажите название инцидента;
   - в поле **Уровень риска** задайте уровень риска;

- в поле **Правило корреляции** из выпадающего списка выберите соответствующее правило корреляции;
- в поле **Категория** выберите категорию инцидента: нарушение политики, сетевая аномалия или уязвимость.

6. Нажмите кнопку **Создать**.

5.3.2 Добавление события в инцидент

Платформа Радар позволяет добавить событие или несколько событий в уже созданный инцидент.

Для этого выполните следующие действия:

1. Включите режим массовых операций над событиями нажав кнопку **Выбрать несколько**.
2. Выберите одно или несколько событий установив флаг в соответствующей карточке/строке таблицы.
3. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт "Добавить к инциденту". Откроется окно "Добавить события" (см. «Рис. 41»).

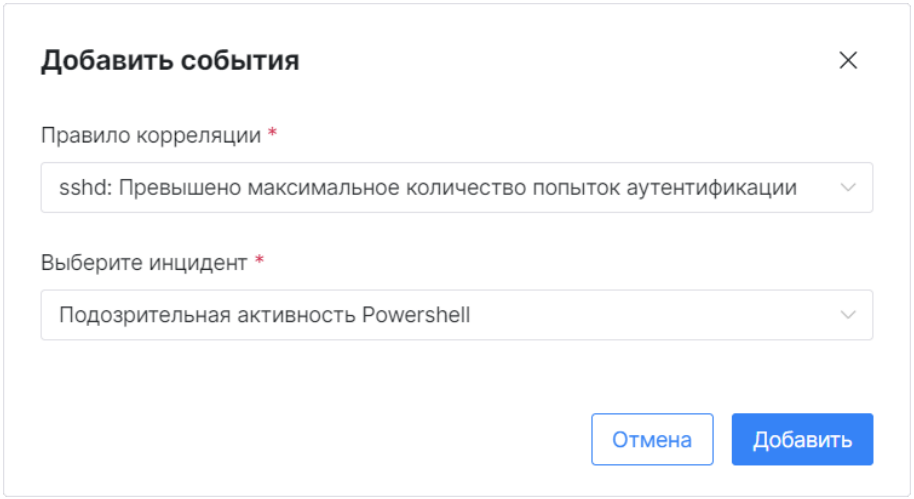


Рис. 41 – Окно "Добавить события"

4. Укажите следующие данные:
   - в поле "Правило корреляции" из выпадающего списка выберите соответствующее правило корреляции;
   - в поле "Инцидент" выберите инцидент, в который будет добавлено событие.
5. Нажмите кнопку **Добавить**.

После успешного добавления события в инцидент платформа предложит вам открыть соответствующий инцидент.

5.3.3 Поиск инцидента

Для поиска инцидента, к которому относится событие, выполните следующие действия:

1. В зависимости от вида, в котором выполняется просмотр списка событий нажмите кнопку в теле события:
   - 

- если включен карточный вид;
   - - если включен табличный вид.
2. Выберите пункт **Найти инцидент**. Откроется окно "Ссылки на инциденты" (см. «Рис. 42»).

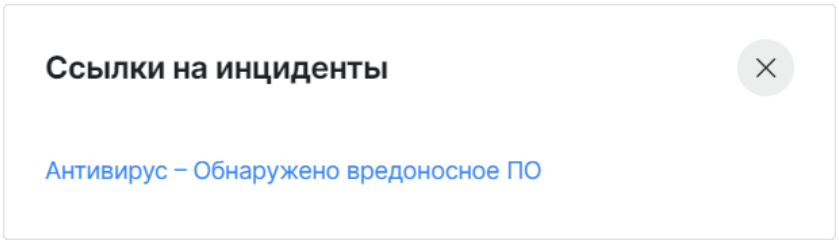


Рис. 42 – Список найденных инцидентов по событию

3. Для открытия инцидента нажмите на нужную ссылку.

5.3.4 Экспорт списка событий

Платформа Радар позволяет выгрузить список событий в файл формата CSV. Для этого выполните следующие действия:

1. Сформируйте список событий.
2. Нажмите кнопку и из выпадающего списка выберите пункт **Экспорт в CSV**.
3. Укажите путь для сохранения файла.

Помимо экспорта сформированного списка событий, в платформе доступен экспорт событий в файлы формата CSV на всю глубину фильтрации:

1. Сформируйте список событий.
2. Нажмите кнопку и из выпадающего списка выберите пункт **Экспортировать**.

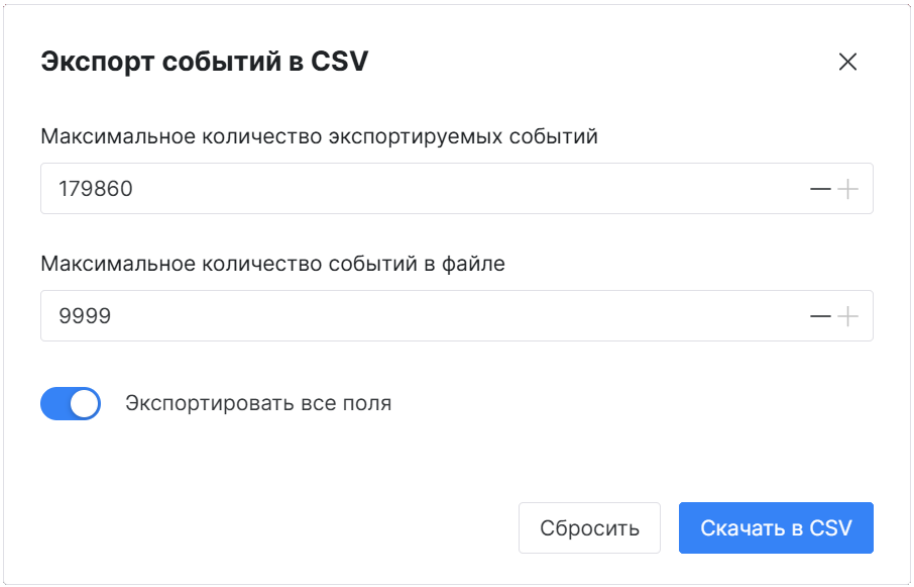


Рис. 43 – Окно "Экспорт событий в CSV"

3. Настройте в окне параметры экспорта:

   - **Максимальное количество экспортируемых событий** – укажите количество событий, которое вы хотите экспортировать. В поле автоматически отображается максимальное число событий, выведенных по примененному фильтру;

     Примечание: чем больше значение, тем дольше будет выполняться операция экспорта.

   - **Максимальное количество событий в файле** – укажите максимальное количество событий, которое будет выгружено в один файл.

     Примечание: чем больше значение, тем объемней будет файл. Ограничение: не более 100000 записей в один файл.

   - **Экспортировать все поля** – при необходимости включите экспорт всех полей события в файл. Если опция выключена, то будет выполнен экспорт только тех полей, которые настроены для отображения в табличном виде (см. раздел «Настройка набора полей для табличного вида»).

4. Нажмите кнопку **Скачать в CSV**. Начнется процесс экспорта, который может занять некоторое время. По ходу выполнения операции будут формироваться и автоматически скачиваться файлы с событиями. Файлы заполняются в соответствии с примененной фильтрацией: от первого события в списке к последнему.

5.3.5 Вспомогательные инструменты для анализа событий

5.3.5.1 Поиск событий

Примечание: начиная с версии 3.7.0 в Платформе Радар заменена поисковая система с **ElasticSearch** на **OpenSearch**. Платформа Радар позволяет искать конкретные события по значениям полей. При этом сохранилась возможность использовать в строке поиска синтаксис строкового поиска Lucene.

Для поиска событий укажите необходимое значение или выражение в строке поиска. Результаты поиска выводятся автоматически по мере заполнения поля.

Пример 1. Поиск всех событий, в которых поле elastic_key имеет значение "Разобрано" (см. «Рис. 44»).

Синтаксис elastic_key: (parsed).

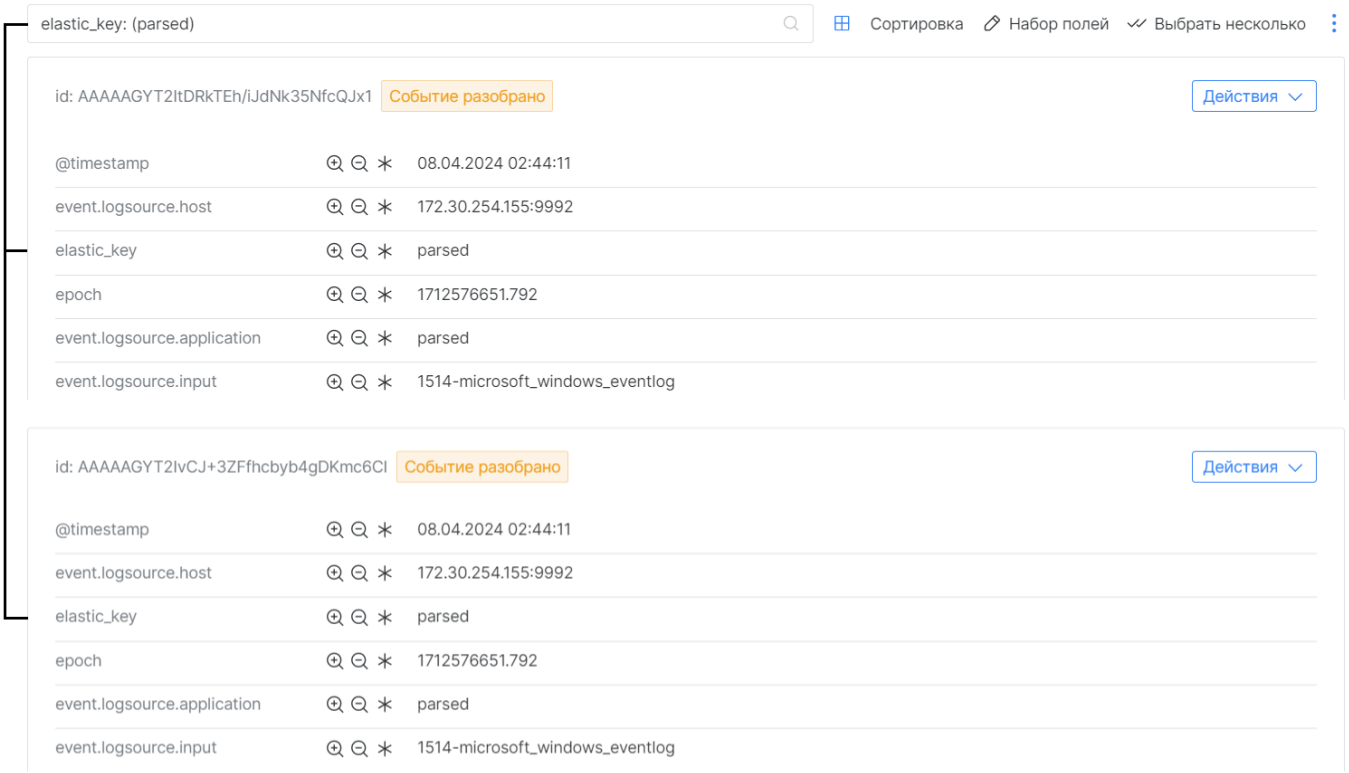


Рис. 44 – Поиск всех событий, в которых поле elastic_key имеет значение "Разобрано"

Пример 2. Поиск всех событий, в которых поле elastic_key имеет значение отличное от "Разобрано" (см. «Рис. 45»).

Синтаксис: elastic_key: (NOT parsed)

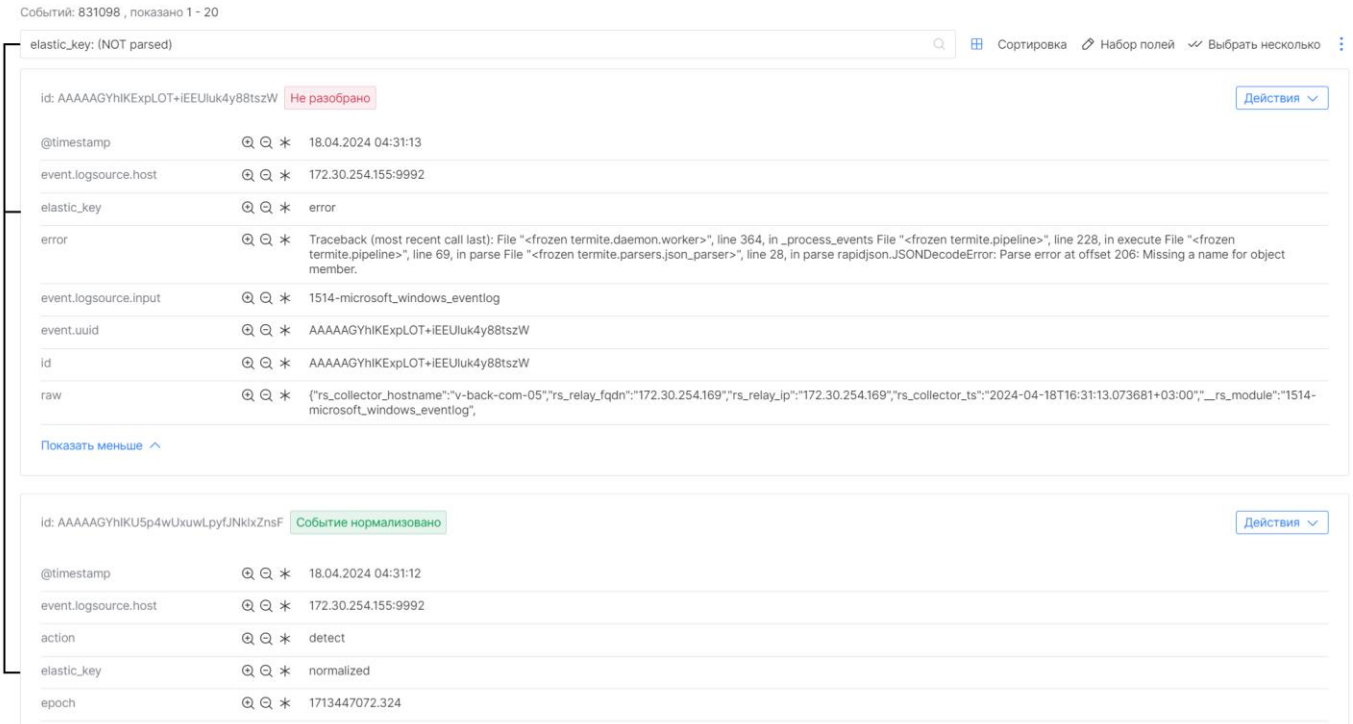


Рис. 45 – Поиск всех событий, в которых поле elastic_key имеет значение отличное от "Разобрано"

Пример 3. Поиск по конкретному значению поля (см. «Рис. 46»).

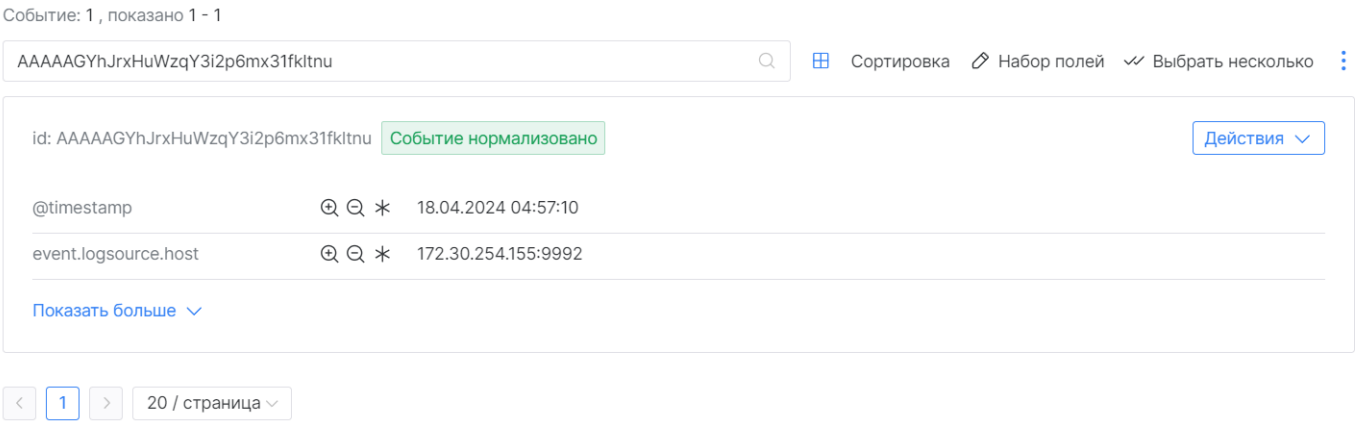


Рис. 46 – Поиск по конкретному значению

5.3.5.2 Просмотр событий по сформированной агрегации

Платформа Радар позволяет просматривать события, данные по которым были сформированы по результату агрегации.

Для этого настройте агрегации (см. раздел «Добавление агрегации») и нажмите на соответствующую ссылку в таблице результатов (см. «Рис. 47»).

Рис. 47 – Просмотр результатов агрегации

Произойдет переход на страницу "События", где в условиях фильтрации будет применен соответствующий запрос.

5.3.5.3 Настройка плотности отрисовки потока событий

При необходимости вы можете задать плотность отрисовки потока событий на графике. Доступны следующие значения:

- по годам;
- по месяцам;
- по дням;
- по часам: по три часа, по одному часу;
- по минутам: по тридцать минут, по десять минут, по одной минуте;

- по секундам.

Для изменения плотности отрисовки в правом верхнем углу графика "Поток событий" из выпадающего списка выберите необходимое значение (см. «Рис. 48»).

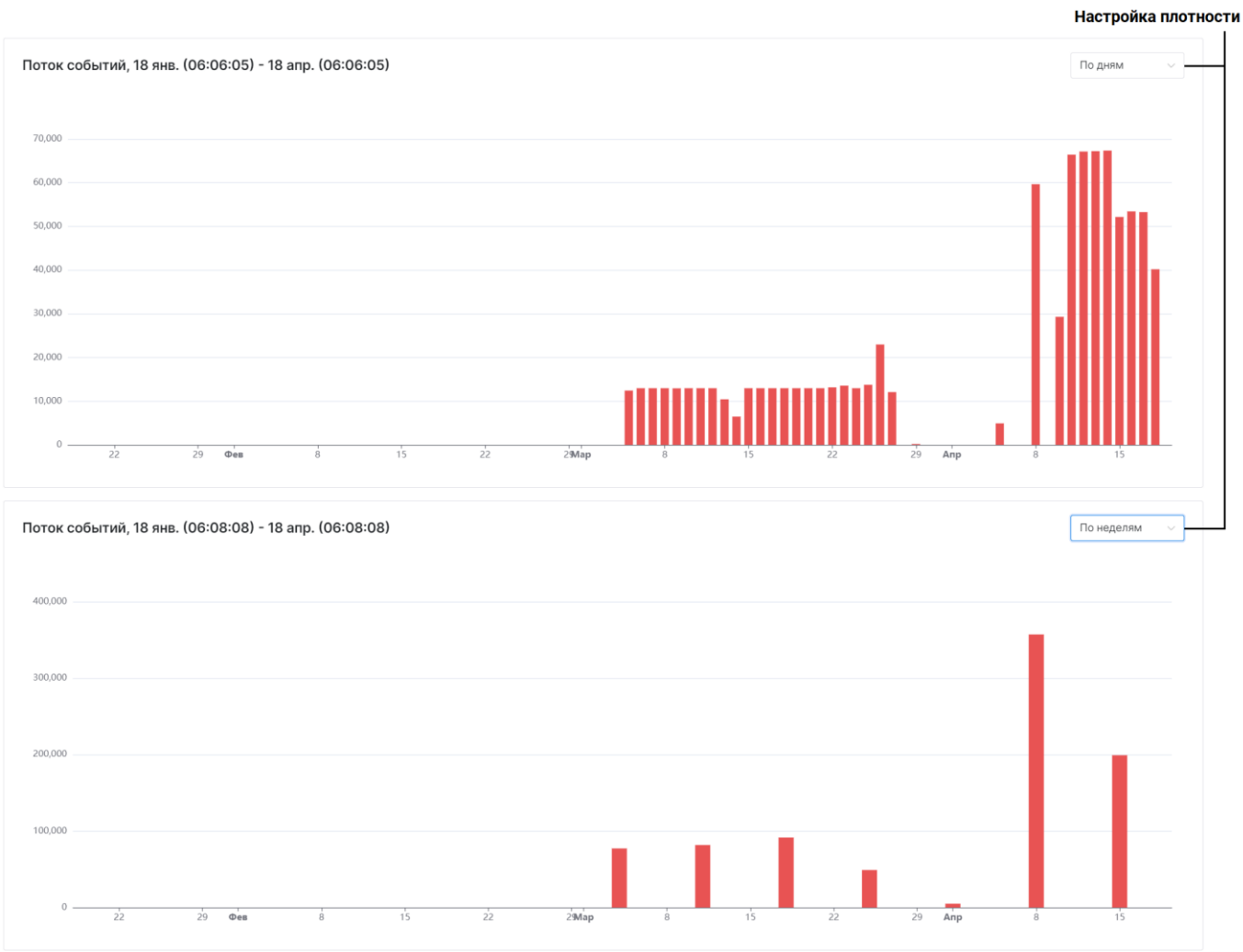


Рис. 48 – Настройка плотности отрисовки потока событий

5.3.5.4 Сортировка событий

Платформа позволяет сортировать порядок событий в списке по значениям выбранных полей.

Для этого нажмите кнопку **Сортировка**. Откроется окно настройки сортировки (см. «Рис. 49»).

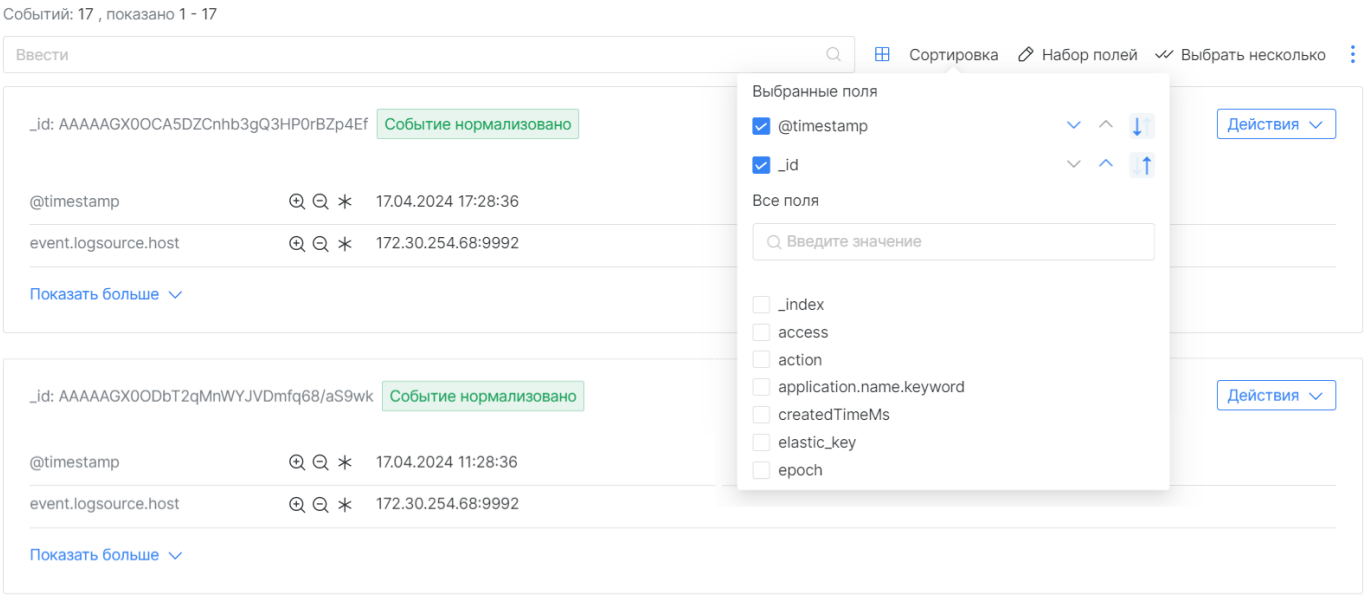


Рис. 49 – Настройка сортировки списка событий

Для настройки сортировки воспользуйтесь следующими приемами:

- для выбора полей, по которым будет выполняться сортировка, установите флаги в соответствующих полях;
- сортировка выполняется в порядке добавления полей. Для изменения порядка сортировки используйте кнопки ^ / v;
- для полей, по которым выполняется сортировка, можно задать направление сортировки:
  - ↓ - от последнего к первому;
  - ↑ - от первого к последнему.

5.3.5.5 Настройка набора полей для табличного вида

Для табличного вида списка событий вы можете настроить набор полей для отображения в таблице.

Для этого включите табличный вид по кнопке и нажмите кнопку **Набор полей**. Откроется окно "Выбор набора полей" (см. «Рис. 50»).

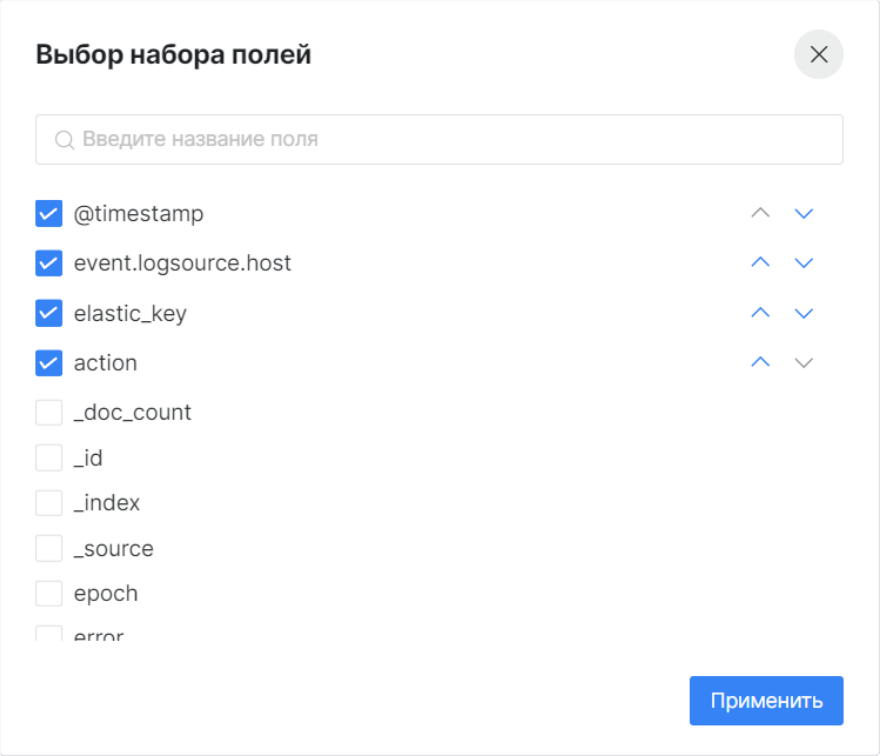


Рис. 50 – Окно "Выбор набора полей"

В окне выполните следующие действия:

1. Выберите поля, информацию по которым необходимо отобразить в табличном виде, установив соответствующие флаги.
2. Настройте порядок столбцов таблицы с помощью кнопок / .
3. Нажмите кнопку **Применить**.

6. Инциденты ИБ

6.1 Инциденты

6.1.1 Общие данные

Платформа Радар предоставляет большой набор инструментов для автоматизации процессов сбора, обработки и корреляции событий информационной безопасности с целью выявления инцидентов ИБ и организации реагирования на них.

Событие информационной безопасности (information security event) – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Инструменты по анализу событий информационной безопасности подробно рассмотрены в разделе «События».

Инцидент информационной безопасности (information security incident) – появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ.

При работе с инцидентами ИБ платформа автоматизирует ряд процессов:

- Оценку событий ИБ и принятие решения: является ли данное событие инцидентом ИБ.
- Оповещение о возникновении инцидента ИБ и назначение инцидента оператору.
- Исследование инцидента и принятие решения по результатам исследования.

Инцидент всегда относится к активу, на котором он выявлен. Значимость актива в инфраструктуре напрямую влияет на оценку угрозы инцидента. Для оценки угрозы инцидента можно использовать несколько параметров:

Срочность. Значение складывается из уровня "значимости" актива, на котором был выявлен инцидент и уровня риска, присвоенному инциденту. На параметр также влияет сетевая видимость актива и то, на сколько инцидент был просрочен.

Уровень риска. Цифровое обозначение уровня угрозы, присвоенному инциденту.

В платформе инцидент принадлежит к одной из трех категорий:

- нарушение политики – это наступление условий, нарушающих политику безопасности эксплуатации актива (задуманную службой безопасности);
- сетевая аномалия – актив проявляет сетевую активность, которую проявлять не должен;
- уязвимость – у злоумышленника есть возможность получить контроль (полный или частичный) над активом.

Стадия обработки инцидента называется статус. В платформе используются следующие статусы инцидентов:

- **ПР Новый** – статус присваивается вне основного рабочего процесса, например для тестирования. Инцидент в данном статусе виден только в интерфейсе администратора;

- **Новый** – статус присваивается, когда инцидент был создан вручную или автоматически;
- **Назначен** – статус присваивается, когда инцидент передали в работу конкретному пользователю или группе пользователей;
- **В работе** – статус присваивается, когда пользователь, на которого назначили инцидент, начал расследование инцидента;
- **Запрошена информация** – обработка инцидента приостановлена, исполнителем 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.

Процесс изменения стадии обработки инцидента приведен на «Рис. 51».

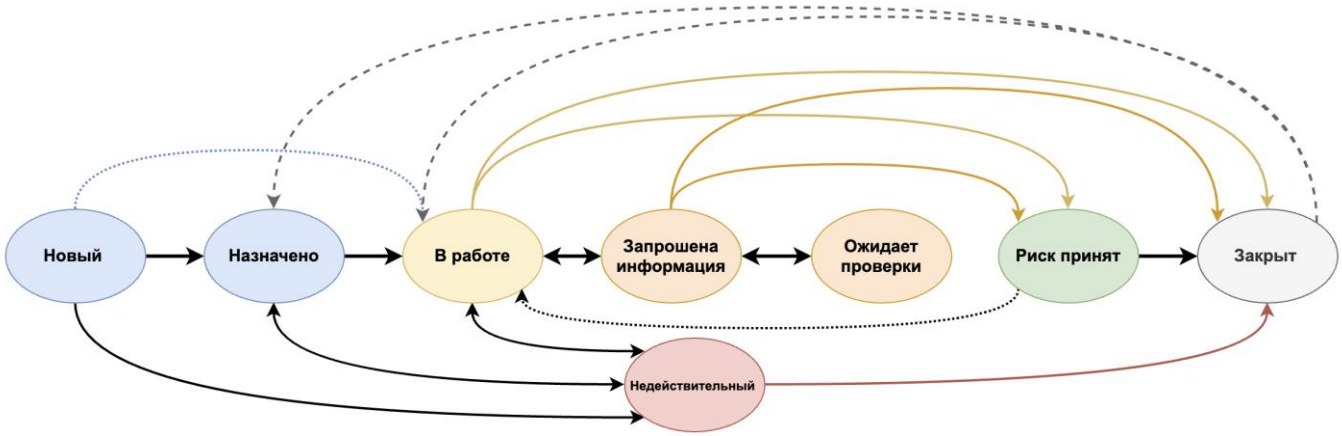


Рис. 51 – Процесс изменения статусов инцидентов

В платформе каждый инцидент всегда принадлежит к определенному типу инцидента. Типы инцидентов это сведения о уязвимости, нарушении политики, аномальной сетевой активности без привязки к активу (подробнее см. раздел «Типы инцидентов»).

Схожие инциденты можно объединить в группы, а их затем назначить пользователям. Это упрощает управление назначением инцидентов сотрудникам и позволяет выполнять массовые операции над инцидентами через группы (подробнее см. раздел «Группы инцидентов»).

Инциденты могут хранить любую дополнительную информацию, добавляемую к инцидентам как в процессе их создания правилами корреляции, так и в процессе расследования операторами (подробнее см. раздел «Дополнительные поля»).

Платформа Радар позволяет отправлять происшествия, выявленные в критической информационной инфраструктуре (КИИ) Российской Федерации, в национальный координационный центр по компьютерным инцидентам (подробнее см. раздел «Происшествия на отправку»).

Работа с инцидентами включает в себя следующие процессы:

1. «Создание инцидента».
2. «Просмотр инцидента».
3. «Назначение инцидента».
4. «Изменение статуса инцидента».
5. «Добавление комментария к инциденту».
6. «Редактирование инцидента».
7. «Просмотр истории изменения инцидента».
8. «Удаление инцидента».

Для работы с инцидентами ИБ перейдите в раздел **Инциденты → Инциденты** (см. «Рис. 52»).

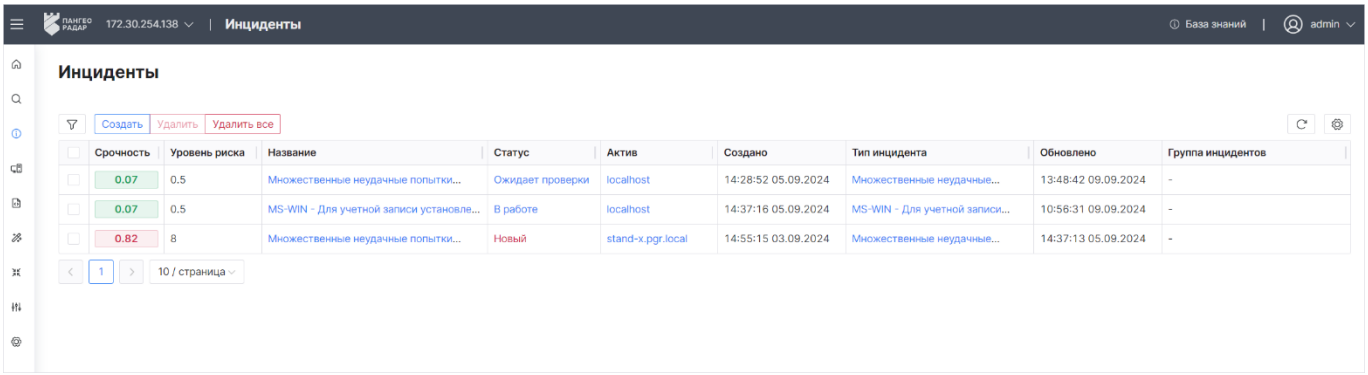


Рис. 52 – Раздел "Инциденты"

В разделе отображается следующая информация об инцидентах:

- **Срочность** – цветовое и цифровое обозначение срочности инцидента;
- **Название** – наименование инцидента;
- **Статус** – состояние инцидента;
- **Создано** – дата и время создания инцидента;
- **Уровень риска** – цифровое обозначение уровня угрозы, присвоенного инциденту;
- **ID** – идентификатор инцидента;
- **Тип инцидента** – наименование типа инцидента;
- **Группа инцидентов** – наименование группы инцидентов, в которую входит инцидент;
- **Актив** – наименование актива, на котором выявлен инцидент;
- **Последнее происшествие** – дата и время последнего происшествия, зафиксированного по инциденту;
- **Кол-во происшествий** – количество происшествий, зафиксированных в инциденте;
- **Кол-во повторных открытий** – количество повторных открытий инцидента;
- **Пользователь** – наименование пользователя, назначенного на разбор инцидента;
- **Группа пользователей** – наименование группы пользователей, назначенной на разбор инцидента;

- **Обновлено** – дата и время изменения информации об инциденте;
- **Категория** – наименование категории, к которой относится инцидент: нарушение политики, сетевая аномалия, уязвимость;
- **Эксплуатируется удаленно** – признак, возможна ли удаленная эксплуатация уязвимости: да, нет;
- **Результат анализа** – результат анализа инцидента.

6.1.2 Создание инцидента

Создание инцидента можно выполнить несколькими способами:

1. Вручную из раздела **Инциденты**.
2. При анализе событий ИБ (см. раздел «Создание инцидента»).
3. При анализе "сработок" правила корреляции (см. раздел «Действия над результатами сработок правила»).
4. Автоматически, по результатам работы следующих механизмов:
    - работы правил корреляции (см. раздел «Правила корреляции»);
    - при работе со сканером уязвимостей (см. раздел «Начните процесс удаления сетевого интерфейса через «универсальные таблицы» или инструмент «боковая панель».

1. Подтвердите удаление в открывшемся окне.
2. Сетевой интерфейс будет удален из платформы.
    - Результаты сканирования»);
    - при контроле установленного программного обеспечения (см. раздел «Наборы правил соответствия ПО»).

Для создания инцидента вручную выполните следующие действия:

1. Перейдите в раздел **Инциденты → Инциденты** и нажмите кнопку **Создать**. Откроется форма "Создание инцидента" (см. «Рис. 53» и «Рис. 54»).

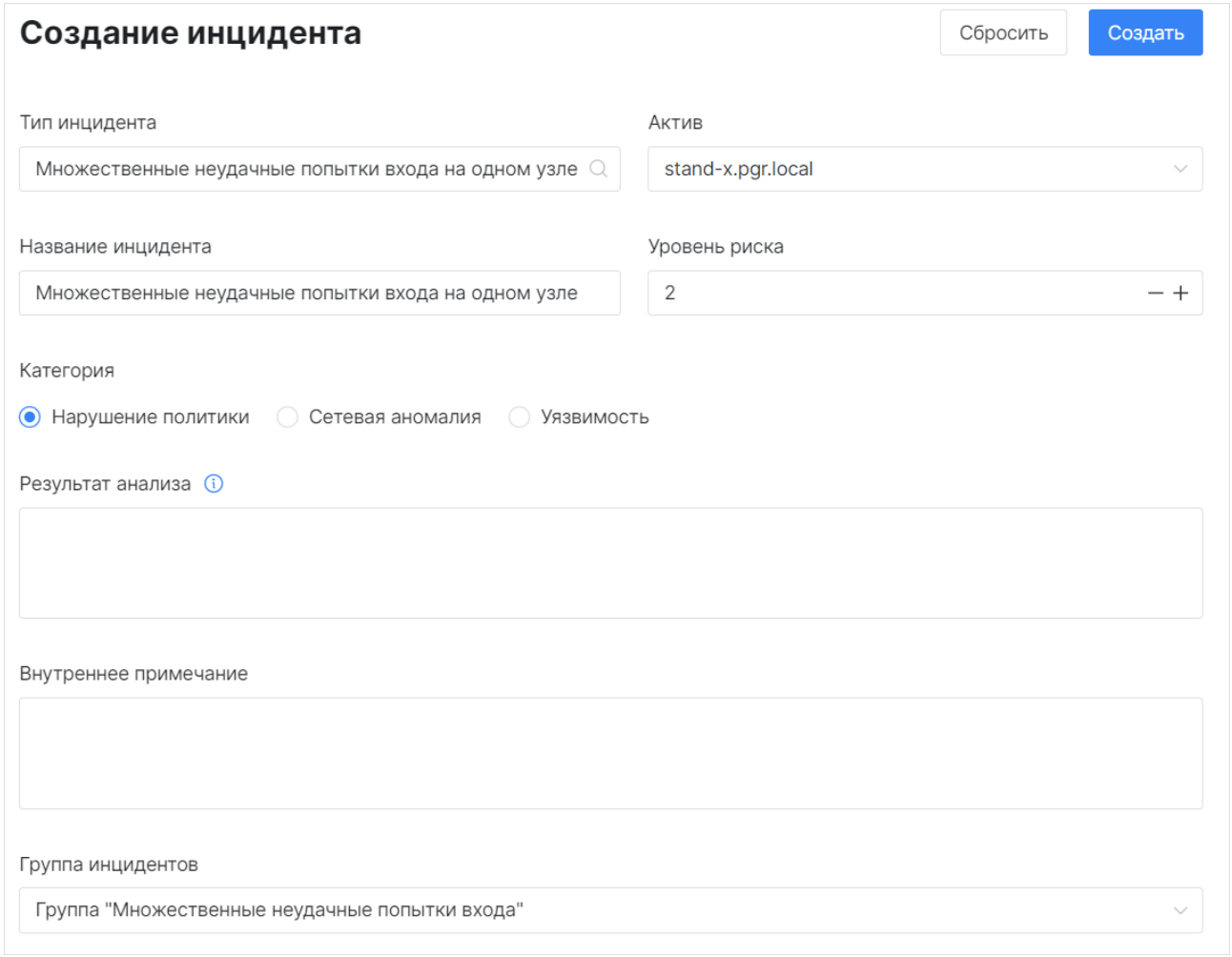


Рис. 53 – Создание инцидента. Общие сведения

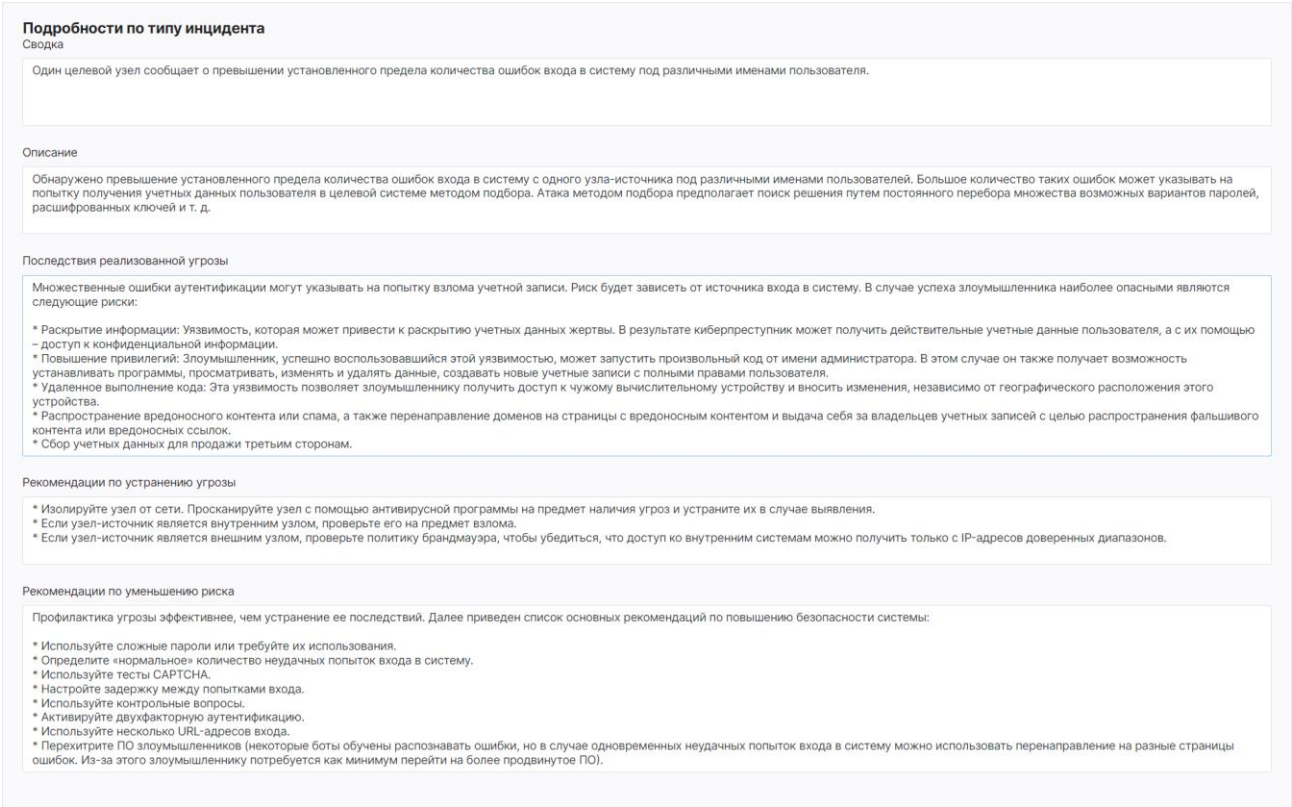


Рис. 54 – Создание инцидента. Подробности по типу инцидента

2. Укажите на форме следующую информацию:
    - в поле **Тип инцидента** из выпадающего списка выберите тип, к которому относится инцидент. При выборе типа инцидента в поля формы будут автоматически добавлены данные из справочника "Типы инцидентов";
    - в поле **Актив** из выпадающего списка выберите устройство, на котором был обнаружен инцидент;
    - в поле **Название инцидента** укажите название инцидента;
    - в поле **Уровень риска** выберите цифровое обозначение уровня риска. Допустимые значения от 0 до 10;
    - в поле **Категория** выберите одну из категорий, в которую входит инцидент: нарушение политики, сетевая аномалия, уязвимость;
    - в случае, если сведения о происшествии инцидента планируется передать во внешнюю систему, то в поле **Результат анализа** необходимо указать соответствующие сведения (см. раздел «Происшествия на отправку»);
    - в поле **Внутреннее примечание** укажите дополнительные сведения об инциденте;
    - в поле **Группа инцидентов** из выпадающего списка выберите группу, в которую следует добавить инцидент (см. раздел «Группы инцидентов»).
3. При необходимости в блоке **Подробности по типу инцидента** актуализируйте информацию о типе инцидента.

    Примечание: при изменении информации в данном блоке будет изменен соответствующий справочник в разделе «Типы инцидентов».
4. Нажмите кнопку **Создать**.

6.1.3 Просмотр инцидента

Для просмотра и анализа инцидента нажмите по ссылке с наименованием инцидента. Откроется форма просмотра инцидента (см. «Рис. 55»).

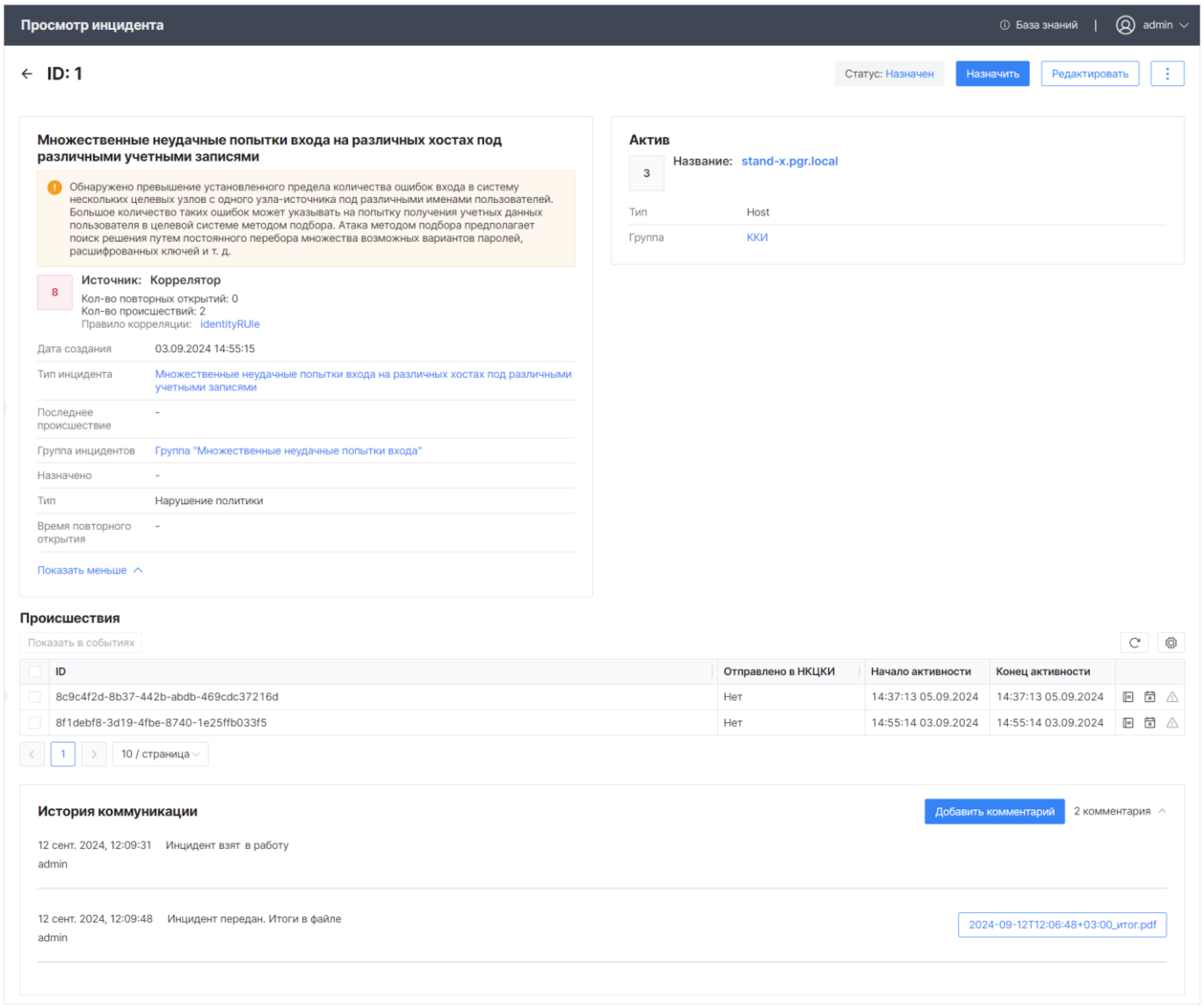


Рис. 55 – Форма просмотра инцидента

На форме просмотра инцидента информация сгруппирована по следующим блокам:

- Общая информация об инциденте.
- Актив – информация об активе, на котором обнаружен инцидент.
- Результат анализа – информация о результатах анализа инцидента. Данный блок отображается если данное поле было заполнено при создании инцидента.
- Происшествия – информация о происшествиях, из которых состоит инцидент.
- История коммуникации в рамках расследования инцидента.

6.1.3.1 Общая информация об инциденте

Пример блока с общей информации об инциденте приведен на «Рис. 56».

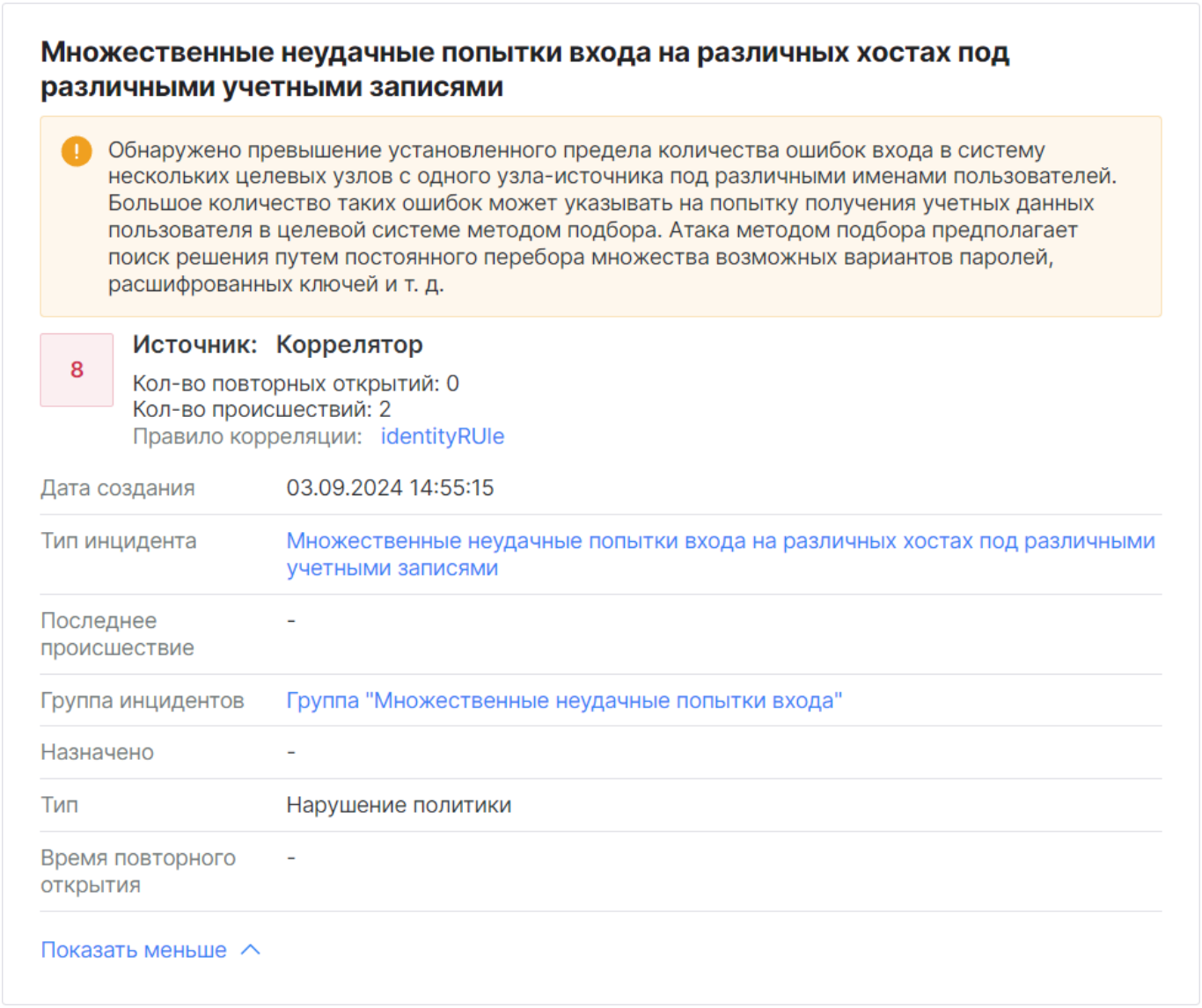


Рис. 56 – Просмотр инцидента. Общая информация

В блоке отображается следующая информация:

- Название инцидента.
- Подробное описание инцидента.
- Цветовое и цифровое значение уровня риска.
- Источник – механизм, с помощью которого был создан инцидент:
    - Коррелятор – инцидент был создан на основе "сработки" правила корреляции;
    - Сканнер уязвимостей – инцидент был создан в результате работы сканнера уязвимостей;
    - Если источник не указан, это означает что инцидент был создан вручную;
    - Контроль ПО – инцидент был создан на основе "сработки" правила контроля установленного ПО.

Информация, отображаемая в блоке "Источник" формируется в зависимости от механизма, с помощью которого был создан инцидент и может содержать следующую информацию:

- Эксплуатируется удаленно (только для сканнера уязвимостей) – признак удаленной эксплуатации, возможные значение: да, нет;
- Правило корреляции (только для коррелятора) – наименование правила, по "сработке" которого был создан инцидент. По ссылке произойдет переход на форму просмотра правила;
- Количество повторных открытий инцидента;
- Количество происшествий, зарегистрированных в инциденте.

- Дата и время создания инцидента.
- Тип инцидента – по ссылке произойдет переход на форму просмотра типа инцидента.
- Последнее происшествие – дата и время последнего зарегистрированного происшествия.
- Информация о пользователях, которым назначен инцидент.
- Тип – категория, к которой относится инцидент: нарушение политики, сетевая аномалия, уязвимость.
- Дата и время повторного открытия.

6.1.3.2 Информация об активе

Пример блока с информацией об активе приведен на «Рис. 57».

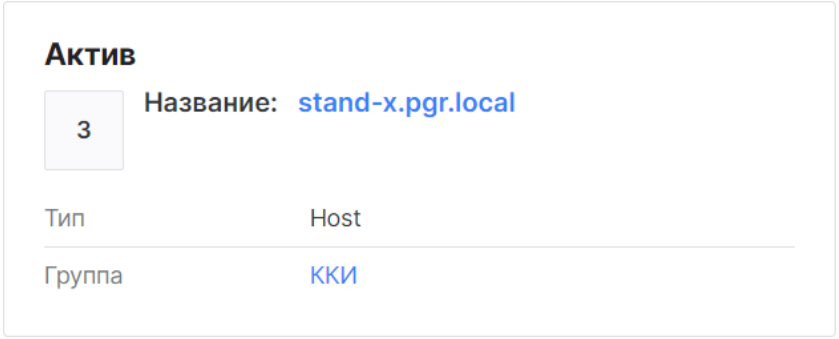


Рис. 57 -- Просмотр инцидента. Информация об активе

В блоке отображается следующая информация:

- Цветовое и цифровое обозначение "значимости" актива.
- Название актива. По ссылке произойдет переход на форму просмотра актива.
- Тип актива.
- Название группы, к которой принадлежит актив. По ссылке произойдет переход на форму просмотра группы активов.

6.1.3.3 Информация о происшествиях

Пример блока с информацией о происшествиях приведен на «Рис. 58».

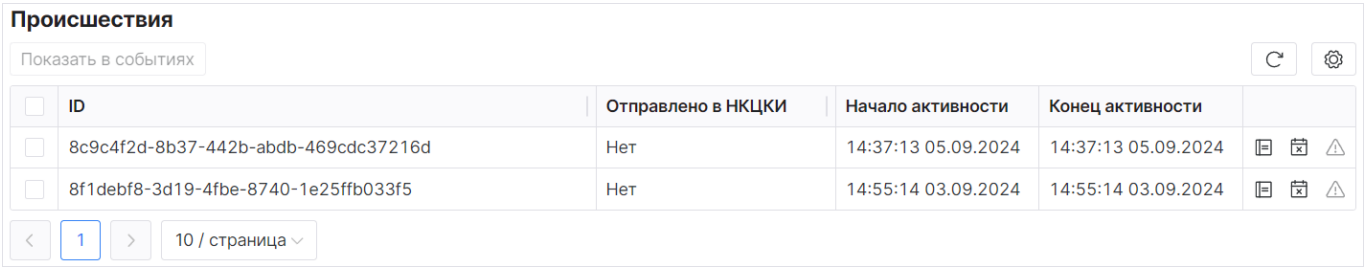


Рис. 58 – Просмотр инцидента. Информация о происшествиях

В блоке отображается следующая информация:

- Уникальный идентификатор происшествия.
- Отправлено в НКЦКИ – признак отправки происшествия в национальный координационный центр по компьютерным инцидентам (подробнее см. раздел «Происшествия на отправку»).
- Дата и время начала и конца активности происшествия.

Для просмотра деталей происшествия нажмите на кнопку . Произойдет переход в раздел **События** с автоматически сформированным фильтром для отображения происшествия на графике потока событий.

Для просмотра события, в котором было зарегистрировано происшествие, нажмите на кнопку . Откроется окно "Результат события" (см. «Рис. 59»).

Рис. 59 – Окно "Результат события"

Если инцидент был создан с помощью сканнера уязвимостей, то доступен просмотр данных об обнаруженной уязвимости. Для этого нажмите кнопку ⚠. Откроется окно "Данные по уязвимости" (см. «Рис. 60»).

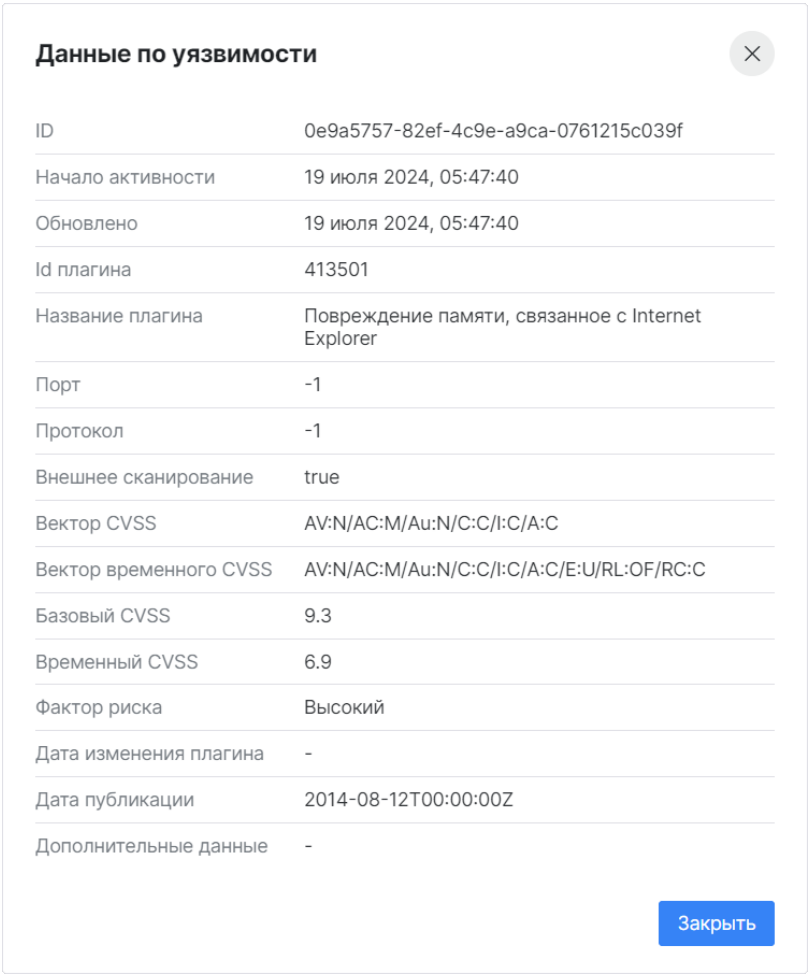


Рис. 60 – Окно "Данные по уязвимости"

6.1.3.4 История коммуникации

Пример блока с информацией об истории коммуникации приведен на «Рис. 61».

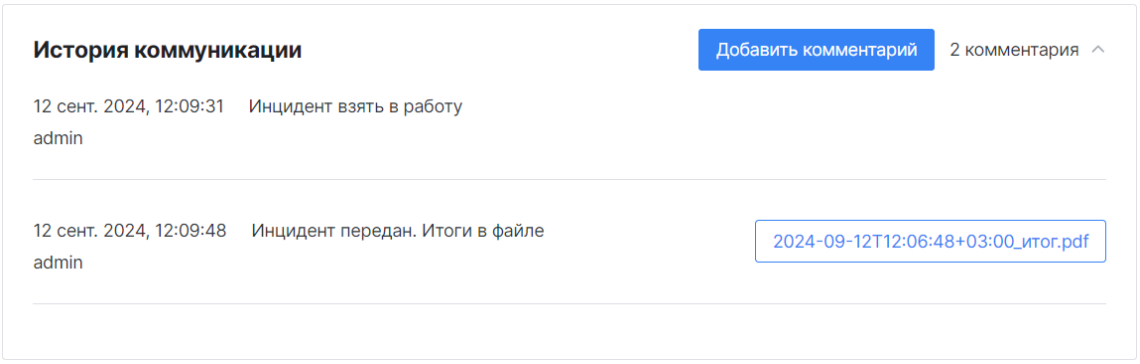


Рис. 61 -- Окно "Данные по уязвимости"

В блоке отображается следующая информация:

- Количество оставленных комментариев.
- Дата и время создания комментария.

- Содержание комментария.
- Список прикрепленных файлов.
- Пользователь, оставивший комментарий.

Для просмотра прикреплённых файлов нажмите на соответствующую ссылку.

6.1.4 Назначение инцидента

1. Перейдите на форму просмотра необходимого инцидента.
2. Нажмите на кнопку **Назначить**. Откроется окно "Назначить" (см. «Рис. 62»).

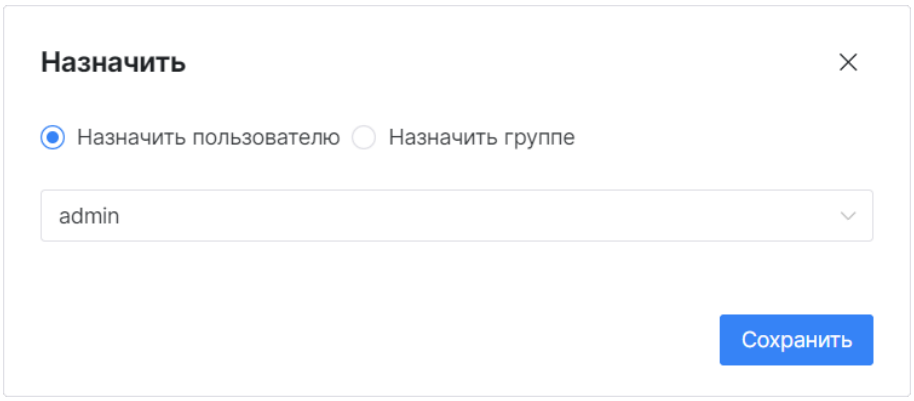


Рис. 62 – Окно "Данные по уязвимости"

3. Выполните в окне следующие действия:
    - выберите способ назначения: конкретному пользователю или группе пользователей;
    - из выпадающего списка выберите пользователя или группу пользователей;
    - нажмите кнопку **Сохранить**.

6.1.5 Изменение статуса инцидента

1. Перейдите на форму просмотра необходимого инцидента.
2. Нажмите на кнопку с текущим статусом инцидента и из выпадающего списка выберите доступный статус. Описание и возможные изменения статусов приведены в разделе «Общая информация».

6.1.6 Добавление комментария к инциденту

1. Перейдите на форму просмотра необходимого инцидента.
2. В блоке **История коммуникации** нажмите на кнопку **Добавить комментарий**. Откроется окно "Добавить комментарий" (см. «Рис. 63»)

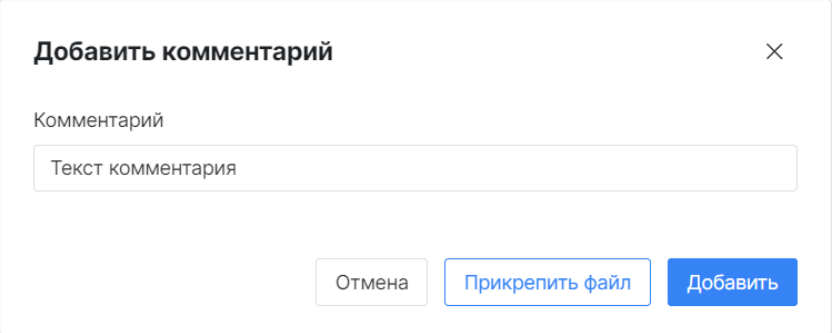


Рис. 63 – Окно "Добавить комментарий"

3. Выполните в окне следующие действия:
    - в поле **Комментарий** укажите необходимые сведения.
    - при необходимости прикрепите файл. Для этого нажмите на кнопку **Прикрепить файл** и в открывшемся окне укажите путь к файлу.
    - нажмите кнопку **Добавить**.

6.1.7 Редактирование инцидента

1. Перейдите на форму просмотра необходимого инцидента и нажмите кнопку **Редактировать**.
2. Внесите необходимые изменения.
3. При необходимости добавьте дополнительные поля в инцидент (подробнее см. раздел «Дополнительные поляе поля»).
4. Сохраните изменения.

6.1.8 Просмотр истории изменения инцидента

Перейдите на форму просмотра необходимого инцидента, нажмите кнопку  и из выпадающего списка выберите пункт **История изменений**. Откроется форма "История изменений" (см. «Рис. 64»).

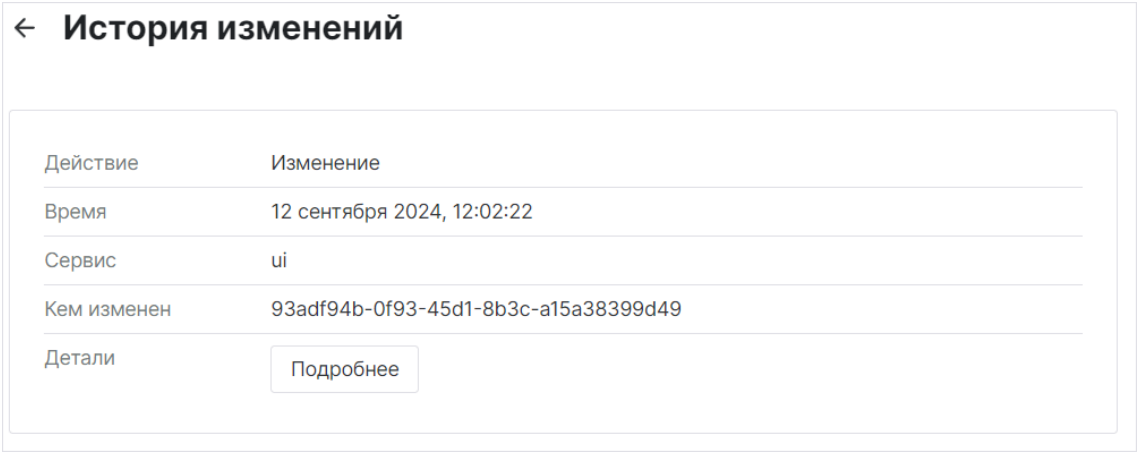


Рис. 64 – История изменений"

На форме отображается следующая информация:

- Действие – тип действия, выполненного над инцидентом: создание, изменение и т.д.;

- Время – дата и время выполнения действия над инцидентом;
- Сервис – название сервиса, через который было выполнено изменение;
- Кем изменен – уникальный идентификатор сервиса или пользователя, выполнившего изменение;
- Детали – просмотр подробного журнала изменения инцидента.

6.1.9 Удаление инцидента

Удаление инцидента можно выполнить несколькими способами:

- Способ 1 – из раздела **Инциденты**;
- Способ 2 – из формы просмотра инцидента.

Способ 1:

1. Выберите один или несколько инцидентов, установив соответствующие флаги.
2. Нажмите кнопку **Удалить**.
3. Подтвердите удаление в открывшемся окне.
4. Для удаления всех инцидентов нажмите кнопку **Удалить все**.

Способ 2:

1. Перейдите на форму просмотра необходимого инцидента, нажмите кнопку  и из выпадающего списка выберите пункт **Удалить**.
2. Подтвердите удаление в открывшемся окне.

6.2 Типы инцидентов

6.2.1 Общие сведения

Типы инцидентов содержат сведения об угрозах, на основе которых создаются инциденты. В платформе каждый инцидент всегда принадлежит к определенному типу инцидента.

В платформе предоставляется большой набор предустановленных типов, но существует возможность добавлять, актуализировать и настраивать типы инцидентов самостоятельно.

Тип инцидента всегда принадлежит к одному из трех типов уязвимостей:

- нарушение политики – это наступление условий, нарушающих политику безопасности эксплуатации актива (задуманную службой безопасности);
- сетевая аномалия – актив проявляет сетевую активность, которую проявлять не должен;
- уязвимость – у злоумышленника есть возможность получить контроль (полный или частичный) над активом.

Работа с типами инцидентов включает в себя следующие процессы:

1. «Просмотр и анализ типа инцидента».
2. «Создание типа инцидента».

3. «Редактирование типа инцидента».
4. «Написать ответственному».
5. «Дублирование типа инцидента».
6. «Дублирование типа инцидента

1. Откройте форму просмотра типа инцидента и нажмите кнопку Дублировать.
2. В открывшемся окне укажите наименование типа инцидента и нажмите кнопку Дублировать.
3. Будет создан новый тип инцидента на основе существующего.

7. Импорт типов инцидентов».
8. «Экспорт типов инцидентов».
9. «Экспорт типов инцидентов в CSV».
10. «Удаление типа инцидента».

Для работы с типами инцидентов перейдите в раздел **Инциденты → Типы инцидентов** (см. «Рис. 65»).

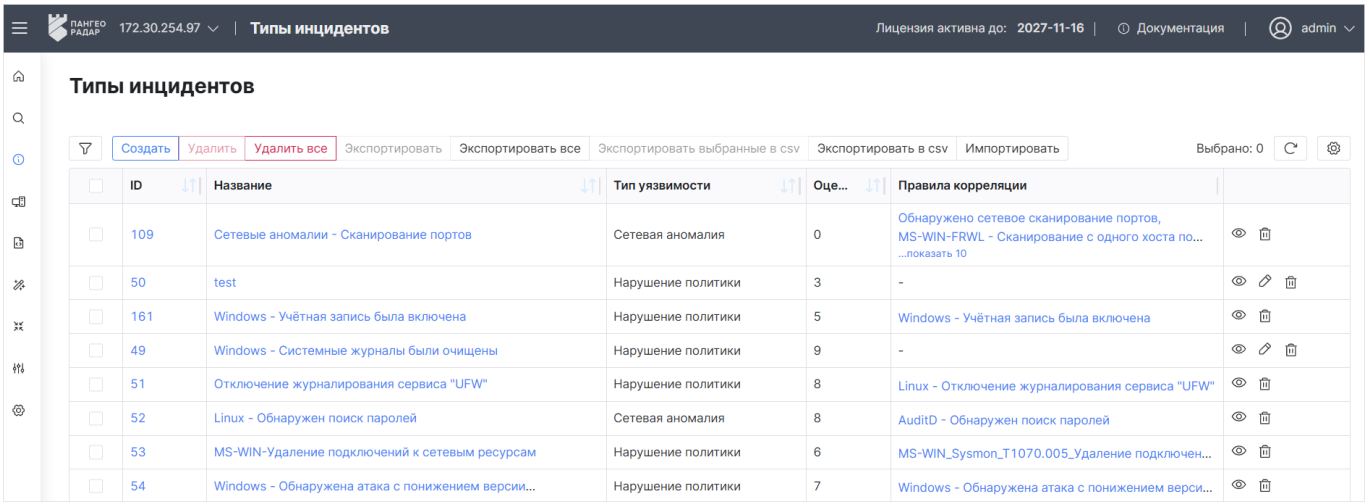


Рис. 65 – Раздел "Типы инцидентов"

В разделе отображается следующая информация:

- **ID** – идентификатор типа инцидента;
- **Название** – наименование типа инцидента;
- **Тип уязвимости** – наименование типа уязвимости, к которой относится угроза: нарушение политики, сетевая аномалия, уязвимость;
- **Оценка риска** – цифровое обозначение уровня угрозы;
- **Правила корреляции** – список правил корреляций, которые задействуют данный тип инцидента при "сработке". Если у типа инцидента выставлена связь с правилами корреляции, то его нельзя изменить.

Элементы управления универсальными таблицами описаны в разделе «Универсальные таблицы».

6.2.2 Просмотр и анализ типа инцидента

Для работы с типами инцидентов перейдите в раздел **Инциденты → Типы инцидентов**. Для просмотра типа инцидента выберите его из списка (см. «Рис. 66»).

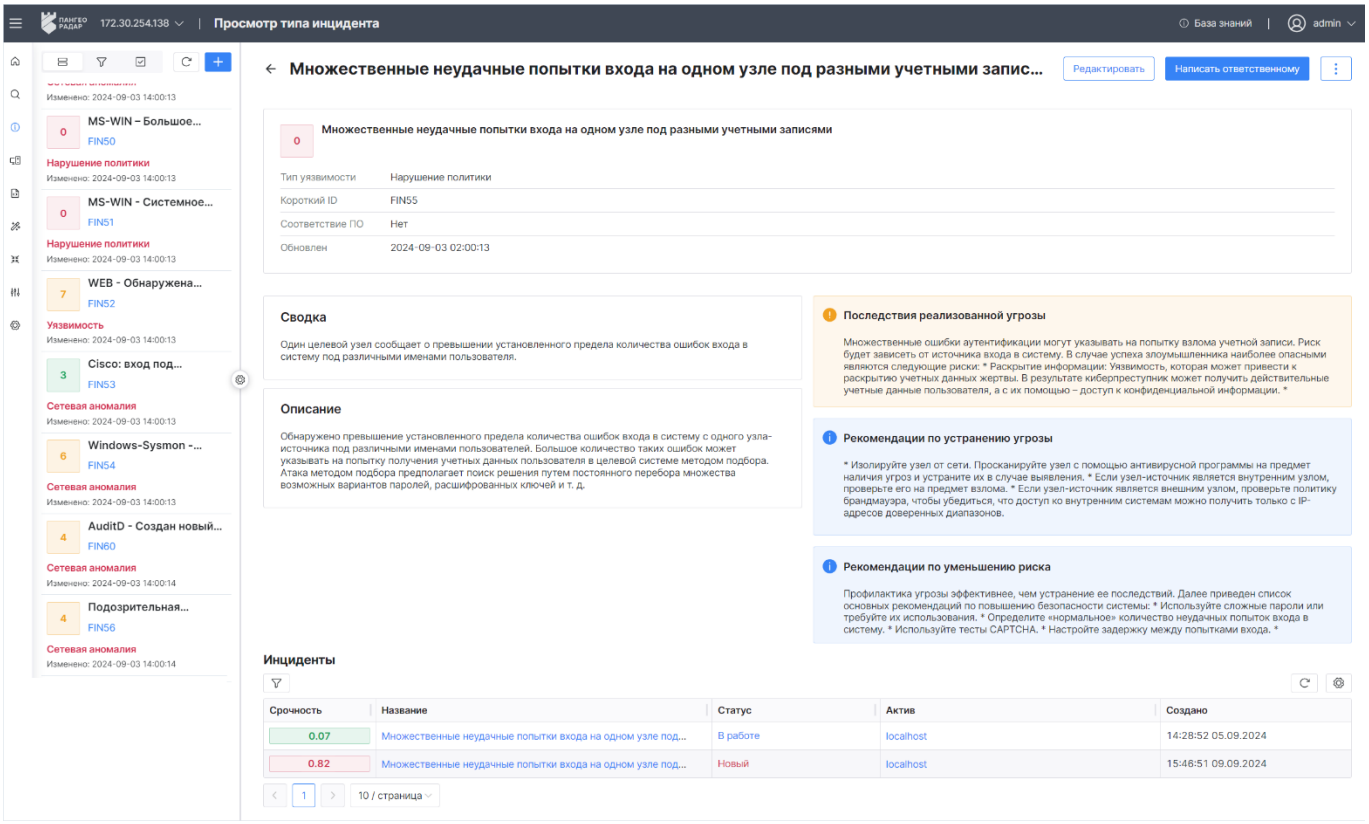


Рис. 66 – Форма просмотра типа инцидента

В боковой панели отображается следующая информация о типах инцидентов:

- Оценка риска – цветовое и цифровое обозначение уровня угрозы;
- Название типа инцидента;
- Уникальный идентификатор типа инцидента (короткая версия);
- Тип уязвимости – наименование типа уязвимости, к которой относится угроза: нарушение политики, сетевая аномалия, уязвимость;
- Дата и время последнего изменения.

В рабочей области помимо информации, отображаемой в боковой панели, отображается следующая информация:

- Признак соответствия ПО: да, нет. Параметр определяет используется данный тип инцидентов для создания инцидентов при оценке соответствия ПО (подробнее см. «Руководство оператора 3.6.10» раздел «Оценка соответствия ПО»);
- Сводка – краткое описание угрозы;
- Описание – подробное описание угрозы;
- Последствия реализованной угрозы – описание последствий, которые могут возникнуть, если угроза была реализована;

- Рекомендации по устранению угрозы – описание действий, которые рекомендуется предпринять для устранения угрозы;
- Рекомендации по уменьшению риска – список основных действий, которые рекомендуется предпринять для предотвращения реализации угрозы;
- Таблица со списком инцидентов, которые были созданы с признаком принадлежности к данному типу инцидента.

Элементы управления боковой панелью описаны в разделе «Боковая панель».

6.2.3 Создание типа инцидента

1. Начните процесс создания типа инцидента через «универсальные таблицы» или инструмент «боковая панель». Откроется форма "Создание типа инцидента" (см. «Рис. 67»).

Рис. 67 – Форма "Создание типа инцидента"

2. Укажите на форме следующую информацию:
   - в поле **Название** укажите название типа инцидента;
   - в поле **Тип уязвимости** из выпадающего списка выберите тип угрозы, к которой будет относится тип инцидента: нарушение политики, сетевая аномалия, уязвимость;
   - при необходимости использовать данный тип инцидентов для создания инцидентов при оценке соответствия ПО включите соответствующий переключатель;

     Примечание: для создания инцидентов при оценке соответствия ПО требуется лишь один тип инцидента с данным признаком.

   - в поле **Сводка** укажите краткое описание угрозы;

- в поле **Описание** укажите подробное описание угрозы;
- в поле **Последствия** укажите описание последствий, которые могут возникнуть, если угроза будет реализована;
- в поле **Рекомендации по устранению угрозы** укажите перечень действий, которые необходимо выполнить для устранения угрозы;
- в поле **Рекомендации по уменьшению риска** укажите перечень действий, которые необходимо предпринять для предотвращения возникновения угрозы;
- в поле **Внутренняя заметка** укажите дополнительные сведения, предназначенные для внутреннего использования;
- в поле **Оценка риска** задайте цифровое обозначение уровня угрозы;
- в поле **Комментарий** укажите дополнительные сведения.

3. Нажмите кнопку **Создать**.

6.2.4 Редактирование типа инцидента

1. Начните процесс редактирования типа инцидента через «универсальные таблицы» или инструмент «боковая панель».
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

6.2.5 Написать ответственному

1. Откройте форму просмотра типа инцидента и нажмите кнопку **Написать ответственному**. Откроется окно "Новое сообщение" (см. «Рис. 68»).

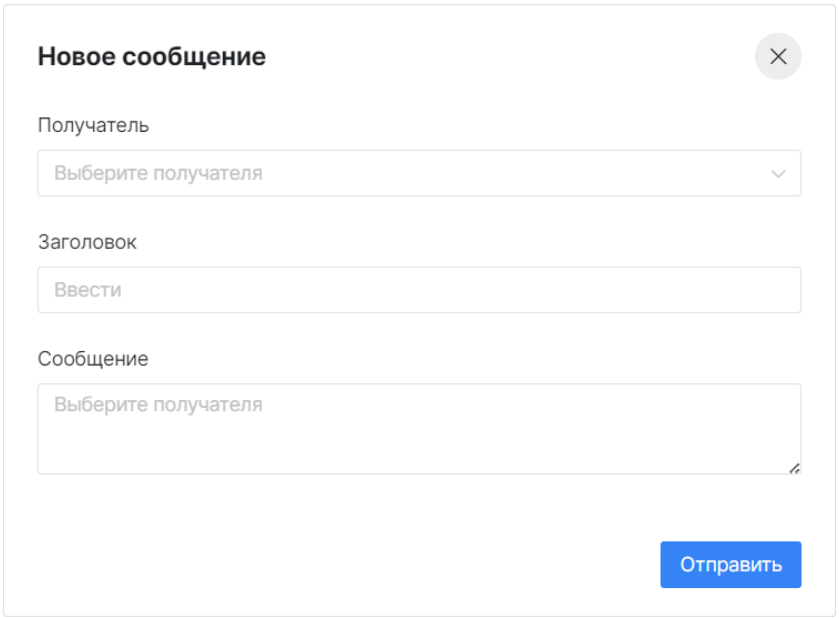


Рис. 68 – Окно "Новое сообщение"

2. Укажите в окне следующую информацию:
   - в поле **Получатель** из выпадающего списка выберите получателя сообщения;

- в поле **Заголовок** укажите тему сообщения;
- в поле **Сообщение** укажите текст сообщения.

3. Нажмите кнопку **Отправить**. Для просмотра списка полученных/отправленных сообщений необходимо перейти в **Профиль пользователя → Сообщения**.
4. К сообщению будет автоматически прикреплена ссылка на соответствующую карточку типа инцидента.

6.2.6 Дублирование типа инцидента

4. Откройте форму просмотра типа инцидента и нажмите кнопку **Дублировать**.
5. В открывшемся окне укажите наименование типа инцидента и нажмите кнопку **Дублировать**.
6. Будет создан новый тип инцидента на основе существующего.

6.2.7 Импорт типов инцидентов

1. Начните процесс импорта типов инцидентов через «универсальные таблицы» или инструмент «боковая панель».
2. В открывшемся окне укажите путь к архиву с данными.
3. Нажмите кнопку **Открыть**.

6.2.8 Экспорт типов инцидентов

1. Начните процесс экспорта типов инцидентов через «универсальные таблицы» или инструмент «боковая панель».
2. Будет сформирован архив с типами инцидентов в формате .zip.
3. Нажмите кнопку **Скачать** и укажите путь для сохранения архива.

6.2.9 Экспорт типов инцидентов в CSV

1. Начните процесс экспорта в CSV типов инцидентов через «универсальные таблицы» или инструмент «боковая панель».
2. В открывшемся окне укажите путь для сохранения файла/файлов в формате .csv.

6.2.10 Удаление типа инцидента

1. Начните процесс удаления типа инцидентов через «универсальные таблицы» или инструмент «боковая панель».
2. Подтвердите удаление в открывшемся окне.
3. Тип инцидента будет удален из платформы.

6.3 Группы инцидентов

Группы инцидентов предназначены для упрощения исследования инцидентов сотрудниками. Схожие инциденты помещают в группы, а их затем назначают пользователям.

Группа инцидентов может быть создана одним из следующих способов:

- вручную, через интерфейс платформы;
- автоматически, с использованием правила корреляции.

Работа с группами инцидентов включает в себя следующие процессы:

1. «Просмотр группы инцидентов».
2. «Создание группы инцидентов».
3. «Редактирование группы инцидентов».
4. «Назначение группы инцидентов пользователю».
5. «Назначение группы инцидентов группе пользователей».
6. «Добавление инцидентов в группу».
7. «Массовое закрытие инцидентов через группу».
8. «Открепление инцидентов от группы».
9. «Удаление группы инцидентов».

Для работы с группами инцидентов перейдите в раздел **Инциденты → Группы инцидентов** (см. «Рис. 69»).

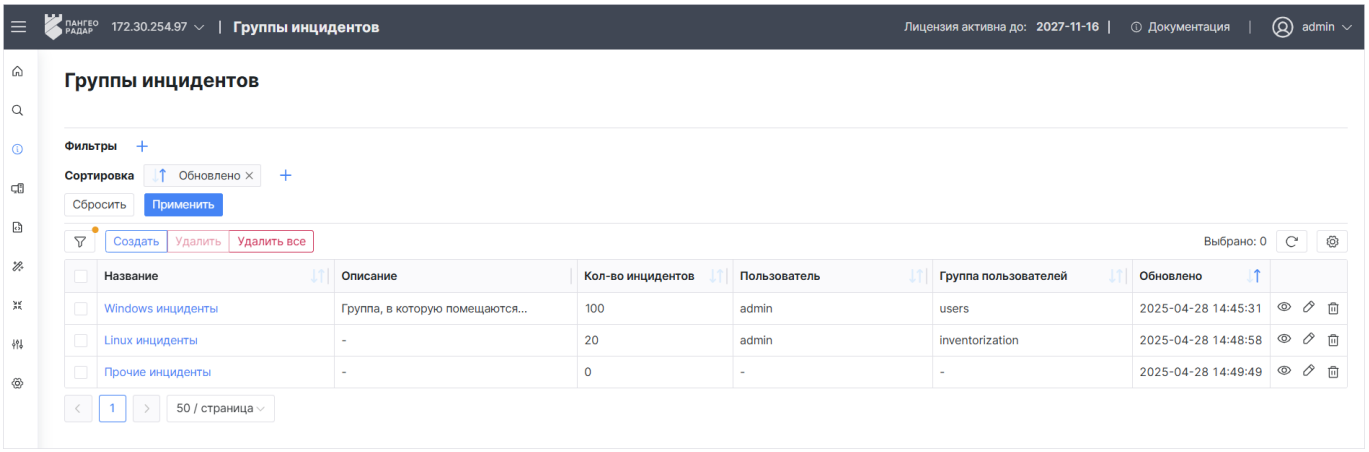


Рис. 69 – Раздел "Группы инцидентов"

В разделе отображается следующая информация:

- **Название** – наименование группы инцидентов;
- **Описание** – описание группы инцидентов;
- **Кол-во инцидентов** – количество инцидентов в группе;
- **Пользователь** – наименование пользователя, которому по умолчанию будут назначаться инциденты, попадающие в данную группу;
- **Группа пользователей** – наименование группы пользователей, которой по умолчанию назначаются инциденты, попадающие в данную группу;
- **Обновлено** – дата и время обновления информации о группе инцидентов.

6.3.1 Просмотр группы инцидентов

Для просмотра группы инцидентов нажмите кнопку в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранной группы инцидентов (см. «Рис. 70»).

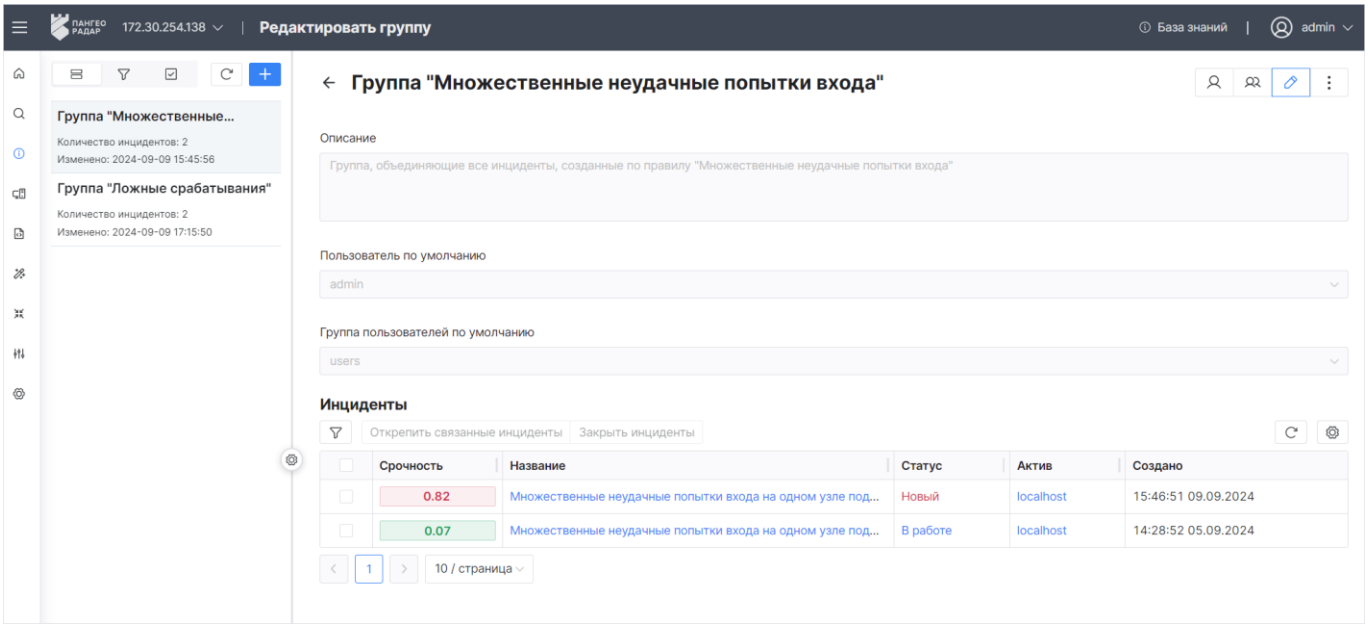


Рис. 70 – Форма просмотра группы инцидентов

В боковой панели отображается следующая информация о группах инцидентов:

- Наименование группы инцидентов;
- Количество инцидентов в группе;
- Дата и время изменения информации о группе.

В рабочей области, помимо информации, отображаемой в боковой панели, отображается следующая информация:

- **Описание** – описание группы инцидентов;
- **Пользователь по умолчанию** – наименование пользователя, которому по умолчанию будут назначаться инциденты, попадающие в данную группу;
- **Группа по умолчанию** – наименование группы пользователей, которой по умолчанию назначаются инциденты, попадающие в данную группу;
- Блок **Инциденты** – содержит таблицу с информацией об инцидентах, входящих в группу:
  - **Срочность** – цветовое и цифровое обозначение срочности инцидента;
  - **Название** – наименование инцидента;
  - **Статус** – состояние инцидента;
  - **Создано** – дата и время создания инцидента;
  - **Уровень риска** – цифровое обозначение уровня угрозы, присвоенного инциденту;
  - **ID** – идентификатор инцидента;
  - **Тип инцидента** – наименование типа инцидента;

- **Группа инцидентов** – наименование группы инцидентов, в которую входит инцидент;
- **Актив** – наименование актива, на котором выявлен инцидент;
- **Последнее происшествие** – дата и время последнего происшествия, зафиксированного по инциденту;
- **Кол-во происшествий** – количество происшествий, зафиксированных в инциденте;
- **Кол-во повторных открытий** – количество повторных открытий инцидента;
- **Пользователь** – наименование пользователя, назначенного на разбор инцидента;
- **Группа пользователей** – наименование группы пользователей, назначенной на разбор инцидента;
- **Обновлено** – дата и время изменения информации об инциденте;
- **Категория** – наименование категории, к которой относится инцидент: нарушение политики, сетевая аномалия, уязвимость;
- **Эксплуатируется удаленно** – признак, возможна ли удаленная эксплуатация уязвимости: да, нет;
- **Результат анализа** – результат анализа инцидента.

6.3.2 Создание группы инцидентов

1. Начните процесс создания группы инцидентов через «универсальные таблицы» или инструмент «боковая панель». Откроется форма "Создать группу инцидентов" (см. «Рис. 71»).

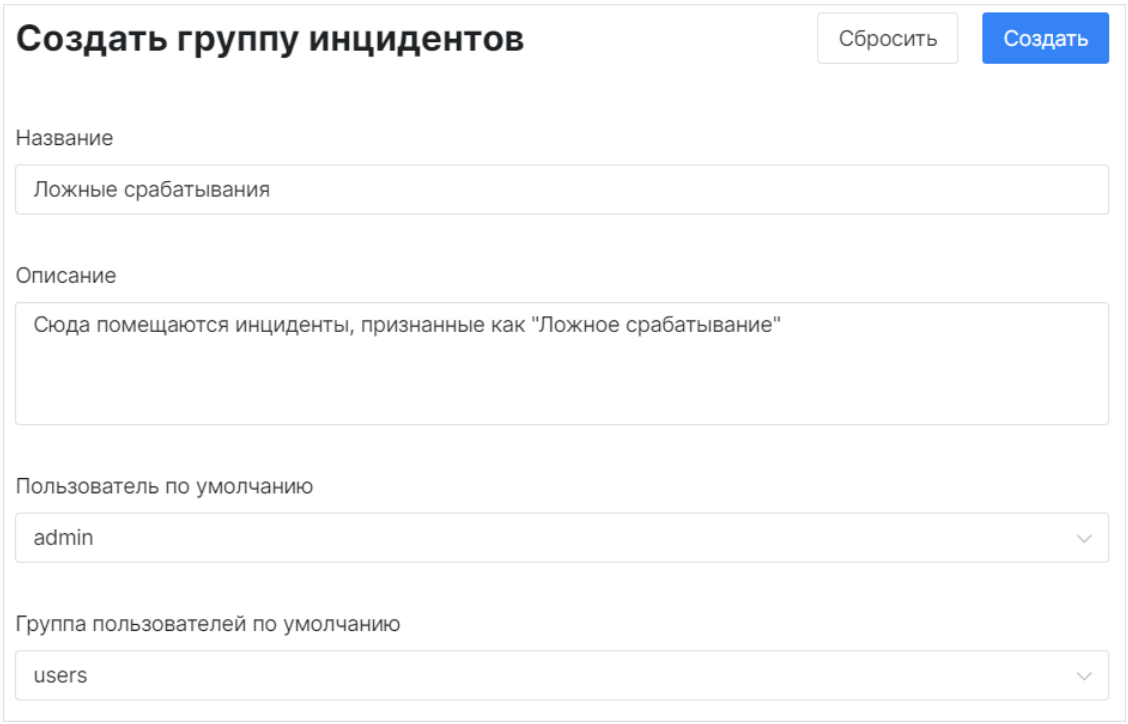


Рис. 71 – Форма "Создать группу инцидентов"

2. Укажите на форме следующую информацию:

- в поле **Название** укажите название группы;
- в поле **Описание** укажите описание группы;
- в поле **Пользователь по умолчанию** выберите пользователя, которому по умолчанию будут назначаться все инциденты из группы;
- в поле **Группа пользователей** по умолчанию выберите группу пользователей, которым по умолчанию будут назначаться все инциденты из группы.

3. Нажмите кнопку **Создать**.

6.3.3 Редактирование группы инцидентов

1. Начните процесс редактирования группы инцидентов через «универсальные таблицы» или инструмент «боковая панель».
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

6.3.4 Назначение группы инцидентов пользователю

1. Откройте форму просмотра группы инцидентов и нажмите кнопку  . Откроется окно "Назначение группы инцидентов".
2. В открывшемся окне из выпадающего списка выберите пользователя, которому необходимо назначить группу и нажмите кнопку **Применить**.

6.3.5 Назначение группы инцидентов группе пользователей

1. Откройте форму просмотра группы инцидентов и нажмите кнопку  . Откроется окно "Назначение группы инцидентов".
2. В открывшемся окне из выпадающего списка выберите группу пользователей, которому необходимо назначить группу и нажмите кнопку **Применить**.

6.3.6 Добавление инцидентов в группу

Добавление инцидентов в группу может быть выполнено следующими способами:

- автоматически, по результатам "сработки" правил корреляции;
- вручную с формы создания/редактирования инцидента (см. раздел «Создание инцидента»).

6.3.7 Массовое закрытие инцидентов через группу

1. Откройте форму просмотра группы инцидентов.
2. В блоке **Инциденты** отметьте необходимые инциденты установив соответствующие флаги.
3. Нажмите кнопку **Закрыть инциденты** и подтвердите действие в открывшемся окне. Выбранные инциденты будут переведены в статус "Закрыт".

6.3.8 Открепление инцидентов от группы

1. Откройте форму просмотра группы инцидентов.

2. В блоке **Инциденты** отметьте необходимые инциденты установив соответствующие флаги.
3. Нажмите кнопку **Открепить связанные инциденты** и подтвердите действие в открывшемся окне. Выбранные инциденты больше не будут входить в данную группу.

6.3.9 Удаление группы инцидентов

1. Начните процесс удаления группы инцидентов через «универсальные таблицы» или инструмент «боковая панель».
2. Подтвердите удаление в открывшемся окне.
3. Группа инцидентов будет удалена из платформы.

6.4 Происшествия на отправку

Внимание! Включение процесса отправки происшествий выполняется в старом интерфейсе. Начиная с версии 4.0.0 старый интерфейс более недоступен, а данная возможность находится на доработке. Вы можете выполнить данную операцию с инстанса, на котором установлена более ранняя версия.

6.5 Дополнительные поля

Платформа позволяет добавлять к инцидентам дополнительные поля, которые можно использовать для более полного описания инцидента.

Дополнительные поля могут быть созданы одним из следующих способов:

- вручную, через интерфейс платформы;
- автоматически, с использованием правила корреляции.

Работа с дополнительными полями включает в себя следующие процессы:

1. Создание дополнительного поля.
2. Редактирование информации о дополнительном поле.
3. Добавление дополнительного поля к инциденту.
4. Просмотр информации о дополнительном поле.
5. Удаление дополнительного поля.

Для работы с дополнительными полями перейдите в раздел **Инциденты → Дополнительные поля** (см. «Рис. 72»).

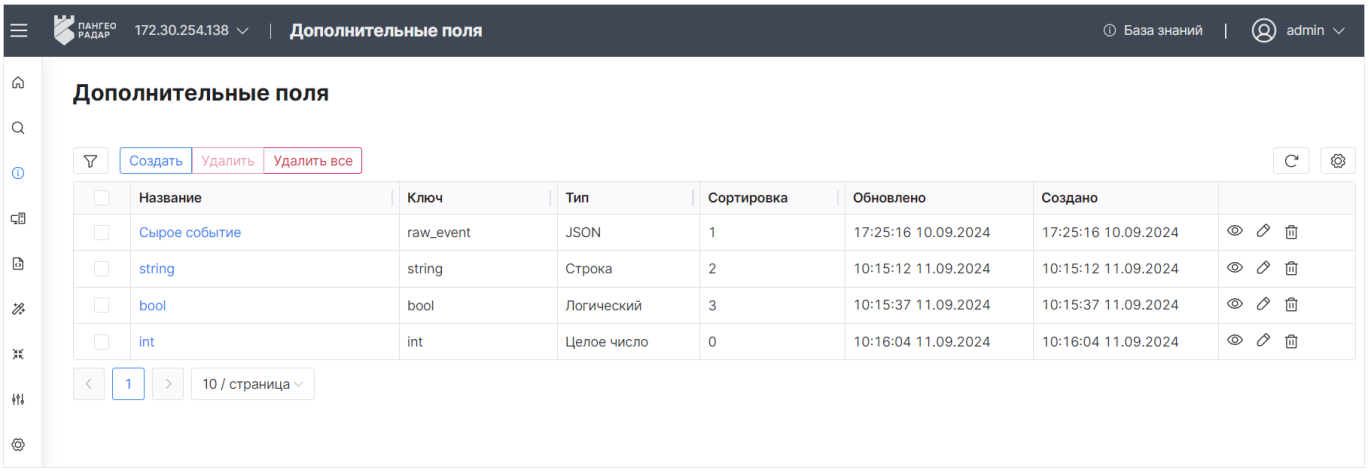


Рис. 72 – Раздел "Дополнительные поля"

В разделе отображается следующая информация:

- Название дополнительного поля. По ссылке произойдет переход на страницу просмотра дополнительного поля;
- Ключ – уникальный ключ, идентифицирующий поле;
- Тип – тип данных, указываемый в дополнительном поле:
  - логический;
  - JSON;
  - строка;
  - целое число;
  - действительное число;
  - дата.
- Сортировка – порядок отображения дополнительных полей в карточке инцидента;
- Обновлено – дата и время изменения информации о дополнительном поле;
- Создано – дата и время создания дополнительного поля.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	**Действие**
	редактирование информации о дополнительном поле
	просмотр дополнительного поля
	удаление записи из таблицы

6.5.1 Создание дополнительного поля

1. Нажмите на кнопку **Создать**. Откроется форма "Создание дополнительного поля" (см. «Рис. 73»).

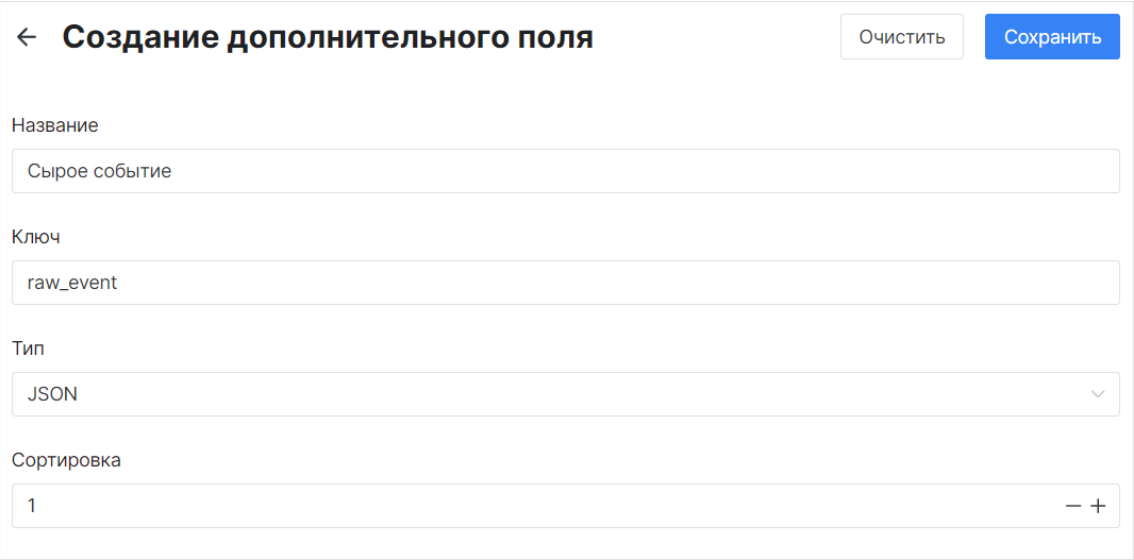


Рис. 73 – Форма "Создание дополнительного поля"

2. Укажите на форме следующую информацию:
    - в поле **Название** укажите название дополнительного поля. Допускается указывать любое название поля на русском или английском языке;
    - в поле **Ключ** укажите уникальный ключ поля. Допускается указывать ключ только на английском языке. Указанный ключ должен быть уникальным в рамках платформы;
    - в поле **Тип** из выпадающего списка выберите тип данных, который будет указываться в поле;
    - в поле **Сортировка** выберите порядок отображения дополнительного поля в карточке инцидента.
3. Нажмите кнопку **Сохранить**.

6.5.2 Редактирование дополнительного поля

1. Выберите из списка необходимое дополнительное поле и нажмите кнопку .
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

6.5.3 Добавление дополнительного поля в инцидент

1. Перейдите в раздел **Инциденты → Инциденты**, выберите инцидент из списка и откройте его на просмотр.
2. Нажмите кнопку **Редактировать**. В блоке **Дополнительные поля** будет отображаться список доступных дополнительных полей.
3. Выберите дополнительное поле для добавления в инцидент и укажите в нем необходимую информацию.
4. Сохраните внесенные изменения.

6.5.4 Просмотр значений дополнительного поля

Открыть на просмотр дополнительное поле можно двумя способами:

- по ссылке по названию поля;
- по кнопке .

Откроется страница "Дополнительное поле <Наименование поля>" (см. «Рис. 74»).

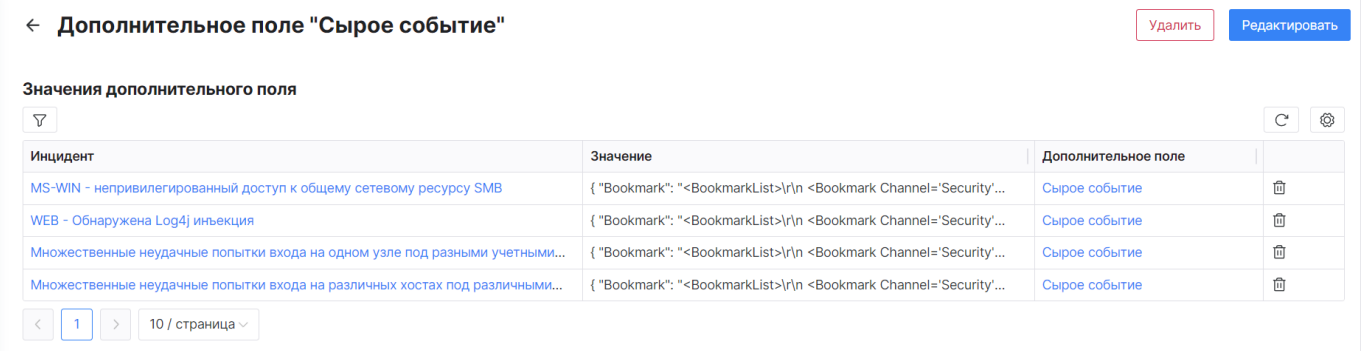


Рис. 74 – Страница просмотра дополнительного поля"

На странице отображается следующая информация:

- **Инцидент** – наименование инцидента, в котором добавлено дополнительное поле. По ссылке произойдет переход на форму просмотра инцидента;
- **Значение** – информация, указанная в дополнительном поле;
- Наименование дополнительного поля.

При необходимости вы можете удалить значение дополнительного поля из выбранного инцидента. Для этого нажмите кнопку в соответствующей строке.

6.5.5 Удаление дополнительного поля

Для удаления дополнительного поля нажмите кнопку в соответствующей строке.

Для удаление всех записей нажмите кнопку **Удалить все**.

Для удаления конкретных записей таблицы установите нужные флаги и нажмите кнопку **Удалить**.

7. Активы

7.1 Активы

7.1.1 Общие данные

Актив: любое техническое средство информационной системы (устройство, подключенное к вычислительной сети, в том числе: сервер, рабочая станция, коммутационное устройство и т.п.), имеющее ценность для предприятия и подлежащее защите от киберугроз.

При отправке и получении данных активы генерируют траффик, который обрабатывается в платформе и на его основе в событиях информационной безопасности регистрируется информация о том, откуда исходит трафик и куда он направляется, например исходные и целевые IP-адреса, FQDN и прочая информация.

Тип сетевой видимости актива может принимать следующие значения:

- 1 – актив напрямую подключен к сети Интернет;
- 2 – актив располагается в демилитаризованной зоне (DMZ);
- 3 – актив подключен к сети Интернет через Proxy-сервер;
- 4 – актив имеет ограниченный доступ к сети Интернет и к ограниченному набору онлайн-сервисов. Например, тонкие клиенты, POS-терминалы, удаленные офисы;
- 5 – актив не подключен к сети.

Сведения об активах в платформу могут быть добавлены следующими способами:

- при обнаружении/создании инцидента;
- по результатам работы сканера уязвимостей;
- по результатам работы сетевого сканера;
- добавлены вручную.

В случае, если у активов используются не статичные IP-адреса, то можно выполнить дополнительную настройку стратегии идентификации активов (подробнее см. раздел «Настройки идентификации активов»)

Уровень влияния актива на выполнение бизнес-процессов компании называется **Значимость**. В платформе значимость актива может принимать следующие значения:

- 1 – ключевой. Данный актив обеспечивает функционирование бизнеса;
- 2 – важный. Данный актив обеспечивает штатную работу компании;
- 3 – некритичный. Данный актив не влияет на штатную работу компании;
- 4 – распределенный. Данный актив находится в составе распределенной системы, которая не задействована в бизнес-процессах;
- 5 – тестовый. Данный актив располагается в тестовой среде. Недоступность данного актива не влияет ни на бизнес-процессы, ни на штатную работу компании.

Активы можно объединить в группы, а затем их назначить ответственным. Это упрощает расследование связанных с активом инцидентов и позволяет выполнять проверку соответствия ПО для группы активов (подробнее см. раздел «Группы активов»).

Для подключения к сети и обмена данным используются сетевые интерфейсы, информация о которых и связанными с ними активами также содержится в платформе (подробнее см. раздел «Сетевые интерфейсы»).

Работа с активами включает в себя следующие процессы:

1. «Просмотр и анализ актива».
2. «Создание актива».
3. «Редактирование актива».
4. «Добавление актива в группу».
5. «Написать ответственному».
6. «Удаление актива».

Для работы с активами перейдите в раздел **Активы → Активы** (см. «Рис. 75»).

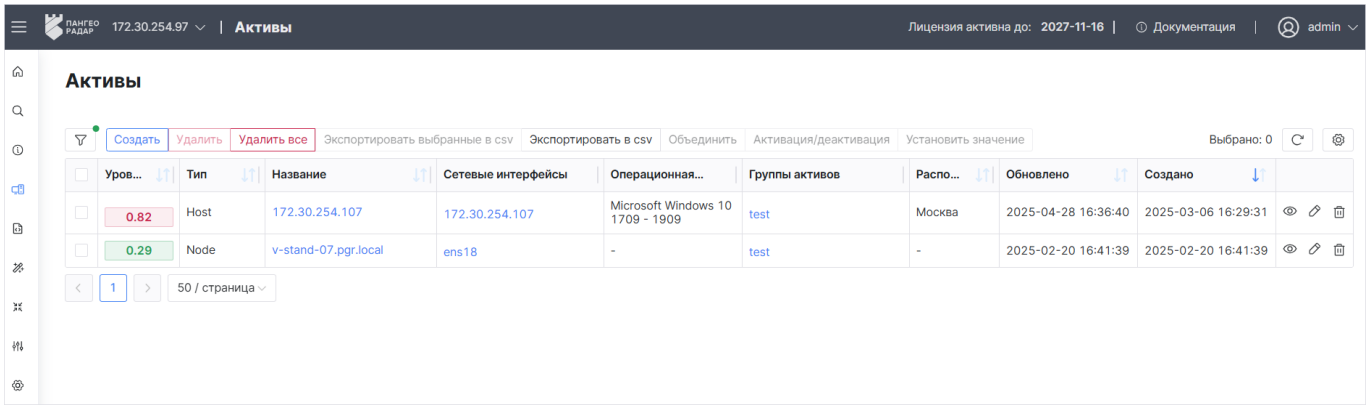


Рис. 75 – Раздел "Активы"

В разделе отображается следующая информация:

- **Уровень риска** – цветовое и цифровое обозначение уровня риска актива;
- **Тип** – типа актива: Host, Node;
- **Название** – наименование актива;
- **Сетевые интерфейсы** – наименование сетевого интерфейса актива;
- **Операционная система** – наименование операционной системы, установленной на активе;
- **Группы активов** – наименование групп активов, в которых состоит актив;
- **Расположение** – геоданные актива;
- **Открытые инциденты** – количество открытых инцидентов на активе
- **Риск принят** – признак, принят ли потенциальный риск дальнейшей эксплуатации актива в текущем состоянии: да, нет;
- **Закрытые инциденты** – количество закрытых инцидентов на активе;

- **Обновлено** – дата и время изменения информации об активе;
- **Создано** – дата и время создания записи об активе в платформе;
- **Значимость актива** – уровень влияния актива на выполнение бизнес-процессов компании;
- **Сетевая видимость** – тип сетевой видимости актива;
- **Группа ответственных** – наименование группы пользователей, которым автоматически назначаются инциденты, выявленные на активе;
- **IP/MAC** – IP и MAC-адрес актива.

7.1.2 Просмотр и анализ актива

Для просмотра актива нажмите кнопку в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного актива (см. «Рис. 76»).

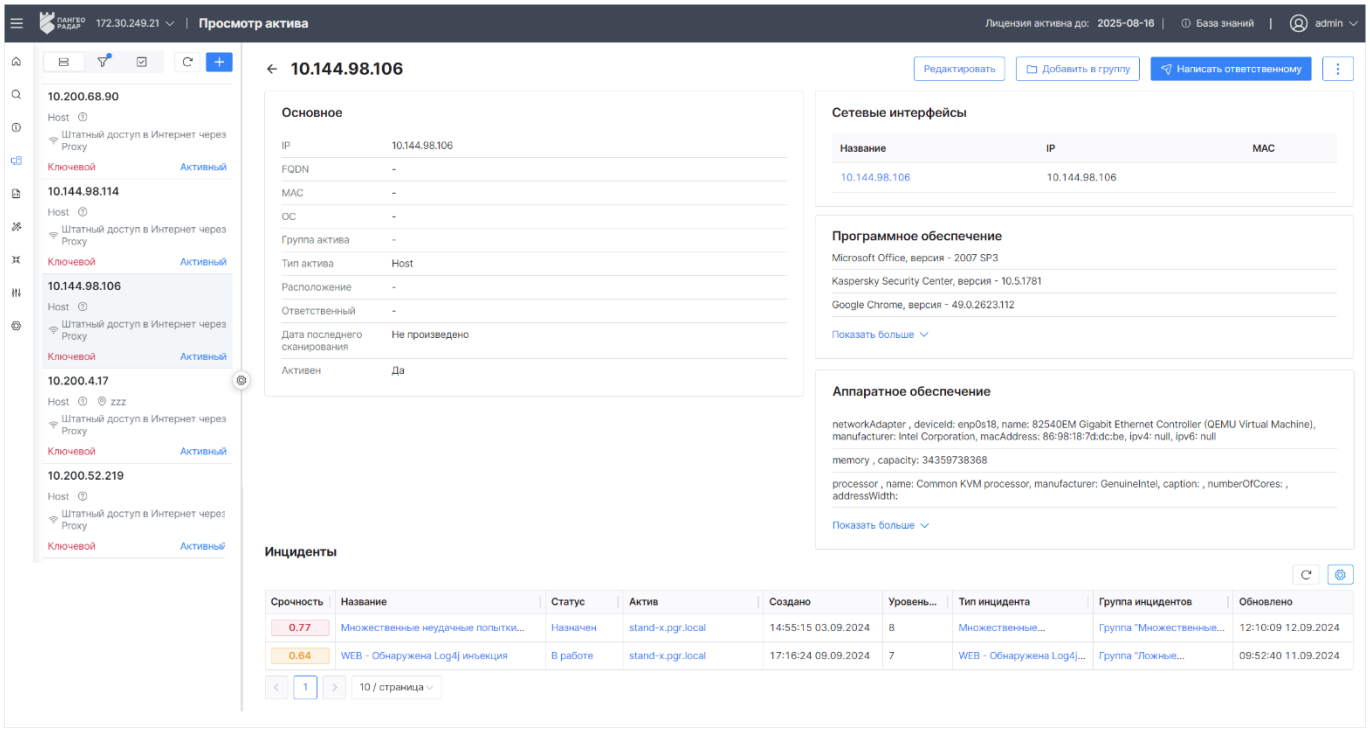


Рис. 76 – Форма просмотра актива

В боковой панели отображается следующая информация об активах:

- Наименование актива;
- Тип актива;
- Расположение актива;
- Сетевая видимость актива;
- Значимость актива;
- Состояние актива.

В рабочей области отображается следующая информация об активах:

- В блоке **Основное** отображается основная информация об активе:

    - IP;
    - FQDN;
    - MAC;
    - ОС;
    - Группа актива;
    - Тип актива;
    - Расположение;
    - Ответственный;
    - Дата последнего сканирования;
    - Состояние актива;
- В блоке **Сетевые интерфейсы** отображается информация о сетевых интерфейсах, входящих в актив:
    - Название;
    - IP;
    - MAC.
- В блоке **Программное обеспечение** отображается информация о списке ПО, установленном на активе;
- В блоке **Аппаратное обеспечение** отображается список аппаратного обеспечения актива;
- В блоке **Инциденты** отображается информация об инцидентах, выявленных на активе (подробнее см. раздел «Инциденты»).

7.1.3 Создание актива

1. Начните процесс создания актива через «универсальные таблицы» или инструмент «боковая панель». Откроется форма "Создание актива" (см. «Рис. 77»).

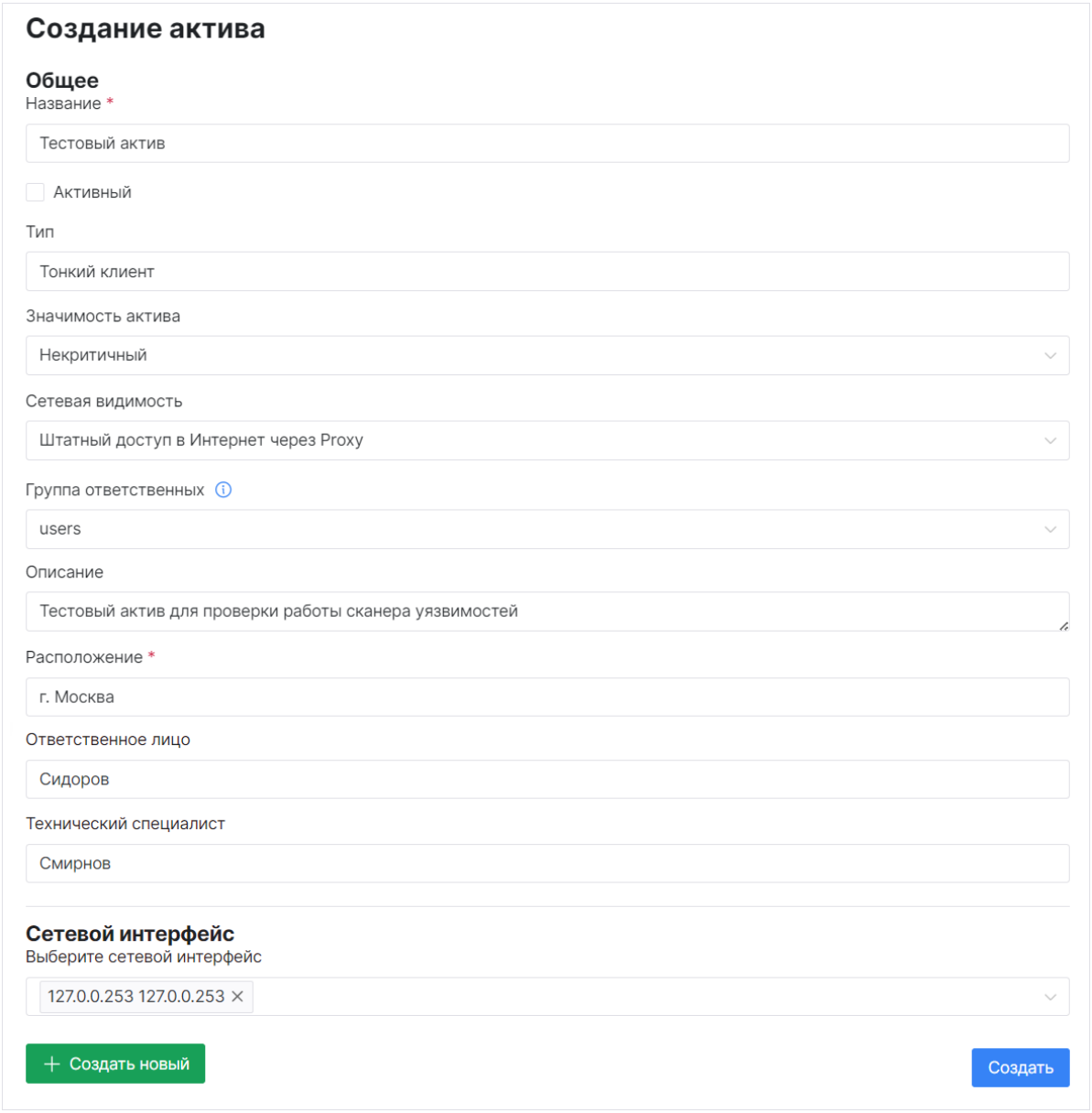


Рис. 77 – Форма "Создание актива"

2. Выполните на форме следующие действия:
   - в поле **Название** укажите наименование актива;
   - установите флаг **Активный**, если данный актив задействован в корпоративной сети;
   - в поле **Тип** укажите тип актива;
   - в поле **Значимость** актива из выпадающего списка выберите значимость актива;
   - в поле **Сетевая видимость** из выпадающего списка выберите сетевую видимость актива;
   - в поле **Группа ответственных** выберите группу пользователей, которой будут автоматически назначаться инциденты, выявленные на активе;
   - в поле **Описание** укажите описание актива;
   - в поле **Расположение** укажите расположение актива;
   - в поле **Ответственное лицо** укажите информацию о владельце актива;

- в поле **Технический специалист** укажите соответствующую информацию;
- в поле **Сетевой интерфейс** из выпадающего списка выберите сетевые интерфейсы, которые входят в состав актива. Если необходимого сетевого интерфейса нет в списке, то вы можете создать его вручную. Для этого нажмите кнопку **Создать новый** и укажите необходимую информацию (подробнее см. раздел «Сетевые интерфейсы»);

3. Нажмите кнопку **Создать**.

7.1.4 Редактирование актива

1. Начните процесс редактирования актива через «универсальные таблицы» или инструмент «боковая панель».
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

7.1.5 Добавление актива в группу

1. Откройте форму просмотра актива и нажмите кнопку **Добавить в группу**.
2. В открывшемся окне из выпадающего списка выберите группу активов (подробнее см. раздел «Группы активов»), в которую необходимо добавить актив.
3. Нажмите кнопку **Сохранить**.

7.1.6 Написать ответственному

1. Откройте форму просмотра актива и нажмите кнопку **Написать ответственному**. Откроется окно "Новое сообщение" (см. «Рис. 78»).

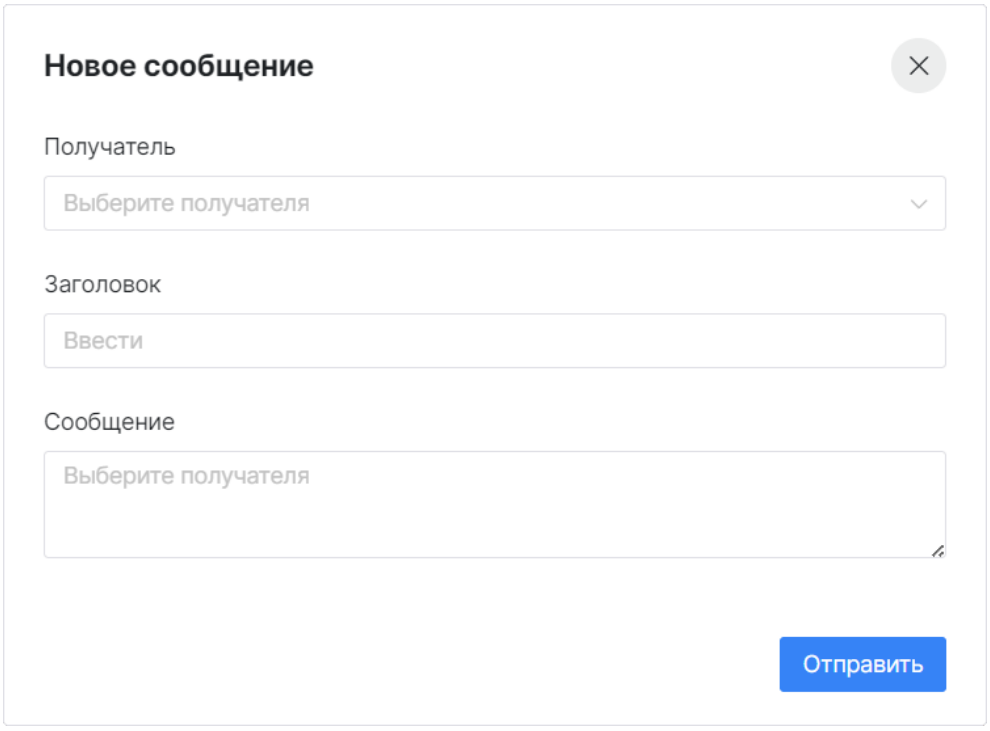


Рис. 78 – Окно "Новое сообщение"

2. Укажите в окне следующую информацию:

- в поле **Получатель** из выпадающего списка выберите получателя сообщения;
- в поле **Заголовок** укажите тему сообщения;
- в поле **Сообщение** укажите текст сообщения.

3. Нажмите кнопку **Отправить**. Для просмотра списка полученных/отправленных сообщений необходимо перейти в **Профиль пользователя → Сообщения**.
4. К сообщению будет автоматически прикреплена ссылка на соответствующую карточку актива.

7.1.7 Удаление актива

1. Начните процесс удаления актива через «универсальные таблицы» или инструмент «боковая панель».
2. Подтвердите удаление в открывшемся окне.
3. Актив будет удален из платформы.

7.2 Группы активов

Для упрощения управления активами их можно поместить в группы.

Работа с группами активов включает в себя следующие процессы:

1. «Создание группы активов».
2. «Просмотр группы активов».
3. «Редактирование группы активов».
4. «Настройка автоматического добавления актива в группу».
5. «Написать ответственному».
6. «Удаление группы активов».

Для работы с группами активов перейдите в раздел **Активы → Группы активов** (см. «Рис. 79»).

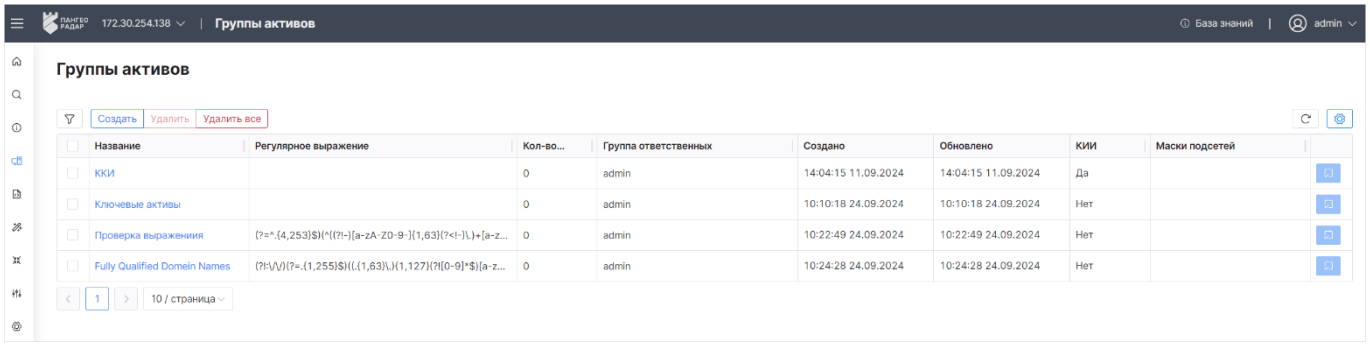


Рис. 79 – Раздел "Группы активов"

В разделе отображается следующая информация о группах активов:

- **Название** – наименование группы активов. По ссылке произойдет переход на форму просмотра группы активов;

- **Регулярное выражение** – стратегия автоматического добавления активов в группу по заданному регулярному выражению, применяемому к FQDN активов. Новые активы, чье FQDN отвечает заданному регулярному выражению, будут автоматически включаться в группу;
- **Кол-во** – количество активов в группе;
- **Группа ответственных** – группа пользователей, назначенная ответственными за данную группу активов;
- **Создано** – дата и время создания группы активов;
- **Обновлено** – дата и время последнего обновления группы активов;
- **Связанные группы пользователей** – группы пользователей, связанные с конкретными активами из данной группы;
- **КИИ** – признак того, относится ля группа активов к критической информационной инфраструктуре;
- **Маска подсетей** – стратегия автоматического добавления активов в группу по заданной маске подсети. Новые активы, попадающие под указанную сетевую маску, будут автоматически включаться в группу.
- Кнопка **Запуск проверки соответствия ПО** (подробнее см. раздел «Результаты соответствия ПО»).

7.2.1 Создание группы активов

1. Нажмите кнопку **Создать**. Откроется форма "Создание группы активов" (см. «Рис. 80»).

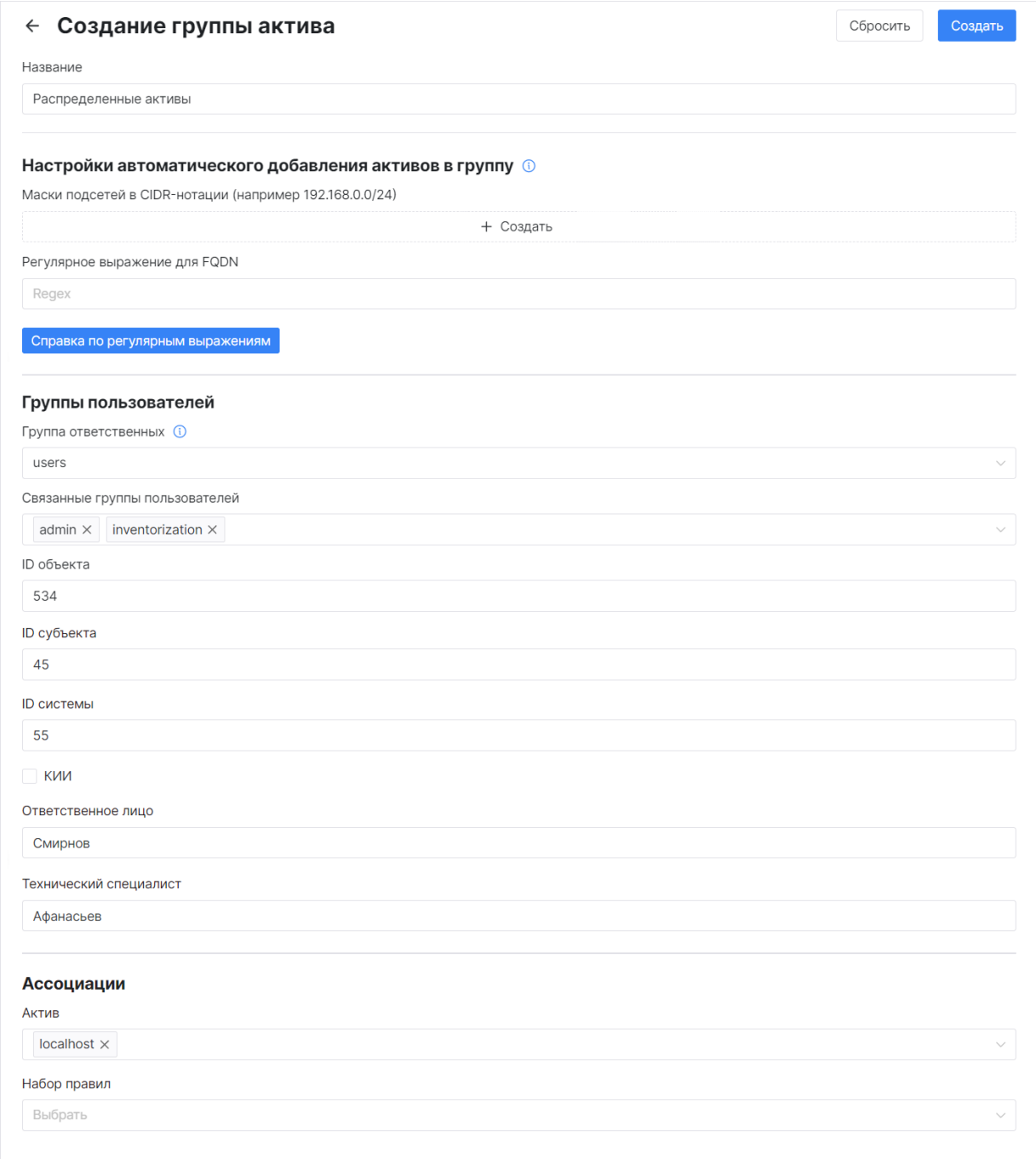


Рис. 80 –Форма "Создание группы активов"

2. Укажите на форме следующую информацию:
    - в поле **Название** укажите наименование группы активов;
    - в блоке **Настройки автоматического добавления активов в группу** настройте стратегию автоматического добавления активов в группу (см. раздел «Настройка автоматического добавления актива в группу»);
    - в блоке **Группы пользователей** укажите следующую информацию:
        - в поле **Группа ответственных** выберите группу, которой автоматически будут назначаться инциденты, выявленные на активах, входящих в данную группу активов;

- в поле **Связанные группы пользователей** укажите связанные группы пользователей;
- в случае, если группа активов относится к критической информационной инфраструктуре, то в полях **ID объекта**, **ID субъекта**, **ID системы** укажите соответствующие идентификаторы, которые указаны в протоколе интеграции с системой "ГосСОПКА", и установите флаг **КИИ**;
- в полях **Ответственное лицо** и **Технический специалист** укажите соответствующую информацию.

- в блоке **Ассоциации** укажите следующую информацию:
  - в поле **Актив** выберите активы, которые следует включить в группу, если необходимые активы уже добавлены в платформу;
  - в поле **Набор правил** выберите правила, по которым активы должны проверяться на соответствие ПО (см. раздел «Создание правила соответствия ПО»).

3. Нажмите кнопку **Создать**.

7.2.2 Просмотр группы активов

Для просмотра и анализа группы активов нажмите по ссылке с наименованием инцидента. Откроется форма просмотра группы активов (см. «Рис. 81»).

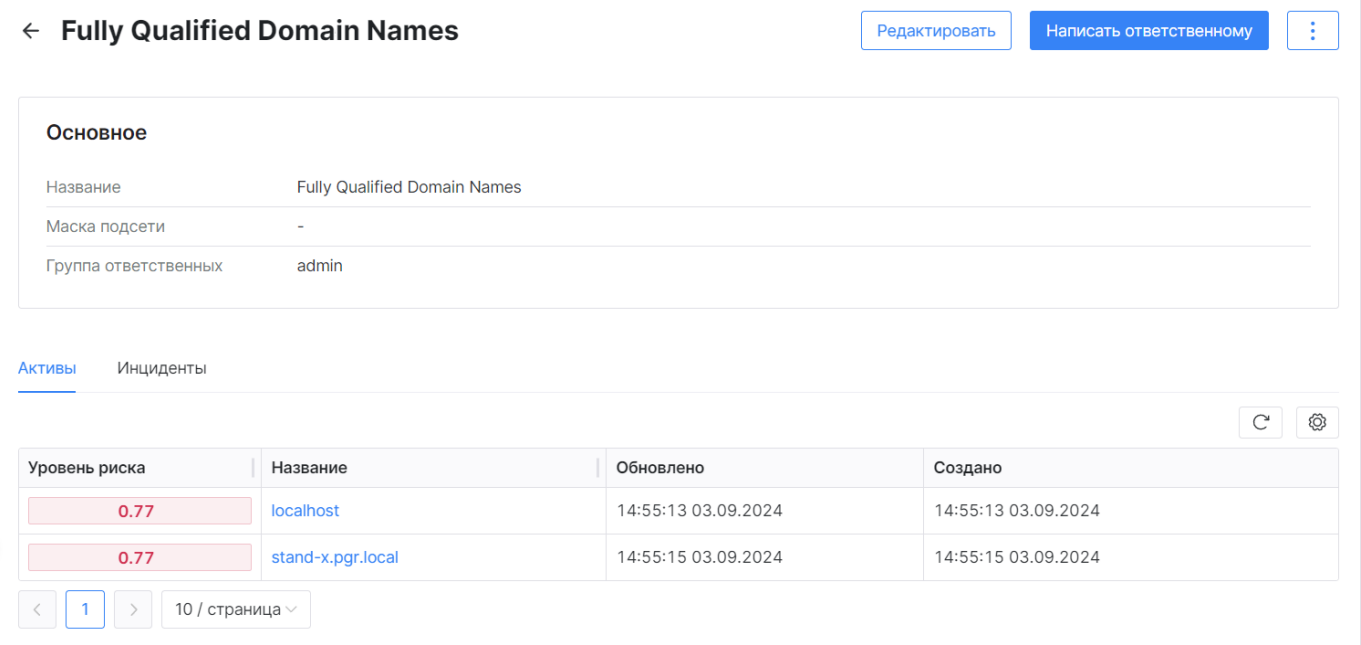


Рис. 81 – Форма просмотра группы активов

На форме просмотра группы отображается следующая информация:

- Основная информация группе: название, маска подсети, группа ответственных;
- Информация об активах, входящих в группу: уровень риска, название актива, дата и время обновления и создания актива;
- Информация об инцидентах, выявленных на активах (см. «Рис. 82»).

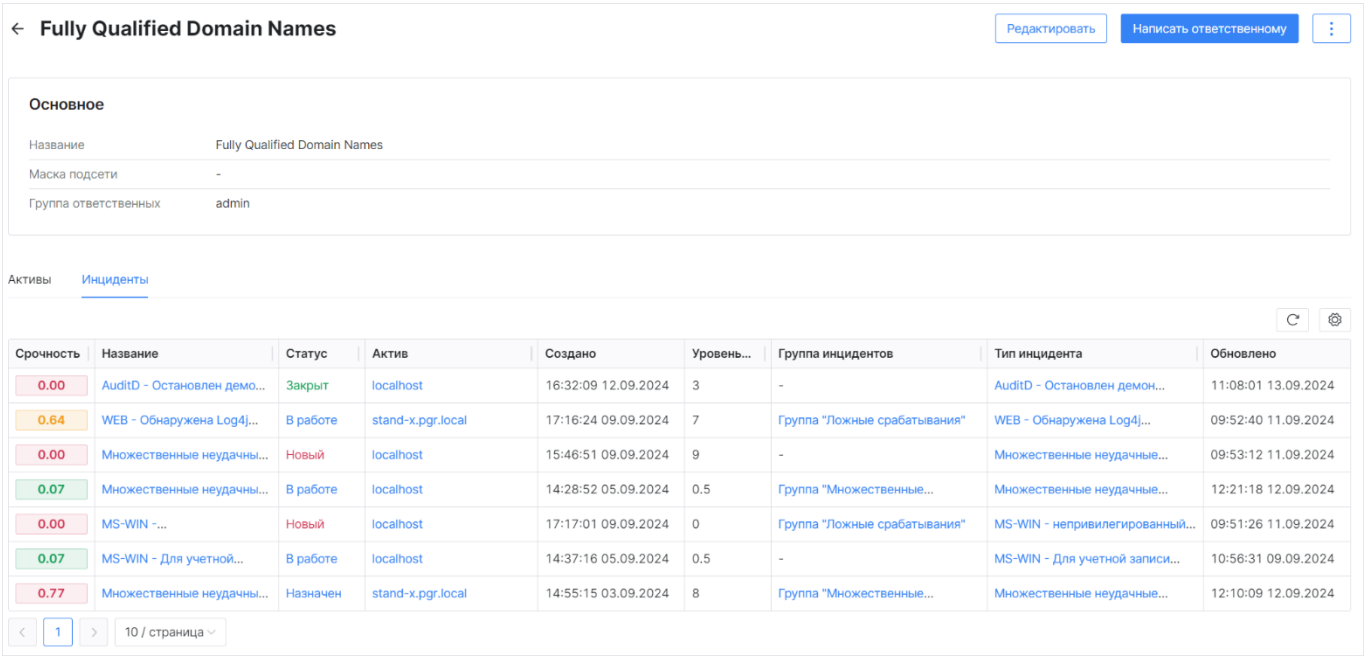


Рис. 82 – Форма просмотра группы активов. Таблица инциденты

7.2.3 Редактирование группы активов

1. Перейдите на форму просмотра необходимой группы активов и нажмите кнопку **Редактировать**.
2. Внесите необходимые изменения.
3. Сохраните изменения.

7.2.4 Настройка автоматического добавления актива в группу

Настройка стратегии автоматического добавления актива в группу выполняется на форме создания/редактирования группы активов в блоке **Настройки автоматического добавления активов в группу** (см. «Рис. 83»).

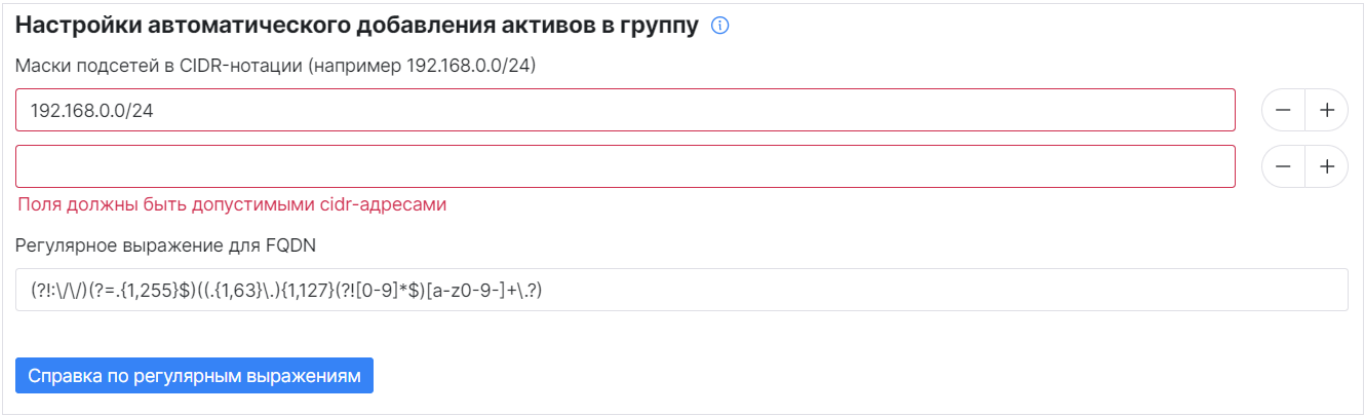


Рис. 83 – Форма создания/редактирования группы активов. Настройка автоматического добавления активов в группу

Стратегию можно настроить двумя способами:

- по маске подсети;
- по регулярному выражению для FQDN.

Выполните следующие действия:

1. В поле **Маски подсетей в CIDR-нотации** укажите маску подсети.
2. Используйте кнопки "+" и "–" для добавления/удаления масок подсетей.
3. В поле **Регулярное выражение для FQDN** укажите регулярное выражение.

7.2.5 Написать ответственному

1. Перейдите на форму просмотра группы активов и нажмите кнопку **Написать ответственному**. Откроется окно "Новое сообщение" (см. «Рис. 84»).

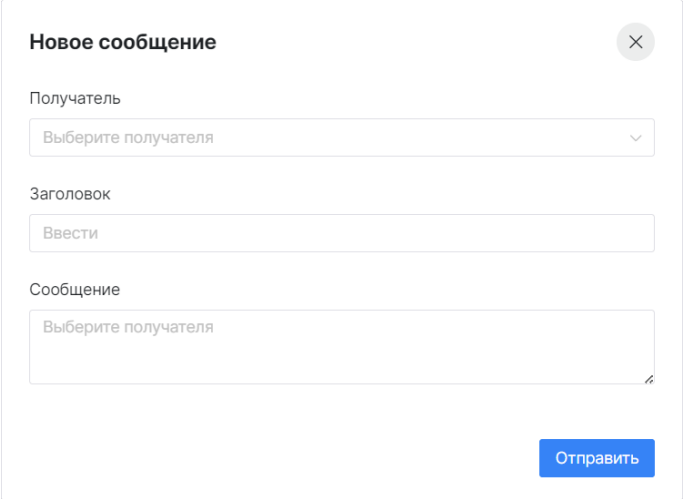


Рис. 84 – Окно "Новое сообщение"

2. Укажите в окне следующую информацию:
   - в поле **Получатель** из выпадающего списка выберите получателя сообщения;
   - в поле **Заголовок** укажите тему сообщения;
   - в поле **Сообщение** укажите текст сообщения.
3. Нажмите кнопку **Отправить**. Для просмотра списка полученных/отправленных сообщений необходимо перейти в **Профиль пользователя → Сообщения**.
4. К сообщению будет автоматически прикреплена ссылка на соответствующую карточку группы активов.

7.2.6 Удаление группы активов

Удаление группы активов можно выполнить следующими способами:

- из раздела **Активы → Группы активов**;
- из формы просмотра группы активов.

Способ 1:

1. Перейдите в раздел **Активы → Группы активов**.
2. Отметьте необходимые группы активов.
3. Нажмите кнопку **Удалить**.
4. Подтвердите удаление в открывшемся окне.
5. Для удаление всех групп активов нажмите кнопку **Удалите все**.

Способ 2:

1. Перейдите на форму просмотра группы активов, нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Удалить**.
2. Подтвердите удаление в открывшемся окне.

7.3 Настройки идентификации активов

Идентификация активов — это сравнение отдельных атрибутов актива (его идентификаторов) с атрибутами существующих активов, о которых есть записи в платформе. По итогам сравнения либо создается запись о новом активе, либо обновляются записи о существующих активах.

Стратегию сравнения можно настроить по следующим идентификаторам:

- **FQDN** – по полному доменному имени актива;
- **MAC** – по Mac-адресу актива;
- **IP** – по IP-адресу актива.

Работа со стратегиями идентификации активов включает в себя следующие процессы:

1. «Создание стратегии идентификации активов».
2. «Редактирование стратегии идентификации активов».
3. «Удаление стратегии идентификации активов».

Для работы со стратегиями идентификации активов перейдите в раздел **Активы → Настройки идентификации активов** (см. «Рис. 85»).

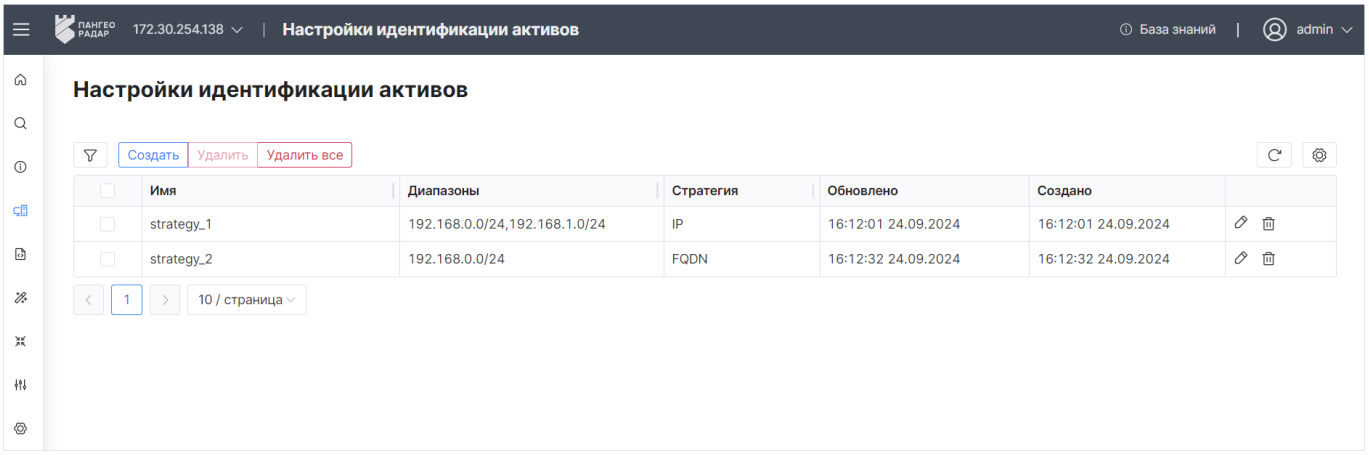


Рис. 85 – Раздел "Настройки идентификации активов"

В разделе отображается следующая информация о стратегиях идентификации активов:

- **Имя** – наименование стратегии идентификации активов;
- **Диапазоны** – диапазоны масок подсетей в CIDR-нотации;
- **Стратегия** – идентификатор актива, по которому выполняется сравнение активов: FQDN, MAC, IP;
- **Обновлено** – дата и время обновление стратегии;
- **Создано** – дата и время создания стратегии.

7.3.1 Создание стратегии идентификации активов

1. Нажмите кнопку **Создать**. Откроется форма "Создание настройки идентификации активов" (см. «Рис. 86»).

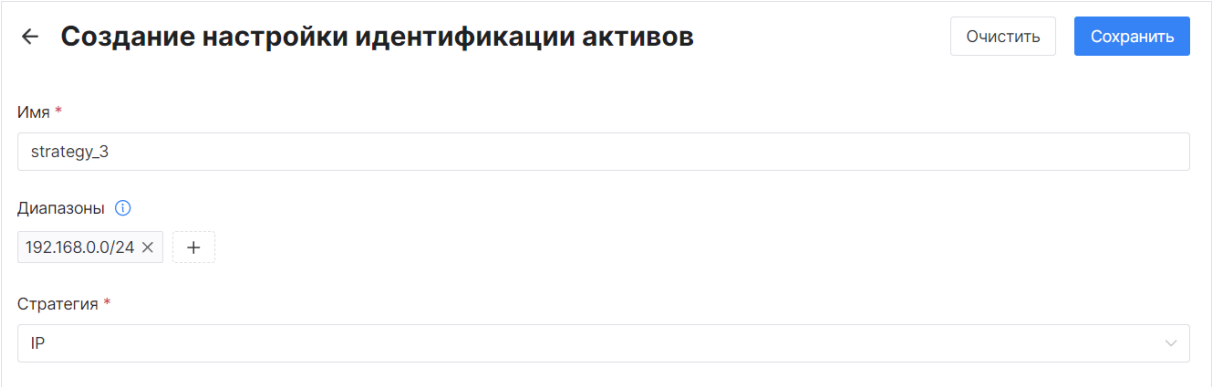


Рис. 86 – Окно "Создание настройки идентификации активов"

2. Укажите на форме следующую информацию:
   - в поле **Имя** укажите уникальное наименование стратегии;
   - в поле **Диапазон** укажите диапазоны масок подсетей в CIDR-нотации;
   - в поле **Стратегия** из выпадающего списка выберите идентификатор, по которому будет выполняться сравнение атрибутов активов.
3. Нажмите кнопку **Сохранить**.

7.3.2 Редактирование стратегии идентификации активов

1. Выберите стратегию и нажмите кнопку .
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

7.3.3 Удаление стратегии идентификации активов

Удаление стратегии идентификации активов выполняется из раздела **Активы → Настройки идентификации активов**.

Для удаления стратегии, выберите необходимую запись в таблице и нажмите кнопку

Для удаления нескольких стратегий установите нужные флаги и нажмите кнопку **Удалить**.

Для удаление всех записей таблицы нажмите кнопку **Удалить все**.

7.4 Сетевые интерфейсы

Платформа Радар собирает и хранит сведения о сетевых интерфейсах, обнаруженных у активов.

Работа с сетевыми интерфейсами автоматизирована и вносить изменения вручную может потребоваться в следующих случаях:

- если от сканера уязвимостей поступили неточные данные о сетевых интерфейсах;

- изменилась сетевая конфигурация в ходе эксплуатации актива. Если заранее известно в каком сетевом диапазоне динамичные адреса, то для диапазона можно настроить стратегию идентификации активов (см. «Настройки идентификации активов»).

Работа с сетевыми интерфейсами включает в себя следующие процессы:

1. «Просмотр сетевого интерфейса».
2. «Создание сетевого интерфейса».
3. «Редактирование сетевого интерфейса».
4. «Удаление сетевого интерфейса».

Для работы с сетевыми интерфейсами перейдите в раздел **Активы → Сетевые интерфейсы** (см. «Рис. 87»).

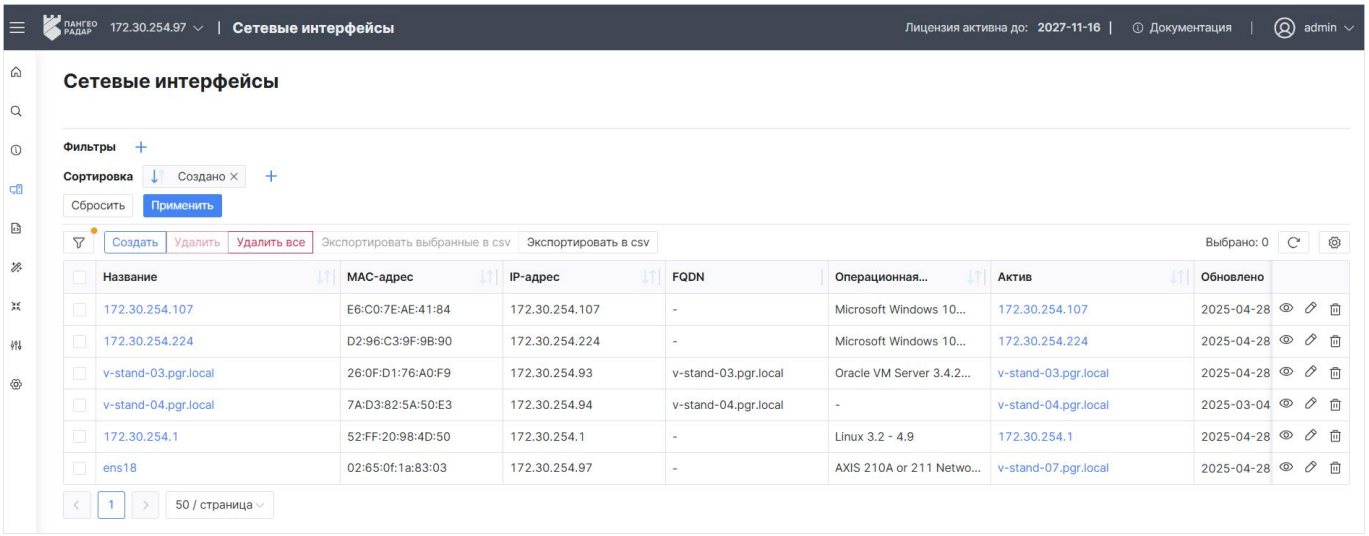


Рис. 87 – Раздел "Сетевые интерфейсы"

В разделе отображается следующая информация:

- **Название** – наименование сетевого интерфейса;
- **MAC-адрес** – MAC-адрес сетевого интерфейса;
- **IP-адрес** – IP-адрес сетевого интерфейса;
- **FQDN** – FQDN актива, на котором установлен сетевой интерфейс;
- **Операционная система** – наименование операционной системы, на которой работает актив;
- **Актив** – наименование актива, на котором установлен сетевой интерфейс;
- **Обновлено** – дата и время обновления информации о сетевом интерфейсе;
- **Создано** – дата и время создания записи о сетевом интерфейсе в платформе.

7.4.1 Просмотр сетевого интерфейса

Для просмотра сетевого интерфейса нажмите кнопку в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного сетевого интерфейса (см. «Рис. 88»).

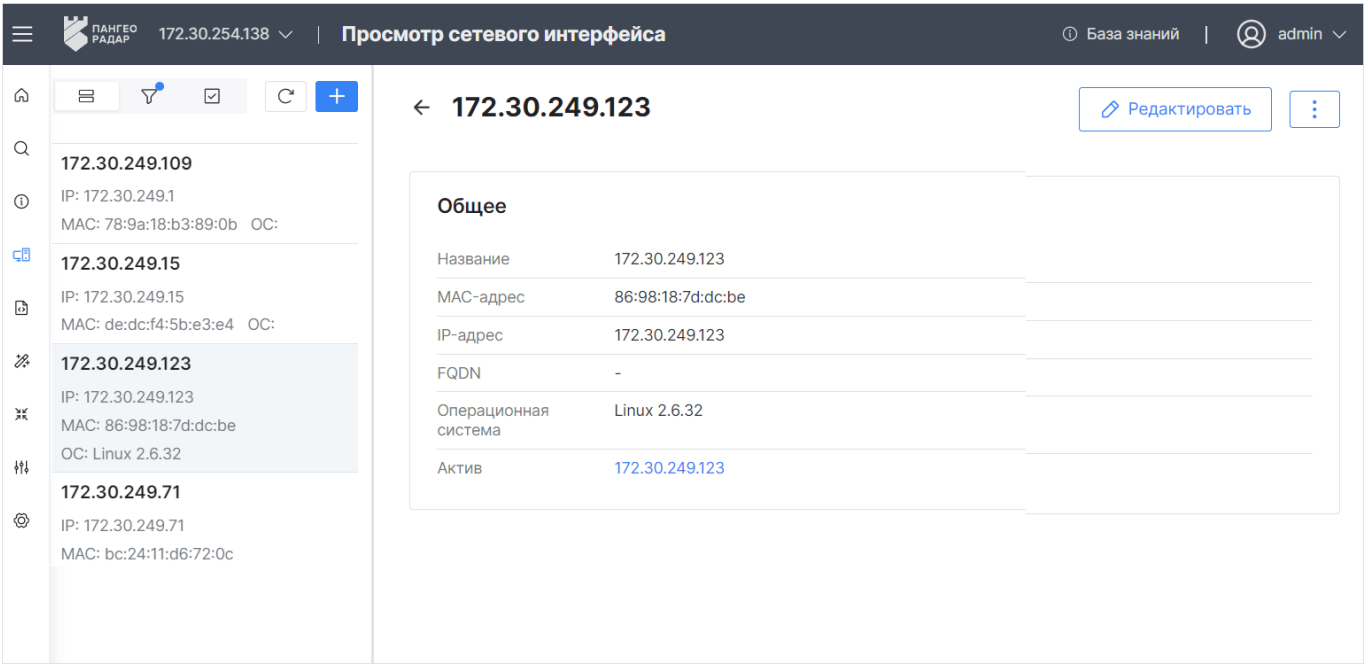


Рис. 88 – Форма просмотра сетевого интерфейса

В боковой панели отображается следующая информация:

- Наименование сетевого интерфейса;
- IP-адрес сетевого интерфейса;
- MAC-адрес сетевого интерфейса;
- Наименование операционной системы.

На форме просмотра отображается следующая информация:

- **Название**;
- **MAC-адрес**;
- **IP-адрес**;
- **FQDN**;
- **Операционная система**;
- **Актив**.

7.4.2 Создание сетевого интерфейса

1. Начните процесс создания сетевого интерфейса через «универсальные таблицы» или инструмент «боковая панель». Откроется форма "Создание сетевого интерфейса" (см. «Рис. 89»).

Рис. 89 – Создание сетевого интерфейса

2. Укажите на форме следующую информацию:
    - в поле **Название** укажите наименование сетевого интерфейса;
    - в поле **MAC-адрес** укажите Mac-адрес сетевого интерфейса;
    - в поле **IP-адрес** укажите IP-адрес сетевого интерфейса;
    - в поле **FQDN** укажите полное доменное имя сетевого интерфейса;
    - в поле **Операционная система** укажите ОС актива, на котором обнаружен сетевой интерфейс;
    - в поле **Активы** из выпадающего списка выберите актив, на котором обнаружен сетевой интерфейс.
3. Нажмите кнопку **Создать**.

7.4.3 Редактирование сетевого интерфейса

1. Начните процесс редактирования сетевого интерфейса через «универсальные таблицы» или инструмент «боковая панель».
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

7.4.4 Удаление сетевого интерфейса

3. Начните процесс удаления сетевого интерфейса через «универсальные таблицы» или инструмент «боковая панель».
4. Подтвердите удаление в открывшемся окне.
5. Сетевой интерфейс будет удален из платформы.

7.5 Результаты сканирования

Под результатами сканирования понимаются данные по наличию уязвимостей, полученные сторонними сканерами уязвимости в ходе работы и импортированные в платформу.

Платформа Радар поддерживает импорт данных сканирования от следующих систем:

- REDCHECK;
- MaxPatrol;
- Nessus;
- OpenVAS.

Работа с результатами сканирования включает в себя следующие процессы:

1. «Импорт результатов сканирования».
2. «Просмотр списка результатов сканирования».
3. «Просмотр результата сканирования».
4. «Сравнение результатов сканирования».
5. «Изменение статуса результата сканирования».

7.5.1 Импорт результатов сканирования

1. Перейдите в раздел **Активы → Результаты сканирования** и нажмите кнопку **Создать**. Откроется форма "Результаты сканирования" (см. «Рис. 90»).

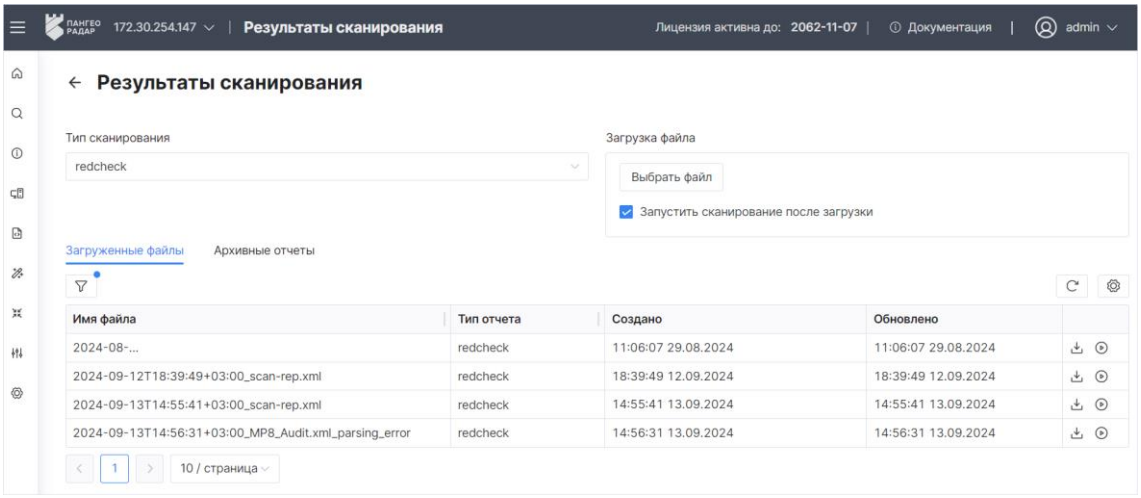


Рис. 90 – Форма импорта результатов сканирования

2. Выполните на форме следующие действия:
   - в поле **Тип** сканирования из выпадающего списка выберите тип сканирования;
   - в поле **Загрузка файла** нажмите на кнопку **Выбрать файл** и в открывшемся окне укажите путь к файлу;
   - если необходимо запустить сканирование после загрузки файла, то установите соответствующий флаг.

3. Информация о загруженных файлах будет отображена на вкладке "Загруженные файлы", информация об обработанных результатах сканирования отображается на вкладке "Архивные отчеты".

4. Для импорта загруженного результата сканирования нажмите кнопку в соответствующей строке.

5. Для скачивания загруженного результата сканирования нажмите кнопку .

7.5.2 Просмотр списка результатов сканирования

Для просмотра списка результатов сканирования перейдите в раздел **Активы → Результаты сканирования** (см. «Рис. 91»).

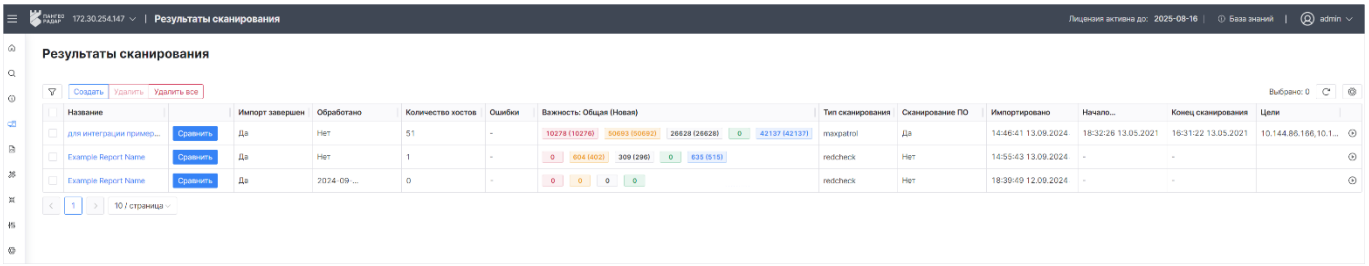


Рис. 91 – Раздел "Результаты сканирования"

В разделе отображается следующая информация о результатах сканирования:

- **Название** – наименование импортированного результата сканирования. По нажатию на ссылку произойдет переход к форме просмотра результата сканирования;
- **Импорт завершен** – состояние успешности завершения импорта результата сканирования: да, нет;
- **Обработано** – состояние обработки результата сканирования;
- **Количество хостов** – количество хостов, обнаруженных в результате сканирования;
- **Ошибки** – наличие ошибок в результатах сканирования;
- **Важность** – отображаются количественные результаты найденных уязвимостей, разделенные на группы важности по цвету согласно оценке CVSS;
- **Тип сканирования** – наименование сканнера уязвимости, который предоставил результаты сканирования;
- **Сканирование ПО** – флаг выполнения сканирования программного обеспечения в результатах сканирования: да, нет;
- **Импортировано** – дата и время импорта результатов сканирования в платформу;
- **Начало сканирования** – дата и время начала сканирования;
- **Конец сканирования** – дата и время окончания сканирования;
- **Цели** – активы (IP-адреса), указанные в задаче сканирования. По наведению мыши на поле, в pop-up окне будет выведен полный список целей сканирования.

В разделе доступны следующие элементы управления:

Кнопка	Действие
Сравнить	сравнение результатов сканирования с существующими данными
	отметить результат сканирования как обработанный или необработанный

7.5.3 Просмотр результата сканирования

Для просмотра и анализа результата сканирования нажмите по ссылке с наименованием результата. Откроется форма просмотра результатов сканирования (см. «Рис. 92»).

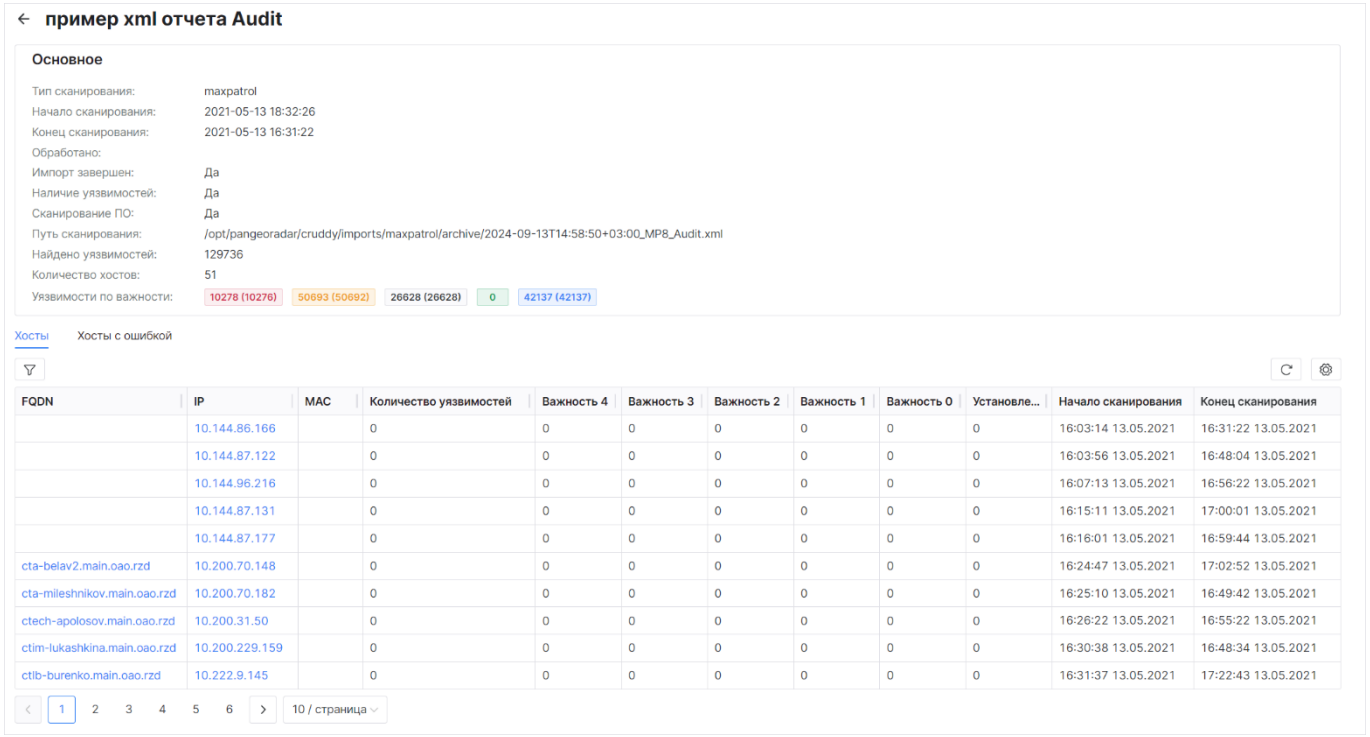


Рис. 92 – Форма просмотра результата сканирования

На форме просмотра результата сканирования информация сгруппирована по следующим блокам:

- Блок **Основное** – основная информация о результате сканирования;
- Таблица **Хосты/Хосты с ошибкой** – информация о просканированных хостах.

7.5.3.1 Основная информация о результате сканирования

Пример блока **Основное** приведен на «Рис. 93».

Рис. 93 – Форма просмотра результата сканирования. Блок "Основное"

В блоке отображается следующая информация:

- **Тип сканирования** – наименование сканнера уязвимости, который предоставил результаты сканирования;
- **Начало сканирования** – дата и время начала сканирования;
- **Конец сканирования** – дата и время окончания сканирования;
- **Обработано** – обработан ли результат сканирования оператором: Да, Нет;
- **Импорт завершен** – завершен ли импорт результатов сканирования: Да, Нет;
- **Наличие уязвимостей** – обнаружены ли уязвимости в ходе обработки результатов сканирования: Да, Нет;
- **Сканирование ПО** – выполнялось ли сканирование ПО: Да, Нет;
- **Путь сканирования** – путь к файлу с результатами сканирования;
- **Найдено уязвимостей** – общее количество найденных уязвимостей;
- **Количество хостов** – количество просканированных хостов;
- **Уязвимости по важности** – количественные результаты найденных уязвимостей, разделенные на группы важности по цвету согласно оценке CVSS.

7.5.3.2 Информация о просканированных хостах

Информация о хостах отображается на следующих вкладках:

- "Хосты";
- "Хосты с ошибкой".

Пример таблицы приведен на «Рис. 94».

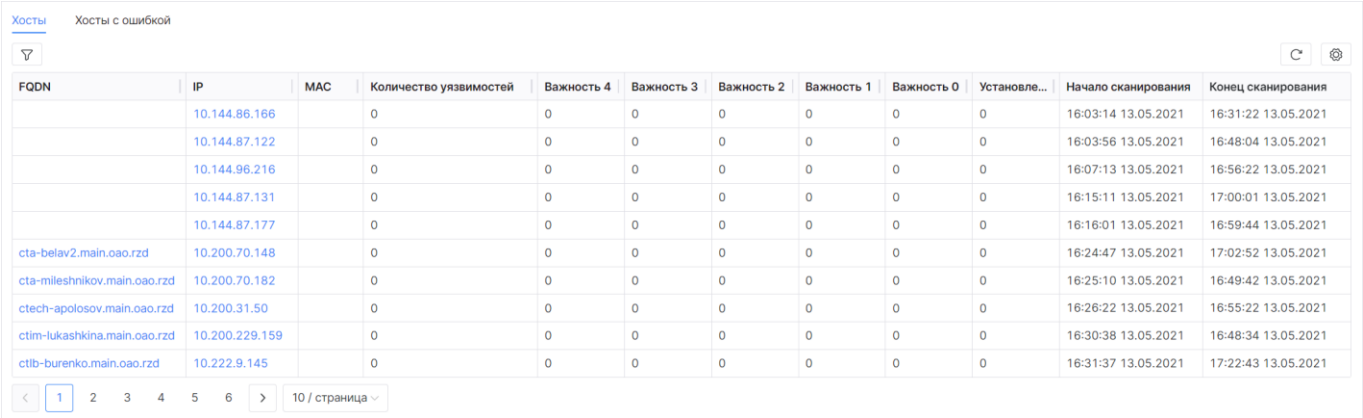


Рис. 94 – Форма просмотра результата сканирования. Блок "Хосты"

В блоке отображается следующая информация:

- **FQDN** – FQDN хоста;
- **IP** – IP-адрес хоста;
- **MAC** – MAC-адрес хоста;
- **Количество уязвимостей** – количество уязвимостей, выявленных на хосте;
- **Важность** – отображаются количественные результаты найденных уязвимостей, разделенные на группы важности от 0 до 4;
- **Установленное ПО** – количество обнаруженного ПО на хосте;
- **Начало сканирования** – дата и время начала сканирования;
- **Конец сканирования** – дата и время окончания сканирования;
- **Ошибка сканирования** – информация об ошибках (только для вкладки "Хосты с ошибкой").

7.5.4 Сравнение результатов сканирования

Для сравнения результатов сканирования с существующими данными перейдите в раздел **Активы → Результаты сканирования** и нажмите кнопку **Сравнить** в строке нужного результата сканирования.

Откроется форма сравнения результатов сканирования. Информация на форме разделена на три вкладки:

- "Новое" – на вкладке отображаются новые уязвимости и предоставляется возможность на их основе создать инциденты;
- "Закрываемые" – на вкладке отображаются уже обнаруженные уязвимости и предоставляется возможность закрыть соответствующие инциденты.;
- "Обработано" – перечень обработанных уязвимостей.

Пример внешнего вида формы сравнения результатов сканирования приведен на «Рис. 95».

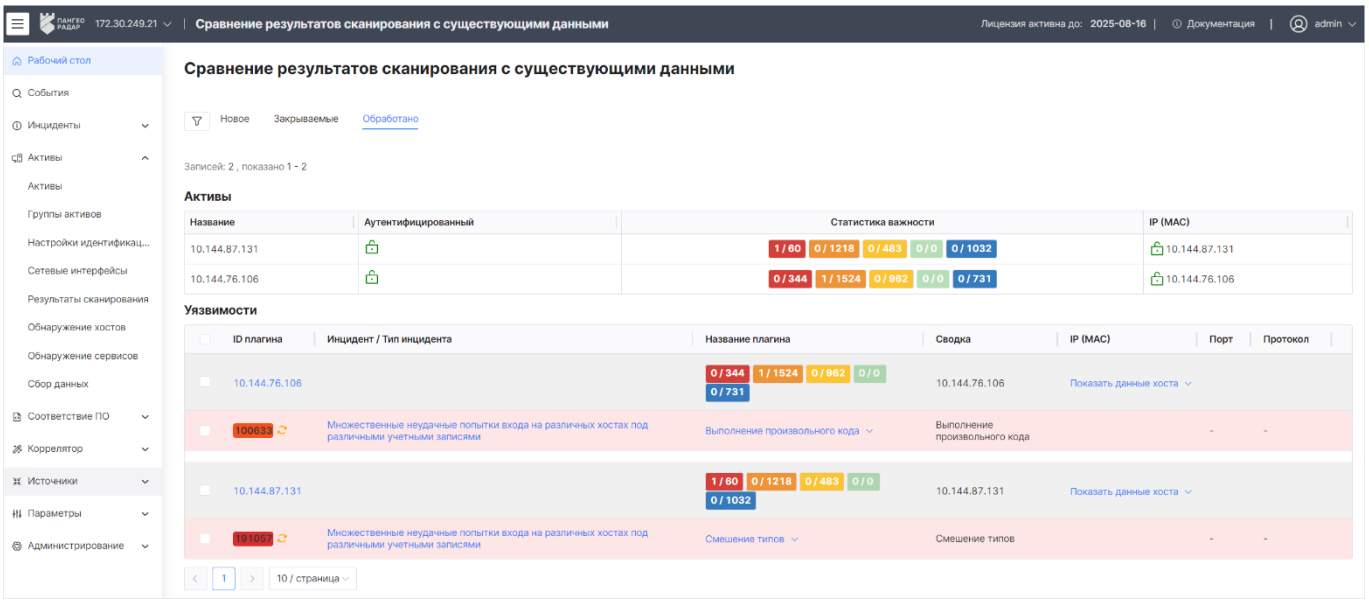


Рис. 95 – Форма сравнения результатов сканирования с существующими данными

Информация на форме разделена по двум таблицам: **Активы** и **Уязвимости**

В таблице **Активы** отображается следующая информация:

- **Название** – наименование актива;
- **Аутентифицированный** – аутентифицированный ли актив в платформе: да (зеленый замок), нет (красный замок);
- **Статистика важности** – количественные результаты найденных уязвимостей, разделенные на группы важности по цвету согласно оценке CVSS;
- **IP (MAC)** – IP или MAC-адрес актива.

В таблице **Уязвимости** информация об уязвимости сгруппирована в две строки:

- **Первая строка**. Отображается детальная информация об активе и статистике важности обнаруженных уязвимостей. Существует возможность показать подробные данные хоста при клике на соответствующую ссылку. Пример приведен на «Рис. 96».

Рис. 96 – Таблица "Уязвимости". Строка с информацией об активе

- **Вторая строка**. Отображается следующая информация:
  - **ID плагина** – ID плагина, который обнаружил уязвимость;
  - **Наименование инцидента/типа инцидента** – если по уязвимости уже существует инцидент, то отображается соответствующая информация;
  - **Название плагина** – наименование плагина, выявившего уязвимость. По ссылке откроется детальная информация о плагине;
  - **Сводка** – сводная информация об уязвимости.

Пример приведен на «Рис. 97».

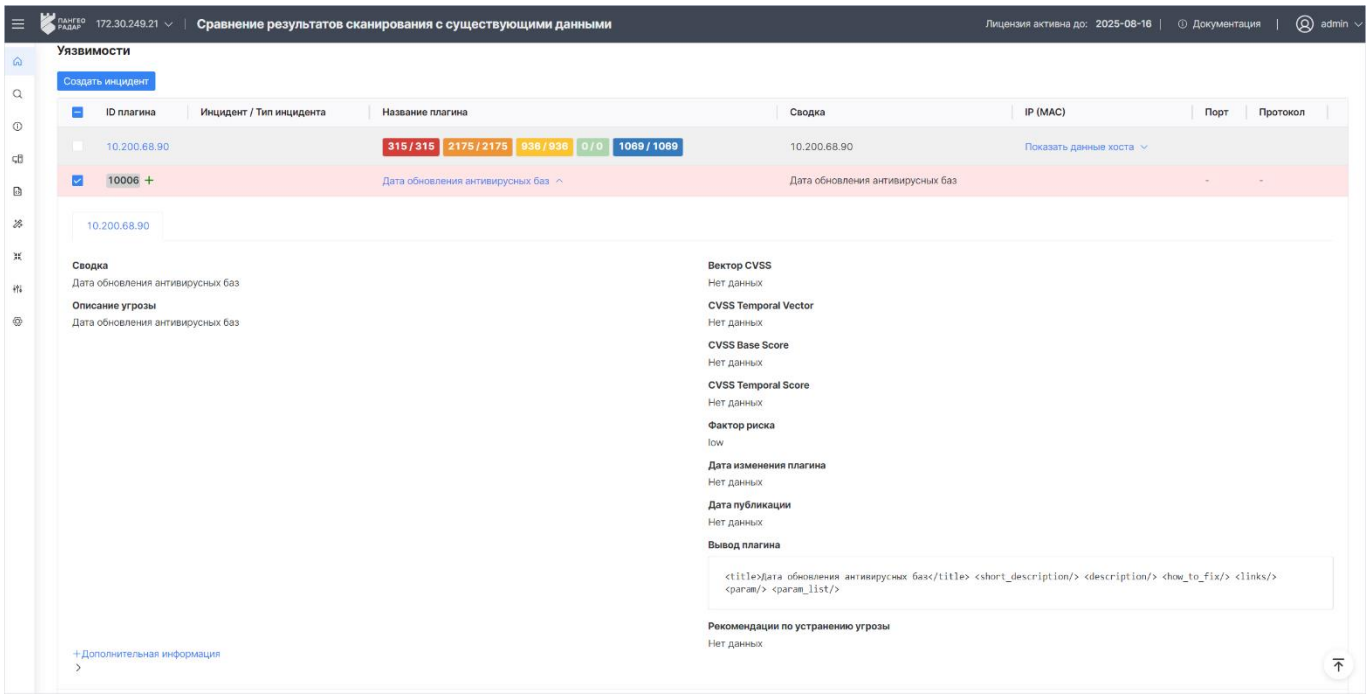


Рис. 97 – Таблица "Уязвимости". Строка с информацией о уязвимости

По результатам сравнения результатов сканирования с существующими данными доступны следующие действия:

1. «Создание инцидентов по результатам сравнения».
2. «Закрытие инцидентов по результатам сравнения».

7.5.4.1 Создание инцидентов по результатам сравнения

1. Откройте результаты сравнения и перейдите на вкладку "Новое".
2. Выберите уязвимости, установив соответствующие флаги.
3. Нажмите кнопку Создать инциденты. Откроется окно "Массовое создание инцидентов".
4. Проверьте в окне информацию о создаваемых инцидентах и подтвердите действие.

7.5.4.2 Закрытие инцидентов по результатам сравнения

1. Откройте результаты сравнения и перейдите на вкладку "Закрываемые".
2. Выберите уязвимости, установив соответствующие флаги.
3. Нажмите кнопку **Закрытие инцидента**. Откроется окно "Массовое закрытие инцидентов".
4. Проверьте в окне информацию о закрываемых инцидентах и подтвердите действие.

7.5.5 Изменение статуса результата сканирования

В **Платформе Радар** результаты сканирования могут находиться в следующих состояниях:

- Обработано – результаты сканирования исследованы ответственным специалистом, выполнено сравнение с текущим состоянием активов.
- Не обработано – результаты сканирования еще не были исследованы.

Для изменения статуса результата сканирования перейдите в раздел **Активы → Результаты сканирования** и нажмите кнопку в соответствующей строке. По наведении курсора мыши на кнопку отобразится информация о том, на какое состояние будет изменен результат сканирования.

7.6 Обнаружение хостов

Под обнаружением хостов подразумевается сканирование подсети, в результате которого может быть получен набор данных, достаточный для идентификации актива.

В результате сканирования может быть создана новая запись об активе или обновлена информация о существующем.

Для выполнения сканирования подсети перейдите в раздел **Активы → Обнаружение хостов** и выполните следующие действия:

1. В поле **IP** укажите IP-адрес подсети.
2. В поле **Подсеть** из выпадающего списка выберите подсеть.
3. Нажмите кнопку **Сканировать**.

По результатам сканирования будет выдан список обнаруженных хостов (см. «Рис. 98»).

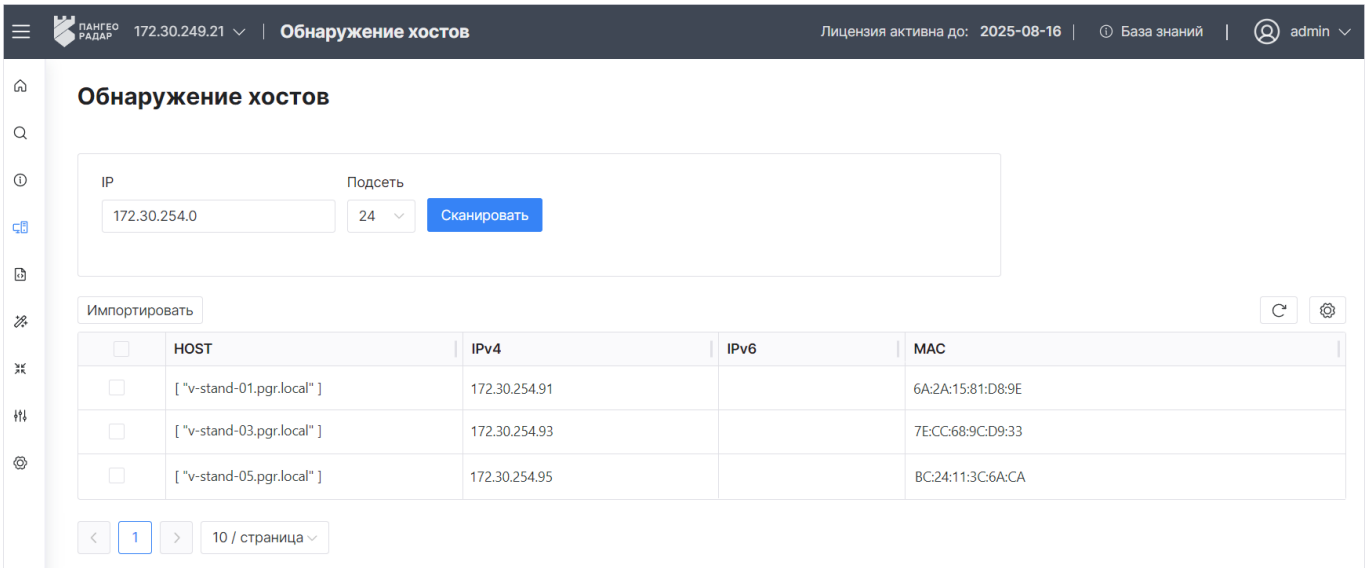


Рис. 98 – Раздел «Обнаружение хостов»

В списке отображается следующая информация:

- **HOST** – наименование хоста;
- **IPv4** – IP-адрес хоста по четвертой версии протокола IP;
- **IPv6** – IP-адрес хоста по шестой версии протокола IP;
- **MAC** – Mac-адрес хоста.

Для создания новых записей об активах или обновлении информации о существующих отметьте необходимые хосты и нажмите кнопку **Импортировать**.

7.7 Обнаружение сервисов

В **Платформу Радар** встроен механизм, который позволяет по запросу собирать данные о сервисах на выбранных активах.

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

Для работы с механизмом по обнаружению сервисов перейдите в раздел **Активы → Обнаружение сервисов**.

Пример собранной информации об активах приведен на «Рис. 99».

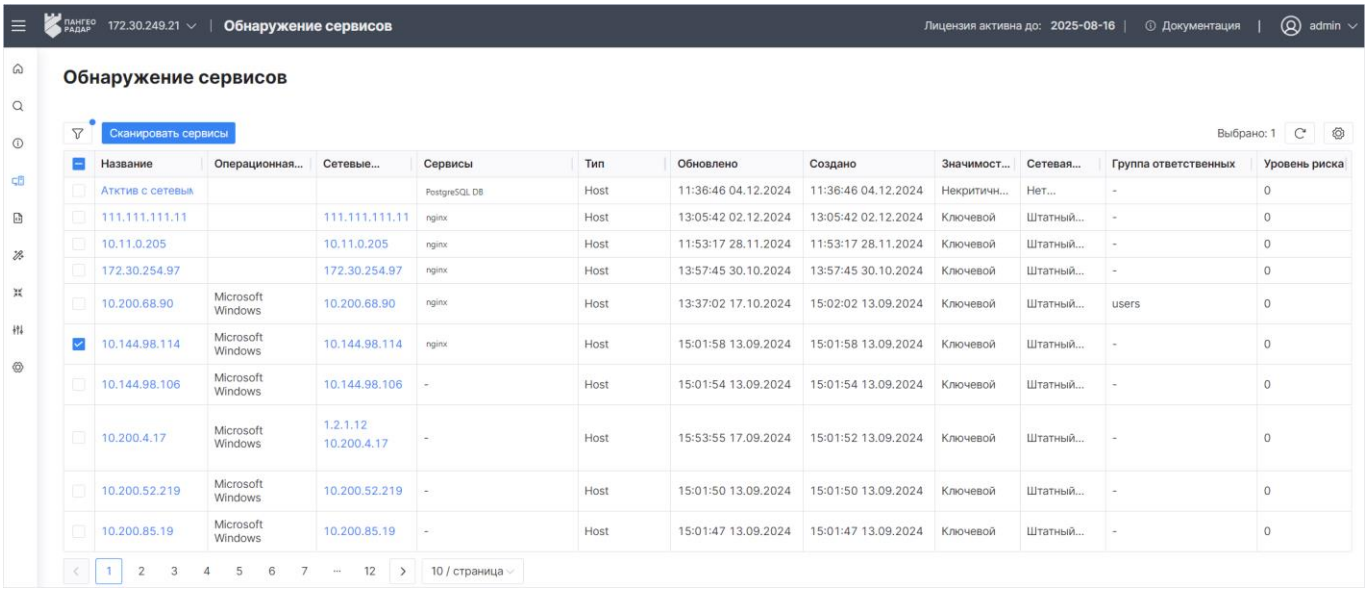


Рис. 99 – Раздел "Сбор данных"

В разделе отображается следующая информация:

- **Название** – наименование актива;
- **Операционная система** – наименование ОС, установленной на активе;
- **Сетевые интерфейсы** – список сетевых интерфейсов актива;
- **Сервисы** – список сервисов, обнаруженных на активе;
- **Тип** – тип обнаруженного сервиса;
- **Создано** – дата и время добавления информации об активе;
- **Обновлено** – дата и время изменения информации об активе;
- **Значимость актива** – уровень влияния актива на выполнение бизнес-процессов компании называется;
- **Сетевая видимость** – тип сетевой видимости актива;
- **Группа ответственных** – группа пользователей, ответственная за разбор инцидентов, выявленных на активе;
- **Уровень риска** – цифровое обозначение уровня риска актива.

Для запуска процесса обнаружения сервисов выполните следующие действия:

1. Выберите активы, с которых необходимо собрать данные, установив соответствующие флаги.
2. Нажмите кнопку **Сканировать сервисы**.
3. Начнется процесс сбора данных с выбранных активов. Процесс может занять некоторое время.

7.8 Сбор данных

В **Платформу Радар** встроен механизм, который позволяет по запросу собирать данные с выбранных активов.

Сбор выполняется с помощью учетных записей для сбора данных (подробнее см. документ «Руководство администратора. Раздел Кластер»).

Результатом работы сбора данных является найденный список установленного аппаратного и программного обеспечения на активе.

Для работы с механизмом по сбору данных перейдите в раздел **Активы → Сбор данных**.

Пример собранной информации об активах приведен на «Рис. 100».

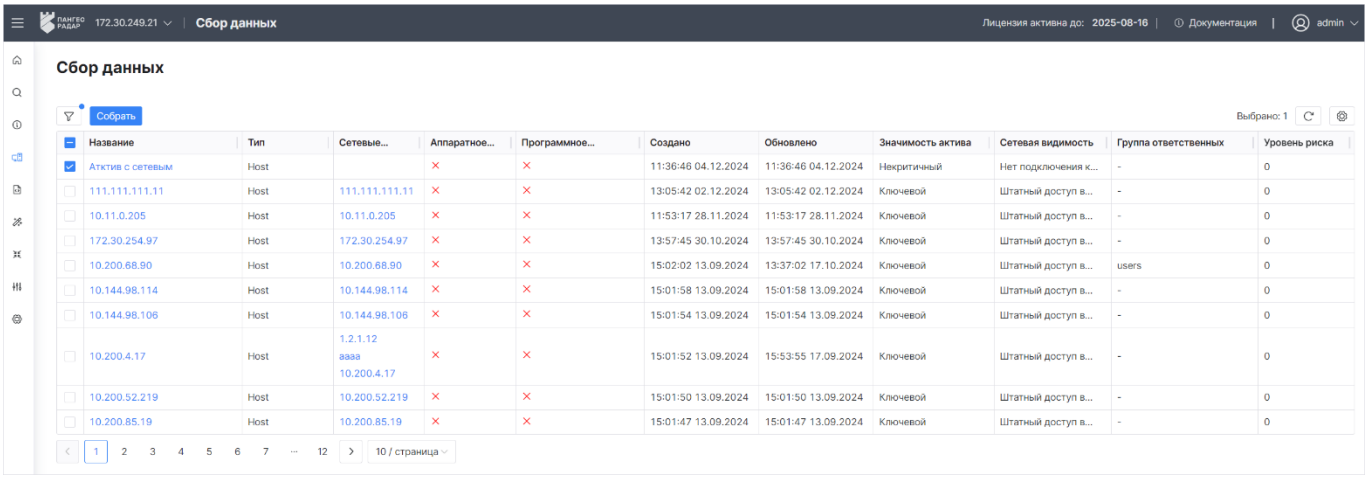


Рис. 100 – Раздел "Сбор данных"

В разделе отображается следующая информация:

- **Название** – наименование актива;
- **Тип** – тип актива;
- **Сетевые интерфейсы** – список сетевых интерфейсов актива;
- **Аппаратное обеспечение** – список аппаратного обеспечения актива;
- **Программное обеспечение** – список программного обеспечения, установленного на активе;
- **Создано** – дата и время добавления информации об активе;
- **Обновлено** – дата и время изменения информации об активе;
- **Значимость актива** – уровень влияния актива на выполнение бизнес-процессов компании называется;

- **Сетевая видимость** – тип сетевой видимости актива;
- **Группа ответственных** – группа пользователей, ответственная за разбор инцидентов, выявленных на активе;
- **Уровень риска** – цифровое обозначение уровня риска актива.

Для сбора данных выполните следующие действия:

1. Выберите активы, с которых необходимо собрать данные, установив соответствующие флаги.
2. Нажмите кнопку **Собрать данные**. Откроется окно "Настройки" (см. «Рис. 101»).

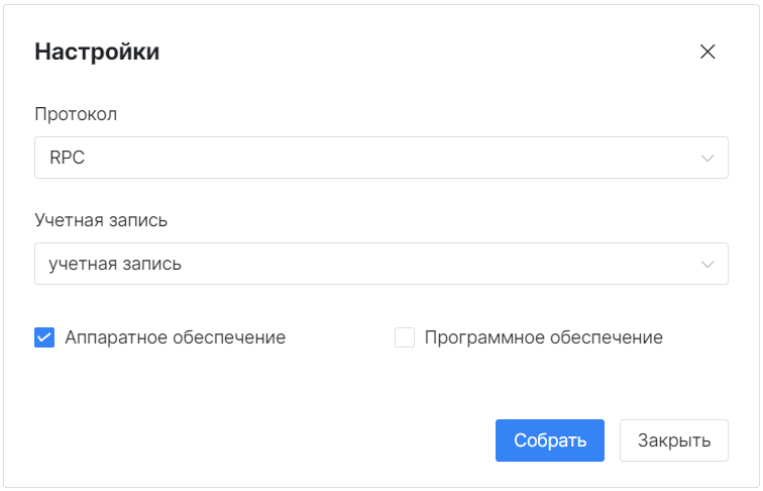


Рис. 101 – Окно "Настройки"

3. Укажите в окне следующую информацию:
    - в поле **Протокол** выберите сетевой протокол, по которому будет выполнено подключение и сбор данных с актива;
    - в поле **Учетная запись** выберите учетную запись, которая будет выполнять подключение к активу. Список доступных учетных записей формируется в зависимости от выбранного протокола;
    - при необходимости собирать информацию об аппаратном и программном обеспечении установите соответствующие флаги.
4. Нажмите кнопку **Собрать**. Начнется процесс сбора данных с выбранных активов. Процесс может занять некоторое время.

При возникновении ошибок при сборе данных обратитесь к документу «Руководство администратора. Раздел Возможные проблемы при эксплуатации платформы».

8. Соответствие ПО

8.1 Общие сведения

Платформа Радар позволяет настроить контроль установленного программного обеспечения. Контролируется ПО, которое устанавливается на активах. Контроль выполняется в соответствии с политиками контроля.

Политика контроля состоит из набора правил, которые могут отслеживать следующую информацию:

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

Политика контроля может быть применена к группе активов.

По результатам проверки соответствия ПО принимается одно из решений "Соответствует" или "Не соответствует".

Актив считается соответствующим политике, если все правила, входящие в политику контроля, дали положительный результат.

Группа активов считается соответствующей политике, если все активы группы соответствуют политике.

По результатам проверки соответствия политикам, платформа автоматически создает соответствующие инциденты ИБ при выполнении следующего условия: добавлен тип инцидента, у которого включена настройка **Использовать для создания инцидентов при оценке соответствия ПО** (см. раздел «Создание типа инцидента»).

Результаты проверки соответствия ПО заданным политикам контроля, отображаются в разделе «Результаты соответствия ПО».

Управление правилами контроля выполняется в разделе «Правила соответствия ПО».

Управление наборами правил контроля (политиками) выполняется в разделе «Наборы правил соответствия ПО».

В разделах «Список ПО» и «Список групп ПО» выполняется управление информацией о программном обеспечении, которое установлено на активах и объединение списка ПО в группы.

8.2 Результаты соответствия ПО

В разделе отображаются сводные результаты всех текущих проверок соответствия ПО.

Работа с результатами соответствия ПО включает в себя следующие процессы:

1. «Запуск процесса проверки соответствия ПО».
2. «Просмотр информации о результате соответствия ПО».
3. «Удаление результатов соответствия ПО».

Для работы с результатами проверок на соответствие ПО перейдите в раздел **Соответствие ПО → Результаты соответствия** (см. «Рис. 102»).

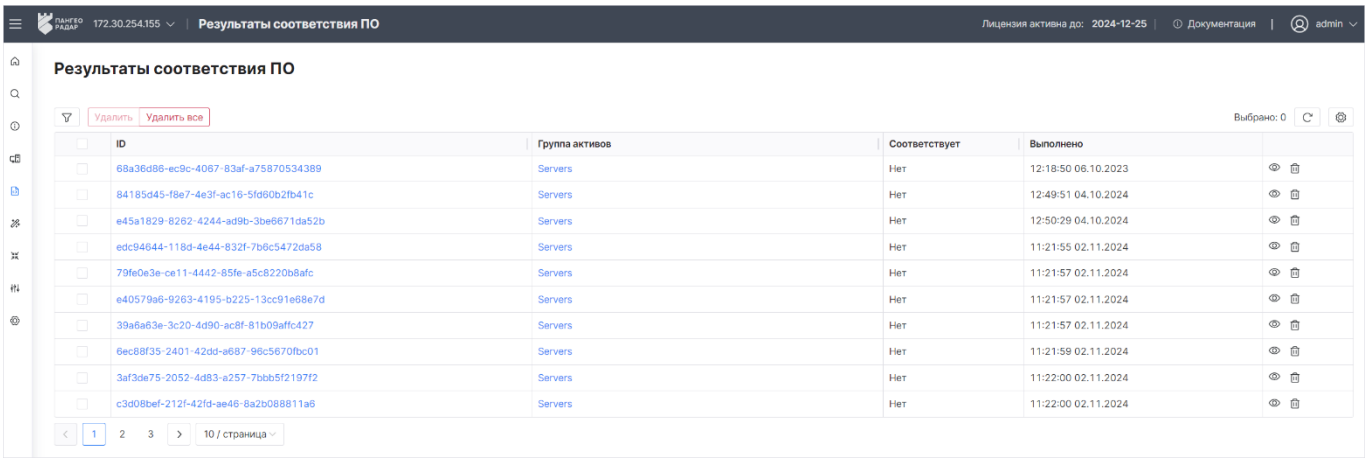


Рис. 102 – Раздел "Результаты соответствия ПО"

В разделе отображается следующая информация о результатах проверки ПО:

- **ID** – идентификатор проверки соответствия ПО. По ссылке произойдет переход на форму просмотра результата соответствия ПО;
- **Группа активов** – наименование группы активов, по которой выполнялась проверка соответствия ПО. По ссылке произойдет переход на форму просмотра группы активов;
- **Соответствует** – результат проведения проверки: соответствует или не соответствует группа активов заданной политике контроля;
- **Выполнено** – дата и время выполнения проверки.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие
	просмотр детализации по проверке
	удаление записи из таблицы

8.2.1 Запуск процесса проверки соответствия ПО

Для запуска процесса проверки соответствия ПО перейдите в раздел **Активы → Группы активов** и нажмите кнопку  (см. «Рис. 103»).

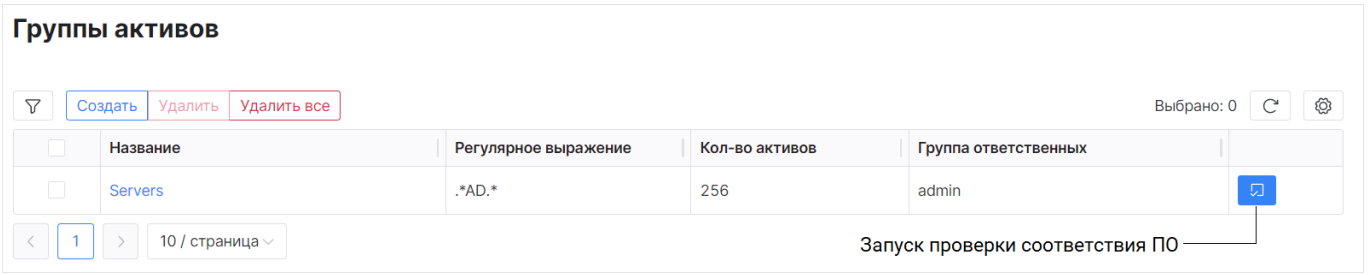


Рис. 103 – Раздел "Группы активов". Запуск проверки соответствия ПО

Будет создана задача на проведение проверки соответствия ПО, а ее результаты отобразятся в разделе **Соответствие ПО → Результаты соответствия**.

8.2.2 Просмотр информации о результате соответствия ПО

Для просмотра детализации о результате соответствия ПО нажмите кнопку . Откроется форма "Результаты соответствия ПО" (см. «Рис. 104»).

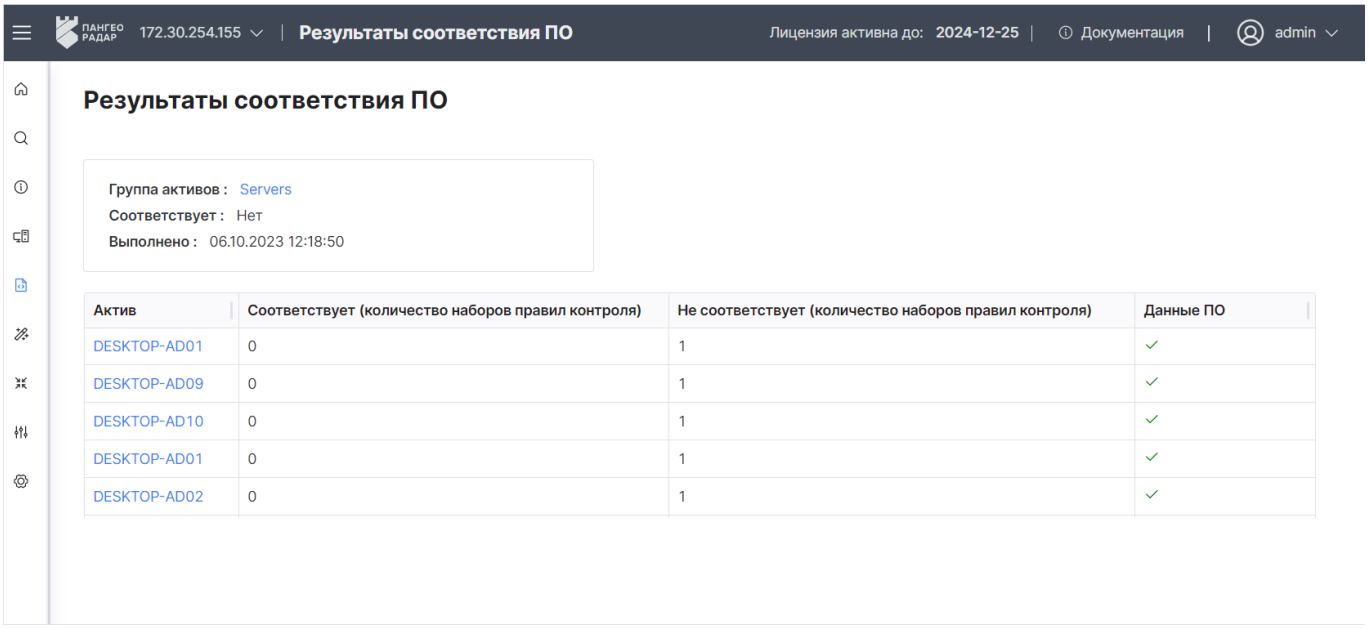


Рис. 104 – Форма "Результаты соответствия ПО"

На форме отображается следующая информация:

- **Группа активов** – наименование группы активов, по которой проводилась проверка соответствия;
- **Соответствует** – все ли активы, входящие в группу, соответствуют политике: да, нет;
- **Выполнено** – дата и время выполнения проверки;
- Информация об активах, входящих в группу:
  - **Актив** – наименование актива;
  - **Соответствует (количество наборов правил контроля)** – количество политик, которые дали положительный (соответствует) результат при проведении проверки соответствия ПО на данном активе;
  - **Не соответствует (количество наборов правил контроля)** – 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.

8.2.3 Удаление результатов соответствия ПО

Удаление результатов соответствия ПО можно выполнить следующими способами:

- удаление конкретного результата соответствия ПО;
- массовое удаление результатов соответствия ПО;
- удаление всех результатов соответствия ПО.

Способ 1. Удаление конкретного результата соответствия ПО:

1. Перейдите в раздел **Соответствие ПО → Результаты соответствия ПО**.
2. В строке нужного результата соответствия ПО нажмите кнопку .
3. Подтвердите удаление в открывшемся окне.

Способ 2. Массовое удаление результатов соответствия ПО:

1. Перейдите в раздел **Соответствие ПО → Результаты соответствия ПО**.
2. Отметьте необходимые результаты соответствия ПО.
3. Нажмите кнопку **Удалить**.
4. Подтвердите удаление в открывшемся окне.

Способ 3. Удаление всех результатов соответствия:

1. Перейдите в раздел **Соответствие ПО → Результаты соответствия ПО**.
2. Нажмите кнопку **Удалите все**.
3. Подтвердите удаление в открывшемся окне.

8.3 Список ПО

В платформе доступен перечень всего программного обеспечения, обнаруженного сканерами уязвимостей при сканировании активов.

Работа со списком ПО включает в себя следующие процессы:

1. «Просмотр информации о ПО».
2. «Просмотр информации об активах, на которых установлено ПО».
3. «Редактирование записи о ПО».
4. «Удаление записи о ПО из платформы».

Для работы со списком ПО перейдите в раздел **Соответствие ПО → Список ПО** (см. «Рис. 105»).

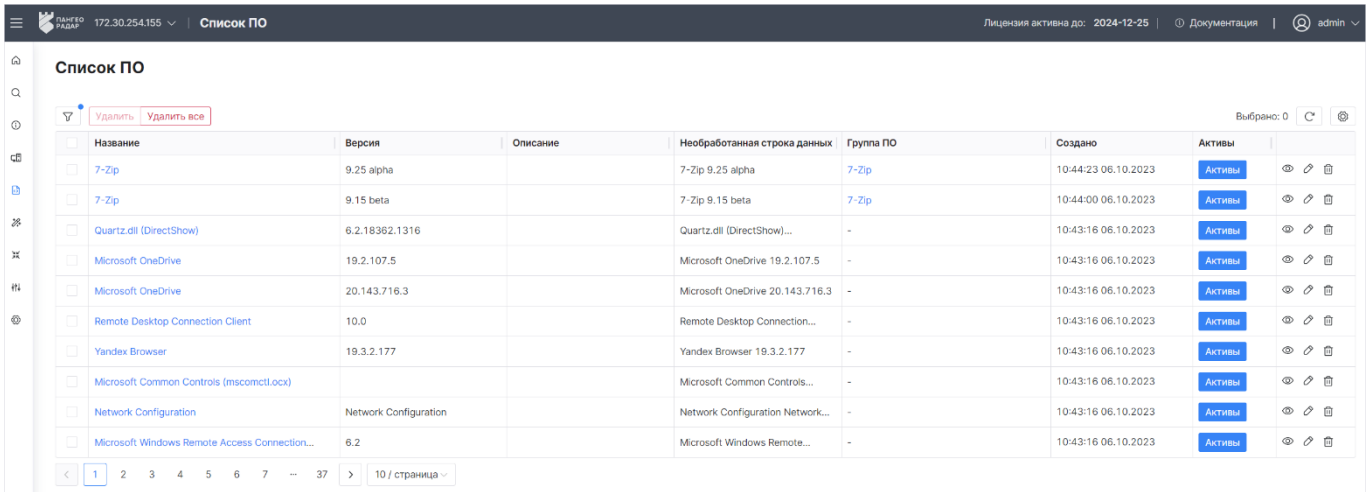


Рис. 105 – Раздел "Список ПО"

В разделе отображается следующая информация о ПО:

- **Название** – наименование ПО в платформе;
- **Версия** – версия ПО;
- **Описание** – дополнительные сведения о ПО;
- **Необработанная строка данных** – данные, полученные напрямую от сканера уязвимостей;
- **Группа ПО** – наименование группы, в которую входит ПО;
- **Создано** – дата и время создания записи о ПО.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие
	изменение записи о ПО
	просмотр детализации по проверке
	удаление записи о ПО
Активы	просмотр списка активов, на которых установлено ПО

8.3.1 Просмотр информации о ПО

Для просмотра информации о ПО нажмите кнопку  . Откроется форма "Данные ПО" (см. «Рис. 106»).

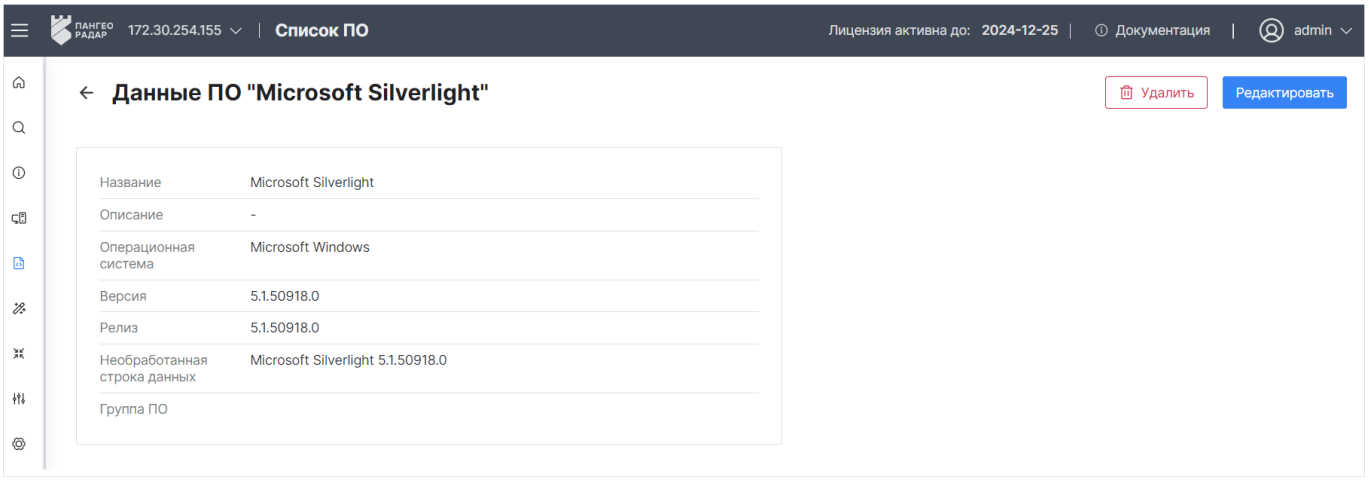


Рис. 106 – Форма "Данные ПО"

На форме отображается следующая информация:

- **Название** – наименование ПО в платформе;
- **Описание** – дополнительные сведения о ПО;
- **Операционная система** – наименование операционной системы, на которой работает ПО;
- **Версия** – версия ПО;
- **Релиз** – информация о технике сборки ПО (билде);
- **Необработанная строка данных** – данные, полученные напрямую от сканера уязвимостей;

- **Группа ПО** – наименование группы, в которую входит ПО.

8.3.2 Просмотр информации об активах, на которых установлено ПО

Для просмотра информации об активах, на которых установлено ПО, нажмите кнопку **Активы**. Откроется страница "Просмотр актива", где в боковой панели будет сформирован список активов, на которых установлено ПО. Подробнее см. раздел «Просмотр и анализ актива».

8.3.3 Редактирование записи о ПО

1. Выберите нужное ПО и нажмите кнопку . Откроется форма "Редактирование ПО" (см. «Рис. 107»).

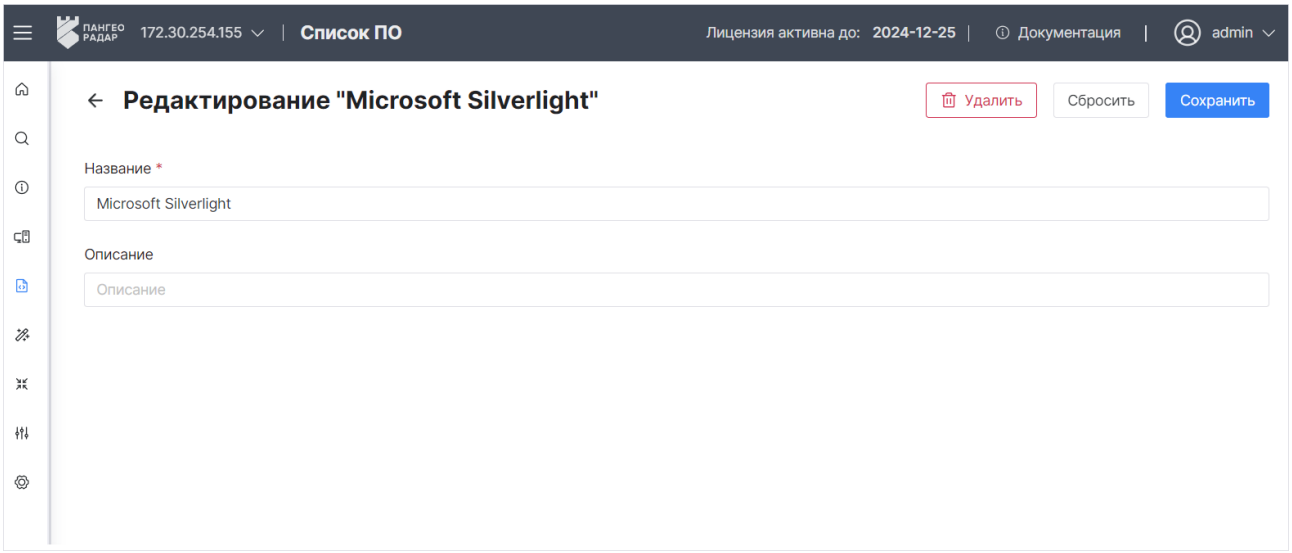


Рис. 107 – Форма «Редактирование списка ПО»

2. В полях **Название** и **Описание** укажите или измените соответствующие данные.
3. Нажмите кнопку **Сохранить**.

8.3.4 Удаление записи о ПО из платформы

Удаление записи о ПО можно выполнить следующими способами:

- удаление конкретной записи о ПО;
- массовое удаление записей о ПО;
- удаление всех записей о ПО.

Способ 1. Удаление конкретной записи о ПО:

1. Перейдите в раздел **Соответствие ПО → Список ПО**.
2. В строке нужной записи о ПО нажмите кнопку или перейдите на форму просмотра необходимой записи и нажмите кнопку **Удалить**.
3. Подтвердите удаление в открывшемся окне.

Способ 2. Массовое записей о ПО:

1. Перейдите в раздел **Соответствие ПО → Список ПО**.

2. Отметьте необходимые записи о ПО.
3. Нажмите кнопку **Удалить**.
4. Подтвердите удаление в открывшемся окне.

Способ 3. Удаление всех записей о ПО:

1. Перейдите в раздел **Соответствие ПО → Список ПО**.
2. Нажмите кнопку **Удалите все**.
3. Подтвердите удаление в открывшемся окне.

8.4 Список групп ПО

Для упрощения управления списком программного обеспечения, их можно объединить в группы.

Работа с группами ПО включает в себя следующие процессы:

1. «Создание группы ПО».
2. «Просмотр группы ПО».
3. «Редактирование группы ПО».
4. «Удаление группы ПО».

Для работы с группами ПО перейдите в раздел **Соответствие ПО → Список групп ПО** (см. «Рис. 108»).

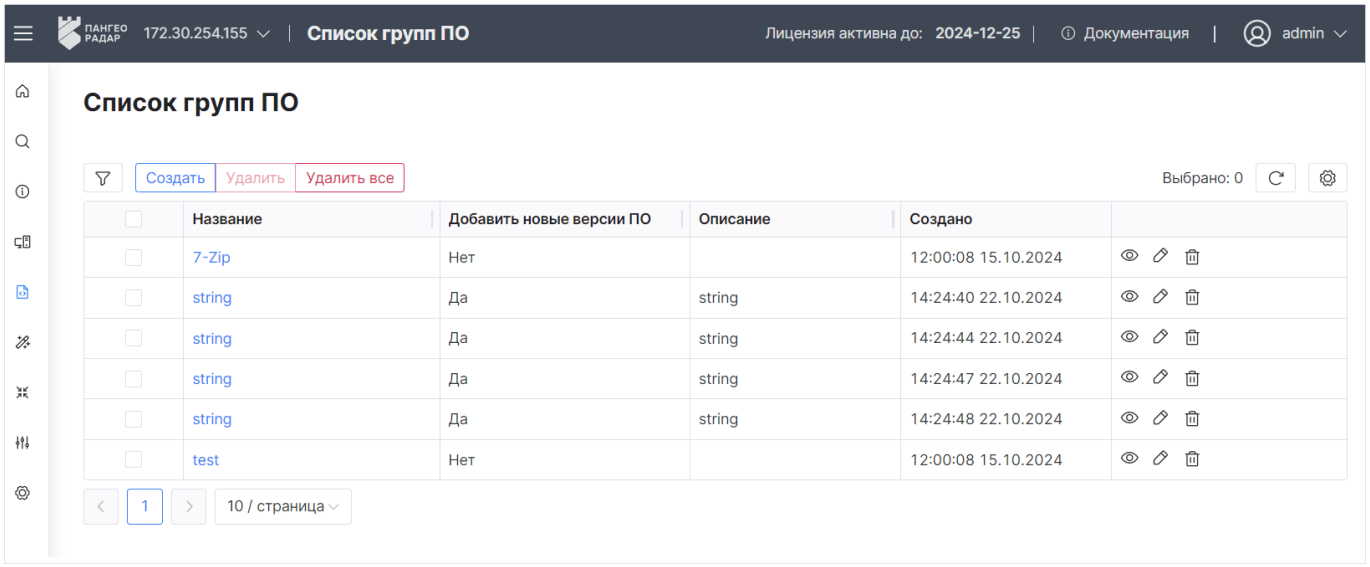


Рис. 108 – Раздел "Список групп ПО"

В разделе отображается следующая информация о группах ПО:

- **Название** – наименование группы ПО;
- **Добавить новые версии ПО** – будут ли в группу автоматически добавляться новые версии ПО: да, нет;
- **Описание** – дополнительные сведения о группе;

- **Создано** – дата и время создания группы.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие
	изменение записи о группе ПО
	просмотр группы ПО
	удаление записи о группе ПО

8.4.1 Создание группы ПО

1. Нажмите кнопку **Создать**. Откроется форма "Создание группы ПО" (см. «Рис. 109»).

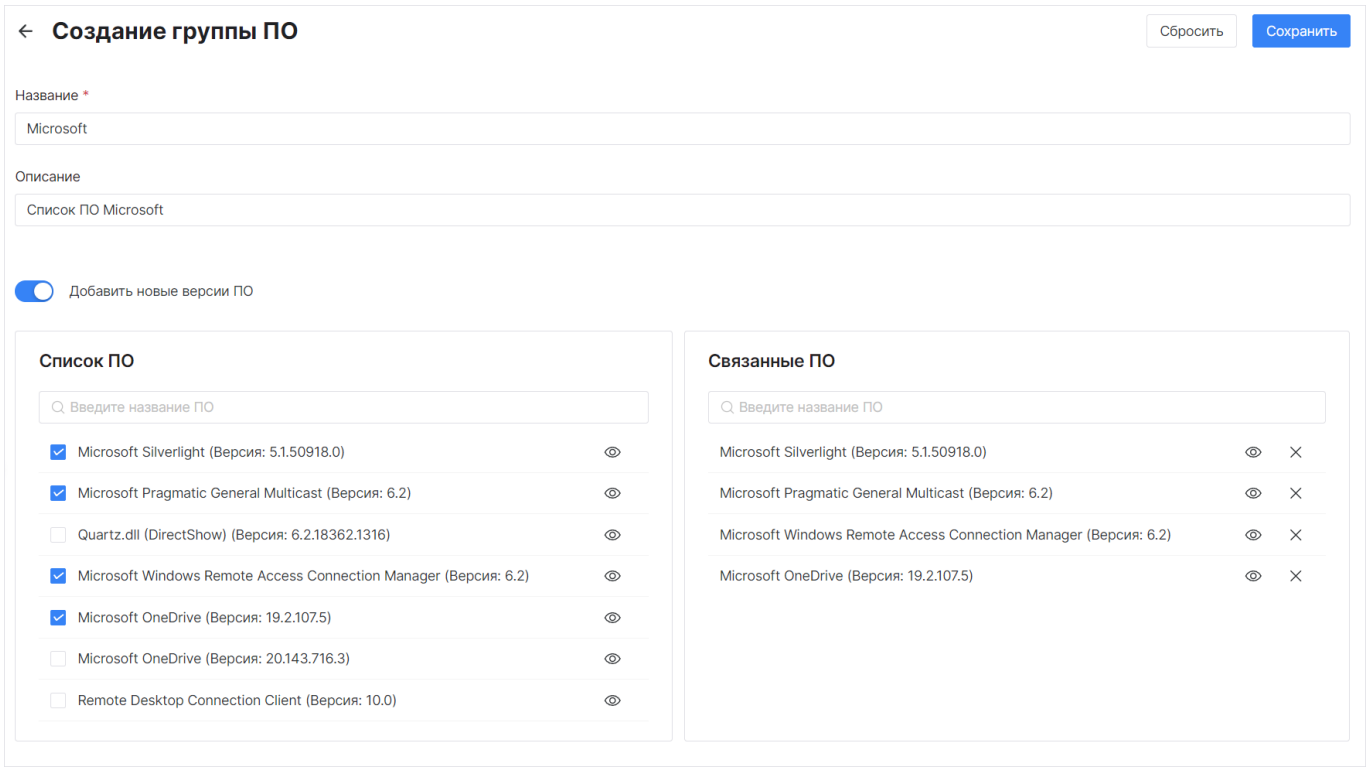


Рис. 109 – Форма "Создание группы ПО"

2. Укажите на форме следующую информацию:
   - в поле **Название** укажите наименование группы ПО;
   - в поле **Описание** укажите описание группы ПО;
   - для автоматического добавления новых версий ПО в группу, установите переключатель **Добавить новые версии ПО** в положение **Включен**;
   - в блоке **Список ПО** выберите ПО, которое будет добавлено в группу. Для этого установите соответствующие флаги. Выбранное ПО будет отображено в блоке **Связанные ПО**.
3. Нажмите кнопку **Сохранить**.

8.4.2 Просмотр группы ПО

Для просмотра информации о группе ПО нажмите кнопку . Откроется форма "Детали группы ПО" (см. «Рис. 110»).

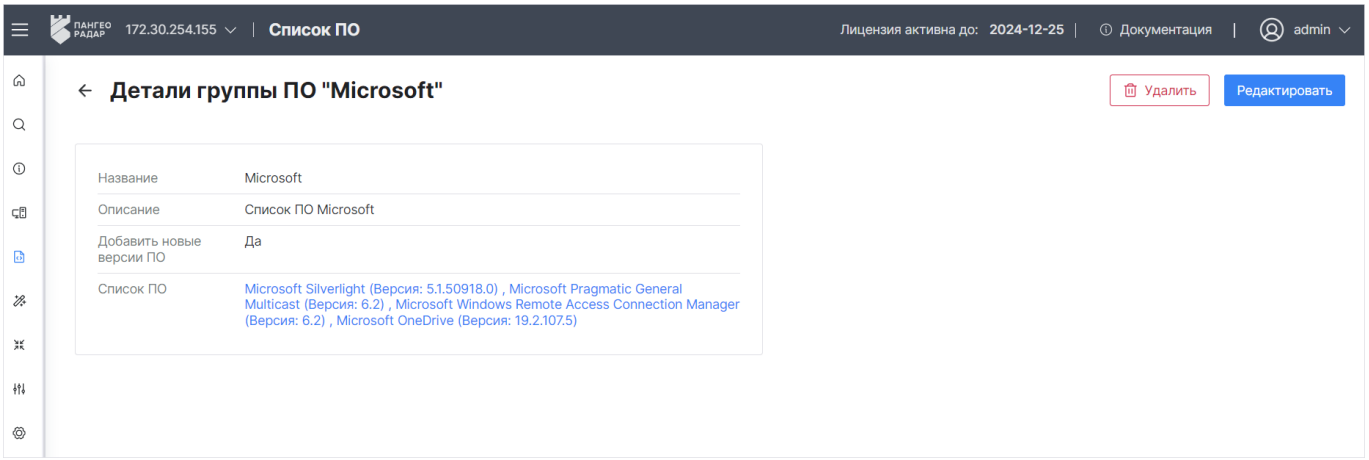


Рис. 110 – Форма "Детали группы ПО"

На форме отображается следующая информация:

- **Название** – наименование группы ПО;
- **Описание** – дополнительные сведения о группе ПО;
- **Добавить новые версии ПО** – будут ли в группу автоматически добавляться новые версии ПО: да, нет;
- **Список ПО** – список ПО, добавленного в группу.

8.4.3 Редактирование группы ПО

1. Выберите нужную группу ПО и нажмите кнопку или перейдите на форму просмотра необходимой группы ПО и нажмите кнопку **Редактировать**.
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

8.4.4 Удаление группы ПО

Удаление группы ПО можно выполнить следующими способами:

- удаление конкретной группы ПО;
- массовое удаление групп ПО;
- удаление всех групп ПО.

Способ 1. Удаление конкретной группы ПО:

1. Перейдите в раздел **Соответствие ПО → Список групп ПО**.
2. В строке нужной группы ПО нажмите кнопку или перейдите на форму просмотра необходимой группы ПО и нажмите кнопку **Удалить**.
3. Подтвердите удаление в открывшемся окне.

Способ 2. Массовое удаление групп ПО:

1. Перейдите в раздел **Соответствие ПО → Список групп ПО**.
2. Отметьте необходимые группы ПО.
3. Нажмите кнопку **Удалить**.
4. Подтвердите удаление в открывшемся окне.

Способ 3. Удаление всех групп ПО:

1. Перейдите в раздел **Соответствие ПО → Список групп ПО**.
2. Нажмите кнопку **Удалите все**.
3. Подтвердите удаление в открывшемся окне.

8.5 Правила соответствия ПО

Правило содержит регулярное выражение, по которому выполняется фильтрация списка ПО при выполнении проверки.

Работа с правилами соответствия ПО включает в себя следующие процессы:

1. «Создание правила соответствия ПО».
2. «Просмотр правила соответствия ПО».
3. «Редактирование правила соответствия ПО».
4. «Удаление правила соответствия ПО».

Для работы с правилами перейдите в раздел **Соответствие ПО → Правила соответствия ПО** (см. «Рис. 111»).

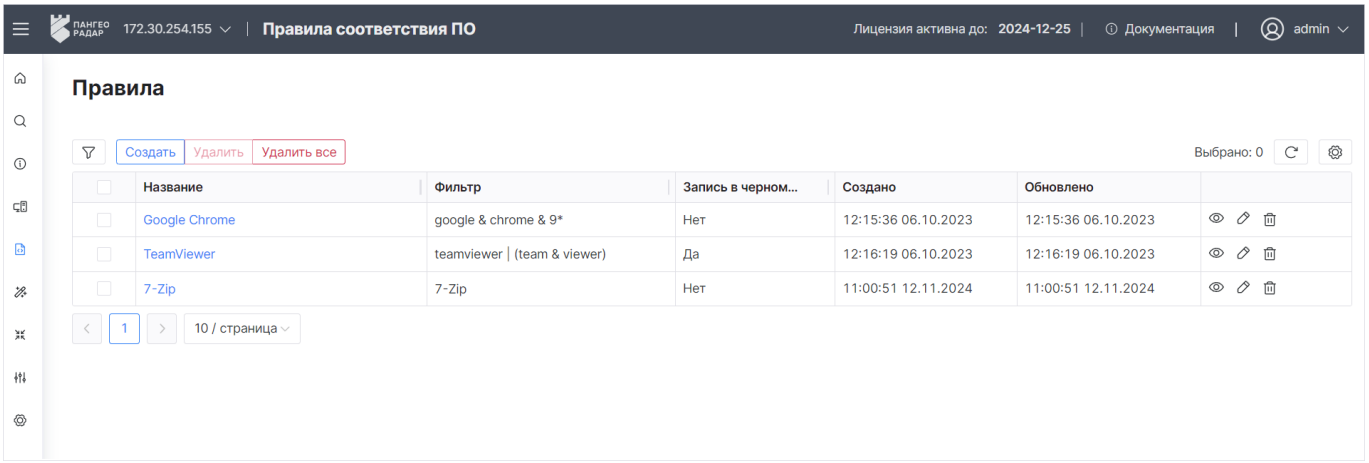


Рис. 111– Раздел "Правила соответствия ПО"

В разделе отображается следующая информация о правилах:

- **Название** – наименование правила;
- **Фильтр** – регулярное выражение, по которому работает правило;
- **Запись в черном списке** – отметка, что данного ПО не должно быть на активе;
- **Создано** –дата и время создания правила;

- **Обновлено** –дата и время изменения информации о правиле.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие
	просмотр правила
	изменение правила
	удаление правила

8.5.1 Создание правила соответствия ПО

1. Нажмите кнопку **Создать**. Откроется форма "Создание правила" (см. «Рис. 112»).

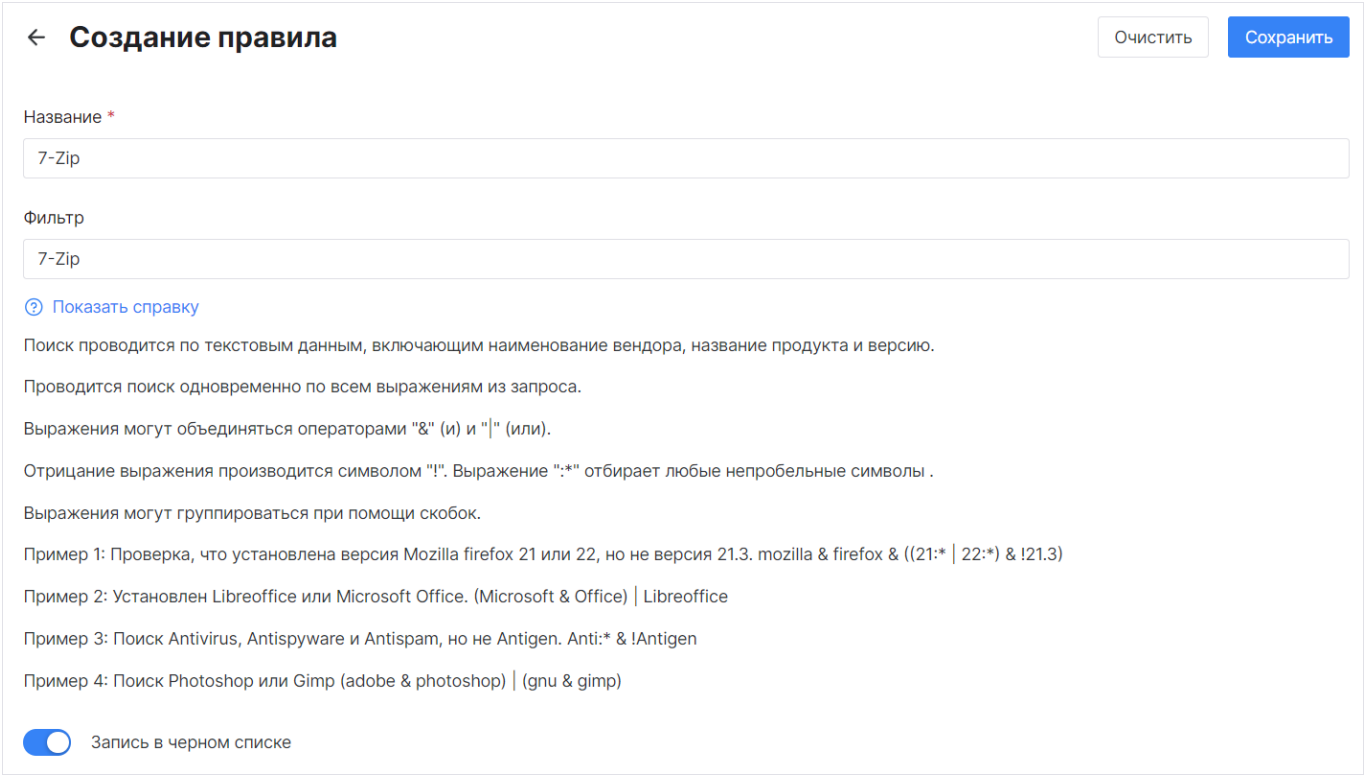


Рис. 112 – Форма "Создание правила"

2. Укажите на форме следующую информацию:
   - в поле **Название** укажите наименование правила;
   - в поле **Фильтр** укажите регулярное выражение, по которому будет проводиться поиск ПО. По кнопке **Показать справку** можно посмотреть подсказку по регулярным выражениям;
   - для поиска записей в черном списке включите соответствующий переключатель.
3. Нажмите кнопку **Сохранить**.

8.5.2 Просмотр правила соответствия ПО

Для просмотра правила соответствия ПО нажмите кнопку . Откроется форма просмотра правила (см. «Рис. 113»).

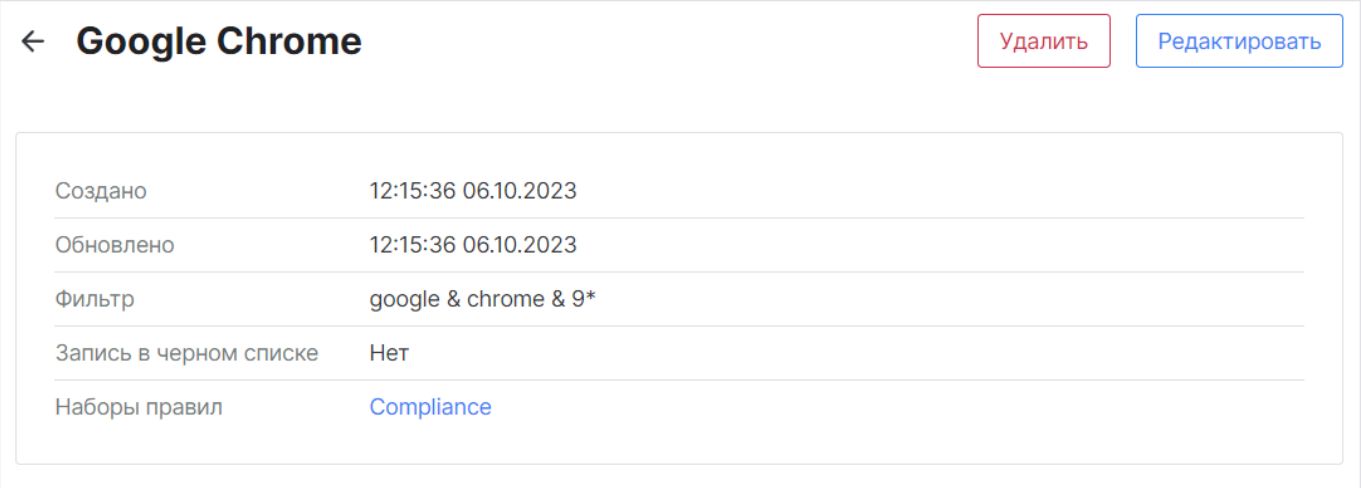


Рис. 113 – Форма просмотра правила"

На форме отображается следующая информация:

- **Создано** – дата и время создания правила;
- **Обновлено** – дата и время изменения информации о правиле;
- **Фильтр** – регулярное выражение, по которому работает правило;
- **Запись в черном списке** – будет ли выполняться поиск ПО в черном списке: да, нет;
- **Наборы правил** – список политик, которые используют правило.

8.5.3 Редактирование правила соответствия ПО

1. В строке нужного правила нажмите кнопку или перейдите на форму просмотра правила и нажмите кнопку **Редактировать**.
2. Внесите необходимые изменения.
3. Сохраните изменения.

8.5.4 Удаление правила соответствия ПО

Удаление правила можно выполнить следующими способами:

- удаление конкретного правила;
- массовое удаление правил;
- удаление всех правил.

Способ 1. Удаление конкретного правила:

1. Перейдите в раздел **Соответствие ПО → Правила соответствия ПО**.

2. В строке нужного правила нажмите кнопку или перейдите на форму просмотра правила и нажмите кнопку **Удалить**.
3. Подтвердите удаление в открывшемся окне.

Способ 2. Массовое удаление правил:

1. Перейдите в раздел **Соответствие ПО → Правила соответствия ПО**
2. Отметьте необходимые правила.
3. Нажмите кнопку **Удалить**.
4. Подтвердите удаление в открывшемся окне.

Способ 3. Удаление всех правил:

1. Перейдите в раздел **Соответствие ПО → Правила соответствия ПО**.
2. Нажмите кнопку **Удалите все**.
3. Подтвердите удаление в открывшемся окне.

8.6 Наборы правил соответствия ПО

Наборы правил соответствия ПО это политики, с помощью которых выполняется проверка соответствия ПО.

Работа с политиками контроля соответствия ПО включает в себя следующие процессы:

1. «Создание политики соответствия ПО».
2. «Просмотр политики соответствия ПО».
3. «Редактирование политики соответствия ПО».
4. «Удаление политики соответствия ПО».

Для работы с политиками контроля перейдите в раздел **Соответствие ПО → Наборы правил соответствия ПО** (см. «Рис. 114»).

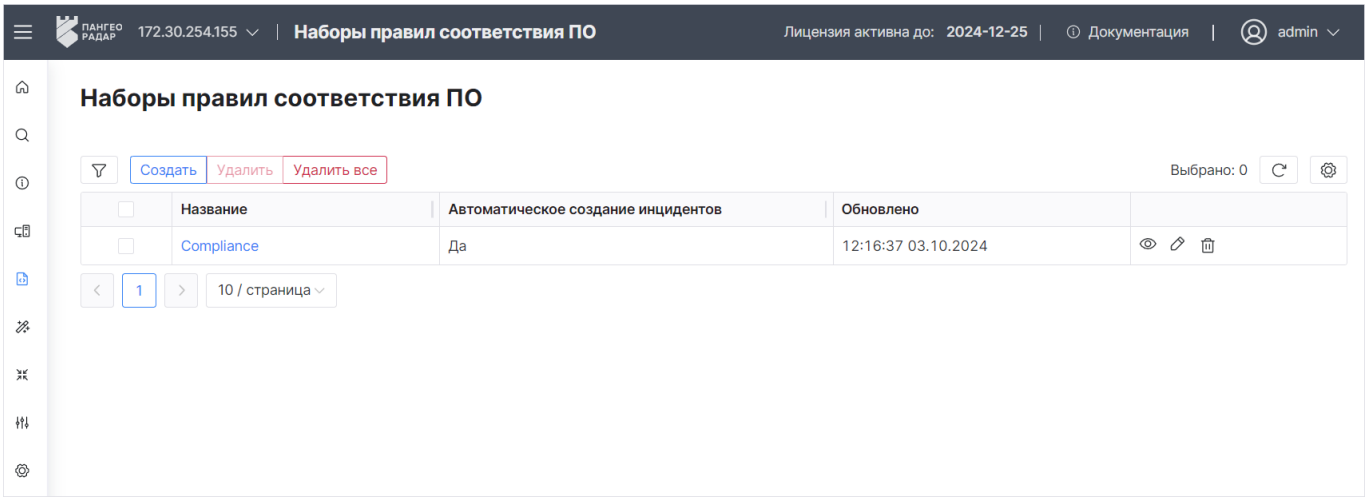


Рис. 114 – Раздел "Наборы правил соответствия ПО"

В разделе отображается следующая информация о политиках:

- **Название** – наименование политики;

- **Автоматическое создание инцидента** – будет ли автоматически создан инцидент по результатам проведения проверки соответствия ПО: да, нет;
- **Обновлено** – дата и время обновления информации о политике.

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие
	просмотр политики
	изменение информации о политике
	удаление политики

8.6.1 Создание политики соответствия ПО

1. Нажмите кнопку **Создать**. Откроется форма "Создать набор правил" (см. «Рис. 115»).

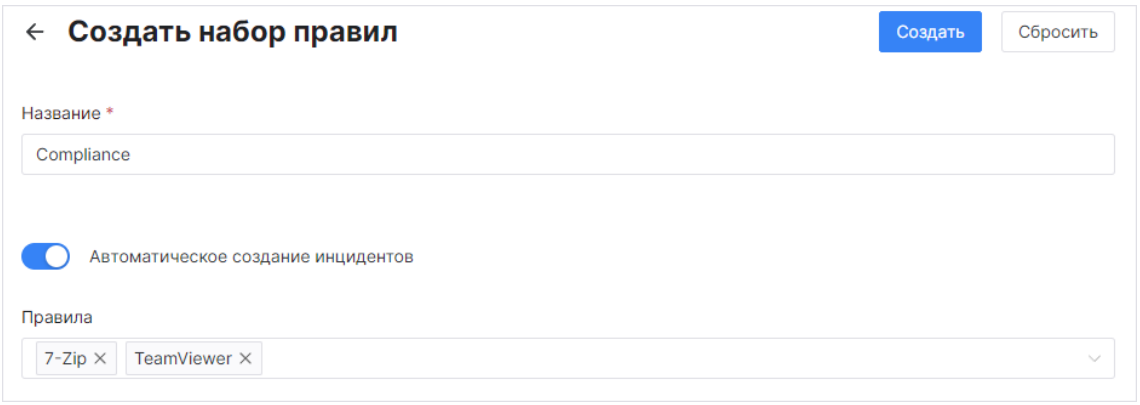


Рис. 115 – Форма "Создать набор правил"

2. Укажите на форме следующую информацию:
   - в поле **Название** укажите наименование политики;
   - для автоматического создания инцидентов по результатам проведения проверки соответствия ПО, установите соответствующий переключатель в положение **Включен**.

     Примечание: Также должен быть добавлен тип инцидента, у которого включена настройка **Использовать для создания инцидентов при оценке соответствия ПО** (см. раздел «Создание типа инцидента»).
   - в поле **Правила** выберите правила, которые будут входить в политику.
3. Нажмите кнопку **Создать**.

8.6.2 Просмотр политики соответствия ПО

Для просмотра политики контроля соответствия ПО нажмите кнопку  . Откроется форма просмотра политики (см. «Рис. 116»).

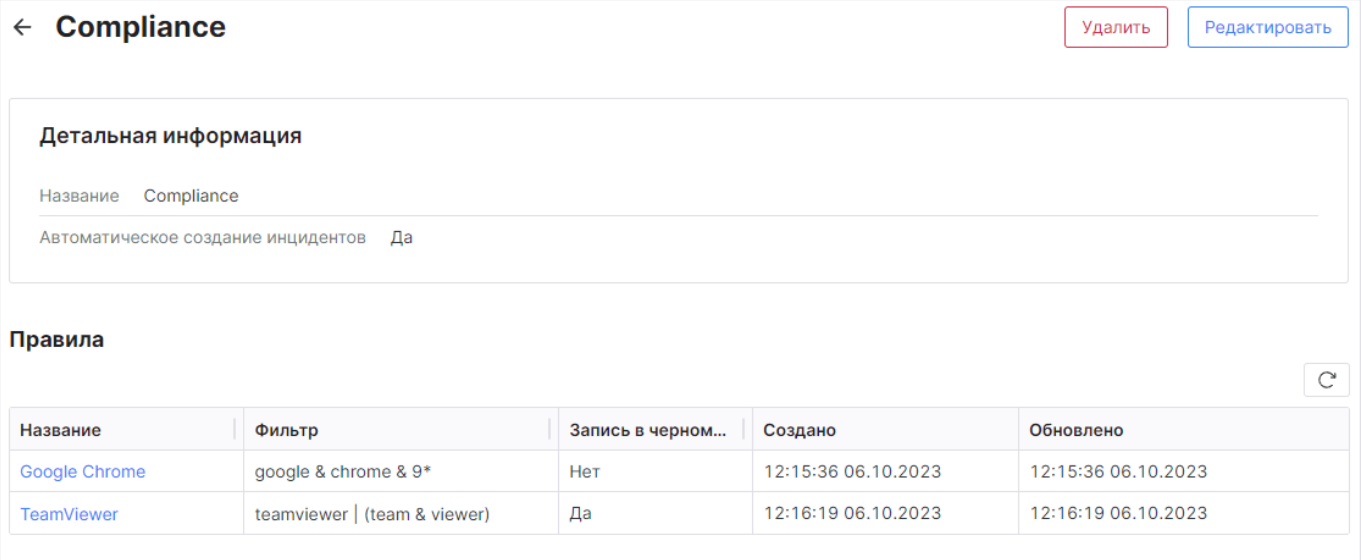


Рис. 116 – Форма просмотра политики"

Информация на форме отображается в следующих блоках:

- Блок **Детальная информация**. В блоке отображается следующая информация:
  - **Название** – наименование политики;
  - **Автоматическое создание инцидента** – будет ли автоматически создан инцидент по результатам проведения проверки соответствия ПО: да, нет.
- Блок **Правила**. В блоке отображается информация о правилах, входящих в политику:
  - **Название** – наименование правила;
  - **Фильтр** – регулярное выражение, по которому работает правило;
  - **Запись в черном списке** – отметка, что данного ПО не должно быть на активе;
  - **Создано** –дата и время создания правила;
  - **Обновлено** –дата и время изменения информации о правиле.

8.6.3 Редактирование политики соответствия ПО

1. В строке нужной политики нажмите кнопку или перейдите на форму просмотра политики и нажмите кнопку **Редактировать**.
2. Внесите необходимые изменения.
3. Сохраните изменения.

8.6.4 Удаление политики соответствия ПО

Удаление политики можно выполнить следующими способами:

- удаление конкретной политики;
- массовое удаление политик;
- удаление всех политик.

Способ 1. Удаление конкретной политики:

1. Перейдите в раздел **Соответствие ПО → Наборы правил соответствия ПО**
2. В строке нужной политики нажмите кнопку  или перейдите на форму просмотра политики и нажмите кнопку **Удалить**.
3. Подтвердите удаление в открывшемся окне.

Способ 2. Массовое удаление политик:

1. Перейдите в раздел **Соответствие ПО → Наборы правил соответствия ПО**
2. Отметьте необходимые политики.
3. Нажмите кнопку **Удалить**.
4. Подтвердите удаление в открывшемся окне.

Способ 3. Удаление всех политик:

1. Перейдите в раздел **Соответствие ПО → Наборы правил соответствия ПО**.
2. Нажмите кнопку **Удалите все**.
3. Подтвердите удаление в открывшемся окне.

9. Коррелятор

9.1 Общие данные

Коррелятор предназначен для выявления последовательностей в потоке событий, отфильтрованных с помощью фильтров потока событий и удовлетворяющих условиям, описанным в правиле корреляции.

Результатом работы коррелятора является так называемая "сработка" правила корреляции, на основании которой может быть создан инцидент и проведен анализ.

Условия для "сработок" правил корреляции задаются в разделе «Правила корреляции». В общем случае правила разрабатываются на скриптовом языке Lua, но **Платформа Радар** позволяет использовать визуальный конструктор для написания правил корреляции.

Правила делятся на два вида:

- линейные - используются для реагирования на определенный вид события в одном экземпляре;
- с группировкой событий - используется, когда необходимо провести корреляцию над сгруппированными по какому-либо принципу событиями.

Для обращения к справочникам используются табличные списки (см. раздел «Табличные списки»). Существуют следующие действия для работы с табличными списками:

- установить значение в табличном списке;
- удалить запись из табличного списка;
- очистка табличного списка.

Для настройки условий фильтраций, который будет применяться к потоку событий, используются фильтры потока событий (см. раздел «Фильтры потока событий»).

Существует возможность передавать поток событий на другой узел (например, выполнена множественная установка платформы на разных узлах), то вы можете настроить пересылку событий (см. раздел «Пересылка событий»).

Код правила корреляции может быть расширен с помощью макросов (см. раздел «Макросы»). Один и тот же макрос может быть использован во множестве правил.

Платформа Радар позволяет осуществлять ретроспективный анализ – проверку гипотез на основе исторических данных, хранимых в системе. Для осуществления ретроспективного анализа можно использовать как существующие правила корреляции, так и вновь созданные (см. раздел «Ретроспективная корреляция»).

9.2 Правила корреляции

Для работы с правилами корреляции перейдите в раздел **Коррелятор → Правила корреляции** (см. «Рис. 117»).

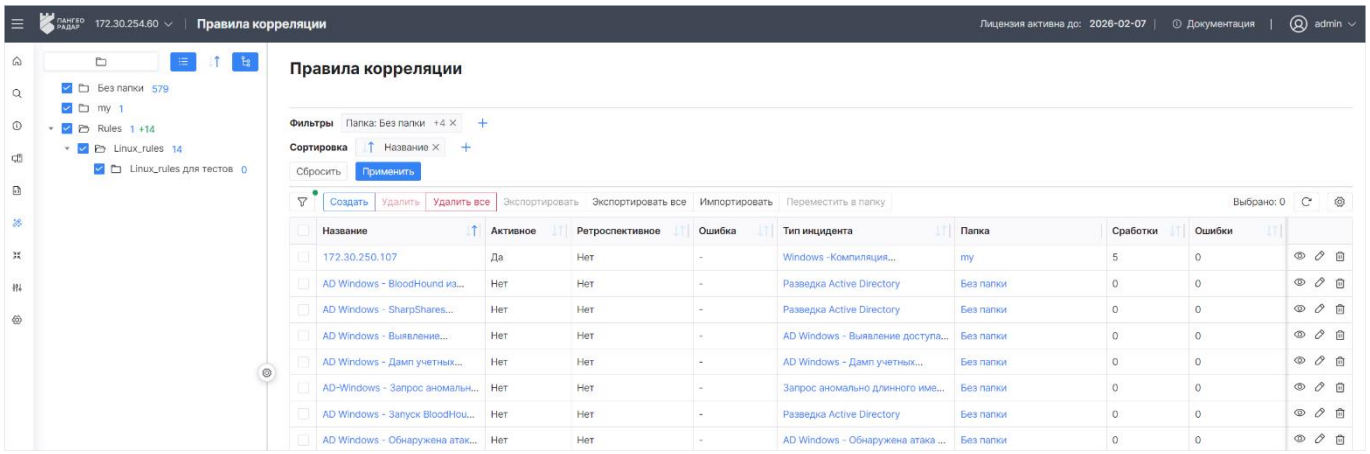


Рис. 117 – Раздел "Правила корреляции". Представление через универсальную таблицу

В разделе отображается следующая информация:

- **Название** – наименование правила корреляции;
- **Активное** – признак активности правила: да, нет;
- **Ретроспективное** – используется ли правило для ретроспективной корреляции: да, нет;
- **Ошибка** – описание ошибки инициализации правила;
- **Тип инцидента** – наименование типа инцидента, по которому работает правило;
- **Папка** – наименование папки структуры контента, в которой находится правило. Подробнее о работе с папками см. раздел «Папки контента».
- **Сработки** – количество "сработок" правила;
- **Ошибки** – количество ошибок инициализации правила;
- **Обновлено** – дата и время изменения информации о правиле;
- **Создано** – дата и время создания правила;
- **ID** – идентификатор правила.

Для переключения режима просмотра правил, нажмите по названию правила в соответствующей колонке или на кнопку в нужной строке. Откроется представление правил через боковую панель, а выбранное правило откроется на просмотр (см. «Рис. 118»).

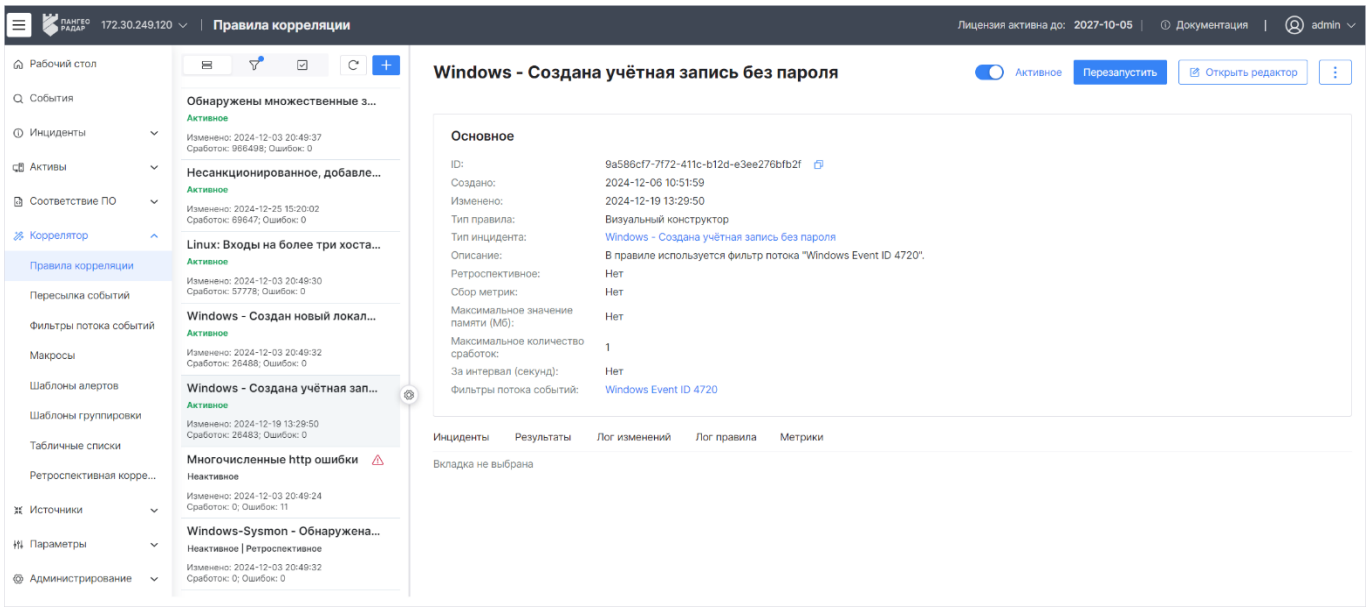


Рис. 118 – Раздел "Правила корреляции". Представление через боковую панель

Раздел состоит из следующих блоков:

- **Список правил корреляции**, в котором отображается следующая информация о правилах:
  - название правила;
  - состояние правила: активно, неактивно;
  - дата последнего изменения правила;
  - количество сработок;
  - количество ошибок.
- **Основное**, в котором отображается общая информация о выбранном правиле.
- **Статистика работы правила**, в котором отображается следующая информация:
  - "Инциденты" – список инцидентов, созданных на основании сработавшего правила;
  - "Результаты" – список "сработок" привила;
  - "Лог изменений" – история изменения правила;
  - "Лог правила" – журнал работы правила;
  - "Метрики" – визуализация информации о "сработках" правила в виде графиков.

9.2.1 Просмотр статистики работы правил

9.2.1.1 Вкладка "Инциденты"

На вкладке отображается список инцидентов, созданных на основе "сработок" правил (см. «Рис. 119»).

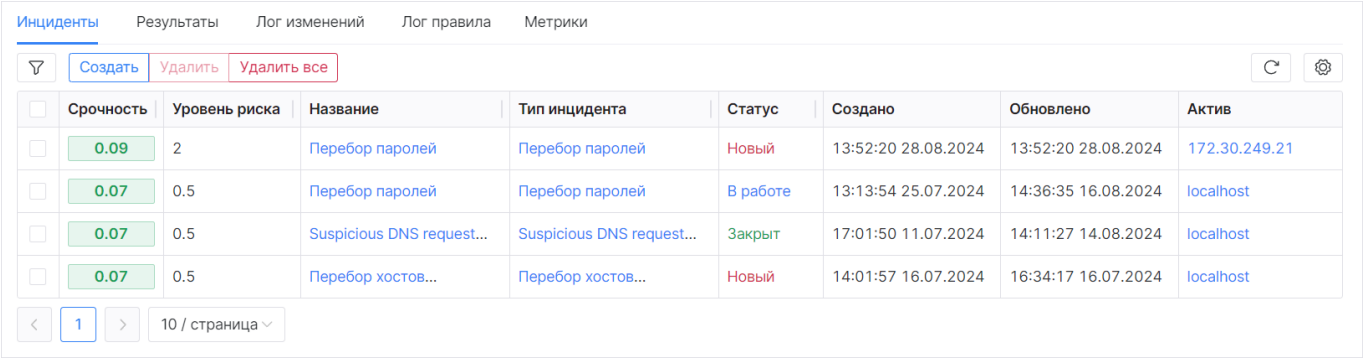


Рис. 119 – Просмотр статистики работы правила. Вкладка "Инциденты"

Полный набор информации, отображаемы в таблице:

- Срочность – цифровое и цветовое обозначение оценки срочности реагирования на инцидент;
- Уровень риска – цифровое и цветовое обозначение уровня угрозы;
- Название – название обнаруженной угрозы. По ссылке произойдет переход к форме просмотра инцидента;
- Тип инцидента – по ссылке произойдет переход к форме просмотра типа инцидента;
- Статус – текущее состояние инцидента;
- Актив – техническое средство информационной системы, на котором произошел инцидент. По ссылке произойдет переход к форме просмотра актива;
- Группа инцидентов – название группы, к которой относится инцидент;
- ID – идентификатор инцидента;
- Последнее происшествие – дата и время последнего происшествия, зарегистрированного в инциденте;
- Кол-во происшествий – количество происшествий в инциденте;
- Кол-во повторных открытий – количество повторных открытий инцидента;
- Пользователь – наименование ответственного пользователя;
- Группа пользователей – наименование ответственной группы пользователей;
- Создано – дата и время создания инцидента;
- Обновлено – дата и время изменения информации об инциденте;
- Категория – категория инцидента;
- Эксплуатируется удаленно – признак удаленной эксплуатации, возможные значение: да, нет;
- Результат анализа – результат анализа инцидента (по наведению мыши во всплывающем окне отобразится полное описание).

Подробнее о работе с инцидентами см. раздел «Инциденты».

9.2.1.2 Вкладка "Результаты"

На вкладке отображается список "сработок" правила корреляции (см. «Рис. 120»).

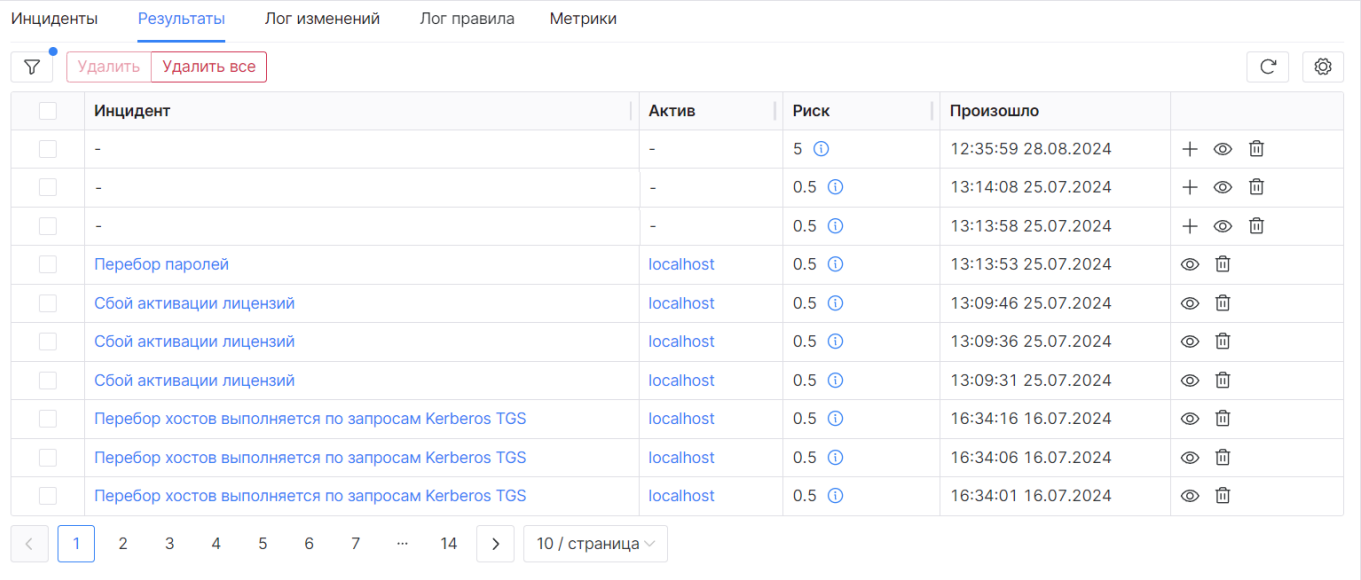


Рис. 120 – Просмотр статистики работы правила. Вкладка "Результаты"

При работе над записями таблицы доступны следующие элементы управления:

Кнопка	Действие
+	создание нового инцидента на основе "сработки" правила (см. раздел «Создание инцидента»)
👁	просмотр событий, вызвавших "сработку" правила (см. раздел «Просмотр события»)
🗑	удаление записи из таблицы

В списке "сработок" правила корреляции отображается следующая информация:

- Инцидент - наименование инцидента, созданного на основе "сработки" правила. По ссылке произойдет переход к форме просмотра инцидента;
- Актив - название актива, на котором произошла "сработка". По ссылке произойдет переход к форме просмотра актива;
- Риск - уровень угрозы;
- Произошло - дата и время "сработки" правила.

9.2.1.3 Вкладка "Лог изменений"

На вкладке отображается журнал изменения правила (см. «Рис. 121»).

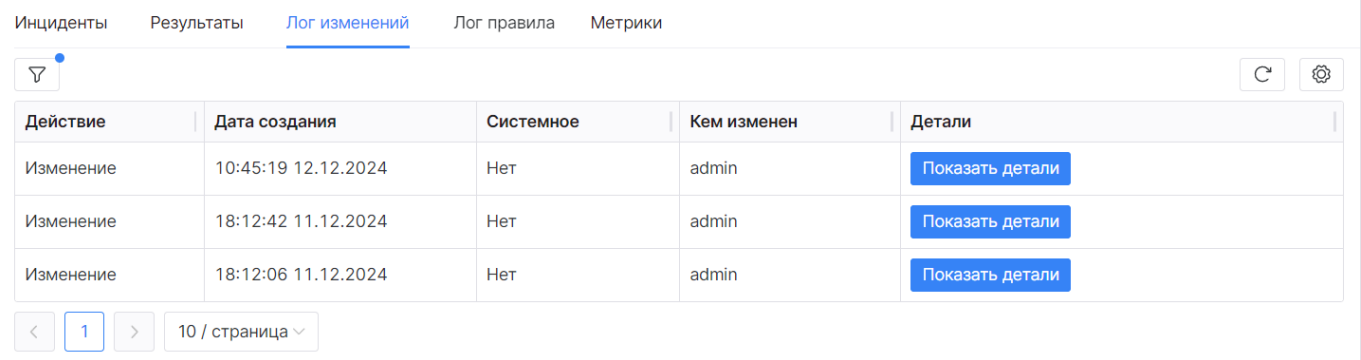


Рис. 121 – Просмотр статистики работы правила. Вкладка "Лог изменений"

В журнале изменений отображается следующая информация:

- Действие - тип действия, выполненного над правилом;
- Дата создания - дата выполнения изменения;
- Системное - признак того, было ли изменение выполнено платформой;
- Пользователь - пользователь, выполнивший изменение.

По кнопке **Показать детали** можно посмотреть детальную информацию об изменении правила.

9.2.1.4 Вкладка "Лог правила"

На вкладке отображается журнал работы правила (см. «Рис. 122»).

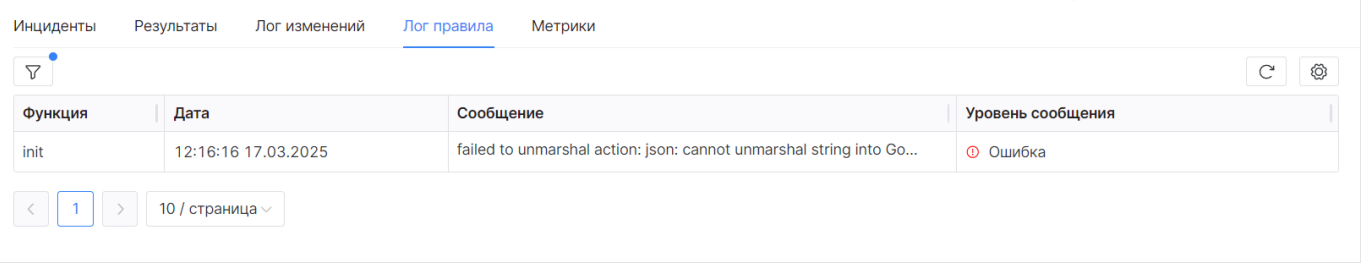


Рис. 122 – Просмотр статистики работы правила. Вкладка "Лог ошибок"

В журнале отображается следующая информация:

- Функция – наименование функции, по которой создано сообщение;
- Дата – дата и время создания сообщения;
- Сообщение – текст сообщения (при наведении мыши отобразится полное описание);
- Уровень сообщения – наименование категории, к которой относится сообщение. Возможные значения: Отладка (debug), Информация (info), Предупреждение (warn), Ошибка (error).

9.2.1.5 Вкладка "Метрики"

На вкладке доступны следующие визуализации метрической информации о "сработке" правила:

- скорость потока событий (см. «Рис. 123»):

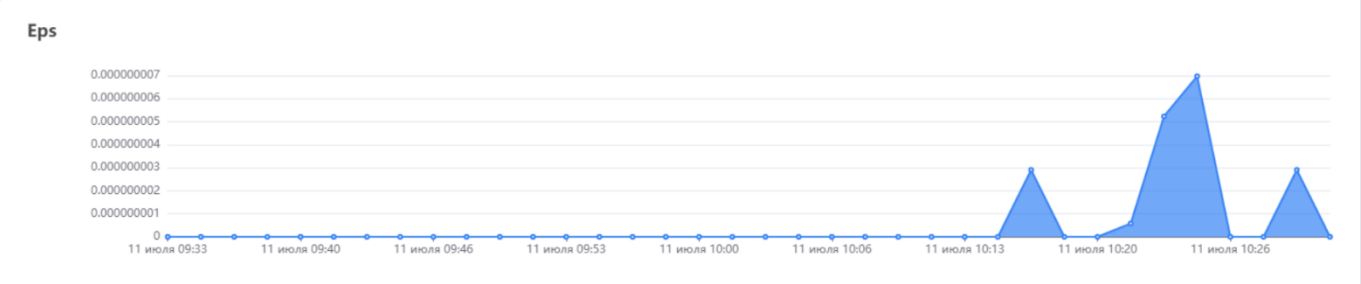


Рис. 123 – Метрика "EPS"

- задействованная память (см. «Рис. 124»):

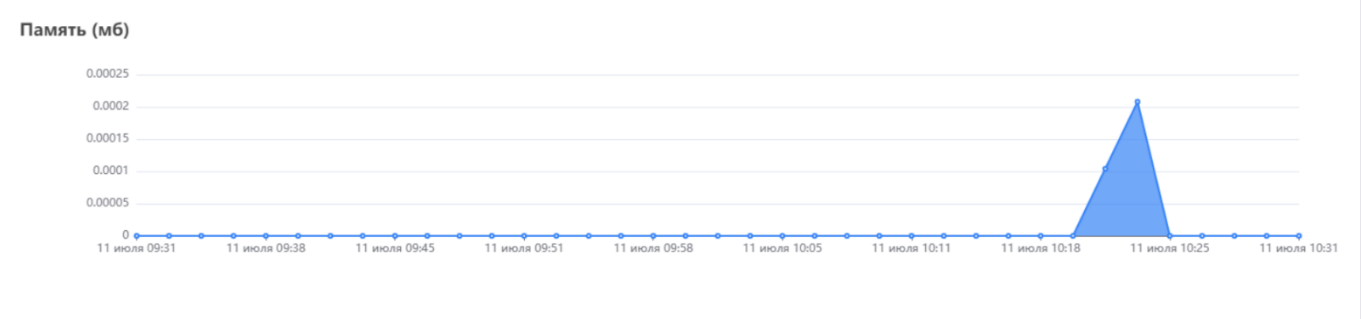


Рис. 124 – Метрика "Память"

- количество накопленных событий в группе (см. «Рис. 125»):

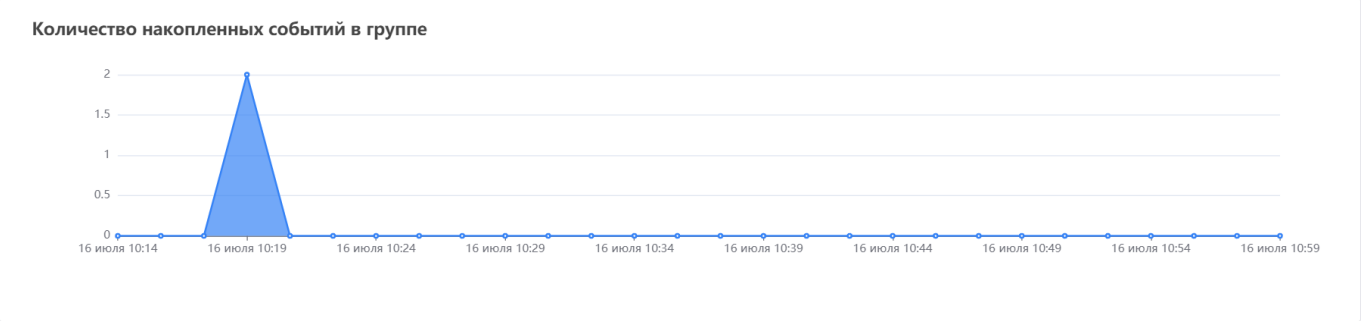


Рис. 125 – Метрика "Количество накопленных событий в группе"

- время выполнения функции *on_logline* (см. «Рис. 126»).

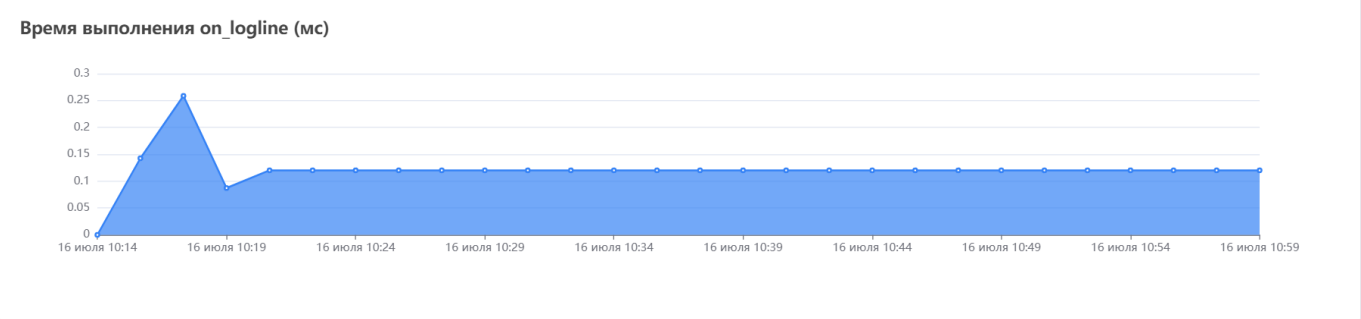


Рис. 126 – Метрика "Время выполнения on_logline"

- время выполнения функции *on_grouped* (см. «Рис. 127»).

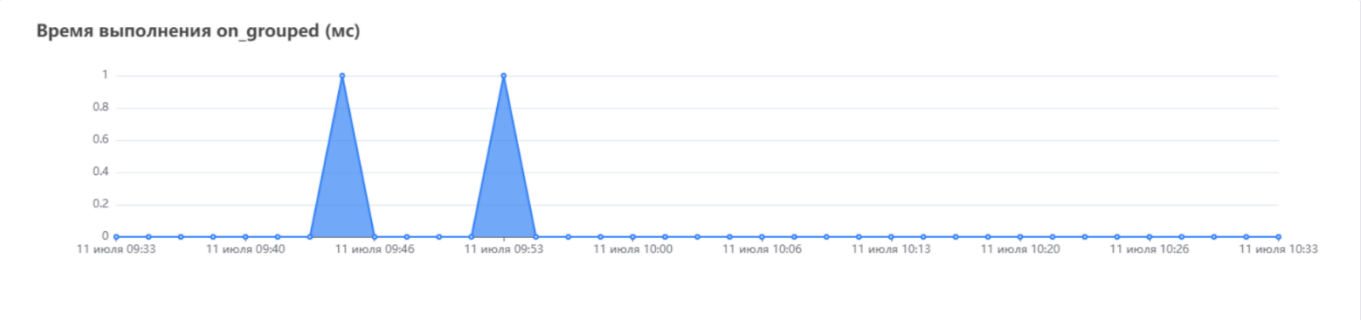


Рис. 127 – Метрика "Время выполнения on_grouped"

- количество ошибок, возникших во время "сработок" правила (см. «Рис. 128»).

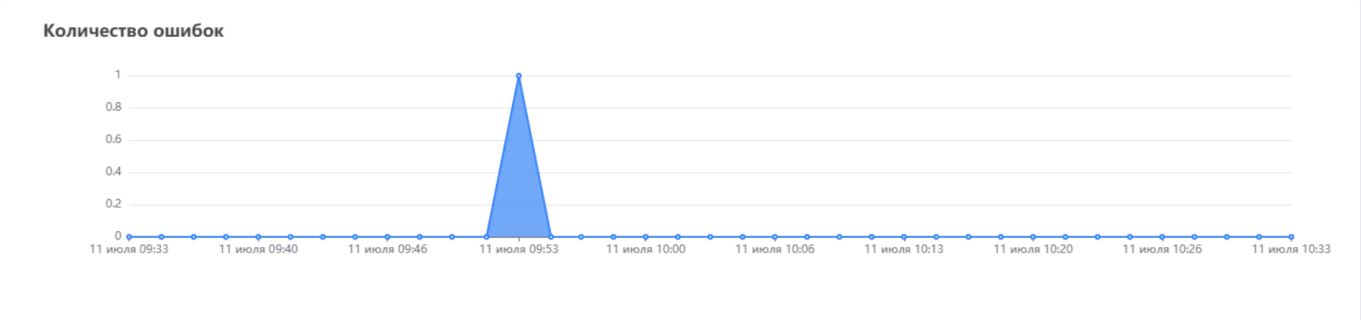


Рис. 128 – Метрика "Количество ошибок"

9.2.2 Создание и настройка правила

Создание правила можно выполнить двумя способами:

- с использованием визуального конструктора - при создании правила не используется скриптовый язык, само правило настраивается с помощью визуальных блоков. При необходимости вы всегда можете конвертировать подобное правило в скриптовый язык Lua (см. раздел «Конвертирование правила в код Lua»);
- помощью скриптового языка Lua - это позволяет использовать весь доступный функционал при написании правила.

9.2.2.1 Создание правила с помощью визуального конструктора

1. Нажмите кнопку  . Откроется окно "Добавить правило" (см. «Рис. 129»).

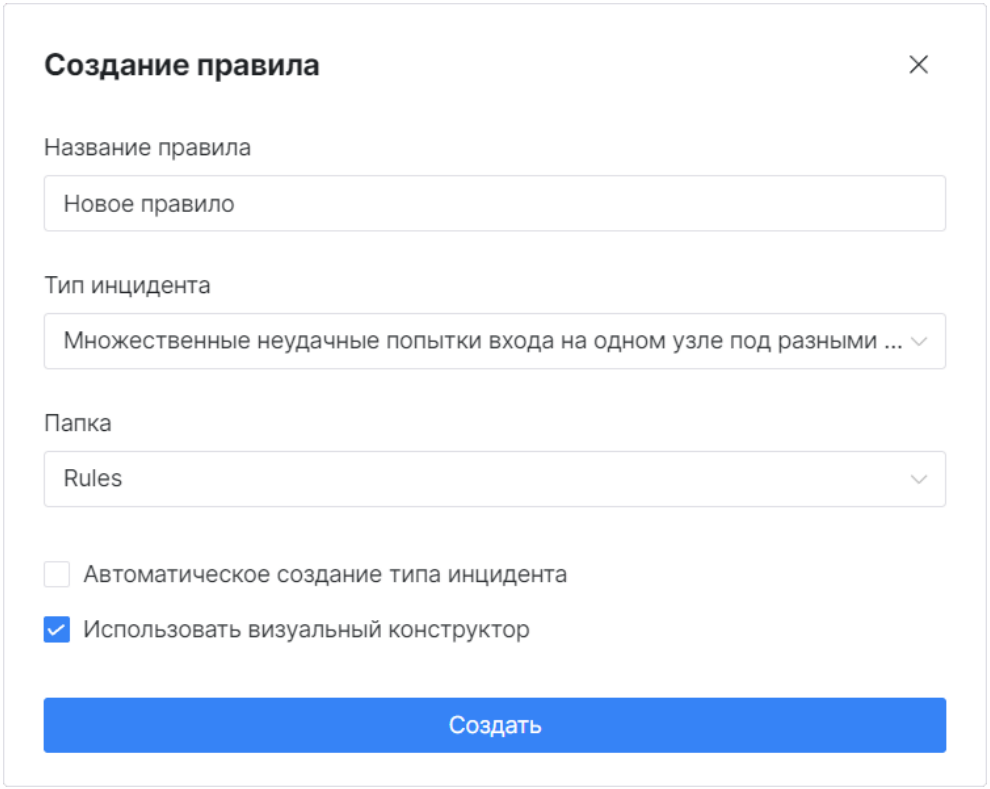


Рис. 129 – Окно "Добавить правило"

2. Укажите в окне следующую информацию:
    - в поле **Название правила** укажите название правила;
    - в поле **Тип инцидента** из выпадающего списка выберите тип инцидента;
    - в поле **Папка** из выпадающего списка выберите папку, в которую следует поместить правило после создания;
    - если исполняемое правило не относится ни к одному из типов инцидента или необходимо создать новый тип инцидента, то установите флаг **Автоматическое создание типа инцидента**. При создании инцидента на основе "сработки" данного правила, будет создан новый тип инцидента, которому будет присвоено наименование правила.

      Примечание: *если опция включена, то убедитесь, что наименование правила корреляции не совпадает ни с одним наименованием типа инцидента*.
    - установите флаг **Использовать визуальный конструктор**;
    - нажмите кнопку **Создать**.
3. Правило будет создано и автоматически откроется визуальный конструктор.
4. Выполните следующие шаги по настройке правила в визуальном конструкторе:
    - Шаг 1. Заполнение основной информации о правиле;
    - Шаг 2. Настройка фильтров потока;
    - Шаг 3. Настройка алерта;
    - Шаг 4. Настройка группера;

- Шаг 5. Настройка условий;
- Шаг 6. Настройка действий;
- Шаг 7. Тестирование правила.

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

9.2.2.1.1 Шаг 1. Заполнение основной информации о правиле

Заполнение основной информации о правиле выполняется на вкладке "Основное" (см. «Рис. 130»).

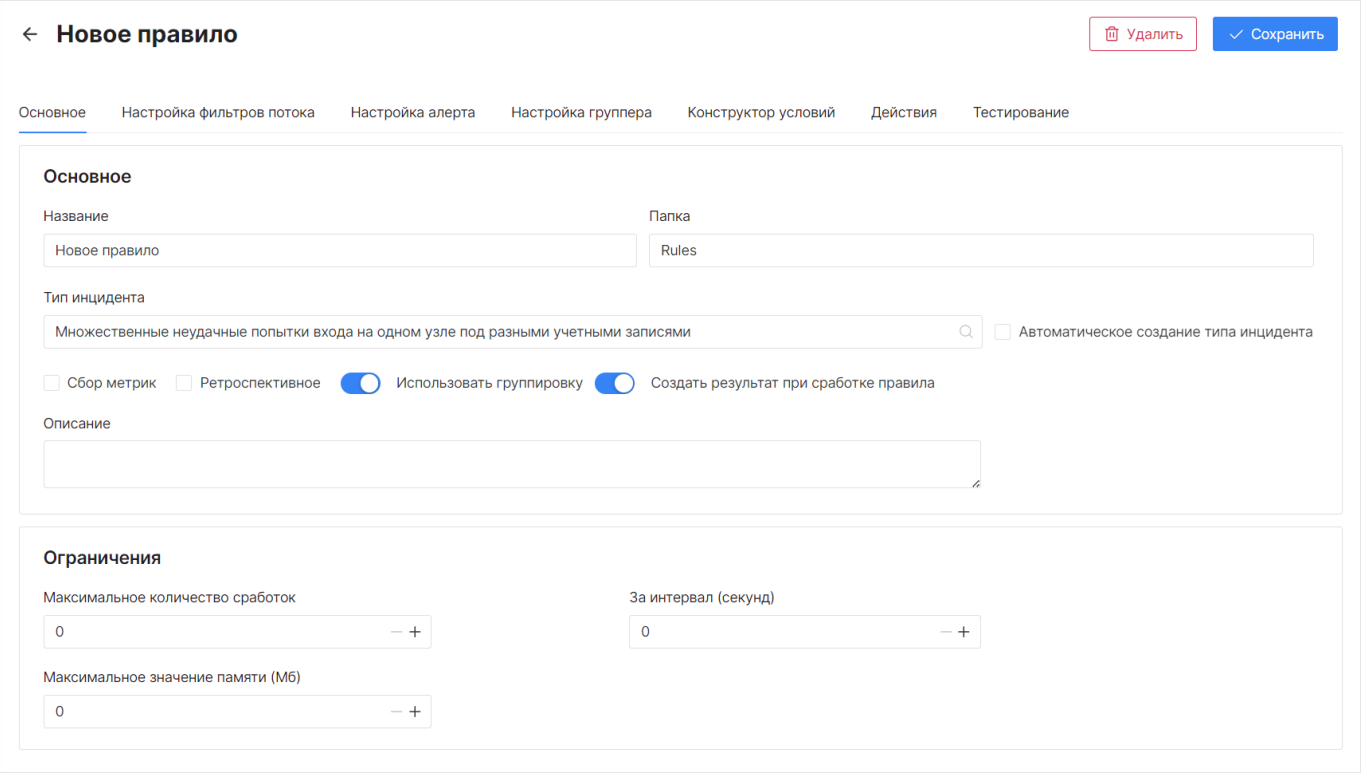


Рис. 130 – Настройка правила. Вкладка "Основное"

Укажите на вкладке следующую информацию:

- при необходимости уточните сведения, указанные в полях **Название, Папка** и **Тип инцидента**;
- для активации сбора дополнительных метрик по данному правилу установите флаг **Сбор метрик**;
- установите флаг **Ретроспективное**, если необходимо провести ретроспективный анализ по данному правилу (подробнее см. раздел «Ретроспективная корреляция»);
- выберите вид правила: линейное или с группировкой событий, установив переключатель **Использовать группировку** в соответствующее положение. Переключатель отвечает за доступность вкладки "Настройки группера";
- если правило при своей "сработке" должно создавать результат, то нужно установить переключатель **Создавать результат при сработке правила**, при этом открывается доступ к настройкам "алерта" где можно указать данные, которые будут сохранены в результате "сработки";

Примечание: "алерт" это функция правила коррелятора, записывающая результат сработки.

- в поле **Описание** укажите дополнительные сведения о правиле;
- в блоке **Ограничения** установите необходимые ограничения:
  - в поле **Максимальное количество сработок** и в поле **За интервал (секунд)** укажите максимальное количество "сработок", которое будет регистрироваться за период времени;
  - в поле **Максимальное значение памяти (Мб)** укажите максимальный допустимый объем памяти, который может использовать правило.

    Примечание: *для снятия ограничений укажите "0".*

9.2.2.1.2 Шаг 2. Настройка фильтров потока

Для работы правила в него необходимо добавить фильтр потока событий. Для этого перейдите на вкладку "Настройка фильтров потока" (см. «Рис. 131»).

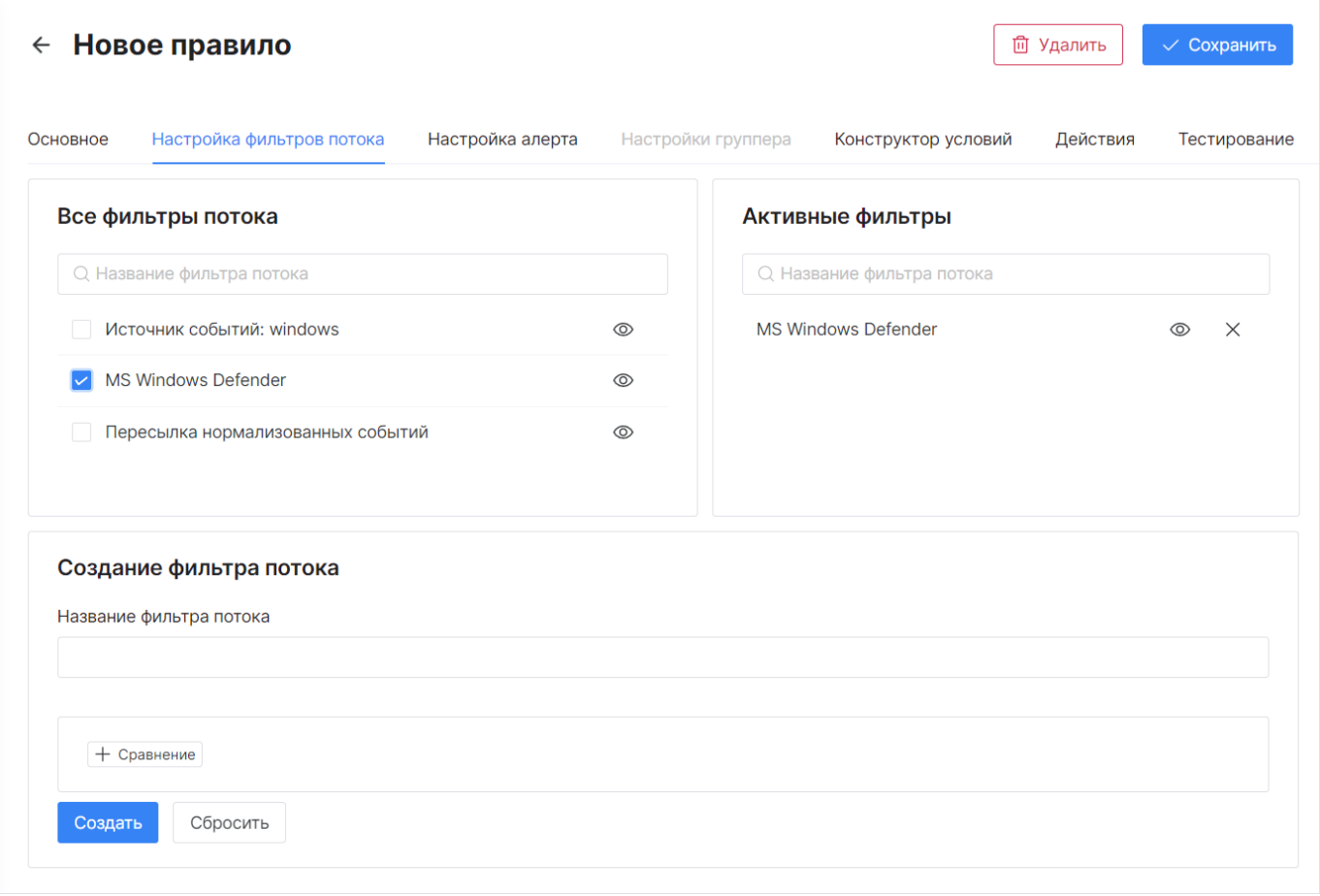


Рис. 131 – Настройка правила. Вкладка "Настройка фильтров потока"

Укажите на вкладке следующую информацию:

- в блоке **Все фильтры потока** выберите фильтры, которые необходимо добавить в правило. Список добавленных в правило фильтров будет отображаться в блоке **Активные фильтры**;
- для удобства настройки доступны следующие элементы управления:

- - просмотр подробной информации о выбранном фильтре;
- - удаление фильтра из правила.

При необходимости можно создать новый фильтр потока в блоке **Создание фильтров потока**. Инструкция по созданию фильтров потока описана в разделе «Фильтры потока событий».

9.2.2.1.3 Шаг 3. Настройка алерта

Если вы на первом шаге выбрали поведение: **Создавать результат при сработке правила**, то необходимо выполнить настройку на вкладке "Настройки алерта" (см. «Рис. 132»).

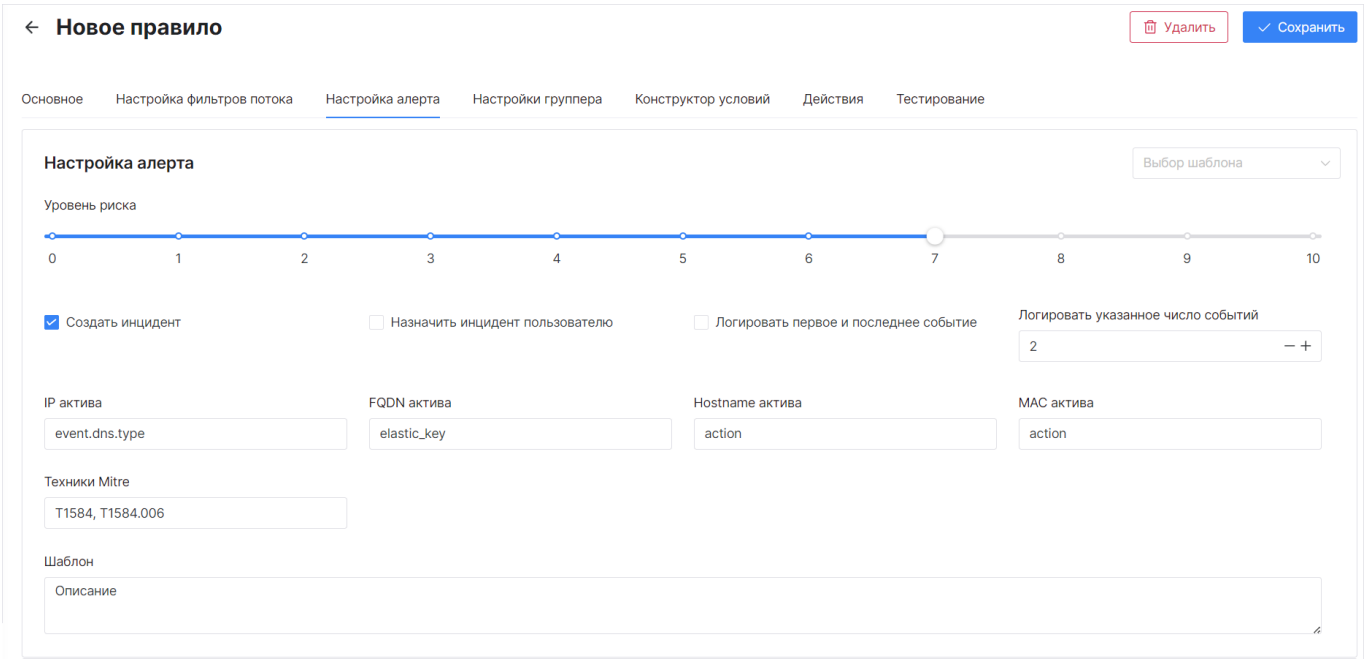


Рис. 132 – Настройка правила. Вкладка "Настройка алерта"

Укажите на вкладке следующую информацию:

- в поле **Уровень риска** выберите цифровое обозначение уровня риска, которое будет присвоено "сработке" правила;
- установите флаг **Создать инцидент** если необходимо автоматически создавать инцидент на основании "сработки" правила;
- установите флаг **Назначить инцидент пользователю** если необходимо автоматически назначать инцидент пользователю;
- выберите количество событий, которые необходимо записывать в журнал:
  - если вы хотите записывать только первое и последнее событие, то установите соответствующий флаг;
  - в обратном случае укажите необходимое значение в поле **Логировать указанное число событий**.
- в поле **IP актива** из выпадающего списка выберите поле, которое будет выступать в качестве IP-адреса актива. Поле может являться частью сводной таблицы событий;
- в поле **FQDN актива** из выпадающего списка выберите поле, которое будет выступать в качестве наименования домена актива. Поле может являться частью сводной таблицы событий;

- в поле **Hostname актива** из выпадающего списка выберите поле, которое будет выступать в качестве наименования хоста актива. Поле может являться частью сводной таблицы событий;
- в поле **MAC актива** из выпадающего списка выберите поле, которое будет выступать в качестве MAC-адреса актива. Поле может являться частью сводной таблицы событий;
- в поле **Техники Mitre** - укажите через запятую идентификаторы техник, используемых киберпреступниками, которые описаны в базе знаний компании Mitre (подробнее см. Techniques - Enterprise | MITRE ATT&CK®);
- в поле **Шаблон** укажите дополнительную информацию об "алерте".

Если у вас подготовлен шаблон, то в поле **Выберите шаблон** выберите шаблон из выпадающего списка. Все поля на вкладке будут заполнены данными из шаблона. Инструкция по созданию шаблонов "алертов" описана в разделе «Шаблоны алертов».

9.2.2.1.4 Шаг 4. Настройка группера

Если вы на первом шаге выбрали вид правила **С группировкой событий**, то необходимо выполнить настройку на вкладке "Настройка группера" (см. «Рис. 133»).

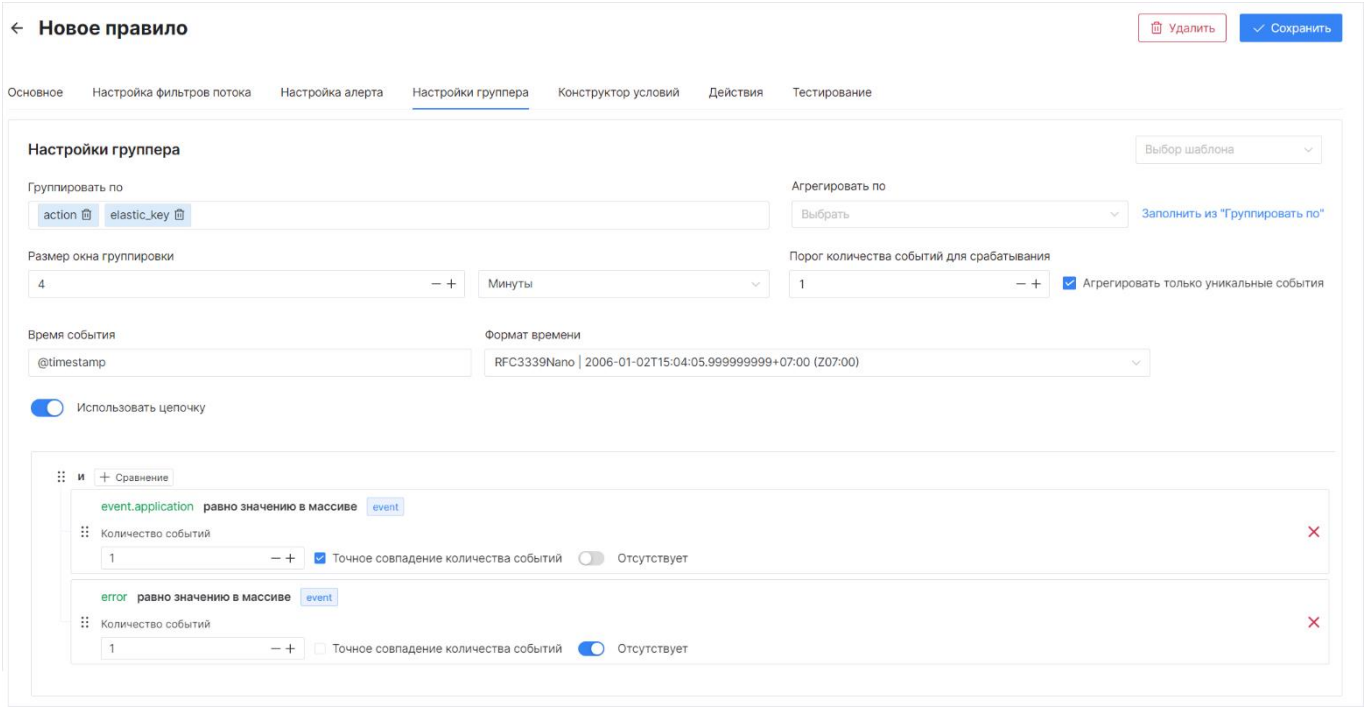


Рис. 133 – Настройка правила. Вкладка "Настройка группера"

Укажите на вкладке следующую информацию:

- в поле **Группировать по** из выпадающего списка выберите поле нормализованного события, по которому будет выполняться группировка. Можно выполнять группировку по нескольким полям;
- в поле **Агрегировать по** из выпадающего списка выберите поле нормализованного события, по которому будет выполняться функция агрегации. Можно выполнить агрегацию по нескольким полям;
- в поле **Размер окна группировки** укажите временной интервал, в течение которого будет выполняться группировка событий;

- в поле **Порог количества событий для срабатывания** укажите количество событий, по достижению которого в окне группировки, будет срабатывать правило;
- для агрегации только уникальных значений установите соответствующий флаг;
- в поле **Время события** из выпадающего списка выберите поле нормализованного события, по которому будет вычисляться время события;
- в поле **Формат времени** из выпадающего списка выберите формат времени события.

Платформа поддерживает возможность отслеживания и группировки подозрительных событий, следующих одно за другим (цепочки событий).

Для этого установите переключатель **Использовать цепочку** в положение "Включен" и выполните следующие действия:

1. Нажмите кнопку **+ Сравнение**. Откроется окно "Настроить условие" (см. «Рис. 134»).

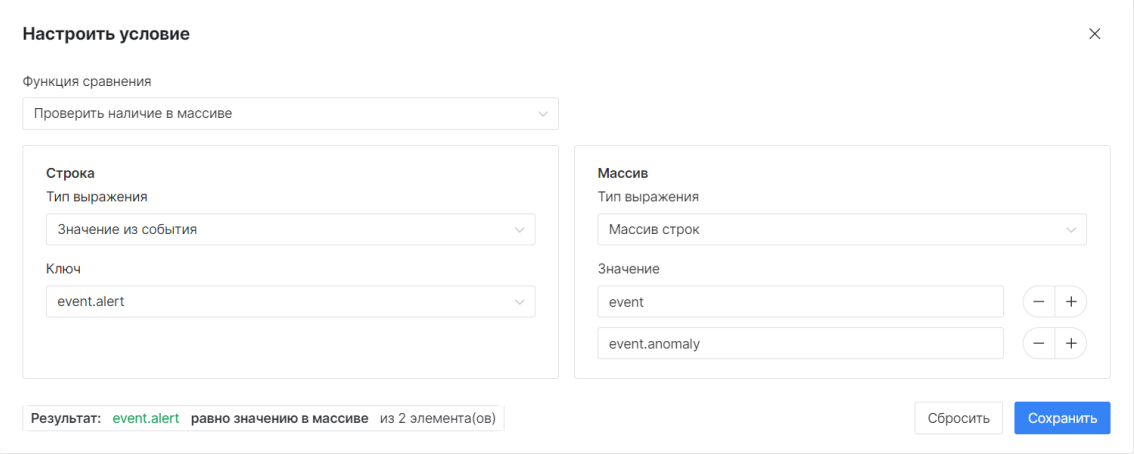


Рис. 134– Окно "Настроить условие"

2. Укажите в окне "Настроить условие" следующую информацию:
    - В поле **Функция сравнения** из выпадающего списка выберите функцию **Проверить наличие в массиве**;
    - В блоке **Строка** настройте первую часть выражения:
        - в поле **Тип выражения** выберите необходимый тип выражения, например "Значение из события";
        - в поле **Ключ** из выпадающего списка выберите поле нормализованного события, по которому будет выявляться цепочка событий.
    - В блоке **Массив** настройте вторую часть выражения:
        - в поле **Тип выражения** выберите необходимый тип выражения, например "Массив строк";
        - в поле **Значение** укажите массив значений, по которым должно проверяться поле, указанное в поле **Ключ**.
    - В блоке **Результат** проверьте правильность заданного выражения;
    - Нажмите кнопку **Сохранить.**
3. Добавьте необходимое количество условий цепочки событий.

4. Настройте дополнительные параметры поведения для добавленных условий цепочки событий (см. «Рис. 135»):

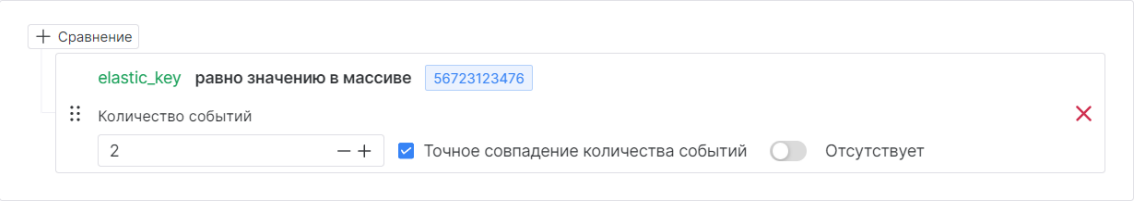


Рис. 135 – Параметры условий цепочки событий

- в поле **Количество событий** укажите минимальное количество найденных событий, подходящих под условие для "сработки" правила;
- для включения проверки строго соответствия количества событий установите флаг **Точное совпадение количества событий**;
- для отключения проверки по выбранному условия установите переключатель **Отсутствует** в положение "Включен".

Если у вас подготовлен шаблон, то в поле **Выберите шаблон** выберите шаблон из выпадающего списка. Все поля на вкладке будут заполнены данными из шаблона. Инструкция по созданию шаблонов группировки описана в разделе «Шаблоны группировки».

9.2.2.1.5 Шаг 5. Настройка условий

Настройка условий "сработки" правила выполняется на вкладке "Конструктор условий" (см. «Рис. 136»).

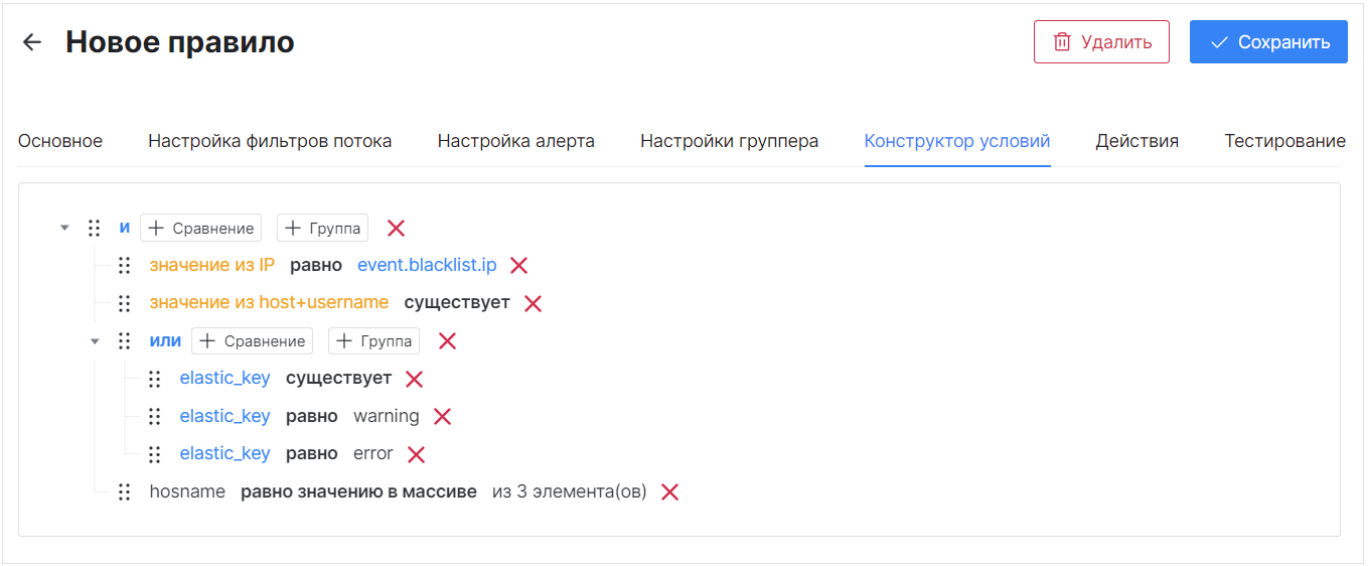


Рис. 136 – Настройка правила. Вкладка "Конструктор условий"

Конструктор представляет из себя набор условий в иерархическом виде.

Правило срабатывает, когда выполнены условия в соответствии с заданной логикой.

В условиях задается сравнение выбранного поля (в **первой** части условия) с указанным значением (во **второй** части условия).

В качестве значения для **первой** и **второй** части условия в общем случае можно указать следующие параметры:

- **Значение из события** - выбор из списка полей нормализованного события;
- **Значение из табличного списка** - выбор из полей существующего табличного списка;
- **Количество записей в табличном списке** - выбор табличного списка из доступных, в котором будет подсчитано количество записей;
- **Ручной ввод строки** - произвольное выражение;
- **Целое число** - в значении указывается целое число;
- **Дробное число** - в значении указывается дробное число;
- **Логическое значение** - выбор из следующих вариантов: "*ложь*" или "*истина*";
- **IP** - в значении указывается IP-адрес;
- **CIDR** - в значении указывается IP-адрес в подсети, указанный в табличном списке;
- **Дата** - указывается дата и время;
- **Отсутствие значения** - значение для сравнения не указывается.

Примечание доступные параметры для **первой** и **второй** части условия формируются в зависимости от выбранной функции сравнения.

При настройке сравнения используются следующие функции:

- **Проверить равенство выражений** (оператор "*равно*") - проверяется полное равенство поля указанному значению. При равенстве поля указанному значению условие считается выполненным.

Для данной функции доступна возможность не учитывать регистр для строковых значений.

- **Проверить наличие значения** (оператор "*существует*") - проверяется существование поля. При существовании поля условие считается выполненным.
- **Проверить значение в массиве** (оператор "*равно значению в массиве*") - осуществляется поиск указанного значения поля в массиве. При успешном поиске условие считается выполненным.
- **Элемент массива должен иметь подстроку** (оператор "*является подстрокой элемента массива*") - проверяется вхождение значения поля в строку в указанном массиве.
- **Один элемент массива должен начинаться с подстроки** (оператор "*является префиксом элемента массива*") - проверяется вхождение значения поля в начало строки каждого элемента массива.
- **Один элемент массива должен заканчиваться на подстроку** (оператор "*является суффиксом элемента массива*") - проверяется вхождение значения поля в конец строки каждого элемента массива.
- **Поиск подстроки в строке** (оператор "*имеет подстроку*") - проверяется вхождение подстроки в выбранное поле.
- **Строка должна проходить regexp** (оператор "*проходит regexp*") - проверяется проверка соответствия поля регулярному выражению.

- **Первое значение больше второго** (оператор "*больше*") - сравнивается поле и указанное значение. Если поле больше значения, условие считается выполненным.
- **Первое значение больше или равно второму** (оператор "*больше или равно*") - сравнивается поле и указанное значение. Если поле больше или равно значению, условие считается выполненным.
- **Первое значение меньше второго** (оператор "*меньше*") - сравнивается поле и указанное значение. Если поле меньше значения, условие считается выполненным.
- **Первое значение меньше или равно второму** (оператор "*меньше или равно*") - сравнивается поле и указанное значение. Если поле меньше или равно значению, условие считается выполненным.
- **Строка начинается с подстроки** (оператор "*начинается с*") - проверяется наличие указанного значения в начале выбранного поля.
- **Строка заканчивается на подстроку** (оператор *"заканчивается на"*) - проверяется наличие указанного значения в конце выбранного поля.
- **Поиск значения в табличном списке** (оператор "*находит*") - проверяется наличие указанного значения в выбранной колонке табличного списка.

Для данной функции доступна возможность не учитывать регистр для строковых значений.

- **Поиск IP в табличном списке** (оператор "*находит*") - проверяется наличие указанного значения IP-адреса в выбранной колонке табличного списка.
- **Значение должно быть в диапазоне** (оператор "*находится между*") - сравнивается поле и указанный диапазон значений. Если поле входит в диапазон, условие считается выполненным.

Для каждой функции можно включить **отрицание**: "не равно", "не существует" и т.д.

Созданные условия можно сгруппировать по следующим операторам:

- **И** - группа условий выполняется и правило срабатывает, только если выполнены все условия в группе;
- **ИЛИ** - группа условий выполняется и правило срабатывает, если хотя бы выполнено одно условие в группе;

На вкладке доступны следующие элементы управления:

Кнопка	**Действие**
+ Сравнение	добавление условия сравнения
+ Группа	добавление группы условий
Обернуть в группу	добавление условия сравнения в группу
	изменение порядка условий сравнения
	удаление условия сравнения из правила

Кнопка	Действие
Нажатие ЛКМ на оператор **И**, **ИЛИ**	настройка поведения для выбранной группы условий
Нажатие ЛКМ на строку условия	редактирование выбранного условия

Для добавления условия выполните следующие действия:

1. Нажмите на кнопку + Сравнение. Откроется окно "Настроить условие" (см. «Рис. 137»).

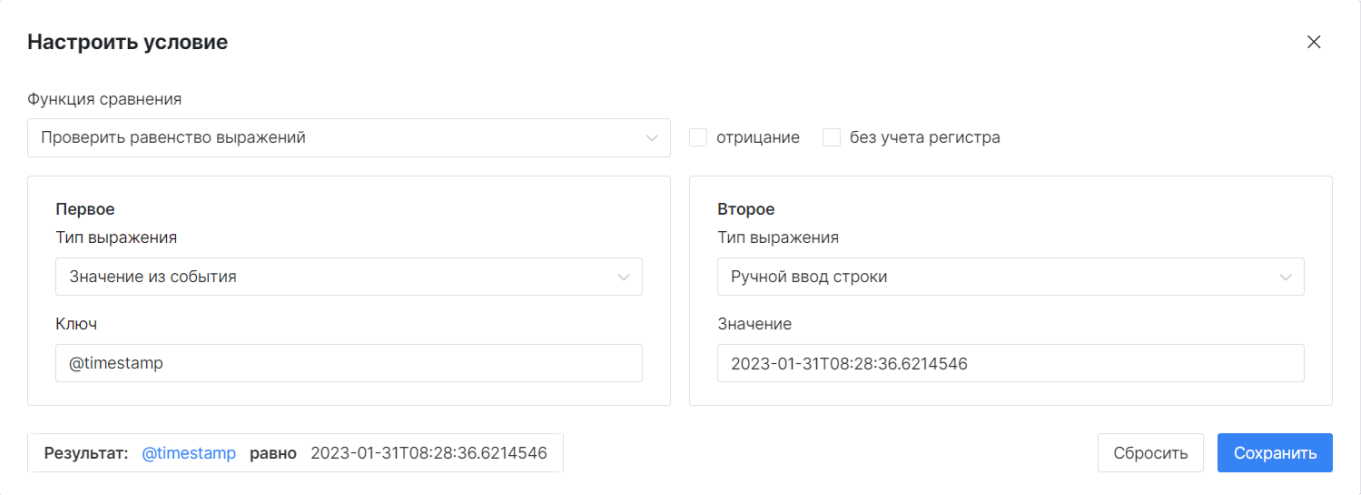


Рис. 137 – Окно "Настроить условие". Пример "Проверить равенство выражений"

2. Выберите в окне функцию сравнения и тип выражения в соответствующих блоках. Будут сформированы поля в зависимости от выбранных значений.
3. В сформированных полях укажите соответствующую информацию.
4. Если необходимо выполнить операцию "отрицание", то установите соответствующий флаг.
5. В блоке **Результат** проверьте правильность заданного выражения.
6. Нажмите кнопку **Сохранить.**
7. Добавьте необходимое количество условий в правило.

Для добавления группы условий выполните следующие действия:

1. Нажмите на кнопку + Группа. Откроется окно "Настроить условие" (см. «Рис. 138»).

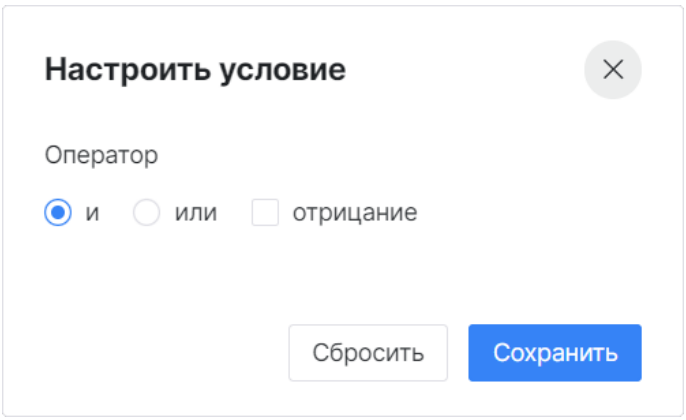


Рис. 138 – Добавление группы. Окно "Настроить условие"

2. Выберите оператор.
3. Если необходимо выполнить операцию "отрицание", то установите соответствующий флаг.
4. Нажмите кнопку **Сохранить**.

9.2.2.1.6 Шаг 6. Настройка действий

При необходимости вы можете настроить действия над табличными списками при "сработке" правила.

Доступны следующие действия:

- установить значение в табличном списке;
- удалить запись из табличного списка;
- очистка табличного списка.

Все действия выполняются последовательно.

В привило можно добавить неограниченное количество действий.

Настройка действий над табличными списками выполняется на вкладке "Действия" (см. «Рис. 139»).

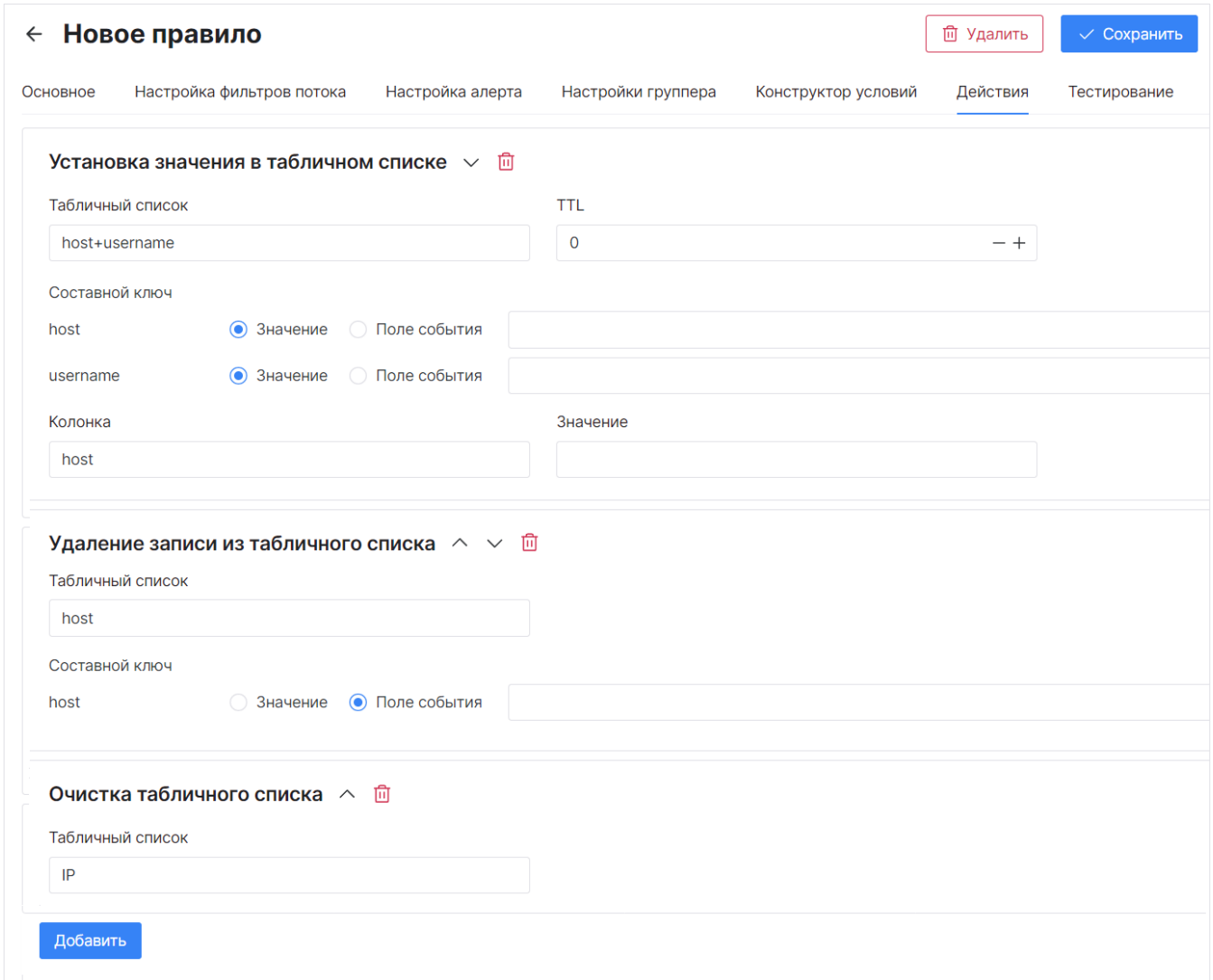


Рис. 139 – Настройка правила. Вкладка "Действия"

Для добавления действия над табличным списком нажмите кнопку **Добавить** и укажите информацию в соответствии с выбранным действием:

- **Установка значения в табличном списке**:
  - в поле **Табличный список** из выпадающего списка выберите табличный список;
  - в поле **TTL** укажите размер окна времени отбора в миллисекундах. События старше указанного времени не будут отбираться для установки значения. Значение "*0*" - без ограничения;
  - в поле **Составной ключ** выберите способ формирования ключа: "*по значению*" или по "*полю события*";
  - в поле **Колонка** из выпадающего списка выберите колонку, в которую будет устанавливаться значение;
  - в поле **Значение** укажите значение, которое будет устанавливаться в соответствующую колонку табличного списка.
- **Удаление записи из табличного списка**:
  - в поле **Табличный список** выберите табличный список, из которого будут удаляться значения;
  - в поле **Составной ключ** укажите ключ, по которому будут удаляться значения.
- **Очистка табличного списка** -- в поле **Табличный список** выберите табличный список, который будет очищаться при "сработке" правила.

9.2.2.1.7 Шаг 7. Тестирование правила

При тестировании правил используется тестовый набор (массив), состоящий из "логлайнов". "Логлайн" это непосредственно само событие, представленное в формате JSON.

Тестирование правила выполняется на вкладке "Тестирование" (см. «Рис. 140»).

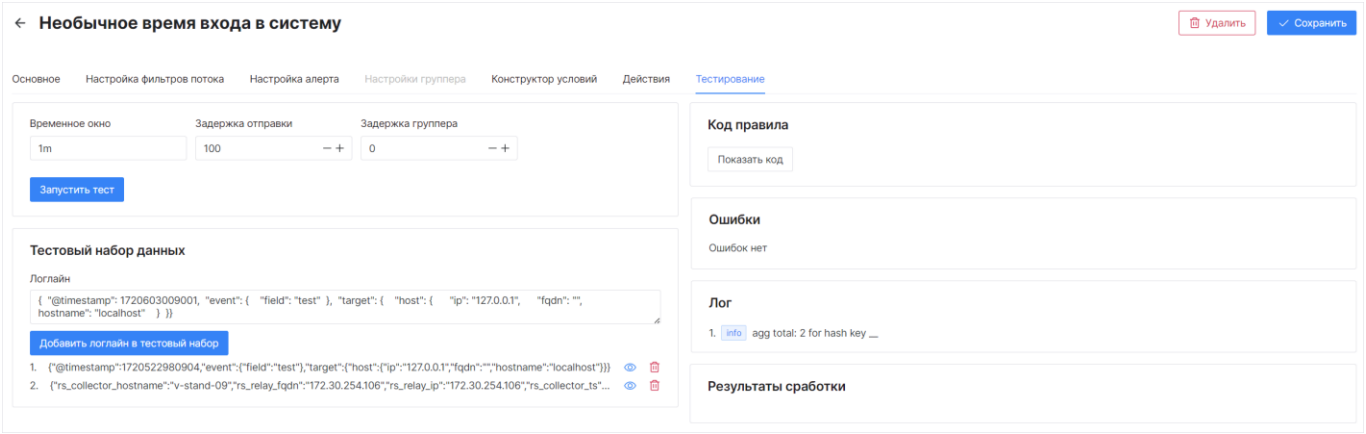


Рис. 140 – Настройка правила. Вкладка "Тестирование"

Для проведения тестирования выполните следующие действия:

1. Укажите на вкладке следующую информацию:
   - в поле **Временное окно** укажите размер временного окна выполнения правила корреляции;

- в поле **Задержка отправки** укажите время задержки отправки событий;
- в поле **Задержка группера** укажите время задержки работы группера;
- все значения задаются в миллисекундах.

2. Нажмите кнопку **Запустить тест**. Будут сформированы результаты проверки правила:
   - в блоке **Код правила** можно посмотреть код правила;
   - в блоке **Ошибки** будет выведен список выявленных ошибок;
   - в блок **Лог** отображается журнал выполнения тестирования;
   - в блоке **Результаты сработки** будет выведен список "сработок" правила.
3. При необходимости вы можете сформировать тестовый набор данных, который будет подаваться на вход правилу корреляции при выполнении тестирования. Для этого в блоке **Тестовый набор данных** укажите логлайн и нажмите кнопку **Добавить логлайн в тестовый набор**. Для управления логлайнами используйте следующие элементы управления:
   - - просмотр подробной информации о выбранном логлайне;
   - - удаление логлайна из тестового набора данных.

9.2.2.2 Создание правила с помощью скриптового языка Lua

1. Нажмите кнопку . Откроется окно "Добавить правило" (см. «Рис. 141»).

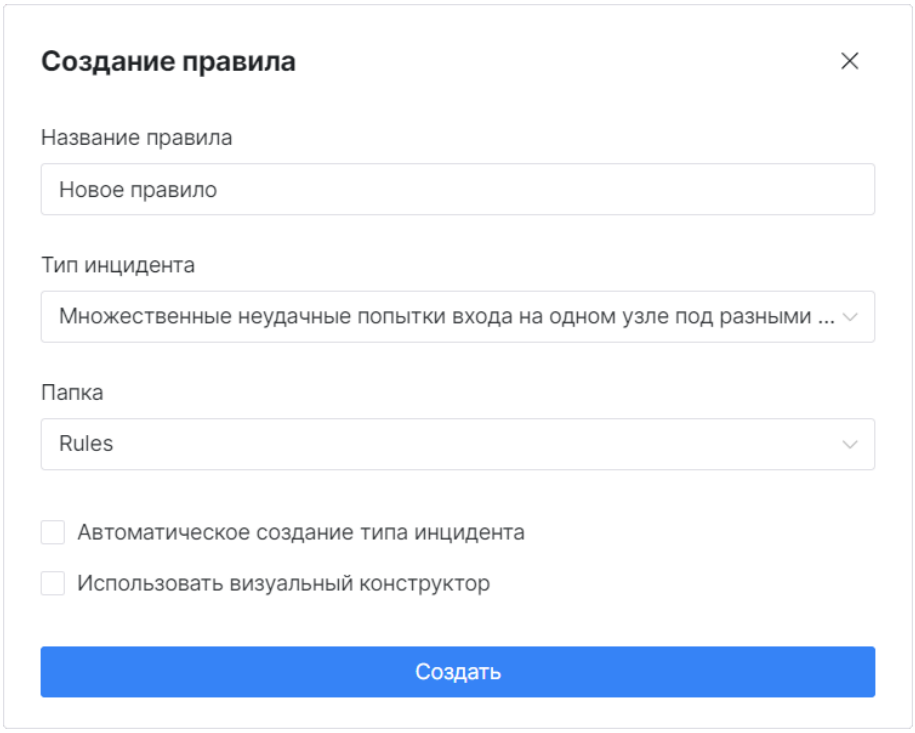


Рис. 141 – Окно "Добавить правило"

2. Укажите в окне следующую информацию:
   - в поле **Название правила** укажите название правила;
   - в поле **Тип инцидента** из выпадающего списка выберите тип инцидента;

- в поле **Папка** из выпадающего списка выберите папку, в которую следует поместить правило после создания;
- если исполняемое правило не относится ни к одному из типов инцидента или необходимо создать новый тип инцидента, то установите флаг **Автоматическое создание типа инцидента**. При создании инцидента на основе "сработки" данного правила, будет создан новый тип инцидента, которому будет присвоено наименование правила.

  Примечание: *если опция включена, то убедитесь, что наименование правила корреляции не совпадает ни с одним наименованием типа инцидента*.
- не устанавливайте флаг **Использовать визуальный конструктор**;
- нажмите кнопку **Создать**.

3. Правило будет создано и автоматически откроется визуальный конструктор для настройки.
4. Выполните следующие шаги по настройке правила в визуальном конструкторе:
   - Шаг 1. Заполнение основной информации о правиле;
   - Шаг 2. Настройка фильтров потока;
   - Шаг 3. Настройка кода правила;
   - Шаг 4. Настройка макросов;
   - Шаг 5. Тестирование работы правила.
5. После выполнения всех шагов нажмите кнопку **Сохранить**.

9.2.2.2.1 Шаг 1. Заполнение основной информации о правиле

Заполнение основной информации о правиле выполняется на вкладке "Основное" (см. «Рис. 142»).

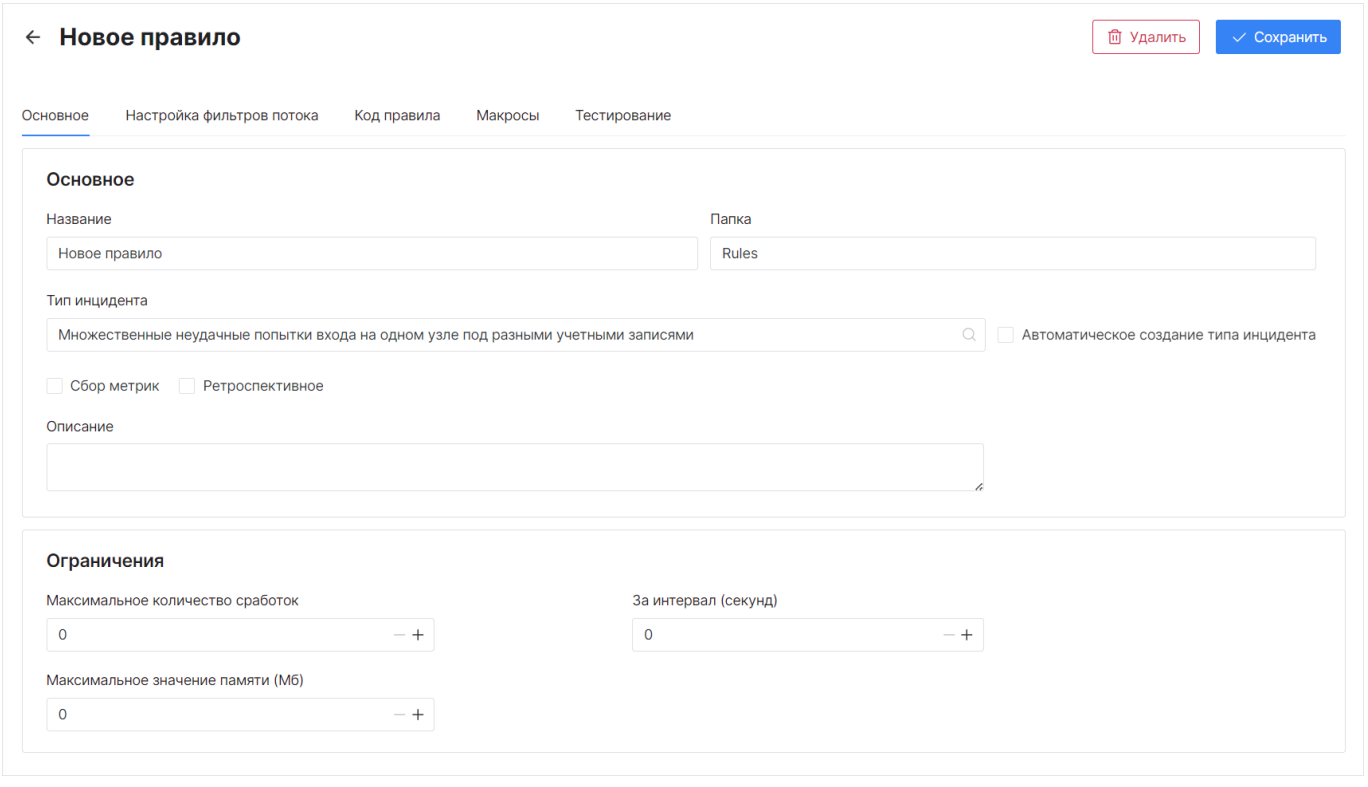


Рис. 142 – Настройка правила на скриптовом языке Lua. Вкладка "Основное"

Укажите на вкладке следующую информацию:

- при необходимости уточните сведения, указанные в полях **Название** и **Тип инцидента**;
- в полях **Ограничение кол-во сработок в сек** и **Ограничение памяти (Мб)** установите необходимые ограничения;
- для активации сбора дополнительных метрик по данному правилу установите флаг **Сбор метрик**;
- установите флаг **Ретроспективное**, если необходимо провести ретроспективный анализ по данному правилу (подробнее см. раздел «Ретроспективная корреляция»);
- в поле **Описание** укажите дополнительные сведения о правиле;
- в блоке **Ограничения** установите необходимые ограничения:
  - в поле **Максимальное количество сработок** и в поле **За интервал (секунд)** укажите максимальное количество "сработок", которое будет регистрироваться за период времени;
  - в поле **Максимальное значение памяти (Мб)** укажите максимальный допустимый объем памяти, который может использовать правило.

    Примечание: *для снятия ограничений укажите "0".*

9.2.2.2.2 Шаг 2. Настройка фильтров потока

Для работы правила в него необходимо добавить фильтр потока событий. Для этого перейдите на вкладку "Настройка фильтров потока" (см. «Рис. 143»).

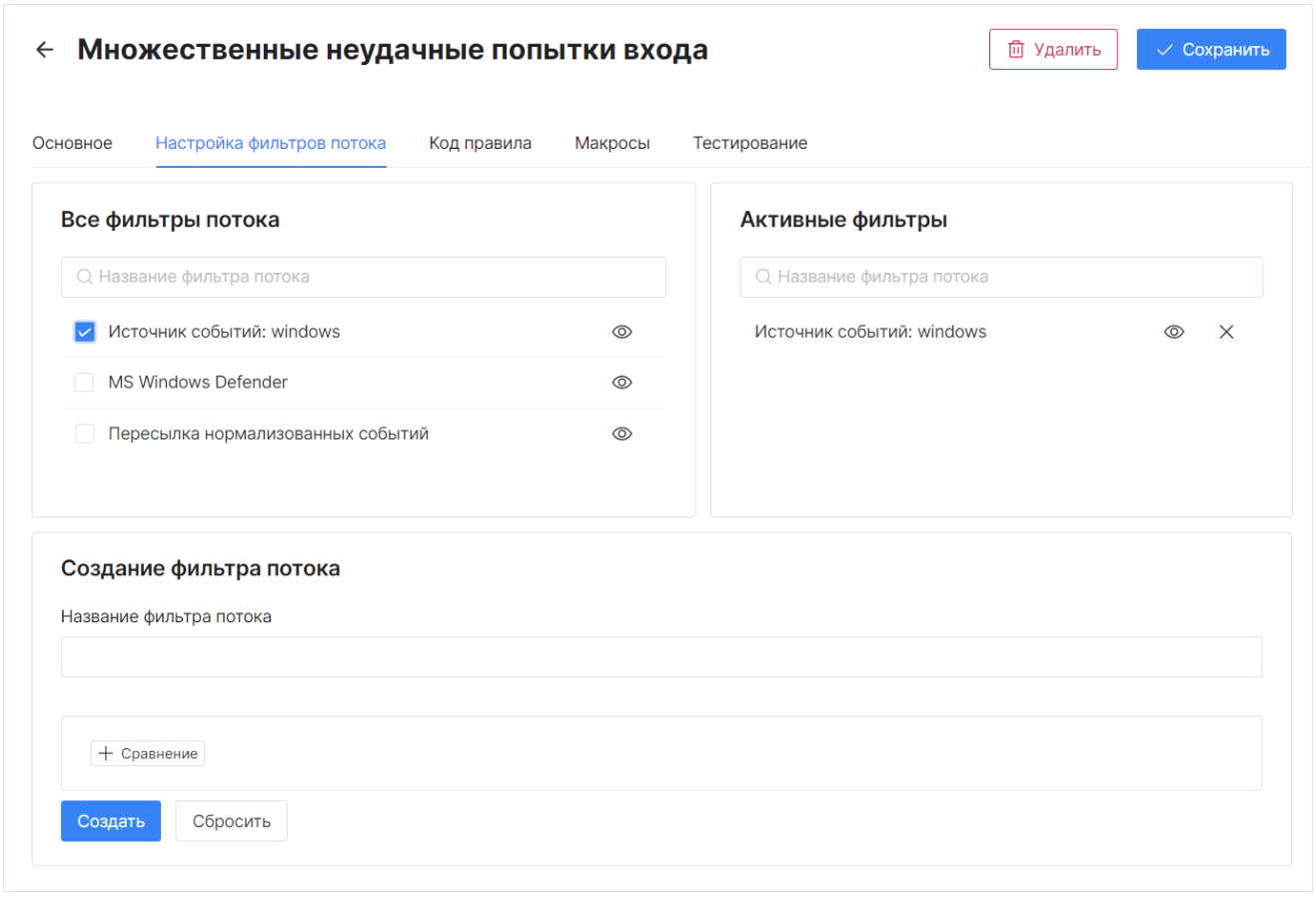


Рис. 143 – Настройка правила на скриптовом языке Lua. Вкладка "Настройка фильтров потока"

Укажите на вкладке следующую информацию:

- в блоке **Все фильтры потока** выберите фильтры, которые необходимо добавить в правило. Список добавленных в правило фильтров будет отображаться в блоке **Активные фильтры**;
- для удобства настройки доступны следующие элементы управления:
  - - просмотр подробной информации о выбранном фильтре;
  - - удаление фильтра из правила.

При необходимости можно создать новый фильтр потока в блоке **Создание фильтров потока**. Инструкция по созданию фильтров потока описана в разделе «Фильтры потока событий».

9.2.2.2.3 Шаг 3. Настройка кода правила

На данном шаге выполняются основные настройки правила с помощью скриптового языка Lua.

Для настройки кода правила перейдите на вкладку "Код правила" и укажите соответствующий код (см. «Рис. 144»).

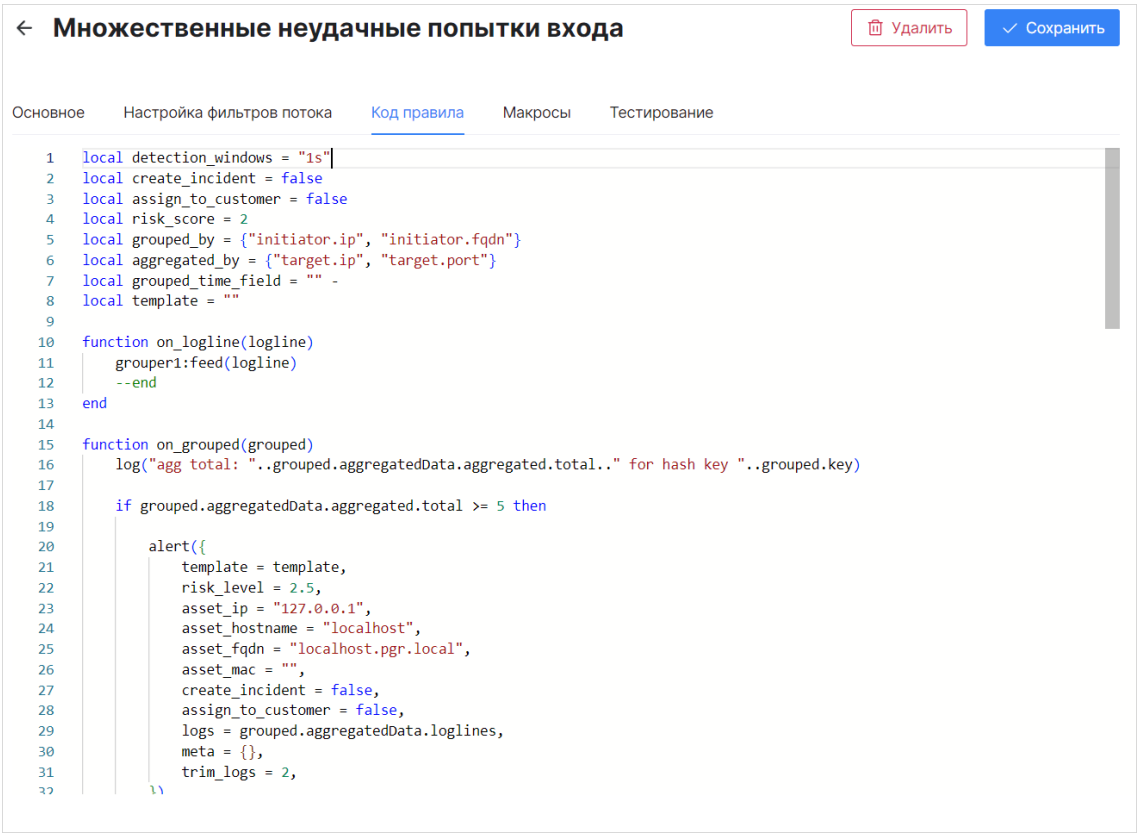


Рис. 144 – Настройка правила на скриптовом языке Lua. Вкладка "Код правила"

9.2.2.2.4 Шаг 4. Настройка макросов

При необходимости использовать один и тот же код в разных правилах корреляции, можно подключить соответствующий макрос

Подключение макросов выполняется на вкладке "Макросы" (см. «Рис. 145»).

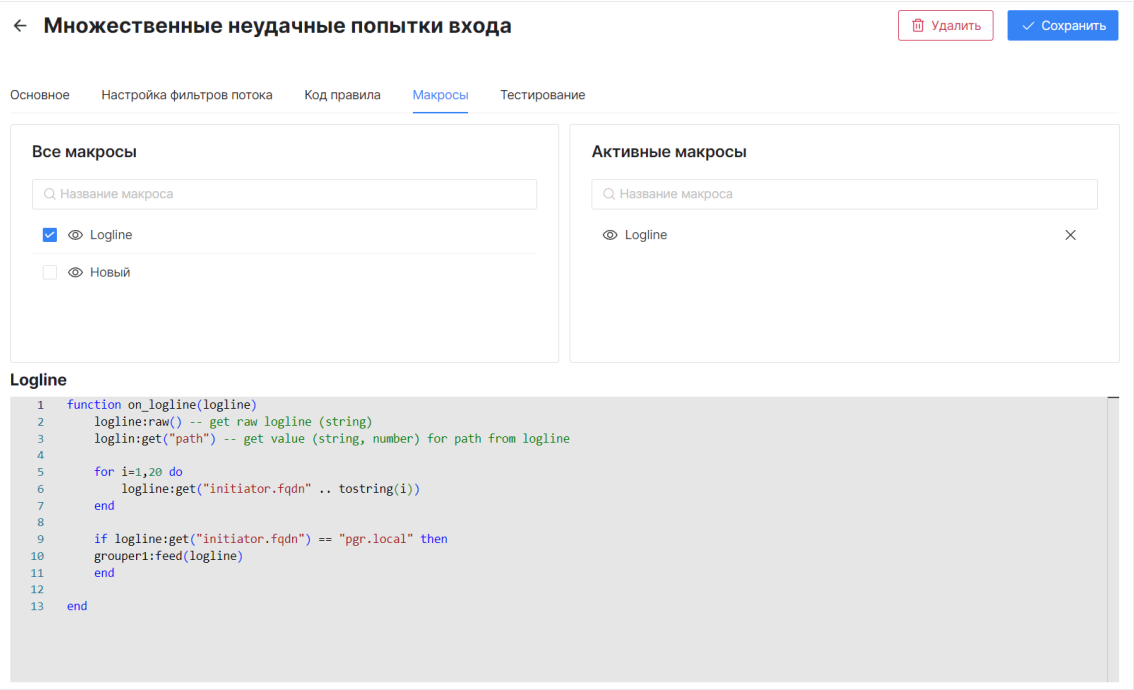


Рис. 145 – Настройка правила на скриптовом языке Lua. Вкладка "Макросы"

Укажите на вкладке следующую информацию:

- в блоке **Все макросы** выберите макросы, которые необходимо добавить в правило. Список добавленных в правило макросов будет отображаться в блоке **Активные макросы**;
- для удобства настройки доступны следующие элементы управления:
  - - просмотр подробной информации о выбранном макросе;
  - - удаление макроса из правила.

Инструкция по созданию макросов описана в разделе «Макросы».

9.2.2.2.5 Шаг 5. Тестирование работы правила

При тестировании правил используется тестовый набор (массив), состоящий из "логлайнов". "Логлайн" это непосредственно само событие, представленное в формате JSON.

Тестирование правила выполняется на вкладке "Тестирование" (см. «Рис. 146»).

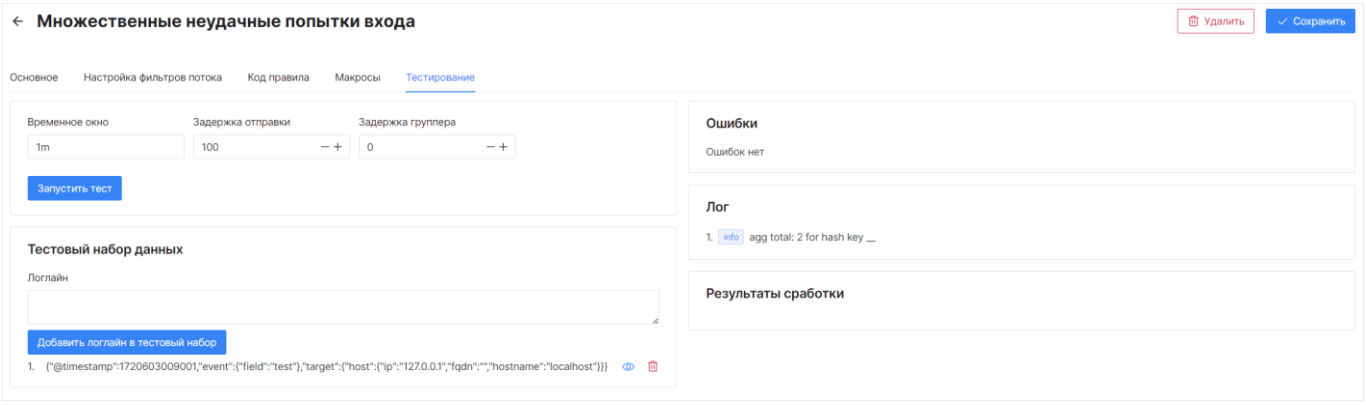


Рис. 146 – Настройка правила на скриптовом языке Lua. Вкладка "Тестирование"

Для проведения тестирования выполните следующие действия:

1. Укажите на вкладке следующую информацию:
    - в поле **Временное окно** укажите размер временного окна выполнения правила корреляции;
    - в поле **Задержка отправки** укажите время задержки отправки событий;
    - в поле **Задержка группера** укажите время задержки работы группера;
    - все значения задаются в миллисекундах
2. Нажмите кнопку **Запустить тест**. Будут сформированы результаты проверки правила:
    - в блоке **Ошибки** будет выведен список выявленных ошибок;
    - в блок **Лог** отображается журнал выполнения тестирования;
    - в блоке **Результаты сработки** будет выведен список "сработок" правила.
3. При необходимости вы можете сформировать тестовый набор данных, который будет подаваться на вход правилу корреляции при выполнении тестирования. Для этого в блоке **Тестовый набор данных** укажите логлайн и нажмите кнопку **Добавить логлайн в тестовый набор**. Для управления логлайнами используйте следующие элементы управления:
    -  - просмотр подробной информации о выбранном логлайне;
    -  - удаление логлайна из тестового набора данных.

9.2.3 Редактирование правила

1. Выберите из списка необходимое правило и нажмите кнопку 

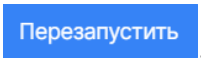
.
2. В зависимости от типа редактируемого правила (с использованием визуального редактора или без) внесите необходимые изменения на соответствующие вкладки.
3. Нажмите кнопку **Сохранить**.

9.2.4 Активация правила

1. Выберите из списка необходимое правило и установите переключатель 

в положение **Активное**.
2. Если в правиле были допущены ошибки, то платформа выдаст соответствующее предупреждение.
3. После активации правило включится в работу на потоке событий используя указанные фильтры. Если при инициализации правила произойдет какая-либо ошибка, то правило будет автоматически деактивировано.

9.2.5 Перезапуск правила

1. Выберите из списка необходимое правило и нажмите кнопку 

.
2. Подтвердите перезапуск в открывшемся окне.
3. Правило будет перезапущено.

9.2.6 Дублирование правила

1. Выберите из списка необходимое правило, нажмите кнопку  и из выпадающего списка выберите пункт **Дублировать**. Откроется окно "Дублировать правило" (см. «Рис. 147»).

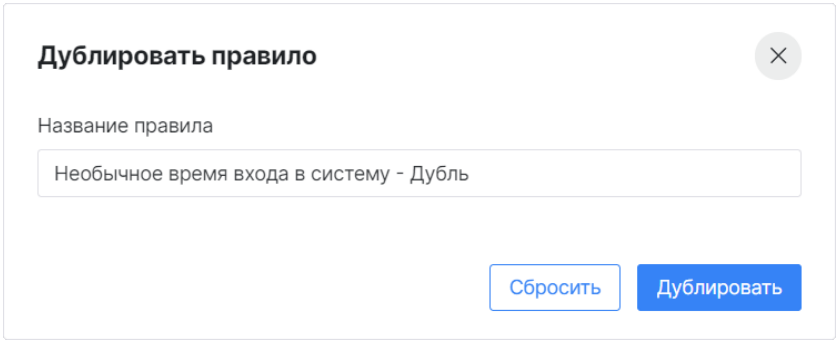


Рис. 147 – Окно "Дублировать правило"

2. Укажите в окне наименование правила.
3. Нажмите кнопку **Дублировать**.

9.2.7 Конвертирование правила в код Lua

При необходимости **Платформа Радар** позволяет конвертировать правила, созданные с помощью визуального конструктора, в скриптовой язык Lua.

Внимание! обратное конвертирование из Lua в визуальный режим не поддерживается, рекомендуется перед конвертированием продублировать правило (сделать резервную копию).

1. Выберите из списка правило, которое было создано с помощью визуального конструктора.
2. Нажмите кнопку  и из выпадающего списка выберите пункт **Конвертировать в Lua**.
3. Подтвердите конвертацию в открывшемся окне.

9.2.8 Импорт правил

1. Нажмите на кнопку  и из выпадающего списка выберите пункт **Импортировать**.
2. В открывшемся окне укажите путь к архиву с правилами.
3. Нажмите кнопку **Открыть**.

9.2.9 Экспорт правил

1. Нажмите на кнопку  и из выпадающего списка выберите пункт **Экспортировать все**.
2. Будет сформирован архив с правилами корреляции в формате `.zip`.
3. Нажмите кнопку **Скачать** и укажите путь для сохранения архива.

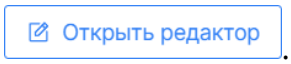
9.2.10 Удаление правила

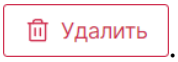
Удаление правила можно выполнить двумя способами.

Способ 1:

1. Выберите из списка необходимое правило, нажмите кнопку  и из выпадающего списка выберите пункт **Удалить**.
2. Подтвердите удаление в открывшемся окне.
3. Правило будет удалено из платформы.

Способ 2:

1. Выберите из списка необходимое правило, нажмите кнопку 

.
2. В окне редактирования правила нажмите кнопку 

.
3. Подтвердите удаление в открывшемся окне.
4. Правило будет удалено из платформы.

9.2.11 Массовые действия над правилами

Над правилами доступны следующие массовые действия:

- **Экспортировать** - экспорт выбранных правил;
- **Удалить** - удаление выбранных правил;
- **Удалить все** - удаление всех правил.

Для выполнения массового действия выполните следующие шаги:

1. Нажмите на кнопку  . Откроется список массовых операций и флаги для выбора правил (см. «Рис. 148»).

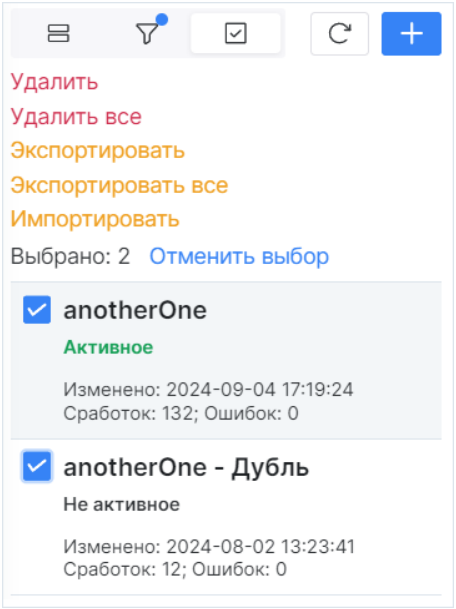


Рис. 148 – Массовые действия над правилами

2. Выберите правила корреляции.
3. Нажмите на соответствующую кнопку.
4. Завершите действие в открывшемся окне.

9.2.12 Действия над результатами сработок правила

9.2.12.1 Создание инцидента

1. Выберите из списка необходимое правило.
2. Перейдите на вкладку "Результаты".
3. Выберите из списка необходимую "сработку" правила и нажмите кнопку +.
4. Будет создан инцидент на основании "сработки" правила.

9.2.12.2 Просмотр события

1. Выберите из списка необходимое правило.
2. Перейдите на вкладку "Результаты".
3. Выберите из списка необходимую "сработку" правила и нажмите кнопку **Показать событие**. Откроется страница просмотра события (см. «Рис. 149»).

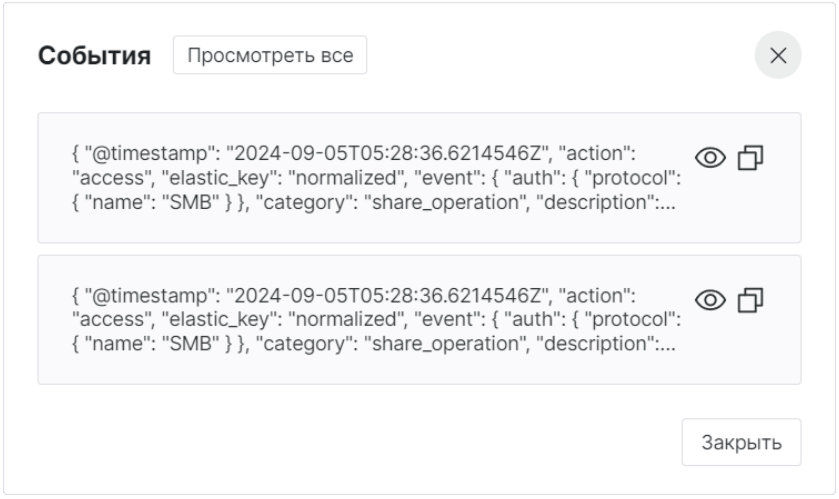


Рис. 149 – Просмотр события

4. Для просмотра события в разделе **Просмотр событий** нажмите кнопку , а для просмотра всех событий нажмите кнопку **Просмотреть все**. Откроется поток событий, который будет сформирован по соответствующему запросу.

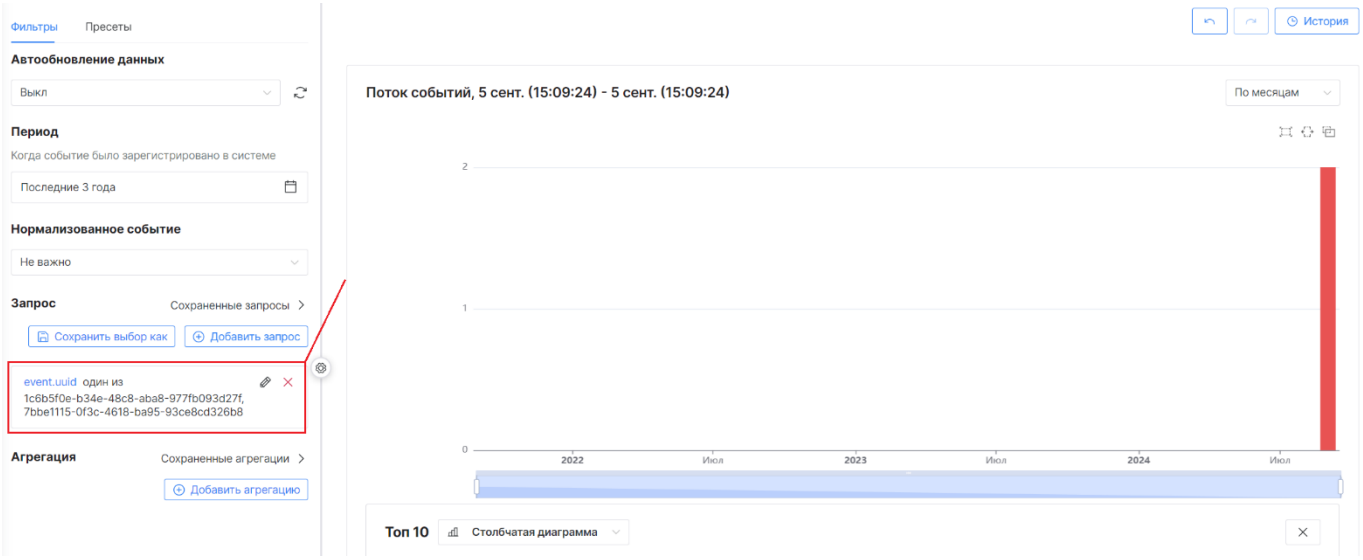


Рис. 150 – Просмотр потока событий по соответствующему запросу

9.3 Пересылка событий

9.3.1 Общие данные

Если **Платформа радар** работает в режиме мультиарендности, то вы можете настроить пересылку событий с одного экземпляра платформы на другой.

При включенной пересылке все события будут отправляться на другой узел.

За пересылку отвечает фильтр потока событий, не связанный с правилом корреляции. Подобный фильтр создается в разделе **Коррелятор → Пересылка событий** (см. «Рис. 151»).

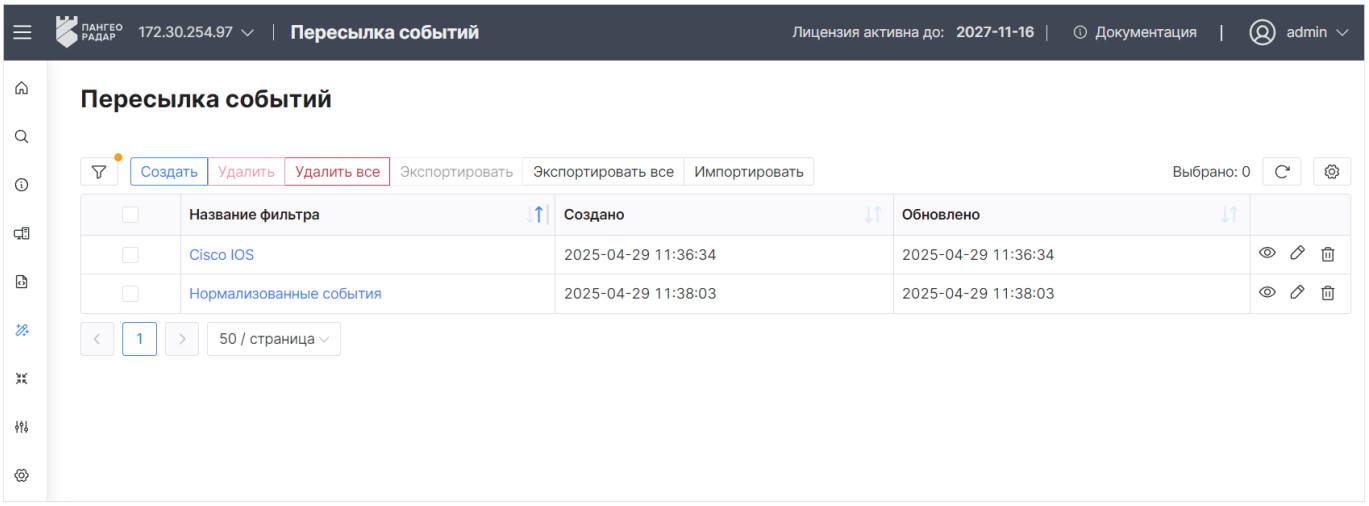


Рис. 151 – Раздел "Пересылка событий"

В разделе отображается следующая информация:

- **Название фильтра** – наименование фильтра для пересылки событий;
- **Создано** – дата и время создания фильтра;
- **Обновлено** – дата и время обновления фильтра.

9.3.2 Включение пересылки событий

1. В веб-интерфейсе платформы перейдите в раздел **Администрирование** → **Кластер** → вкладка **Управление конфигурацией**.
2. Включите пересылку событий. Для этого в древовидном списке параметров сервисов выберите **FlowBalancer** → **Head** и установите параметр **Пересылать события** в значение `true`, а в поле **Ip LogProxy** укажите IP-адрес узла, на который необходимо пересылать события (см. «Рис. 152»).

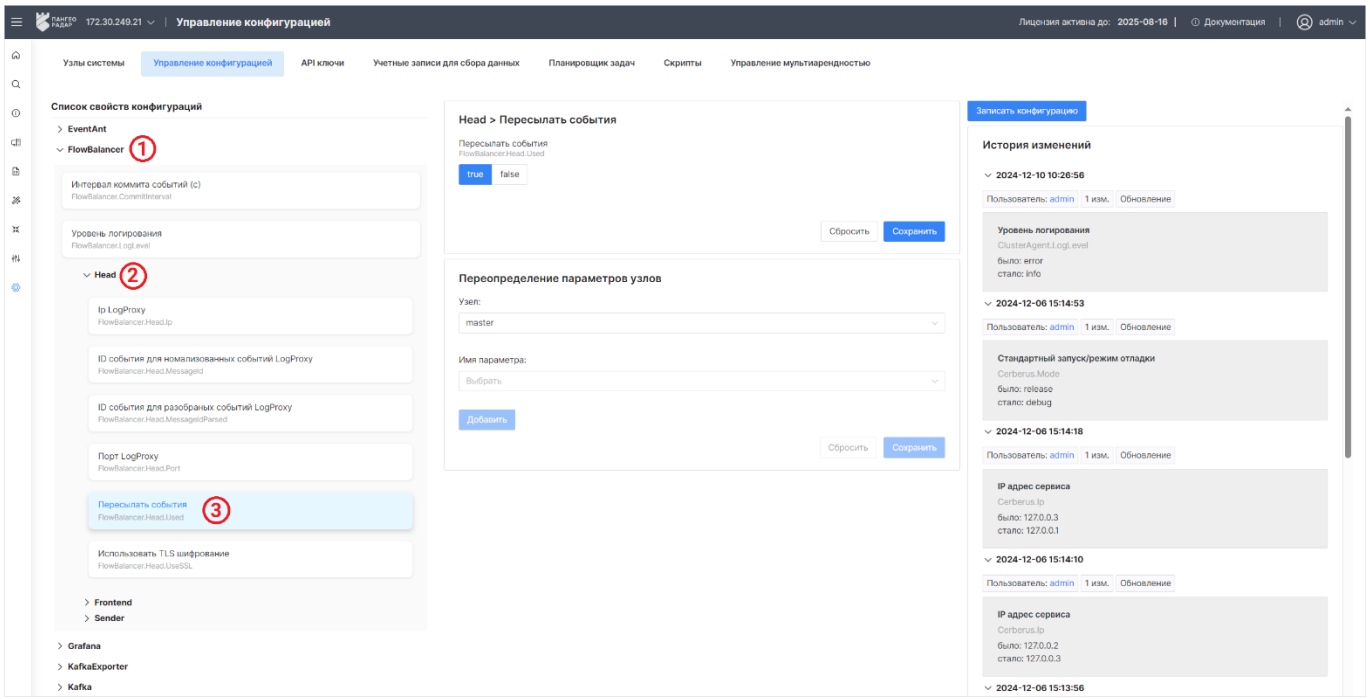


Рис. 152 – Управление конфигурацией сервиса FlowBalancer

3. При необходимости переопределите следующие параметры: Порт LogProxy, ID события для нормализованных событий LogProxy, ID события для разобранных событий LogProxy. Подробнее о настройке сервиса **Log-proxy** см. раздел документ «Работа с источниками событий ИБ».
4. После внесения изменений нажмите кнопку **Записать конфигурацию**.
5. Перейдите в раздел **Коррелятор** → **Пересылка событий** и создайте фильтр для пересылки событий с необходимыми параметрами (см. раздел «Создание фильтра для пересылки событий»).

Проверка работы пересылки событий:

1. Включите пересылку событий.
2. Перейдите в раздел **Коррелятор** → **Пересылка событий** и создайте фильтр со следующими параметрами (см. «Рис. 153»):
   - **Функция сравнения** -- *"Проверить равенство выражений"*;
   - **Тип выражения** -- *"Значение из события"* и *"Ручной ввод строки"* соответственно;
   - **Ключ** -- "*elastic_key*";
   - **Значение** -- "*normalized*".

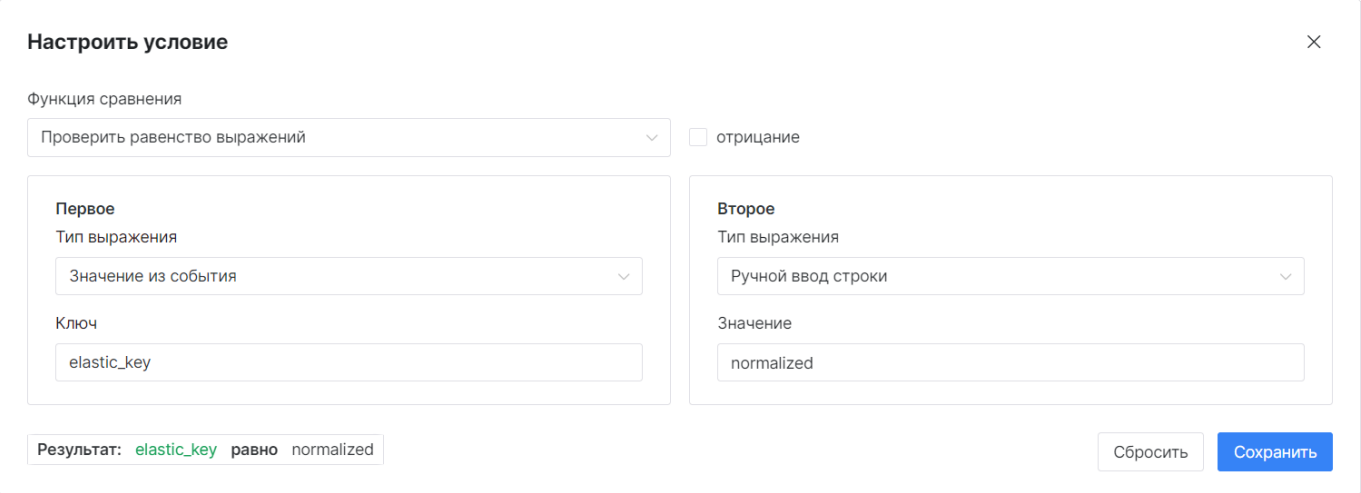


Рис. 153 – Настройка фильтра для пересылки нормализованных событий

3. Включите поток событий на основной узел.
4. На удаленном (дополнительном) узле перейдите в раздел **Просмотр событий** и удостоверьтесь, что пришедшие нормализованные события изначально отправлялись на основной узел.

9.3.3 Просмотр фильтра для пересылки событий

Для просмотра фильтра для пересылки событий нажмите кнопку в нужной строке таблицы или нажмите по ссылке в колонке **Название фильтра**. Откроется представление через боковую панель и форма просмотра выбранного фильтра (см. «Рис. 154»).

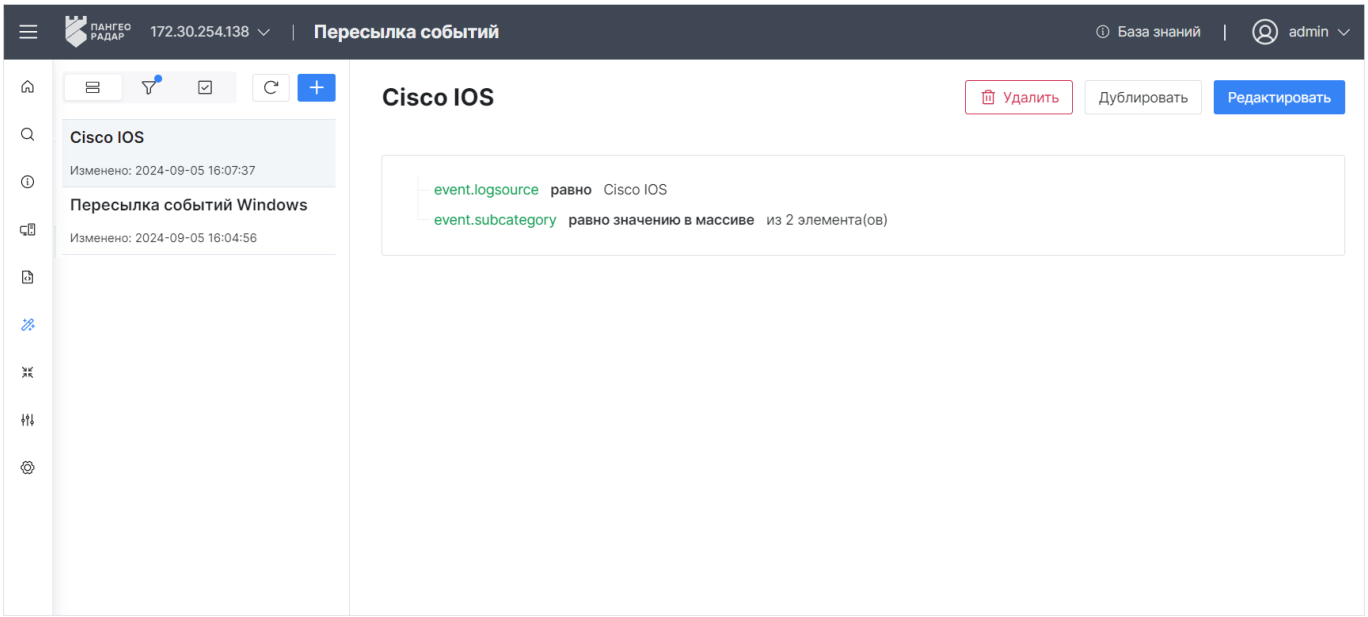


Рис. 154 – Форма просмотра фильтра для пересылки событий

В боковой панели отображается следующая информация:

- название фильтра для пересылки событий;
- количество событий, попавших под условия фильтра;
- количество отброшенных событий;
- дата и время изменения информации о фильтре.

В рабочей области отображаются условия фильтрации. Условия могут принимать следующие значения:

- равно - для условия выполняется функция проверки равенства выражений;
- равно значению в массиве - для условия выполняется функция проверки наличия значения в массиве данных;
- имеет подстроку - для условия выполняется функция поиска подстроки в строке;
- оператор "не" означает что выполняется отрицание при выполнении функции: "не равно", "не равно значению в массиве", "не имеет подстроку".

9.3.4 Создание фильтра для пересылки событий

1. Начните процесс создания фильтра через «универсальные таблицы» или инструмент «боковая панель». Откроется форма "Создание фильтра потока" (см. «Рис. 155»).

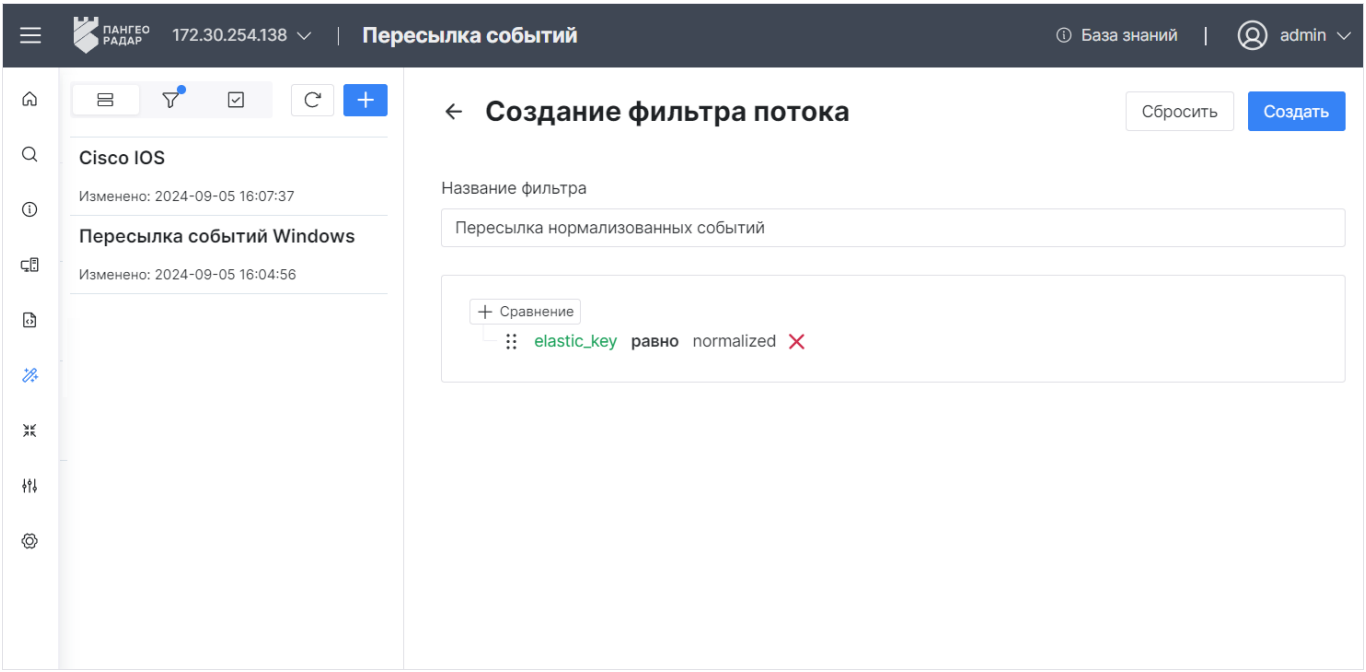


Рис. 155 – Форма "Создание фильтра для пересылки событий"

2. В поле **Название** укажите название фильтра и добавьте условие для сравнения нажав на кнопку **+ Сравнение**. Откроется окно "Настроить условие" (см. «Рис. 156»).

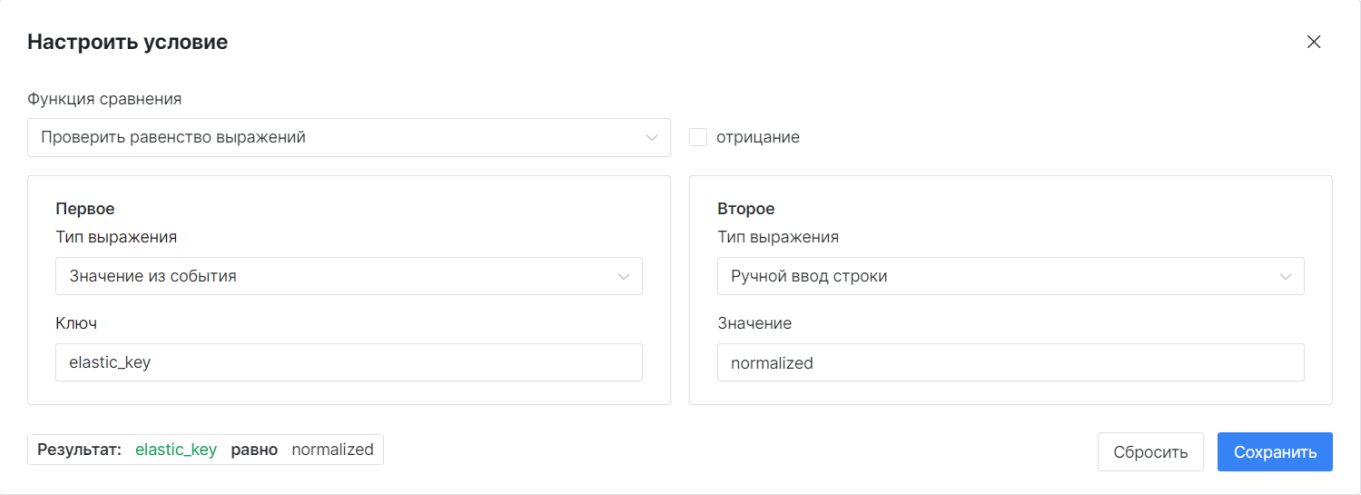


Рис. 156 – Окно "Настроить условие"

3. Укажите в окне "Настроить условие" следующую информацию:
    - В поле **Функция сравнения** из выпадающего списка выберите функцию сравнения:
        - "Проверить равенство выражений";
        - "Проверить наличие в массиве";
        - "Поиск подстроки в строке".
    - Если необходимо выполнить операцию "отрицание", то установите соответствующий флаг;
    - В блоке **Первое** настройте первую часть выражения:
        - в поле **Тип выражения** выберите необходимый тип выражения, например "Значение из события";
        - в поле **Ключ** из выпадающего списка выберите поле нормализованного события, по которому будет происходить фильтрация.
    - В блоке **Второе** настройте вторую часть выражения:
        - в поле **Тип выражения** выберите необходимый тип выражения, например "Ручной ввод строки";
        - в поле **Значение** укажите значение, по которому должно проверяться поле указанное в поле **Ключ**. Если выбрана функция "Проверить наличие в массиве", то укажите массив значений.
    - В блоке **Результат** проверьте правильность заданного выражения.
    - Нажмите кнопку **Сохранить.**
4. Добавьте необходимое количество условий в фильтр для пересылки событий.
5. Нажмите кнопку **Сохранить**.

9.3.5 Редактирование фильтра для пересылки событий

1. Начните процесс редактирования фильтра через «универсальные таблицы» или инструмент «боковая панель».

2. Внесите необходимые изменения:
    - для добавления нового условия нажмите кнопку **+ Сравнение**;
    - для изменения условия нажмите по строке выбранного условия;
    - для изменения порядка условий используйте кнопку ⠿;
    - для удаления условия из фильтра используйте кнопку ✕.
3. Нажмите кнопку **Сохранить**.

9.3.6 Дублирование фильтра для пересылки событий

1. Откройте фильтр на просмотр и нажмите кнопку **Дублировать**. Откроется окно "Дублировать фильтр потока событий" (см. «Рис. 157»).

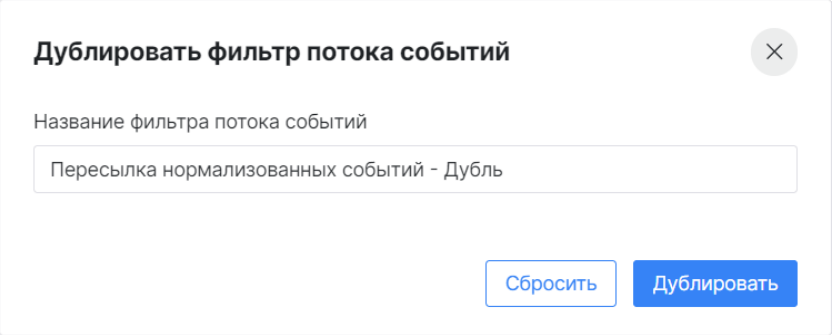


Рис. 157 - *Окно "Дублировать фильтр потока событий"*

2. Укажите в окне наименование фильтра.
3. Нажмите кнопку **Дублировать**.

9.3.7 Импорт фильтров

1. Начните процесс импорта фильтров через «универсальные таблицы» или инструмент «боковая панель».
2. В открывшемся окне укажите путь к архиву с фильтрами.
3. Нажмите кнопку **Открыть**.

9.3.8 Экспорт фильтров

1. Начните процесс экспорта фильтров через «универсальные таблицы» или инструмент «боковая панель».
2. Будет сформирован архив с фильтрами в формате .zip.
3. Нажмите кнопку **Скачать** и укажите путь для сохранения архива.

9.3.9 Удаление фильтра

1. Начните процесс удаления фильтра через «универсальные таблицы» или инструмент «боковая панель».
2. Подтвердите удаление в открывшемся окне.
3. Фильтр будет удален из платформы.

9.4 Фильтры потока событий

9.4.1 Общие данные

Фильтры отвечают за фильтрацию потока событий по заданным условиям.

Для работы с фильтрами перейдите в раздел **Коррелятор → Фильтры потока событий** (см. «Рис. 158»).

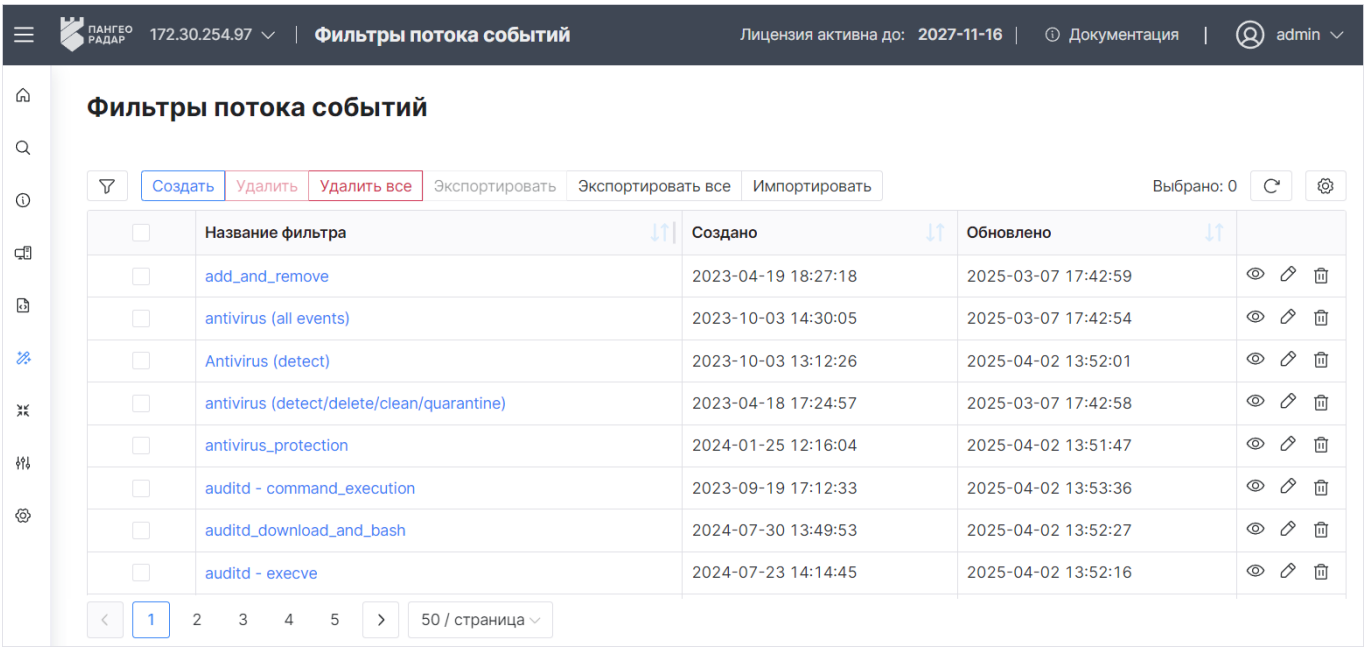


Рис. 158 – Раздел "Фильтры потока событий"

В разделе отображается следующая информация:

- **Название фильтра** – наименование фильтра потока событий;
- **Создано** – дата и время создания фильтра;
- **Обновлено** – дата и время обновления фильтра.

9.4.2 Просмотр фильтра потока событий

Для просмотра фильтра потока событий нажмите кнопку в нужной строке таблицы или нажмите по ссылке в колонке **Название фильтра**. Откроется представление через боковую панель и форма просмотра выбранного фильтра (см. «Рис. 159»).

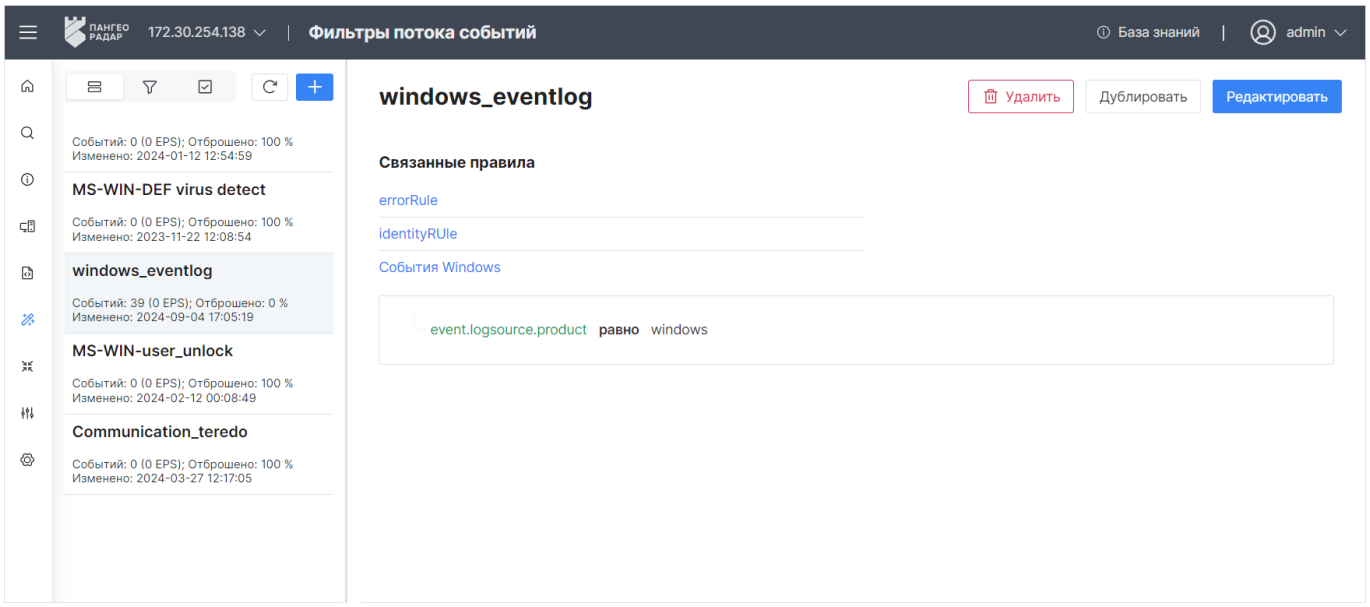


Рис. 159 – Форма просмотра фильтра потока событий

В боковой панели отображается следующая информация о фильтрах:

- наименование фильтра;
- количество событий, попавших под условия фильтра;
- количество отброшенных событий;
- дата и время последнего изменения фильтра.

В рабочей области отображается следующая информация о выбранном фильтре:

- список правил корреляции, в которых используется фильтр потока событий;
- список условий, заданных для фильтра. Условия могут принимать следующие значения:
  - равно - для условия выполняется функция проверки равенства выражений;
  - равно значению в массиве - для условия выполняется функция проверки наличия значения в массиве данных;
  - имеет подстроку - для условия выполняется функция поиска подстроки в строке;
  - оператор "не" означает что выполняется отрицание при выполнении функции: "не равно", "не равно значению в массиве", "не имеет подстроку".

9.4.3 Создание фильтра потока событий

1. Начните процесс создания фильтра через «универсальные таблицы» или инструмент «боковая панель». Откроется окно "Создание фильтра потока" (см. «Рис. 160»).

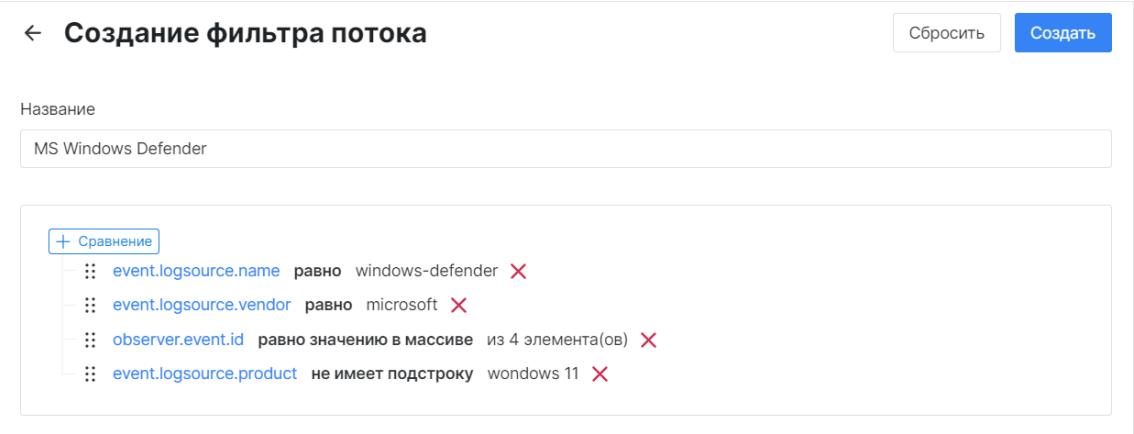


Рис. 160 – Окно "Создание фильтра потока"

2. В поле **Название** укажите название фильтра и добавьте условие для сравнения нажав на кнопку **+ Сравнение**. Откроется окно "Настроить условие" (см. «Рис. 161»).

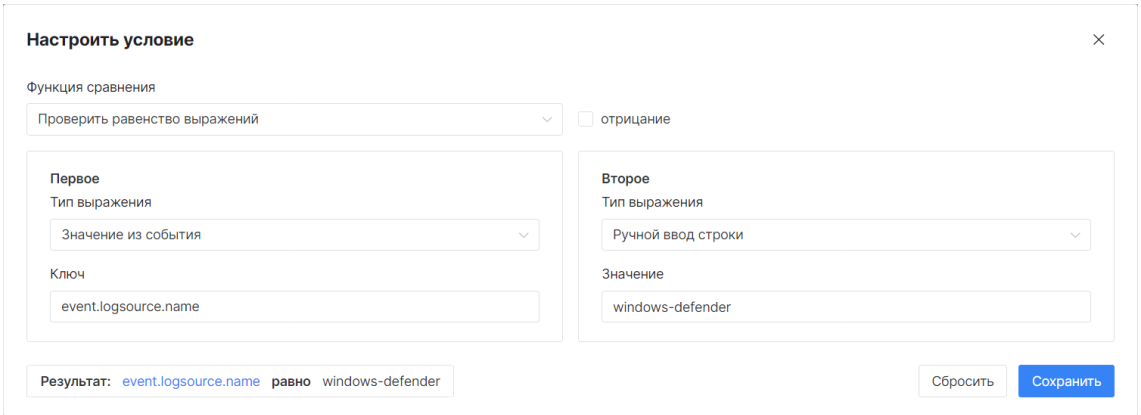


Рис. 161 – Окно "Настроить условие"

3. Укажите в окне "Настроить условие" следующую информацию:
   - В поле **Функция сравнения** из выпадающего списка выберите функцию сравнения:
     - "Проверить равенство выражений";
     - "Проверить наличие в массиве";
     - "Поиск подстроки в строке".
   - Если необходимо выполнить операцию "отрицание", то установите соответствующий флаг;
   - В блоке **Первое** настройте первую часть выражения:
     - в поле **Тип выражения** выберите необходимый тип выражения, например "Значение из события";
     - в поле **Ключ** из выпадающего списка выберите поле нормализованного события, по которому будет происходить фильтрация.
   - В блоке **Второе настройте** вторую часть выражения:
     - в поле **Тип выражения** выберите необходимый тип выражения, например "Ручной ввод строки";

- в поле **Значение** укажите значение, по которому должно проверяться поле, указанное в поле **Ключ**. Если выбрана функция "Проверить наличие в массиве", то укажите массив значений.

- В блоке **Результат** проверьте правильность заданного выражения.
- Нажмите кнопку **Сохранить.**

4. Добавьте необходимое количество условий в фильтр потока событий.
5. Нажмите кнопку **Сохранить**.

9.4.4 Редактирование фильтра потока событий

1. Начните процесс редактирования фильтра через «универсальные таблицы» или инструмент «боковая панель».
2. Внесите необходимые изменения:
   - для добавления нового условия нажмите кнопку **+ Сравнение**;
   - для изменения условия нажмите по строке выбранного условия;
   - для изменения порядка условий используйте кнопку ⠿;
   - для удаления условия из фильтра используйте кнопку ✕.
3. Нажмите кнопку **Сохранить**.

9.4.5 Дублирование фильтра потока событий

1. Откройте фильтр на просмотр и нажмите кнопку **Дублировать**. Откроется окно "Дублировать фильтр потока событий" (см. «Рис. 162»).

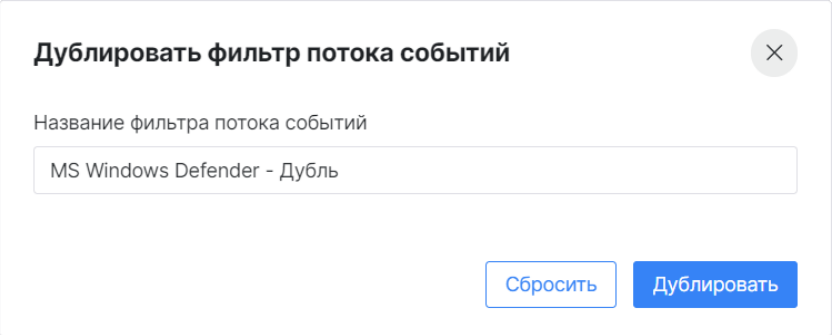


Рис. 162 – Окно "Дублировать фильтр потока событий"

2. Укажите в окне наименование фильтра.
3. Нажмите кнопку **Дублировать**.

9.4.6 Импорт фильтров потока событий

1. Начните процесс импорта фильтров через «универсальные таблицы» или инструмент «боковая панель».
2. В открывшемся окне укажите путь к архиву с фильтрами.
3. Нажмите кнопку **Открыть**.

9.4.7 Экспорт фильтров потока событий

1. Начните процесс экспорта фильтров через «универсальные таблицы» или инструмент «боковая панель».
2. Будет сформирован архив с фильтрами в формате .zip.
3. Нажмите кнопку **Скачать** и укажите путь для сохранения архива.

9.4.8 Удаление фильтра потока событий

1. Начните процесс удаления фильтра через «универсальные таблицы» или инструмент «боковая панель».
2. Подтвердите удаление в открывшемся окне.
3. Фильтр будет удален из платформы.

9.5 Макросы

9.5.1 Общие данные

Макросы – это подключаемые общие модули к правилам корреляции, которые могут содержать, как и переменные, так и расширять функционал с помощью функций.

Если вы хотите установить для разных правил модуль с одинаковым поведением, то подключите соответствующий макрос к правилам.

Макросы, как и правила корреляции, разрабатываются на скриптовом языке Lua.

Для работы с макросами перейдите в раздел **Коррелятор → Макросы** (см. «Рис. 163»).

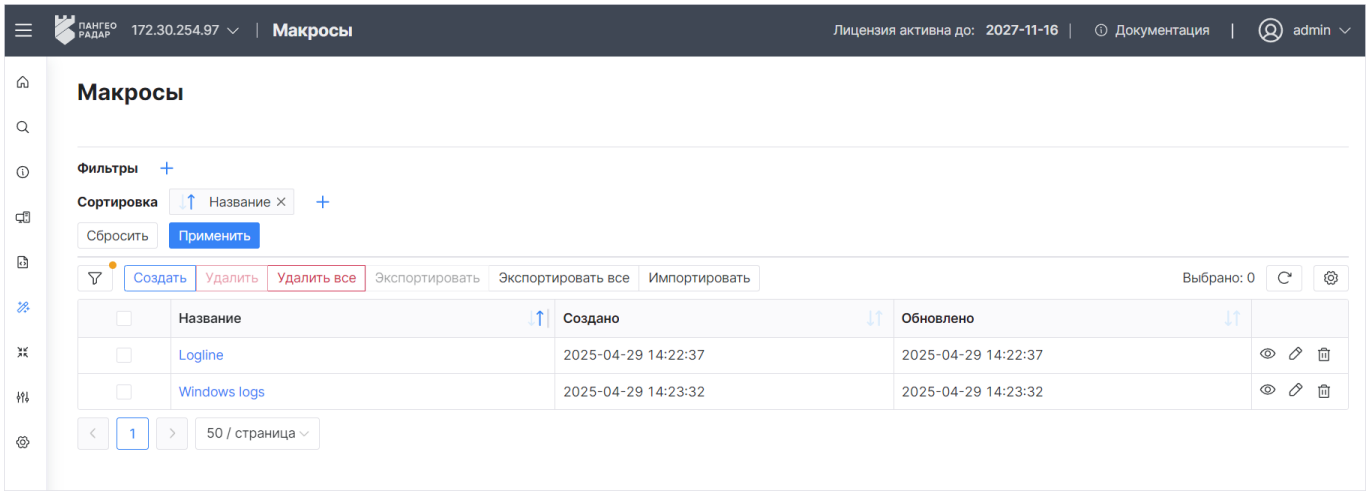


Рис. 163 – Раздел "Макросы"

В разделе отображается следующая информация:

- **Название** – наименование макроса;
- **Создано** – дата и время создания макроса;
- **Обновлено** – дата и время обновления макроса.

9.5.2 Просмотр макроса

Для просмотра макроса нажмите кнопку в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного макроса (см. «Рис. 164»).

Рис. 164 – Форма просмотра макроса

В боковой панели отображается следующая информация о макросах:

- наименование макроса;
- дата и время последнего изменения макроса.

В рабочей области отображается тело макроса.

9.5.3 Создание макроса

1. Начните процесс создания макроса через «универсальные таблицы» или инструмент «боковая панель». Откроется окно "Создание макроса" (см. «Рис. 165»).

Рис. 165 – Окно "Создание макроса"

2. Укажите в окне название и код макроса.

3. Нажмите кнопку **Сохранить**.

9.5.4 Редактирование макроса

1. Начните процесс редактирования макроса через «универсальные таблицы» или инструмент «боковая панель».
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

9.5.5 Дублирование макроса

1. Откройте макрос на просмотр и нажмите кнопку **Дублировать**. Откроется окно "Дублировать макрос" (см. «Рис. 166»).

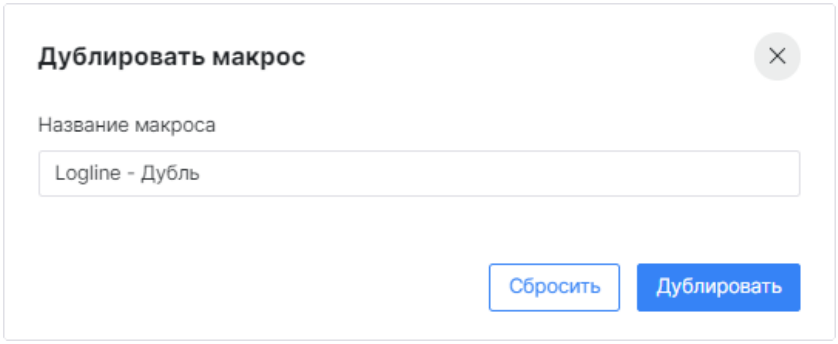


Рис. 166 – Окно "Дублировать макрос"

2. Укажите в окне наименование макроса.
3. Нажмите кнопку **Дублировать**.

9.5.6 Импорт макросов

1. Начните процесс импорта макросов через «универсальные таблицы» или инструмент «боковая панель».
2. В открывшемся окне укажите путь к архиву с макросами.
3. Нажмите кнопку **Открыть**.

9.5.7 Экспорт макросов

1. Начните процесс экспорта макросов через «универсальные таблицы» или инструмент «боковая панель».
2. Будет сформирован архив с макросами в формате .zip.
3. Нажмите кнопку **Скачать** и укажите путь для сохранения архива.

9.5.8 Удаление макроса

1. Начните процесс удаления макроса через «универсальные таблицы» или инструмент «боковая панель».
2. Подтвердите удаление в открывшемся окне.
3. Макрос будет удален из платформы.

9.6 Шаблоны алертов

9.6.1 Общие данные

При настройке правила корреляции вы можете использовать заранее подготовленные шаблоны "алертов", в которых можно настроить следующее поведение при сработке правила:

- присвоение уровня риска;
- автоматическое создание инцидента;
- автоматическое назначение инцидента пользователю.

Для работы с шаблонами "алертов" перейдите в раздел **Коррелятор → Шаблоны алертов** и выберите шаблон из списка (см. «Рис. 167»).

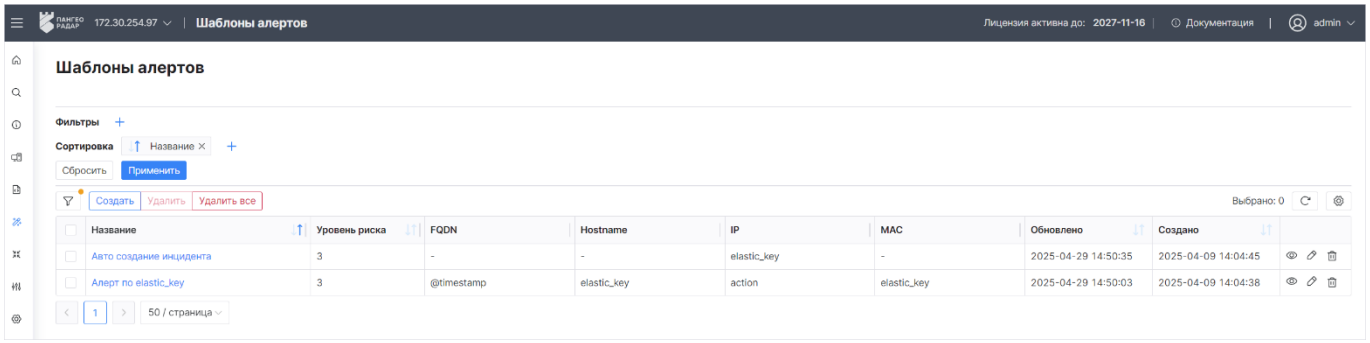


Рис. 167 – Раздел "Шаблоны алертов"

В разделе отображается следующая информация:

- **Название** – наименование шаблона "алерта";
- **Уровень риска** – цифровое обозначение уровня угрозы, которое будет присвоено инциденту в результате "сработки" правила;
- **FQDN** – поле события, которое будет определяться как FQDN актива;
- **Hostname** – поле события, которое будет определяться как Hostname актива;
- **IP** – поле события, которое будет определяться как IP-адрес актива;
- **MAC** – поле события, которое будет определяться как MAC-адрес актива;
- **Обновлено** – дата и время изменения информации о шаблоне;
- **Создано** – дата и время создания шаблона.

9.6.2 Просмотр шаблона "алерта"

Для просмотра шаблона нажмите кнопку в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного шаблона (см. «Рис. 168»).

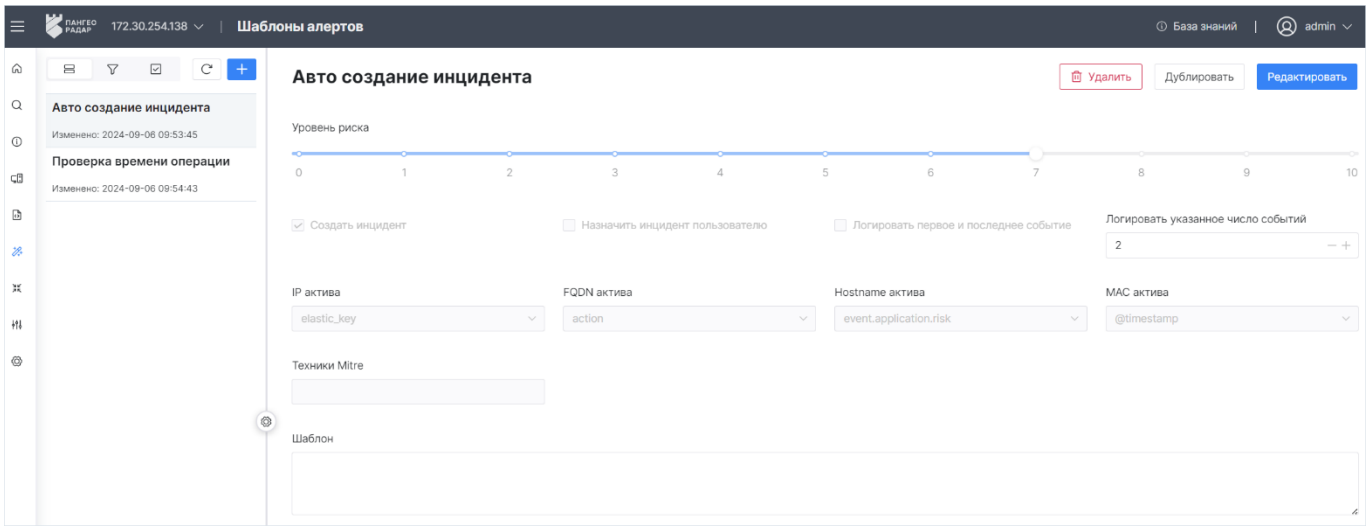


Рис. 168 –Форма просмотра шаблона «алерта»

В боковой панели отображается следующая информация о шаблонах:

- наименование шаблона;
- дата и время последнего изменения шаблона.

В рабочей области отображается структура данных и внешний вид шаблона.

9.6.3 Создание шаблона "алерта"

1. Начните процесс создания шаблона через «универсальные таблицы» или инструмент «боковая панель». Откроется окно "Создать шаблон" (см. «Рис. 169»).

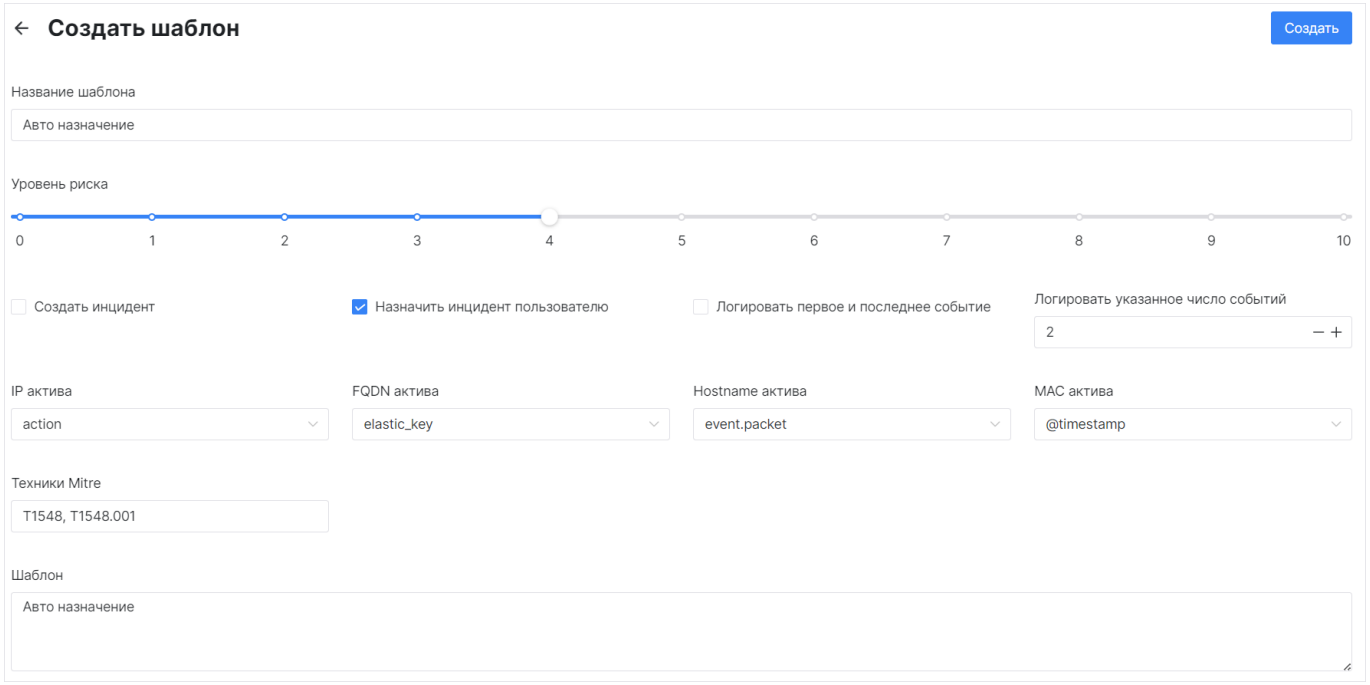


Рис. 169 – Окно "Создать шаблон"

2. Укажите в окне следующую информацию:
    - в поле **Название шаблона** укажите название шаблона "алерта";

- в поле **Уровень риска** выберите цифровое обозначение уровня риска, которое будет присвоено "сработке" правила;
- установите флаг **Создать инцидент** если необходимо автоматически создавать инцидент на основании "сработки" правила;
- установите флаг **Назначить инцидент пользователю** если необходимо автоматически назначать инцидент пользователю;
- выберите количество событий, которые необходимо записывать в журнал:
  - если вы хотите записывать только первое и последнее событие, то установите соответствующий флаг;
  - в обратном случае укажите необходимое значение в поле **Логировать указанное число событий**.
- в поле **IP актива** из выпадающего списка выберите поле, которое будет выступать в качестве IP-адреса актива. Поле может являться частью сводной таблицы событий;
- в поле **FQDN актива** из выпадающего списка выберите поле, которое будет выступать в качестве наименования домена актива. Поле может являться частью сводной таблицы событий;
- в поле **Hostname актива** из выпадающего списка выберите поле, которое будет выступать в качестве наименования хоста актива. Поле может являться частью сводной таблицы событий;
- в поле **MAC актива** из выпадающего списка выберите поле, которое будет выступать в качестве MAC-адреса актива. Поле может являться частью сводной таблицы событий;
- в поле **Техники Mitre** - укажите через запятую идентификаторы техник, используемых киберпреступниками, которые описаны в базе знаний компании Mitre (подробнее см. Techniques - Enterprise | MITRE ATT&CK®);
- в поле **Шаблон** укажите дополнительную информацию об "алерте".

3. Нажмите кнопку **Создать**.

9.6.4 Редактирование шаблона "алерта"

1. Начните процесс редактирования шаблона через «универсальные таблицы» или инструмент «боковая панель».
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

9.6.5 Дублирование шаблона "алерта"

1. Откройте шаблон на просмотр и нажмите кнопку **Дублировать**. Откроется окно "Дублировать шаблон алерта" (см. «Рис. 170»).

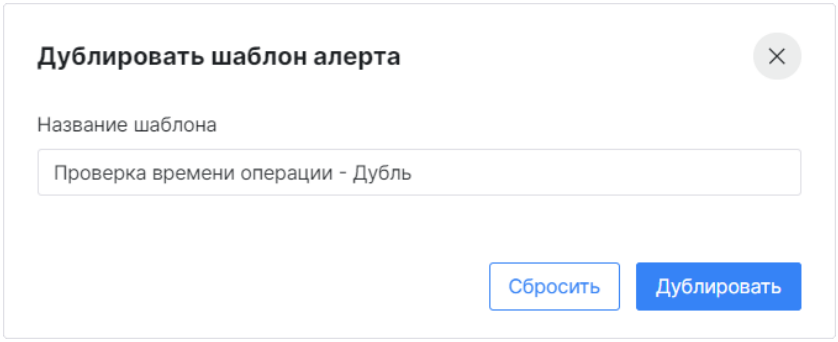


Рис. 170 – Окно "Дублировать шаблон алерта"

2. Укажите в окне наименование шаблона.
3. Нажмите кнопку **Дублировать**.

9.6.6 Удаление шаблона "алерта"

1. Начните процесс удаления шаблона через «универсальные таблицы» или инструмент «боковая панель».
2. Подтвердите удаление в открывшемся окне.
3. Шаблон алерта будет удален из платформы.

9.7 Шаблоны группировки

9.7.1 Общие данные

При настройке правила корреляции вы можете использовать заранее подготовленные шаблоны группировки событий.

Группировка выполняется по выбранному полю нормализованного события.

Платформа поддерживает возможность отслеживания и группировки подозрительных событий, следующих одно за другим (цепочки событий).

Для работы с шаблонами группировки перейдите в раздел **Коррелятор → Шаблоны группировки** (см. «Рис. 171»).

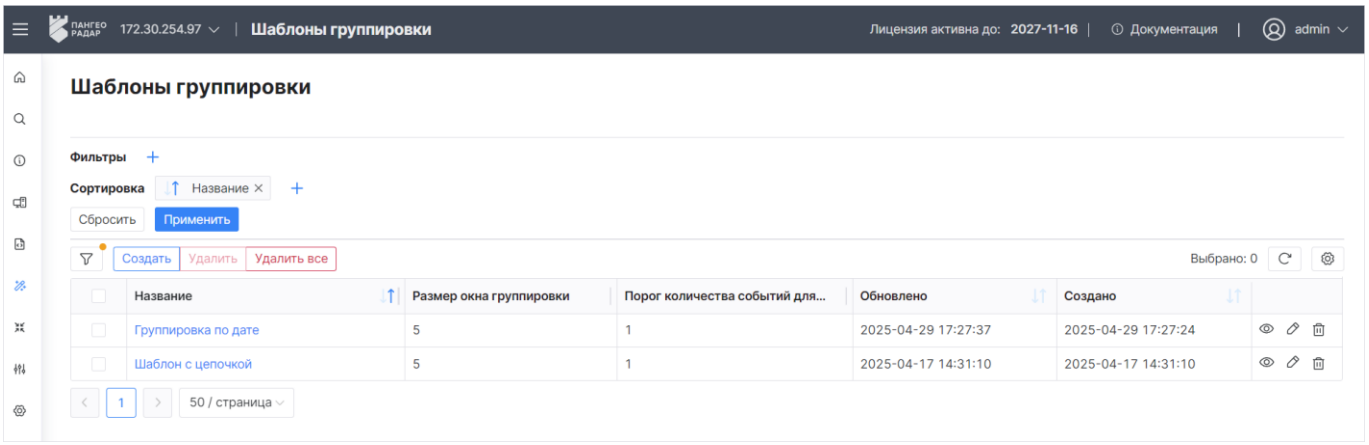


Рис. 171 – Раздел "Шаблоны группировки"

В разделе отображается следующая информация:

- **Название** – наименование шаблона группировки;
- **Размер окна группировки** – временной интервал, в течение которого будет выполняться группировка событий;
- **Порог количества событий для срабатывания** – количество событий, по достижению которого в окне группировки, будет срабатывать правило;
- **Обновлено** – дата и время изменения информации о шаблоне;
- **Создано** – дата и время создания шаблона.

9.7.2 Просмотр шаблона группировки

Для просмотра шаблона нажмите кнопку в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного шаблона (см. «Рис. 172»).

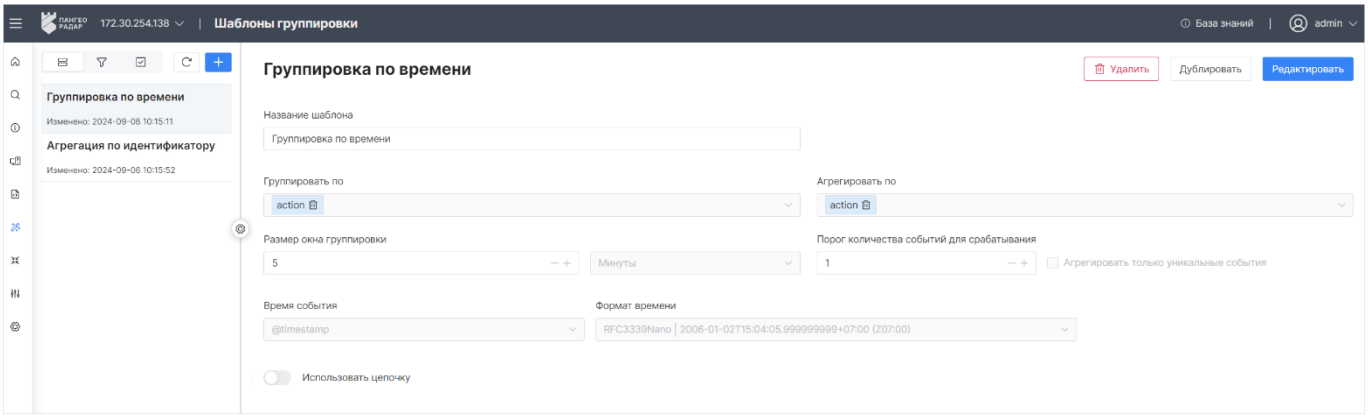


Рис. 172 – Форма просмотра шаблона группировки

В боковой панели отображается следующая информация о шаблонах:

- наименование шаблона;
- дата и время последнего изменения шаблона.

В рабочей области отображается структура данных и внешний вид шаблона.

9.7.3 Создание шаблона группировки

1. Начните процесс создания шаблона через «универсальные таблицы» или инструмент «боковая панель». Откроется окно "Создать шаблон" (см. «Рис. 173»).

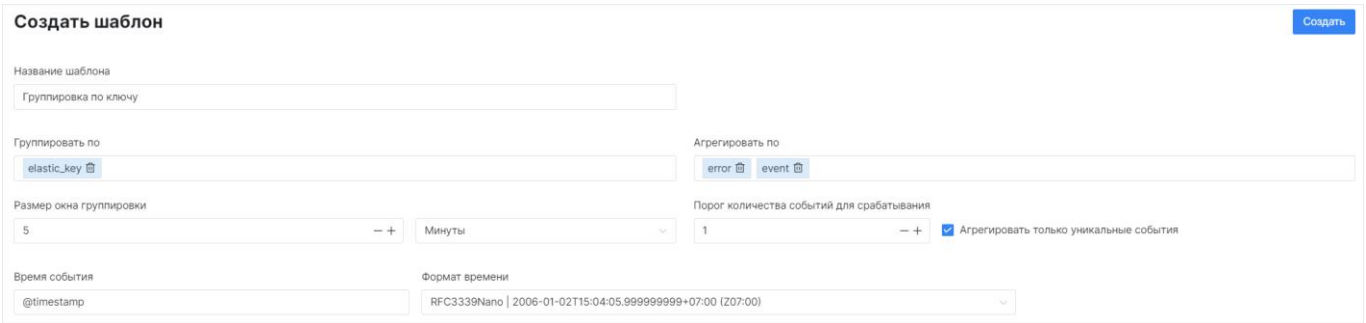


Рис. 173 – Форма "Создать шаблон"

2. Укажите в окне следующую информацию:

- в поле **Название шаблона** укажите название шаблона группировки;
- в поле **Группировать по** из выпадающего списка выберите поле нормализованного события, по которому будет выполняться группировка. Можно выполнять группировку по нескольким полям;
- в поле **Агрегировать по** из выпадающего списка выберите поле нормализованного события, по которому будет выполняться функция агрегации. Можно выполнить агрегацию по нескольким полям;
- в поле **Размер окна группировки** укажите временной интервал, в течение которого будет выполняться группировка событий;
- в поле **Порог количества событий для срабатывания** укажите количество событий, по достижению которого в окне группировки, будет срабатывать правило;
- для агрегации только уникальных значений установите соответствующий флаг;
- в поле **Время события** из выпадающего списка выберите поле нормализованного события, по которому будет вычисляться время события;
- в поле **Формат времени** из выпадающего списка выберите формат времени события.

3. При необходимости настройте цепочку событий. Для этого установите соответствующий переключатель в положение "Включен" и добавьте условия для цепочки событий нажав на кнопку **+ Сравнение**. Откроется окно "Настроить условие" (см. «Рис. 174»).

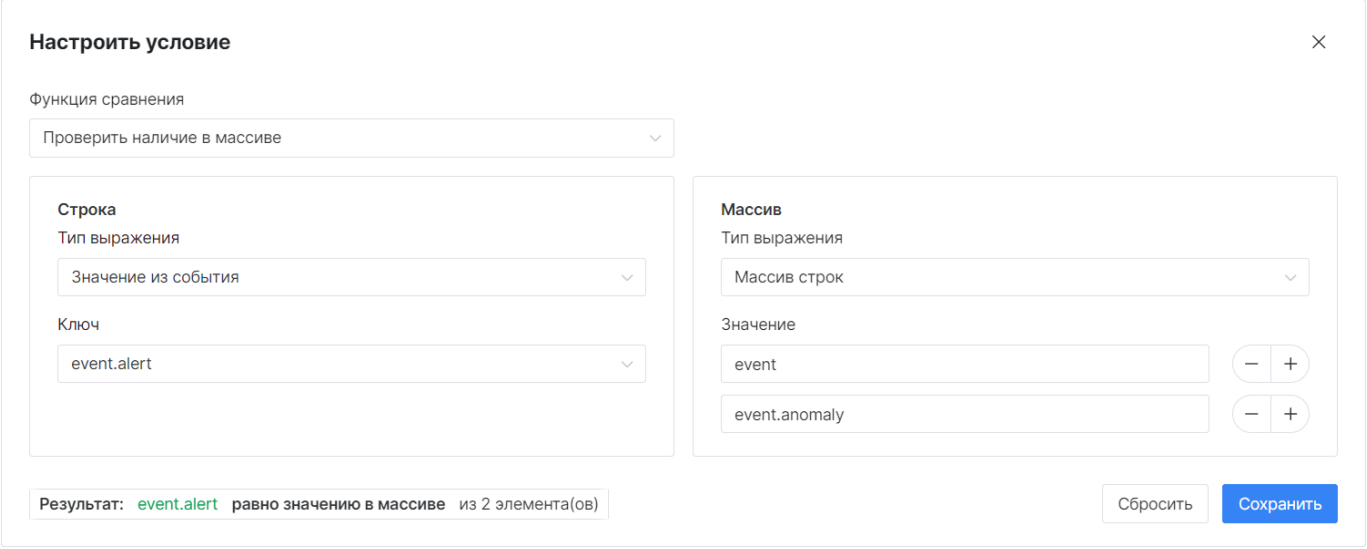


Рис. 174 – Окно "Настроить условие"

4. Укажите в окне "Настроить условие" следующую информацию:
   - В поле **Функция сравнения** из выпадающего списка выберите функцию **Проверить наличие в массиве**;
   - В блоке **Строка** настройте первую часть выражения:
     - в поле **Тип выражения** выберите необходимый тип выражения, например "Значение из события";

- в поле **Ключ** из выпадающего списка выберите поле нормализованного события, по которому будет выявляться цепочка событий.

- В блоке **Массив** настройте вторую часть выражения:
  - в поле **Тип выражения** выберите необходимый тип выражения, например "Массив строк";
  - в поле **Значение** укажите массив значений, по которым должно проверяться поле, указанное в поле **Ключ**.
- В блоке **Результат** проверьте правильность заданного выражения;
- Нажмите кнопку **Сохранить.**

5. Добавьте необходимое количество условий цепочки событий.
6. Настройте дополнительные параметры поведения для добавленных условий цепочки событий (см. «Рис. 175»):

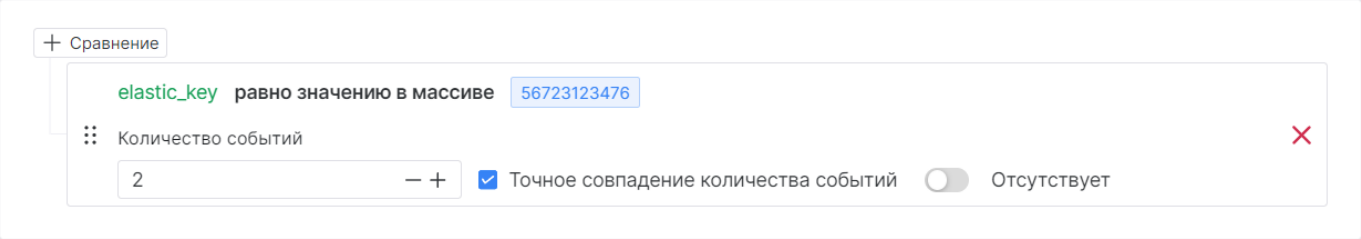


Рис. 175 – Параметры условий цепочки событий

- в поле **Количество событий** укажите минимальное количество найденных событий, подходящих под условие для "сработки" правила;
- для включения проверки строго соответствия количества событий установите флаг **Точное совпадение количества событий**;
- для отключения проверки по выбранному условия установите переключатель **Отсутствует** в положение "Включен".

7. Нажмите кнопку **Создать**.

9.7.4 Редактирование шаблона группировки

1. Начните процесс редактирования шаблона через «универсальные таблицы» или инструмент «боковая панель».
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

9.7.5 Дублирование шаблона группировки

1. Откройте шаблон на просмотр и нажмите кнопку **Дублировать**. Откроется окно "Дублировать шаблон группировки" (см. «Рис. 176»).

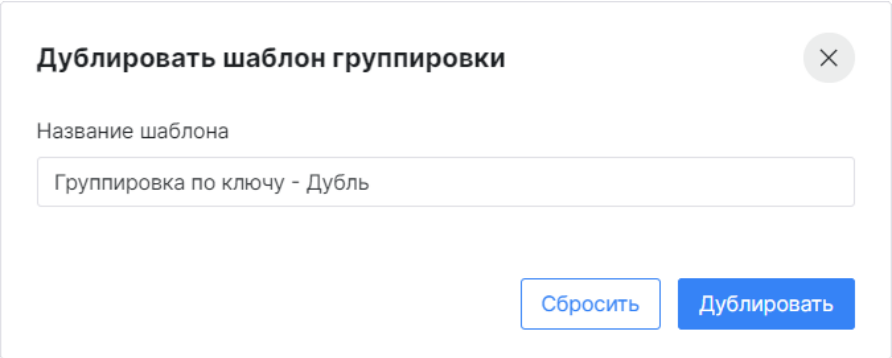


Рис. 176 – Окно "Дублировать шаблон группировки"

2. Укажите в окне наименование шаблона.
3. Нажмите кнопку **Дублировать**.

9.7.6 Удаление шаблона группировки

1. Начните процесс удаления шаблона через «универсальные таблицы» или инструмент «боковая панель».
2. Подтвердите удаление в открывшемся окне.
3. Шаблон группировки будет удален из платформы.

9.8 Табличные списки

9.8.1 Общие данные

Табличные списки (Rapid Value Store), являются видом активного хранилища -- автоматически изменяемого, в зависимости от условий.

Табличные списки могут использоваться для следующих целей:

- для обращения к справочным данным;
- для дополнительной фильтрации при работе с обогащением из таких источников как: Active Directory, Активы;
- для добавления идентификаторов активов и пользователей в "карантин", для исключения повторных "сработок" правил до решения инцидента;
- для реализации механизма "черных" и "белых" списков.

Хранилища могут быть созданы вручную и автоматически. Автоматическое создание хранилища включает в себя следующие способы:

- посредством обработки событий от источника "Kaspersky-SecurityCenter-db-host-activity" и правила "AV_KES_Hosts with old bases and without workable antivirus";
- посредством исполнения скриптов, получающих информацию из Active Directory активов Платформы.

Табличные списки поддерживают следующие типы полей:

- `string` - указывается строка;
- `integer` - указывается целое число;

- `bigint` - указывается целое число произвольной точности;
- `double` - указывается целое или дробное число с двойной точностью;
- `IP` - указывается IP-адрес,
- `CIDR` - указывается IP-адрес подсети.

При написании правил корреляции для их вызова в коде правила необходимо использовать функцию `RVS`.

Для работы с табличными списками перейдите в раздел **Коррелятор → Табличные списки** и выберите хранилище из списка (см. «Рис. 177»).

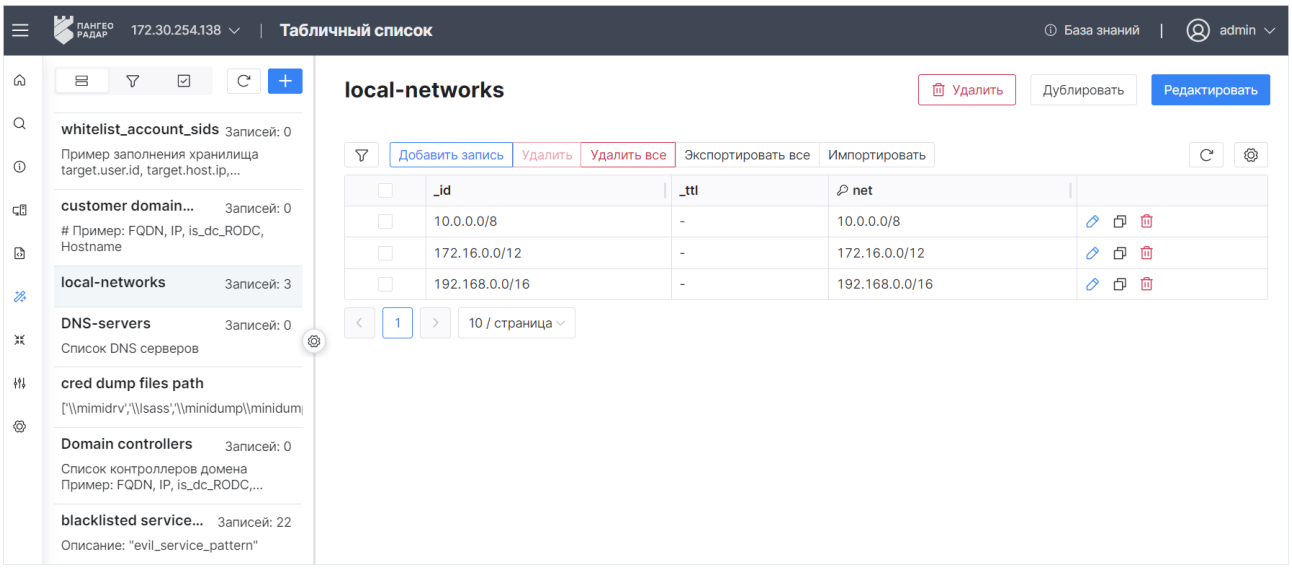


Рис. 177 – Раздел "Табличные списки"

Набор отображаемых данных формируется в зависимости от настроек выбранного табличного списка.

Значком отмечены поля, которые являются "ключами" для формирования уникального идентификатора записи (поле `_id`). По этому идентификатору правила будут обращаться к нужной записи из табличного списка. Признак "ключа" указывается для поля на этапе создания табличного списка. Необходимо соблюдать уникальность поля `_id`.

9.8.2 Создание табличного списка

1. Нажмите кнопку **Создать табличный список**. Откроется окно "Создание табличного списка" (см. «Рис. 178»).

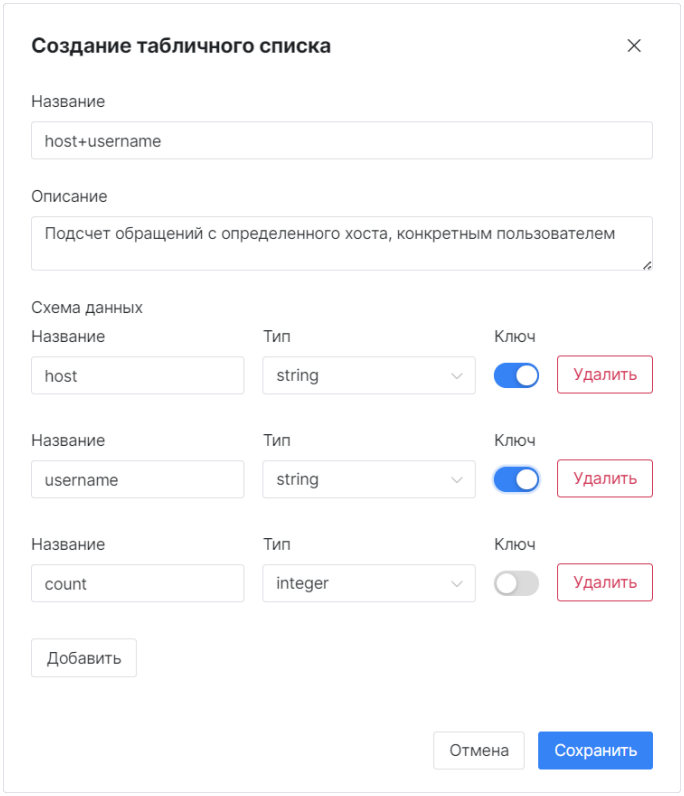


Рис. 178 – Окно "Создание табличного списка"

2. Укажите в окне следующую информацию:
    - в поле **Название** укажите название табличного списка;
    - в поле **Описание** укажите дополнительные сведения о табличном списке;
    - в блоке **Схема данных** настройте поля табличного списка:
        - в поле **Название** укажите название поля схемы данных;
        - в поле **Тип** из выпадающего списка выберите тип поля: `string`, `integer`, `bigint`, `double`, `IP`, `CIDR`;
        - в поле **Ключ** при необходимости установите признак "ключ". Ключ служит для формирования уникального идентификатора записи табличного списка;
        - добавьте необходимое количество полей в схему данных табличного списка. Для этого нажмите кнопку **Добавить**.
3. Нажмите кнопку **Сохранить**.

9.8.3 Работа с записями табличного списка

Над записями табличного списка доступны следующие операции:

- Добавление записи.
- Редактирование записи.
- Дублирование записи.
- Экспорт записей.
- Импорт записей.
- Удаление записей.
- Массовые операции над записями.

Добавление записи выполняется следующим способом:

1. Выберите табличный список и нажмите кнопку **Добавить запись**. Откроется окно "Создание записи" (см. «Рис. 179»).

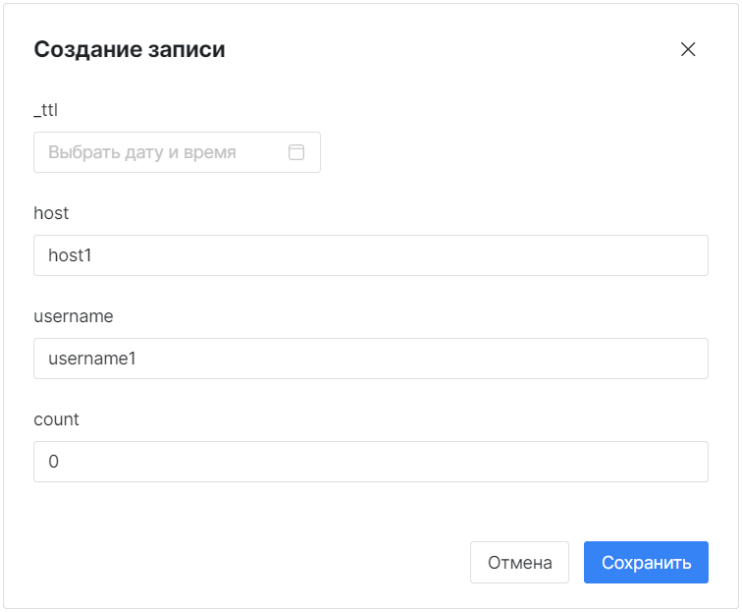


Рис. 179 – Окно "Создание записи"

2. Окно "Создание записи" формируется в зависимости от настроенной схемы данных табличного списка. Укажите в окне соответствующие данные.
3. В поле **ttl** укажите дату, до наступления которой запись табличного списка будет действительна;
4. Нажмите кнопку **Сохранить**.

9.8.4 Редактирование табличного списка

1. Выберите из списка необходимый табличный список и нажмите кнопку **Редактировать**.
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

9.8.5 Дублирование табличного списка

1. Выберите из списка необходимый табличный список и нажмите кнопку **Дублировать**. Откроется окно "Дублирование табличного списка" (см. «Рис. 180»).

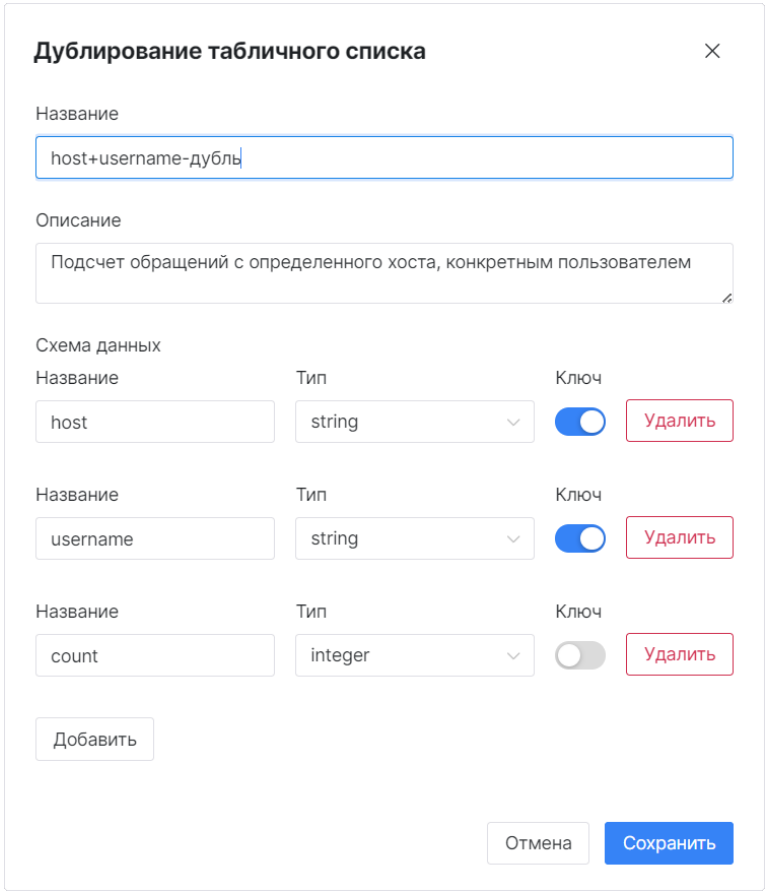


Рис. 180 – Окно "Дублирование табличного списка"

2. Укажите в окне наименование табличного списка.
3. Нажмите кнопку **Сохранить**.

9.8.6 Импорт табличных списков

1. Нажмите на кнопку ☑ и из выпадающего списка выберите пункт **Импортировать**.
2. В открывшемся окне укажите путь к архиву с табличными списками.
3. Нажмите кнопку **Открыть**.

9.8.7 Экспорт табличных списков

1. Нажмите на кнопку ☑ и из выпадающего списка выберите пункт **Экспортировать все**.
2. Будет сформирован архив с табличными списками в формате .zip.
3. Нажмите кнопку **Скачать** и укажите путь для сохранения архива.

9.8.8 Удаление табличного списка

1. Выберите из списка необходимый табличный список и в рабочей области нажмите кнопку **Удалить**.
2. Подтвердите удаление в открывшемся окне.
3. Табличный список будет удален из платформы.

9.8.9 Массовые действия над табличными списками

Над табличными списками доступны следующие массовые действия:

- **Экспортировать** - экспорт выбранных табличных списков;
- **Удалить** - удаление выбранных табличных списков;
- **Удалить все** - удаление всех табличных списков.

Для выполнения массового действия выполните следующие шаги:

1. Нажмите на кнопку ☑. Откроется список массовых операций и флаги для выбора табличных списков (см. «Рис. 181»).

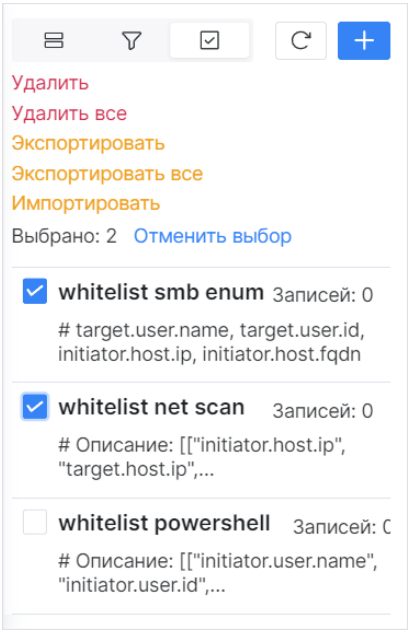


Рис. 181 – Массовые действия над табличными списками

2. Выберите табличные списки.
3. Нажмите на соответствующую кнопку действия.
4. Завершите действие в открывшемся окне.

9.9 Ретроспективная корреляция

9.9.1 Общие данные

Платформа Радар позволяет осуществлять повторную корреляцию по сохраненным ранее событиям потока.

Ретроспективную корреляцию событий можно использовать в следующих случаях:

- для проверки гипотез по добавлению новых правил корреляции;
- для проверки событий после обновления данных табличных списков;
- для проверки событий по правилам, работа которых была приостановлена.

Для перевода правила в режим ретроспективного анализа необходимо выполнить следующие условия:

- правило должно быть "активно";
- для правила выставлен признак "Ретроспективное".

Для выполнения ретроспективной корреляции необходимо создать задачу с одним из правил, подходящих для проведения анализа.

Для управления задачами для ретроспективной корреляции перейдите в раздел **Коррелятор → Ретроспективная корреляция** (см. «Рис. 182»).

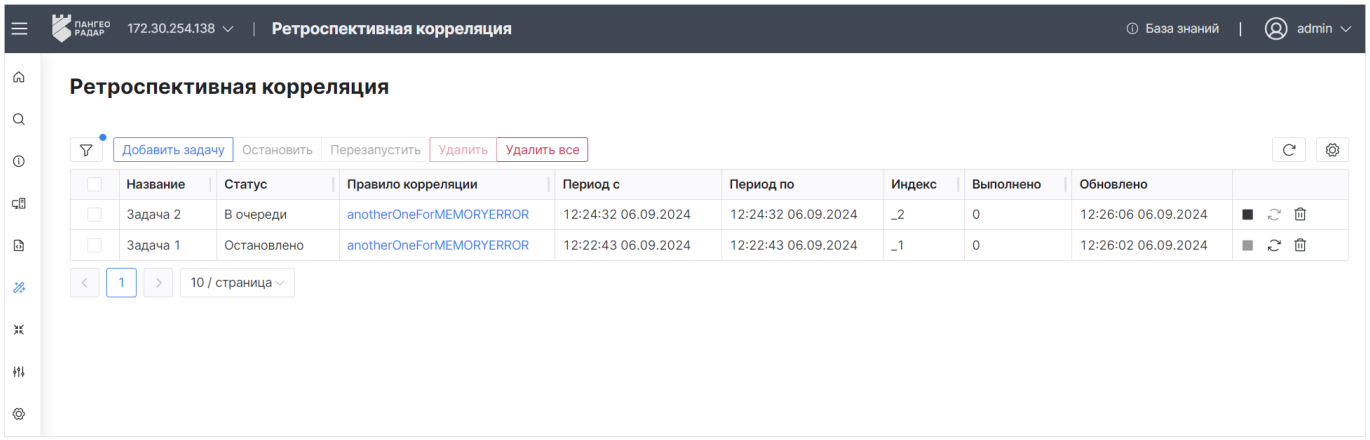


Рис. 182 – Раздел "Ретроспективная корреляция"

В разделе отображается следующая информация:

- **Название** - название задачи ретроспективной корреляции;
- **Статус** - текущее состояние задачи:
  - Остановлено;
  - В очереди;
  - Ошибка;
  - Выполняется.
- **Период с** и **Период по** - период выполнения задачи;
- **Правило корреляции** - наименование правила корреляции, по которому выполняется задача. По ссылке открывается форма просмотра правила;
- **Индекс** - индексы событий, по которым проводится анализ;
- **Выполнено** - количество выполнений задачи.

9.9.2 Добавление задачи для ретроспективной корреляции

1. Нажмите кнопку **Добавить задачу**. Откроется окно "Создать задачу" (см. «Рис. 183»).

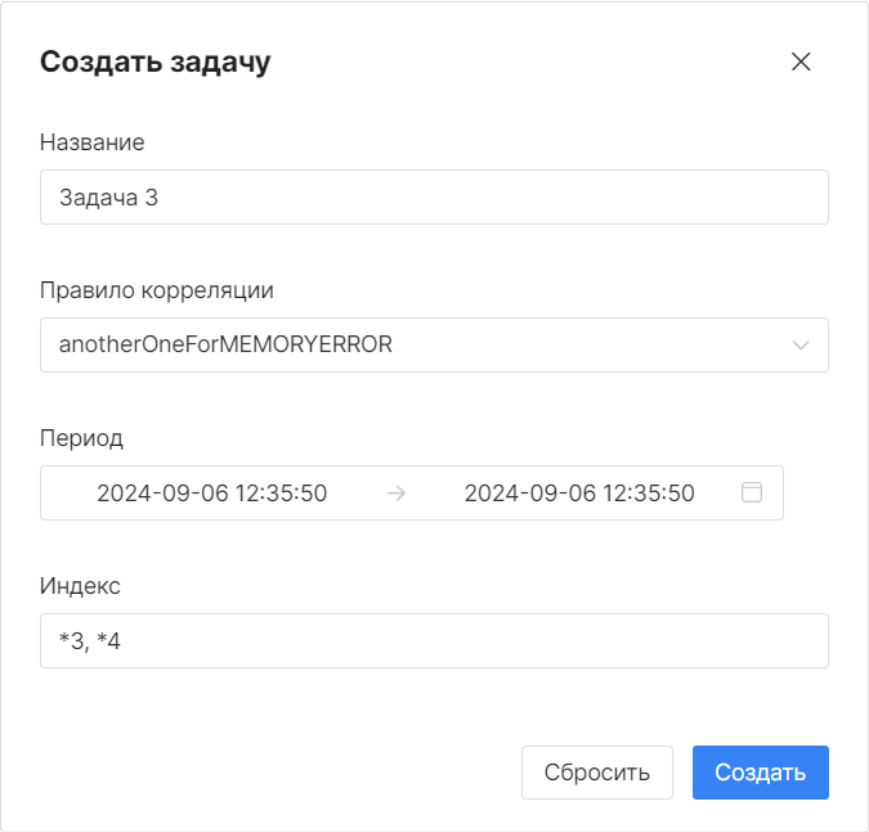


Рис. 183 – Окно "Создать задачу"

2. Укажите в окне следующую информацию:
    - в поле **Название** укажите название задачи;
    - в поле **Правило** из выпадающего списка выберите правило для ретроспективного анализа;
    - в поле **Период** укажите период выполнения задачи;
    - в поле **Индекс** укажите индексы событий, по которым будет выполняться задача (поддерживается wildcard символ "*").
3. Нажмите кнопку **Создать**.

9.9.3 Остановка задачи

1. Выберите задачу в таблице и в соответствующей строке нажмите кнопку ■.
2. Выполнение задачи будет остановлено.

9.9.4 Перезапуск задачи

1. Выберите задачу в таблице и в соответствующей строке нажмите кнопку ↻.
2. Выполнение задачи будет заново запушено.

9.9.5 Удаление задачи

1. Выберите задачу в таблице и в соответствующей строке нажмите кнопку 🗑.
2. Задача будет удалена.

9.9.6 Массовые действия над задачами

Над задачами доступны следующие массовые действия:

- **Остановить** - остановка выполнения выбранных задач;
- **Перезапустить** - повторный запуск выбранных задач;
- **Удалить** - удаление выбранных задач;
- **Удалить все** - удаление всех задач.

Для выполнения массового действия выполните следующие шаги:

1. Отметьте в таблице необходимые задачи, установив соответствующие флаги.
2. Нажмите на соответствующую кнопку действия.
3. Завершите действие в открывшемся окне.

10. Параметры

В разделе выполняется управление следующими параметрами **Платформы Радар**:

- «Основные параметры». Настройка общих параметров **Платформы Радар**.
- «Оповещения по задержкам». Настройка автоматических оповещений по задержкам в обработке инцидентов, формируемых **Платформой Радар**.
- «Черный список ID плагинов». Настройка списка ID плагинов сканеров уязвимости, которые будут игнорироваться в процессе работы.
- «Фоновые задачи». Просмотр информации о фоновых задачах, запущенных в **Платформе Радар**.
- «Интеграции». Управление экземплярами интеграций со сторонними системами.
- «Типы интеграций». Просмотр доступных классов систем, с которым можно настроить интеграцию, а также переключение платформы в режим работы с соответствующим типом интеграции.
- «Папки контента». Управление папками для структурирования пользовательского контента.
- «Шаблоны». Управление шаблонами форм пользовательского контента.

10.1 Основные параметры

Для выполнения настройки основных параметров **Платформы Радар** перейдите в раздел **Параметры → Основные параметры** (см. «Рис. 184»).

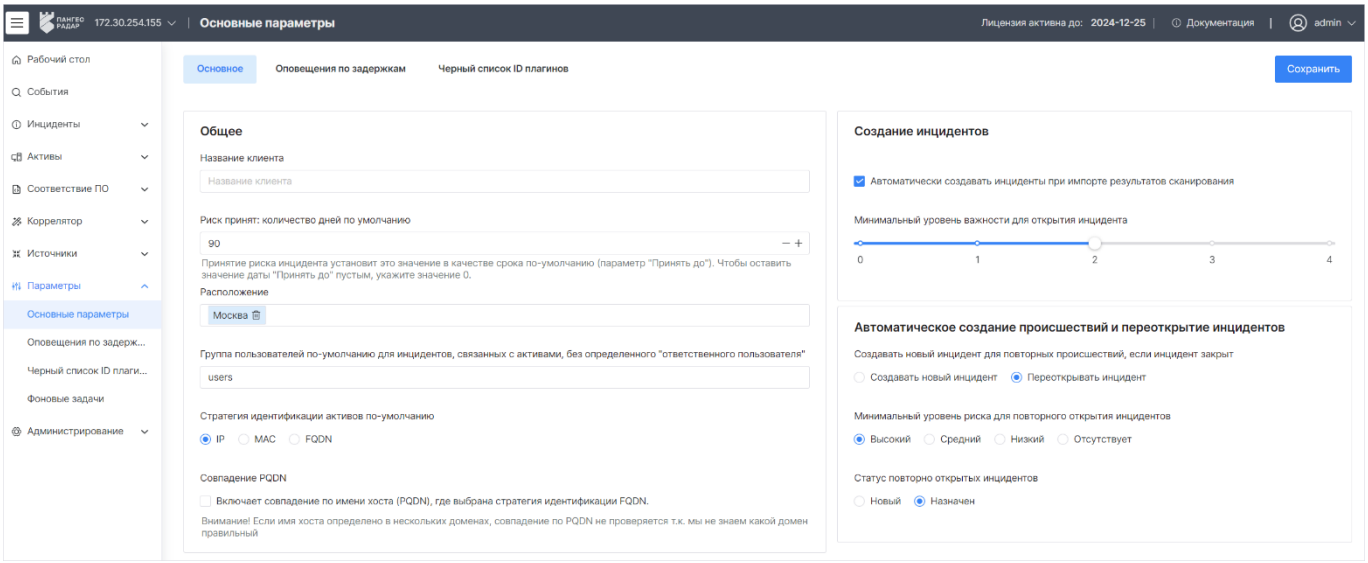


Рис. 184 – Раздел "Основные параметры"

Раздел содержит следующие блоки:

- **Общие** –настройка значений по умолчанию для различных параметров платформы;
- **Создание инцидентов** – настройка автоматического создания инцидентов;

- **Автоматическое создание происшествий и переоткрытие инцидентов** – настройка поведения платформы при возникновении повторных происшествий.

После внесения любых изменений, для того чтобы они вступили в силу, необходимо нажать кнопку **Сохранить**.

Общие

Для настройки значений по умолчанию выполните следующие действия:

- в поле **Название клиента** укажите наименование организации, в которой установлена **Платформа Радар**;
- в поле **Риск принят: количество дней по умолчанию** укажите количество дней, по истечении которых будет принят риск инцидента. Значение будет автоматически добавлено в поле инцидента **Принять до**. Чтобы оставить значение поля **Принять до** пустым, укажите значение 0;
- в поле **Расположение** укажите город, в котором располагается организация;
- в поле **Группа пользователей по умолчанию** выберите из списка группу пользователей, которая будет назначаться по умолчанию для инцидентов, связанных с активами без назначенного "ответственного пользователя";
- в поле **Стратегия идентификации активов по умолчанию** выберите одну из стратегий (IP, FQDN, MAC), которая будет применена при идентификации активов, в случае если актив не попал ни под одну, настроенную пользователем, стратегию;
- если выбрана стратегия идентификации по FQDN, то выберите поведение платформы: включать или не включать совпадение по имени хоста (PQDN).

Внимание! *Если имя хоста определено в нескольких доменах, совпадение по PQDN не проверяется*.

Создание инцидентов

- при необходимости включите автоматическое создание инцидентов при импорте результатов сканирования, установив соответствующий флаг;
- установите минимальный уровень важности для открытия инцидента.

Автоматическое создание происшествий и переоткрытие инцидентов

Выберите поведение платформы при возникновении повторных происшествий в закрытом инциденте:

- Создавать новый инцидент;
- Переоткрывать инцидент. В этом случае необходимо указать следующие параметры:
  - выберите минимальный уровень риска для повторного открытия инцидента: высокий, средний, низкий, отсутствует;
  - выберите статус повторно открытых инцидентов: новый, назначен.

10.2 Оповещения по задержкам

Для выполнения настройки автоматических оповещений по задержкам в обработке инцидентов операторами, перейдите в раздел **Параметры → Оповещения по задержкам** (см. «Рис. 185»).

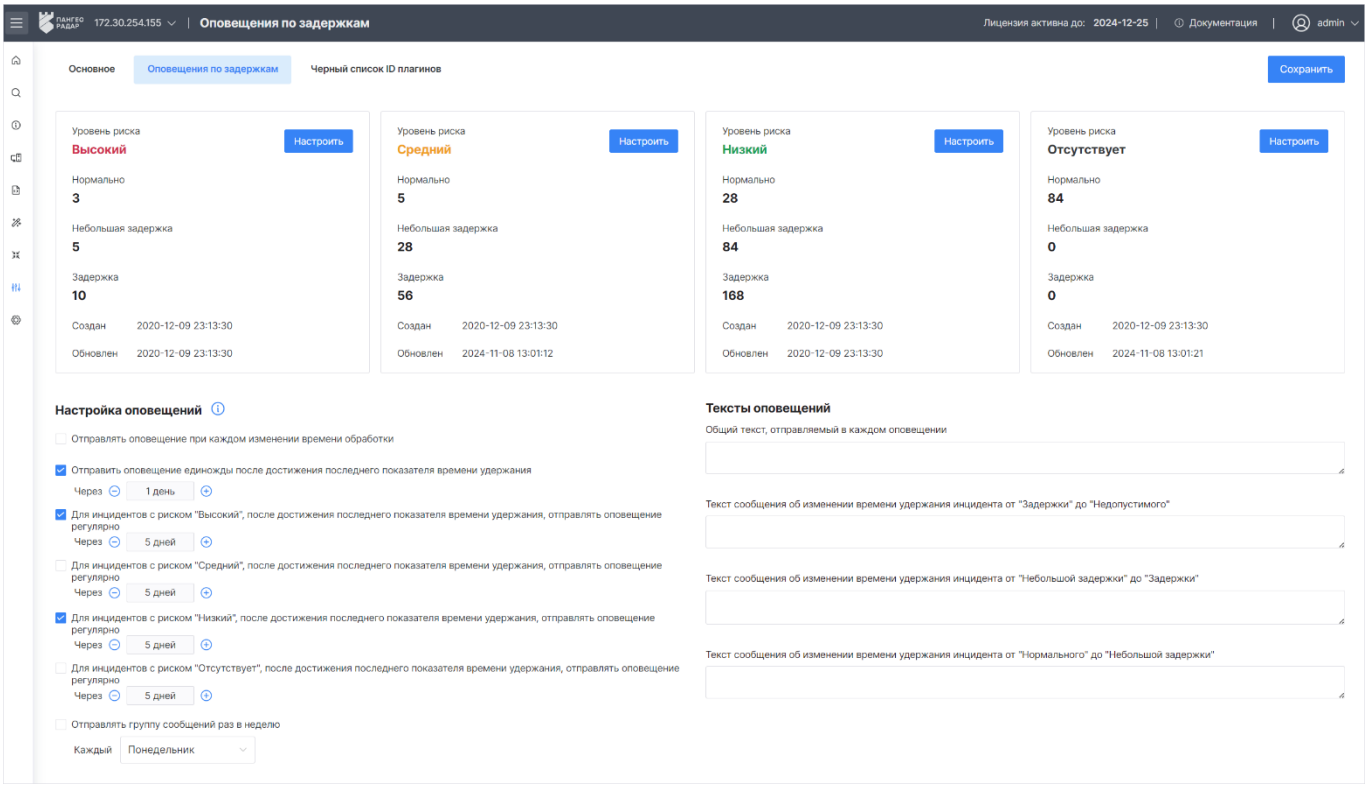


Рис. 185 – Раздел "Оповещения по задержкам"

Раздел содержит следующие блоки:

- Блок настроек временных отсечек для оповещений;
- Блок настройки режимов отправки оповещений;
- Блок настройки текстов для оповещений.

Блок настроек временных отсечек для оповещений

Для каждого уровня риска (высокий, средний, низкий, отсутствует) можно настроить 3 контрольных отсечки по времени разбора инцидента:

- **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.

Для настройки времени контрольных отсечек выполните следующие действия:

1. Выберите уровень риска, для которого будет выполнена настройка и в соответствующем блоке нажмите кнопку **Настроить**. Откроется окно "Редактирование уровня риска" (см. «Рис. 186»).

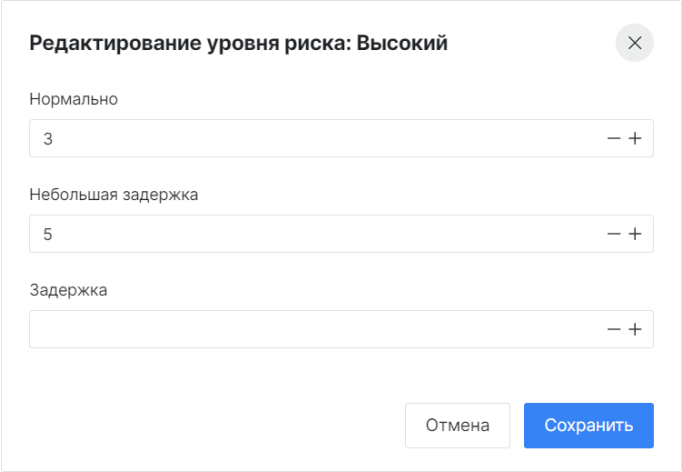


Рис. 186 – Окно "Редактирование уровня риска"

2. В полях **Нормально**, **Небольшая задержка**, **Задержка** укажите необходимое количество дней.
3. Нажмите кнопку **Сохранить**.

Блок настройки режимов отправки оповещений

В **Платформе Радар** возможно настроить следующие режимы отправки оповещений:

- **Отправлять оповещения при каждом изменении времени обработки** – при активации опции оповещение будет отправляться при прохождении каждой временной отсечки, указанной для разбора инцидента.
- **Отправлять оповещение единожды через <...> дн., после достижения последнего показателя времени удержания** – при активации опции оповещение будет отправляться после прохождения последней сконфигурированной временной отсечки.
- **Для инцидентов с риском "Высокий" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания** – при активации опции оповещение для инцидентов с высоким риском будет отправляться после прохождения последней сконфигурированной временной отсечки.
- **Для инцидентов с риском "Средний" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания** – при активации опции оповещение для инцидентов со средним риском будет отправляться после прохождения последней сконфигурированной временной отсечки.
- **Для инцидентов с риском "Низкий" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания** – при активации опции оповещение для инцидентов с низким риском будет отправляться после прохождения последней сконфигурированной временной отсечки.
- **Для инцидентов с риском "Отсутствует" отправлять оповещение регулярно каждые <...> дн., после достижения последнего показателя времени удержания** – при активации

опции оповещение для инцидентов с отсутствующим риском будет отправляться после прохождения последней сконфигурированной временной отсечки.

- **Отправлять группу сообщений раз в неделю. День недели <...>** – при активации опции все накопившиеся оповещения будут отправляться единожды в указанный день.

Блок настройки текстов для оповещений

Для оповещений по задержкам в обработке инцидентов можно настроить следующий текст:

- 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".

10.3 Черный список ID плагинов

Для настройки списка ID плагинов сканеров уязвимости, которые будут игнорироваться в процессе работы, перейдите в раздел **Параметры → Черный список ID плагинов** (см. «Рис. 187»).

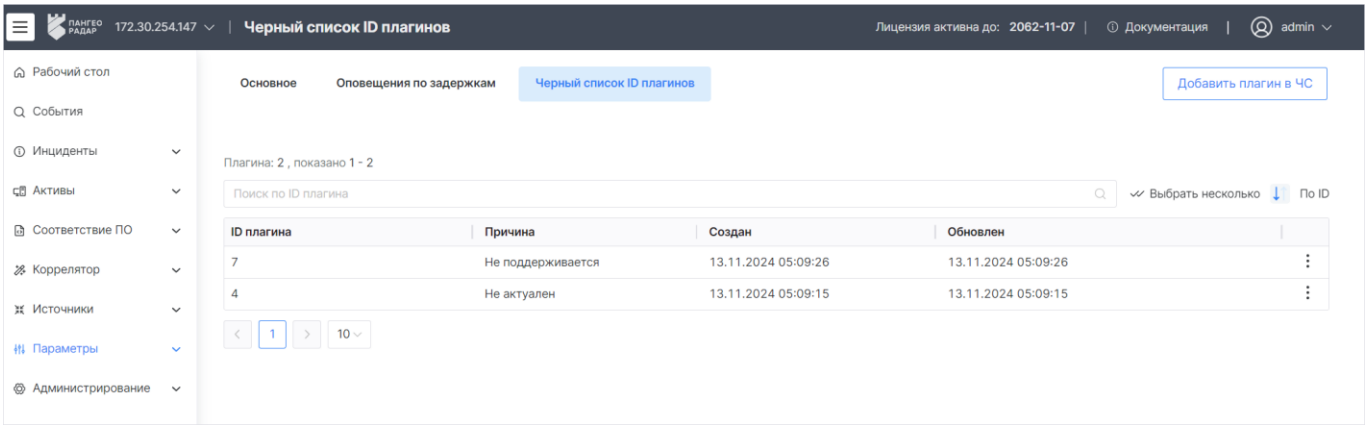


Рис. 187 – Раздел "Черный список ID плагинов"

В разделе отображается следующая информация:

- **ID плагина** – идентификатор плагина;
- **Причина** – описание причины добавления плагина в черный список;
- **Создан** – дата и время создания записи о добавлении плагина в черный список;
- **Обновлен** – дата и время обновления записи о добавлении плагина в черный список;

Для добавления плагина в черный список выполните следующие действия:

1. Нажмите кнопку **Добавить плагин в ЧС**. Откроется окно добавления плагина в ЧС (см. «Рис. 188»).

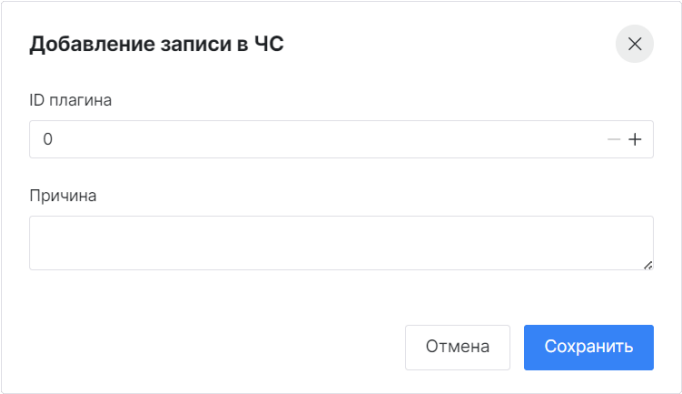


Рис. 188 – Добавление плагина в ЧС"

2. Укажите в окне следующую информацию:
    - в поле **ID** укажите идентификатор плагина;
    - в поле **Причина** укажите причину добавления плагина в черный список.
3. Нажмите кнопку **Сохранить**.

10.4 Фоновые задачи

В разделе отображается информация о запущенных задачах ретроспективной корреляции, синхронизации и отчетов.

Для просмотра информации о фоновых задачах, запущенных в **Платформе Радар** перейдите в раздел **Параметры → Фоновые задачи** (см. «Рис. 189»).

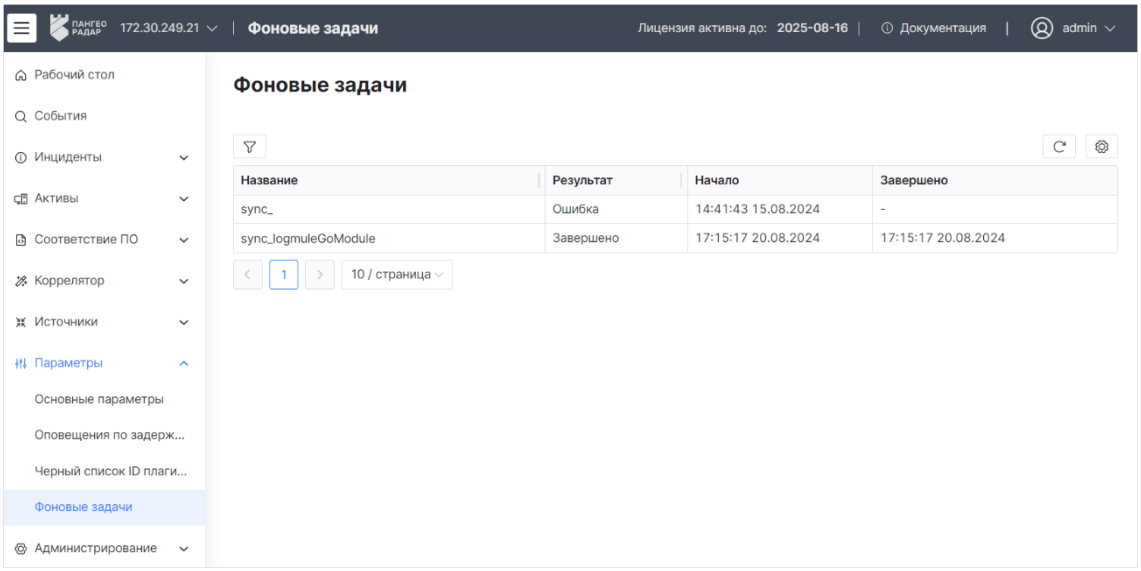


Рис. 189 – Раздел "Фоновые задачи"

В разделе отображается следующая информация:

- **Название** – наименование задачи;
- **Результат** – описание результата выполнения задачи (контекст зависит от задачи);
- **Начало** – дата и время запуска задачи;
- **Завершено** – дата и время завершения задачи.

10.5 Интеграции

Платформа Радар позволяет добавлять интеграции со сторонними системами.

Различные классы систем, с которым можно настроить интеграцию, называются в платформе **Типами интеграций**. Для каждого типа поддерживаемой системы может быть одновременно настроено несколько интеграций.

Интеграции могут находится в следующих состояниях:

- **Активно** – по интеграции выполняется взаимодействие со сторонней системой;
- **Неактивно** – по интеграции не выполняется взаимодействие со сторонней системой.

В платформе поддерживаются следующие типы интеграций:

- «RT Protect EDR» – система обнаружения целенаправленных атак и сложных угроз;
- «Kaspersky Security Center» – универсальная консоль централизованного управления различными решениями, продуктами и сервисами, которые обеспечивают информационную безопасность корпоративной ИТ-инфраструктуры.

Примечание: *Процессы работы с различными типами интеграций рассмотрены в соответствующих разделах*.

Все действия над интеграциями выполняются в разделе **Параметры → Интеграции** (см. «Рис. 190»).

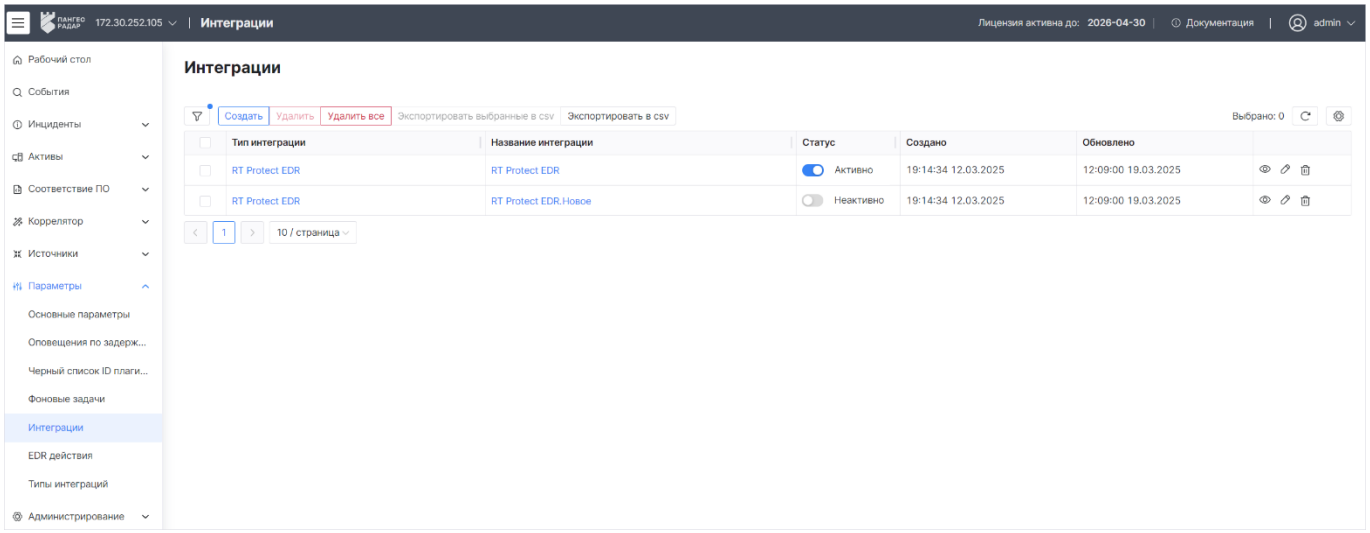


Рис. 190 – Раздел "Интеграции"

В разделе отображается следующая информация:

- **Тип интеграции** – наименование типа интеграции, к которой относится интеграция;
- **Название интеграции**;
- **Статус** – состояние интеграции: Активно, Неактивно;
- **Создано** – дата и время создания интеграции;
- **Обновлено** – дата и время обновления информации об интеграции.

В разделе используются стандартные элементы управления, которые доступны через «универсальные таблицы» или инструмент «боковая панель».

10.6 Типы интеграций

Для просмотра поддерживаемых в платформе типов интеграций перейдите в раздел **Параметры → Типы интеграций** (см. «Рис. 191»).

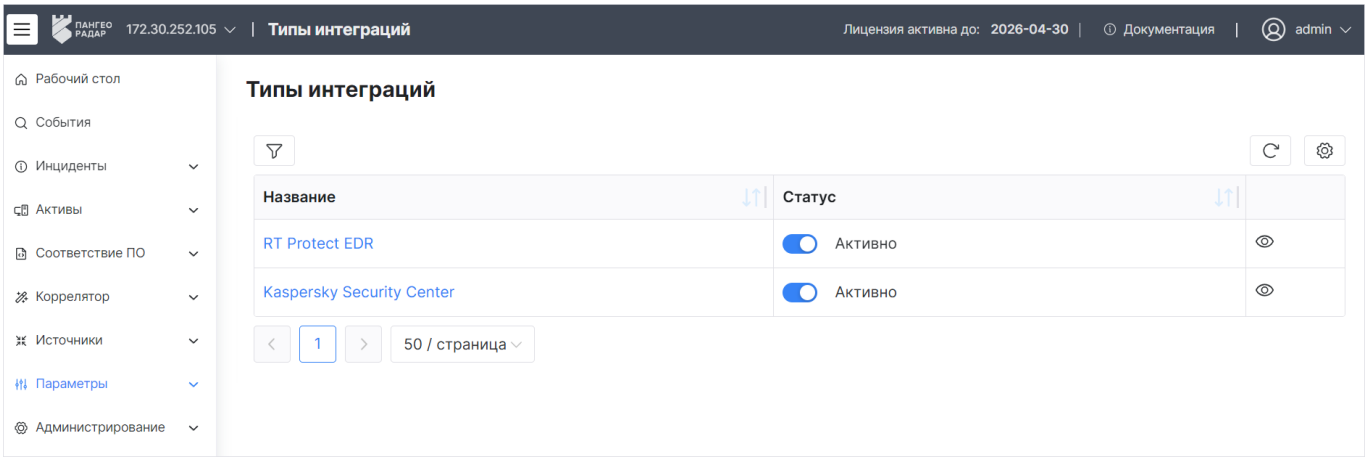


Рис. 191 – Раздел "Типы интеграций"

В разделе отображается наименование сторонних систем, с которыми в платформе можно настроить интеграцию.

Тип интеграции может находится в следующих состояниях:

- **Активно** – платформа переведена в режим взаимодействия с данным типом интеграции. В этом режиме могут быть изменены элементы интерфейса платформы и появятся дополнительные функции для поддержки интеграции;
- **Неактивно** – в данном состоянии платформа не поддерживает дополнительные функции необходимые для работы интеграций, настроенных для данного типа.

Для включения поддержки типа интеграции в платформе переведите соответствующий переключатель в состояние **Активно**.

Для просмотра подробной информации о типе интеграции нажмите кнопку .

Примечание: Подробная информация о каждом типе интеграции рассмотрена в соответствующих разделах.

10.7 Папки контента

Общие принципы работы с содержимом папок описано в разделе (см. раздел **Интерфейс** → «Папки контента»).

Для работы с папками перейдите в раздел **Параметры → Папки контента** (см. «Рис. 192»).

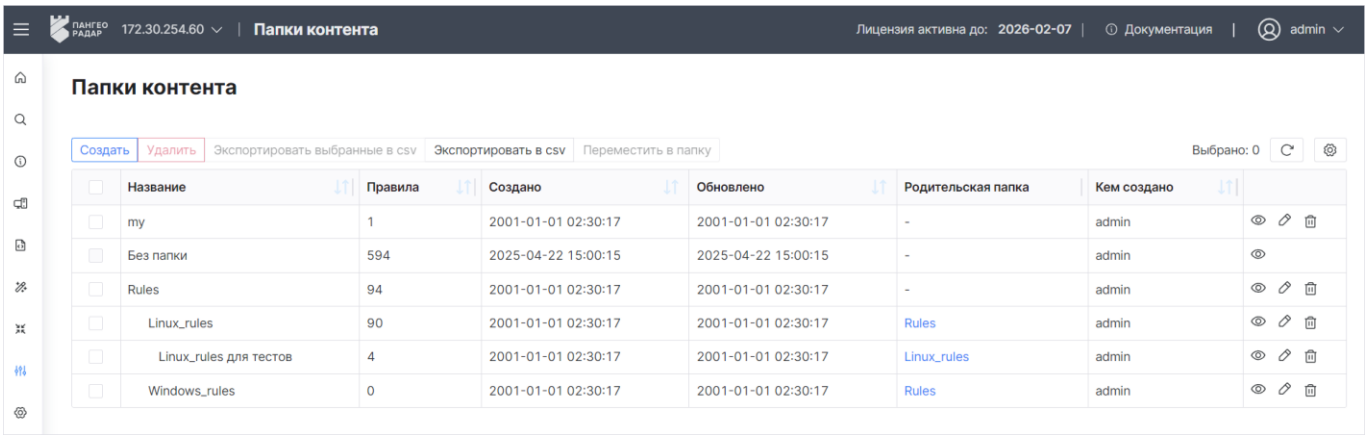


Рис. 192 – Раздел "Папки контента"

В разделе отображается следующая информация:

- **Название** – наименование папки. Смещение наименования папки означает вложенность данной папки относительно папки выше по списку;
- **Правила** – количество правил, помещенных в папку;
- **Создано** – дата и время создания папки;
- **Обновлено** – дата и время обновления информации о папке;
- **Кем создано** – наименование пользователя, создавшего папку.

Примечание: В каталоге "Без папки" содержится неструктурированный контент. Данный каталог является системным и не может быть удален.

В разделе используются стандартные элементы управления, которые доступны через «универсальные таблицы».

10.8 Шаблоны

Общие принципы работы с шаблонами описаны в разделе **Интерфейс** → «Шаблоны объектов».

Управление шаблонами выполняется в разделе **Параметры** → **Шаблоны** (см. «Рис. 193»).

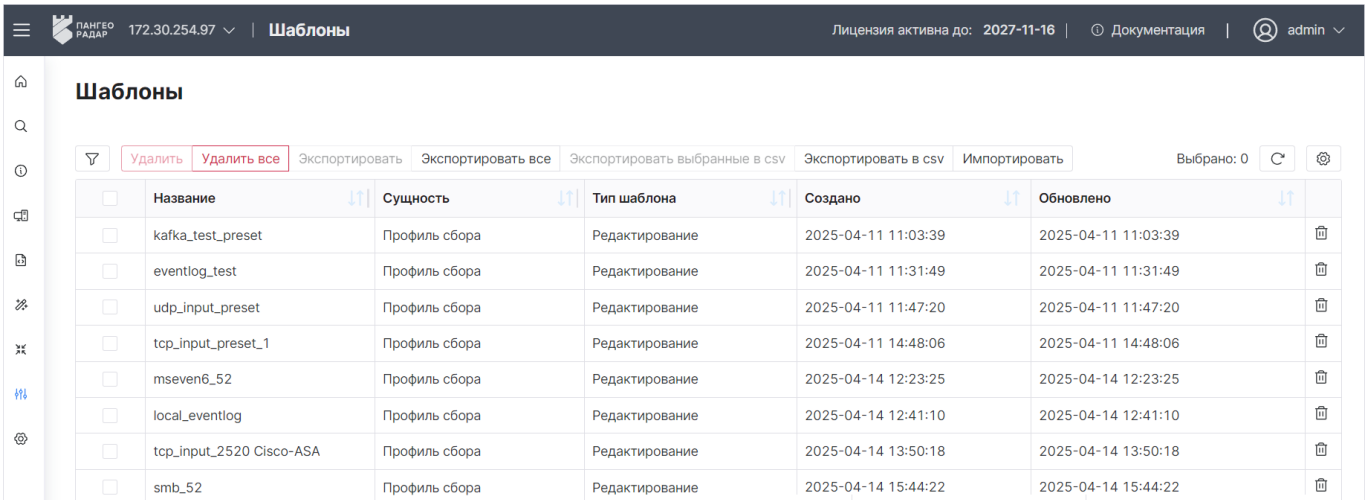


Рис. 193 – Раздел "Шаблоны"

В разделе отображается следующая информация о шаблонах:

- **Название** – наименование шаблона;
- **Сущность** – тип пользовательского контента, для которого настроен шаблон;
- **Тип шаблона** – тип формы, для которой настроен шаблон: создание или редактирование;
- **Создано** – дата и время создания шаблона;
- **Обновлено** – дата и время обновления информации о шаблоне.

11. Рабочие столы

11.1 Общие данные

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

Отображение информации выполняется с помощью следующих типов виджетов:

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

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

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

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

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

Пример интерфейса раздела представлен на «Рис. 194».

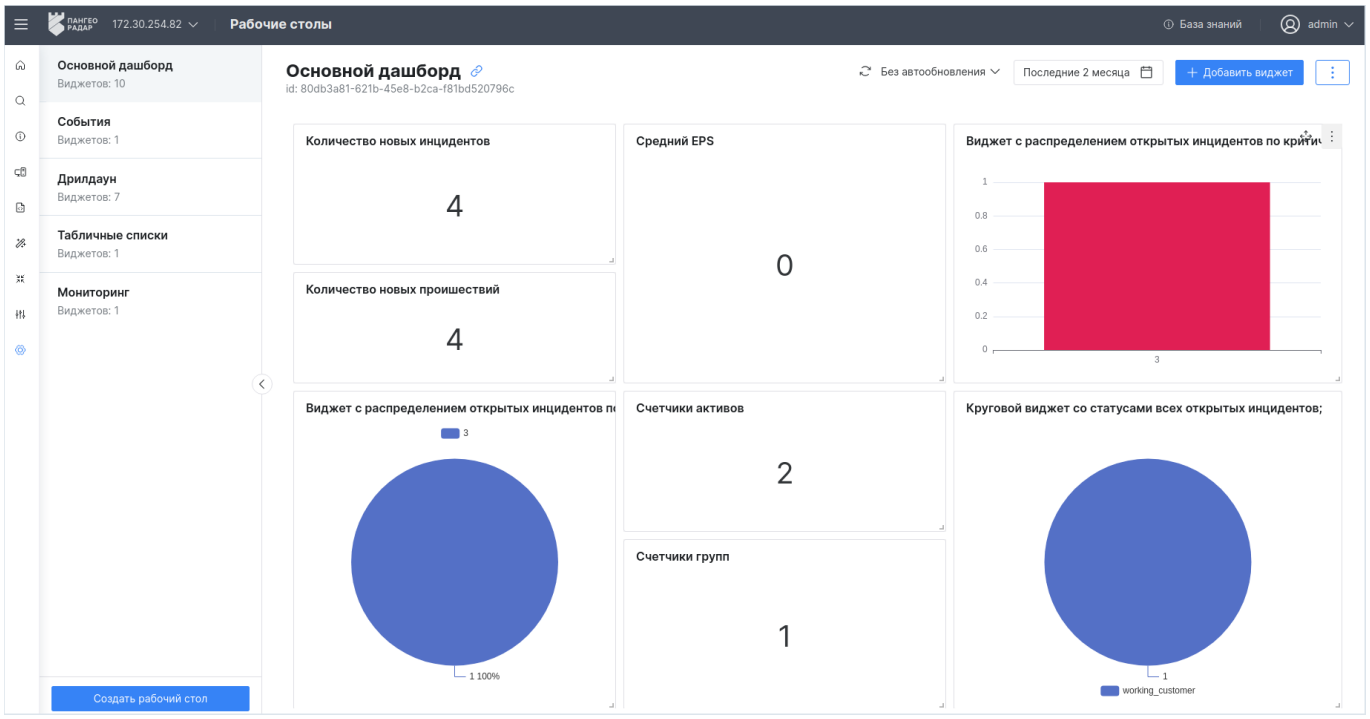


Рис. 194 – Интерфейс раздела "Рабочие столы"

Раздел состоит из следующих блоков:

- **Список рабочих столов**, в котором отображается информация о доступных рабочих столах:
  - название рабочего стола;
  - количество виджетов, добавленных на рабочий стол.
- **Рабочая область**, в которой отображается информация о выбранном рабочем столе:
  - название рабочего стола;
  - идентификатор рабочего стола;
  - информация о виджетах, добавленных на рабочий стол: заголовок, описание и содержимое виджета (см. «Рис. 195»);
  - режим автообновления рабочего стола;
  - период времени, за который формируется информация для рабочего стола.

Пример отображения информации о виджете приведен на «Рис. 195».

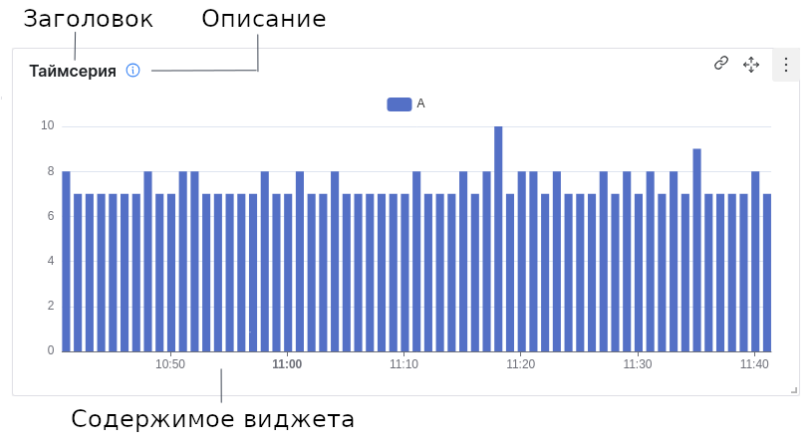


Рис. 195 – Пример виджета

На странице доступны следующие элементы управления рабочим столом:

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

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

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

11.2 Создание рабочего стола

Перейдите в раздел **Администрирование → Рабочие столы** и нажмите кнопку Создать рабочий стол. Откроется окно "Создание рабочего стола" (см. «Рис. 196»).

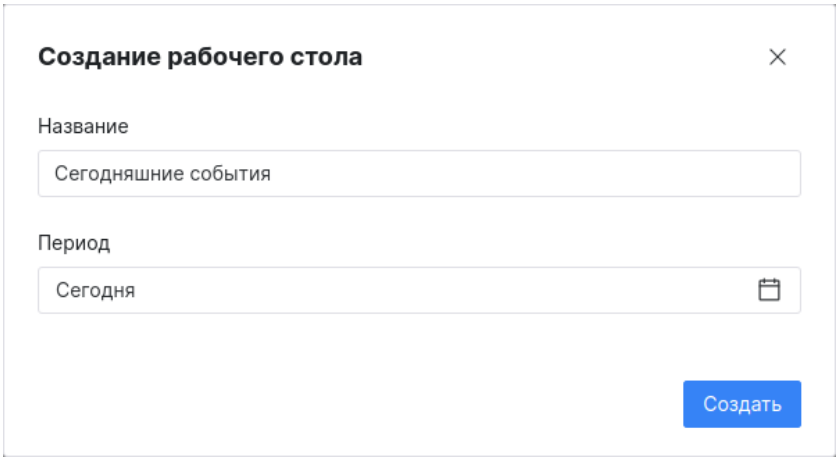


Рис. 196 – Окно "Создание рабочего стола"

Выполните следующие действия:

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

После создания рабочего стола рекомендуется выполнить следующие действия:

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

11.3 Редактирование рабочего стола

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

Откроется страница редактирования рабочего стола (см. «Рис. 197»).

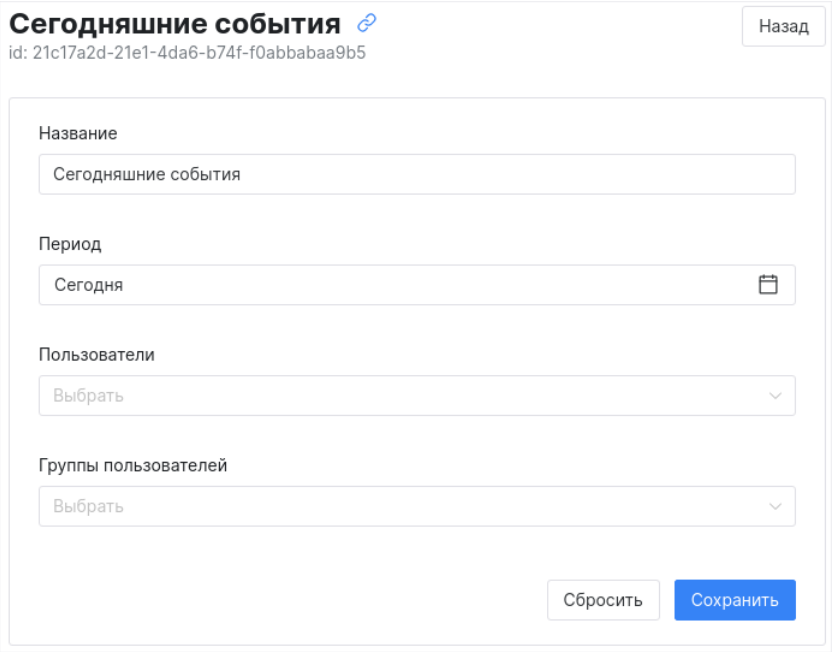


Рис. 197 – Страница редактирования рабочего стола

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

Настроить права доступа пользователей к рабочему можно следующими способами:

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

11.4 Управление виджетами

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

При работе с виджетами выполняются следующие процессы:

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

11.4.1 Установка периода и обновление данных виджетов

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

Для этого выполните следующие действия:

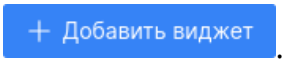
1. Нажмите кнопку  . Откроется окно выбора временного диапазона.
2. Выберите период. Доступные значения:
    - за все время;
    - текущие: минута, час, день, месяц, год;
    - последние: минуты, часы, месяца, года;
    - период можно указать вручную в соответствующих полях. Поддерживается формат дат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

Для обновления отображаемых данных нажмите кнопку  .

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

11.4.2 Добавление виджета на рабочий стол

Для добавления виджета на рабочий стол выполните следующие действия:

1. Выберите нужный рабочий стол и нажмите кнопку 

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

11.4.3 Переход к табличному представлению данных

Платформа позволяет перейти к табличному представлению данных выбранного виджета.

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

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

11.4.4 Редактирование виджета

Для редактирования виджета выполните следующие действия:

1. Перейдите на рабочий стол и выберите виджет.

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

11.4.5 Копирование настроек виджета

Для копирования настроек виджета выполните следующие действия:

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

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

11.4.6 Изменение расположения виджета

Для изменения расположения виджета выполните следующие действия:

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

11.4.7 Изменение размера виджета

Для изменения размера виджета выполните следующие действия:

1. Перейдите на рабочий стол и выберите виджет.
2. Нажмите и удерживайте правый нижний угол виджета (см. «Рис. 198»).

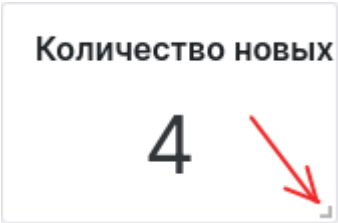


Рис. 198 – Кнопка изменения размера виджета

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

11.4.8 Удаление виджета

Для удаления виджета с рабочего стола выполните следующие действия:

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

11.5 Копирование рабочего стола

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

11.6 Создание отчета

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

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

Для этого выберите нужный рабочий стол и выполните следующие действия:

1. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Создать отчет**. Откроется окно "Создание отчета" (см. «Рис. 199»).

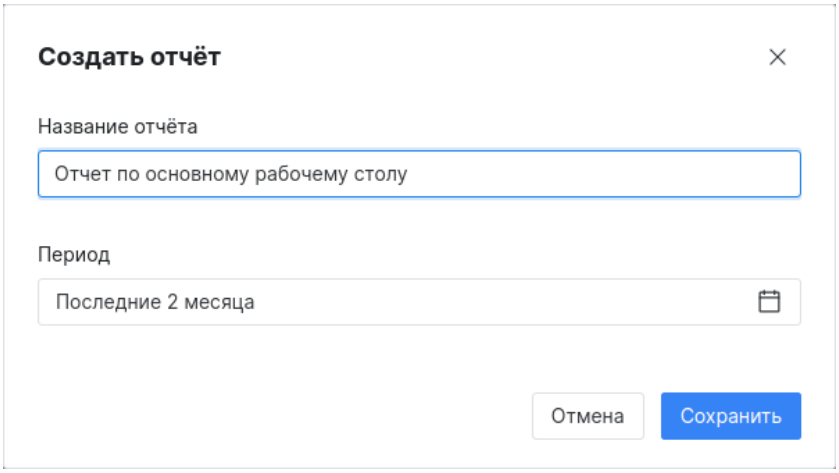


Рис. 199 – Окно "Создать отчет"

2. Укажите следующие данные:
   - в поле "Название отчета" укажите название отчета;
   - в поле "Период" из выпадающего списка выберите период формирования отчета.
3. Нажмите кнопку **Сохранить**. Откроется страница с отчетом (см. «Рис. 200»).

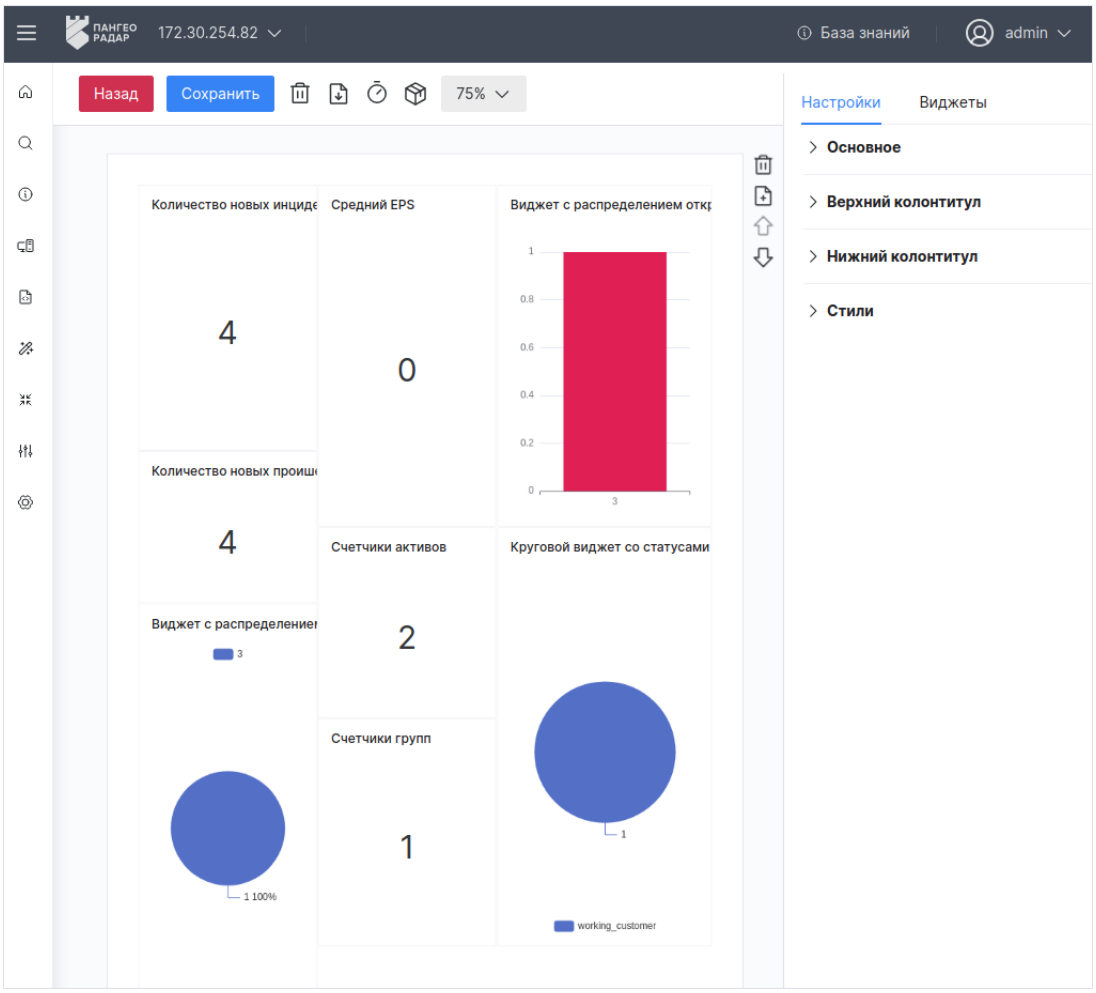


Рис. 200 – Страница с отчетом

Дальнейшие действия над отчетом выполняются в разделе «Отчеты».

11.7 Удаление рабочего стола

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

11.8 Grafana. Единицы измерения и временной диапазон

Grafana поддерживает следующие единицы измерения временного диапазона:

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

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

В таблице приведены примеры временных диапазонов:

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

12. Конструктор виджетов

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

Перейти в конструктор виджетов можно несколькими способами:

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

Внешний вид конструктора виджетов приведен на «Рис. 201».

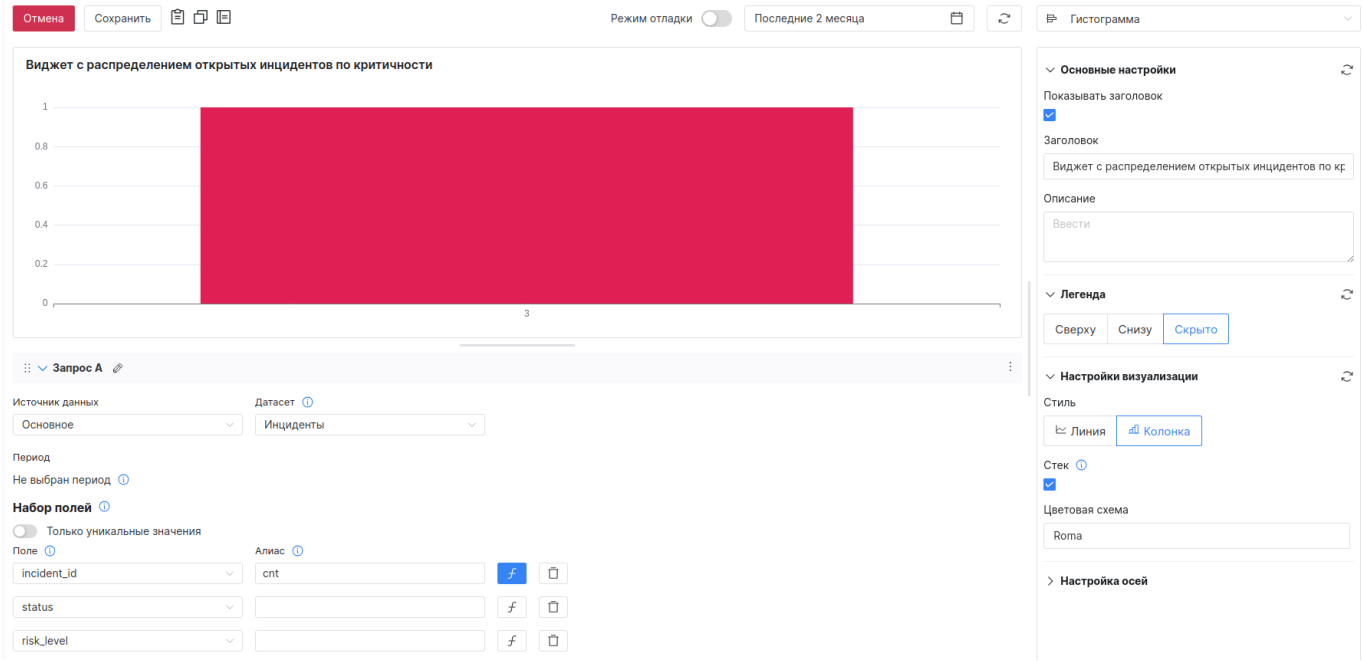


Рис. 201 – Страница "Конструктор виджетов"

Конструктор состоит из следующих блоков:

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

Панель действий

Блок располагается вверху страницы конструктора виджетов (см. «Рис. 202»).

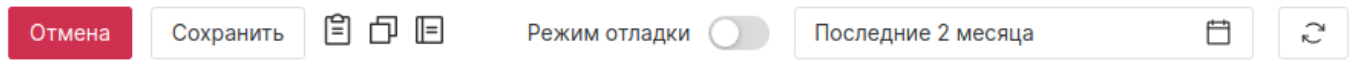


Рис. 202 – Конструктор виджетов. Блок "Панель действий"

На панели действий доступны следующие элементы управления:

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

Режим визуализации/Режим отладки

Блок располагается по центру конструктора. Переключение между режимами выполняется с помощью переключателя **Режим отладки**. В режиме визуализации можно посмотреть то, как виджет будет выглядеть на рабочем столе или странице отчета (см. «Рис. 203»).

Рис. 203 – Конструктор виджетов. Блок "Режим визуализации"

В режиме отладки можно посмотреть корректность работы написанных запросов (см. «Рис. 204»).

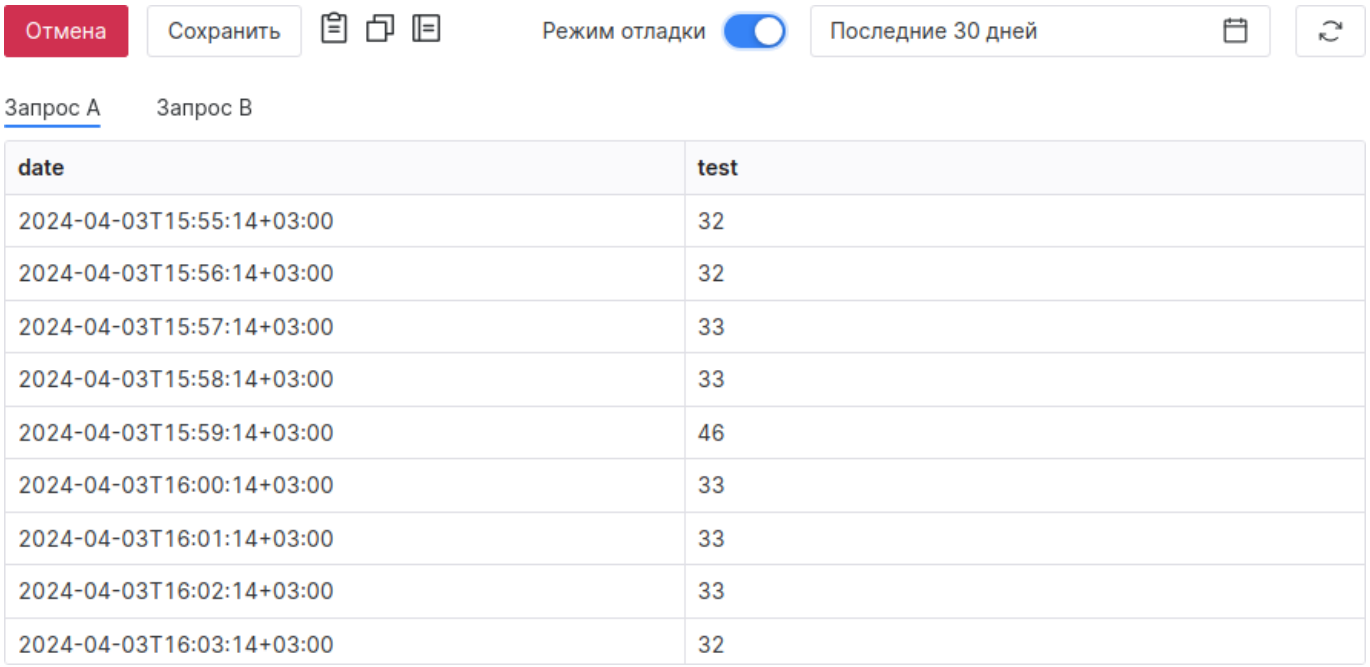


Рис. 204 – Конструктор виджетов. Блок "Режим отладки"

Конструктор запросов

Блок располагается под режимом визуализации/отладки (см. «Рис. 205»).

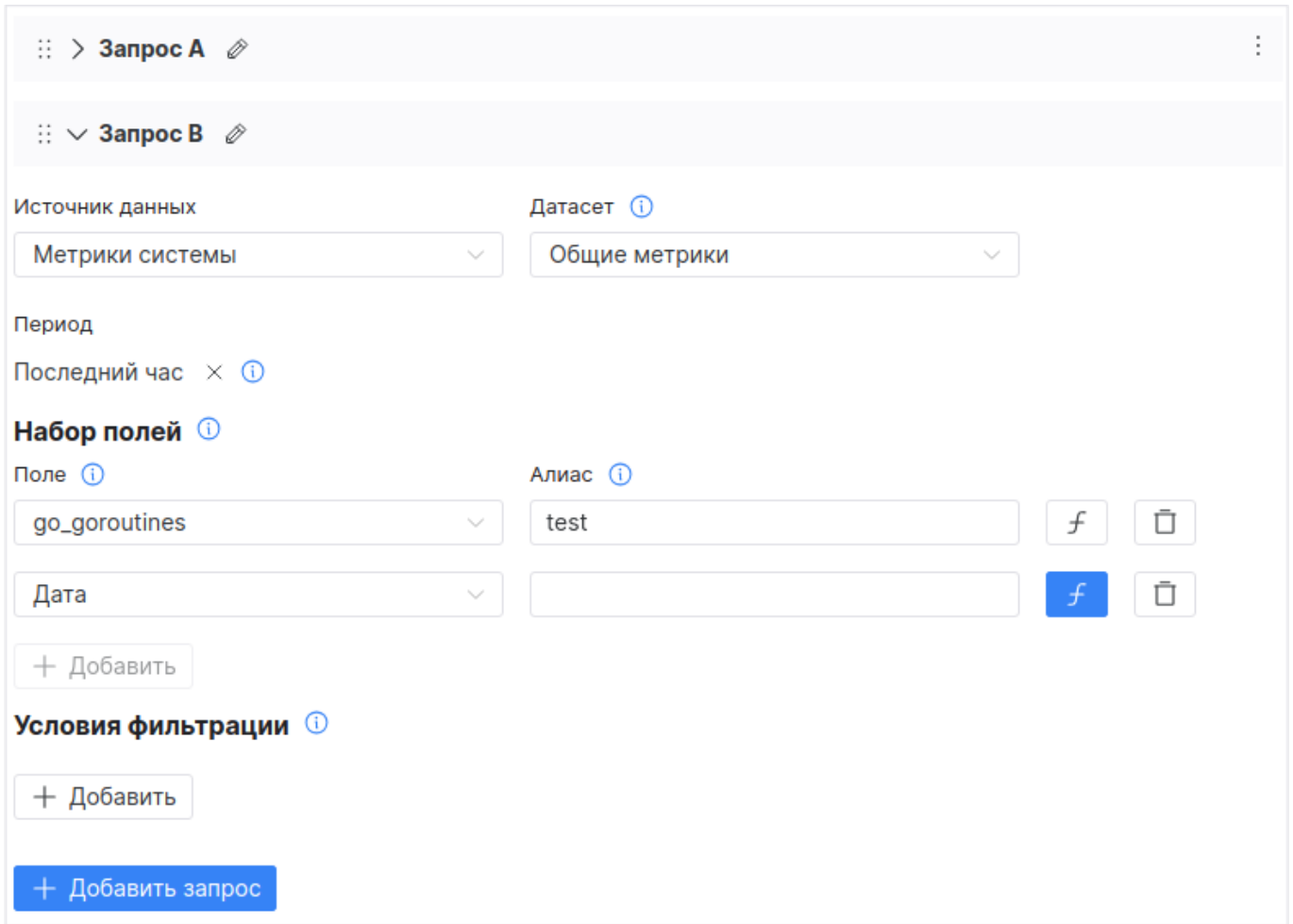


Рис. 205 – Конструктор виджетов. Блок "Конструктор запросов"

В конструкторе запросов доступны следующие элементы управления запросами:

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

Настройка внешнего вида виджета

Блок располагается в правой части страницы конструктора и формируется в зависимости от выбранного виджета (см. «Рис. 206»).

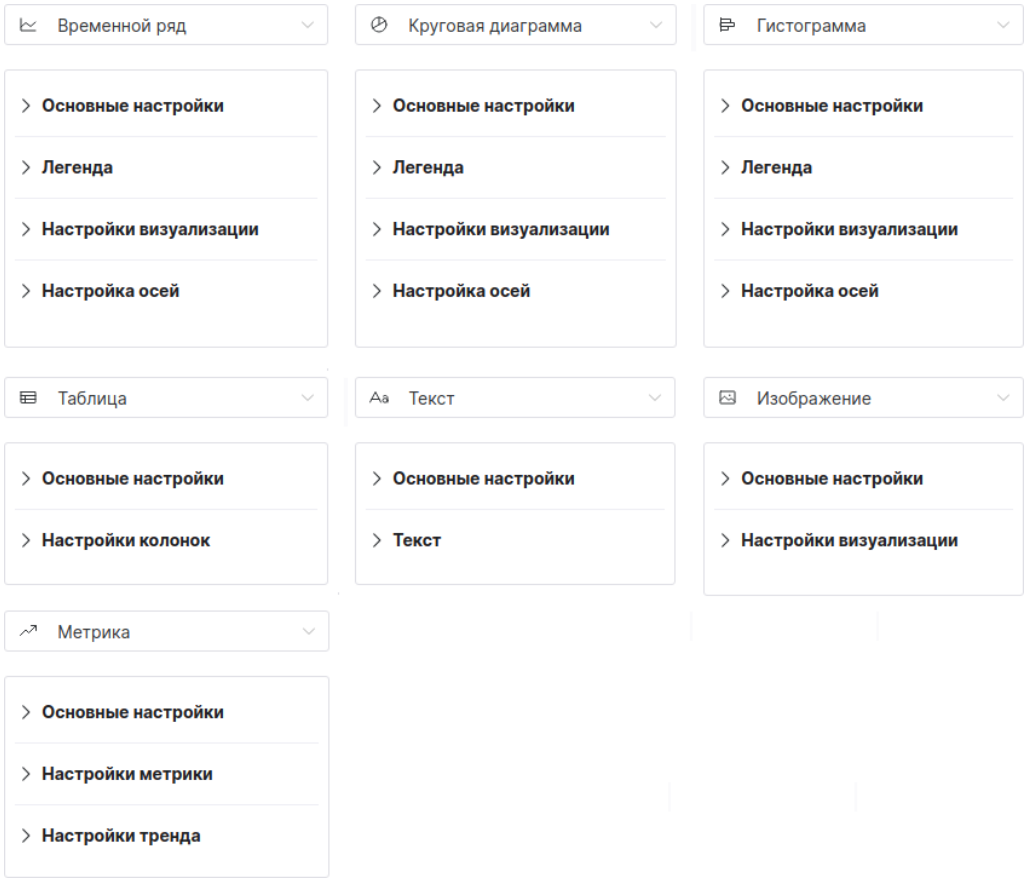


Рис. 206 – Конструктор виджетов. Блок "Настройка внешнего вида виджета"

12.1 Особенности работы в конструкторе

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

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

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

Стандартный процесс настройки виджета может выглядеть следующим образом:

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

12.2 Конструктор запросов

Управление запросами включает в себя следующие процессы:

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

12.2.1 Добавление запроса

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

Для начала процесса добавления запроса нажмите кнопку + Добавить запрос.

При необходимости вы можете изменить наименование запроса нажав кнопку .

Добавление запроса можно условно разделить на несколько шагов:

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

12.2.1.1 Шаг 1. Выбор источника данных и датасета

На данном шаге необходимо выбрать источник данных, информация из которого будет обрабатываться запросом, и соответствующий набор данных - датасет (см. «Рис. 207»).

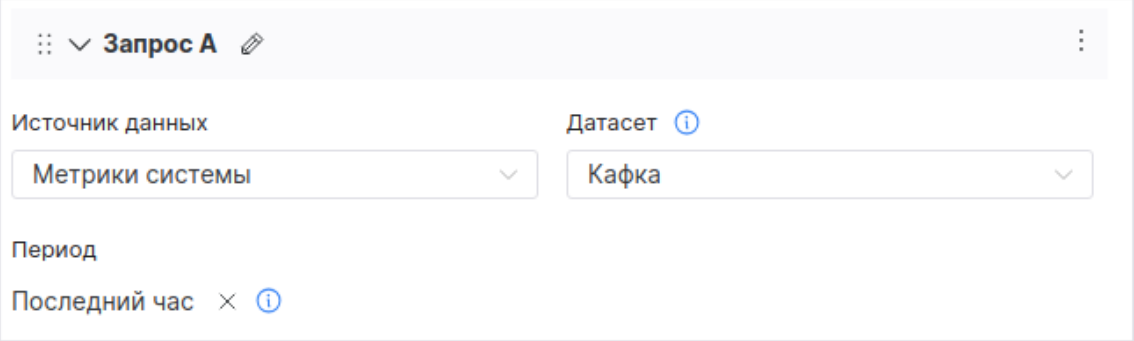


Рис. 207 – Конструктор запросов. Выбор источника данных, датасета и периода

Соответствие источников данных и датасетов приведено в таблице:

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

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

12.2.1.2 Шаг 2. Выбор периода формирования запроса

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

Для изменения периода формирования запроса (см. «Рис. 207») выполните следующие действия:

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

12.2.1.3 Шаг 3. Настройка набора полей

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

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

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

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

Для настройки набора полей выполните следующие действия:

1. Если вы хотите, чтобы в запросе отображались только уникальные значения полей, то включите переключатель **Только уникальные значения**.
2. Нажмите кнопку + Добавить.
3. Появятся параметры для настройки поля (см. «Рис. 208»).

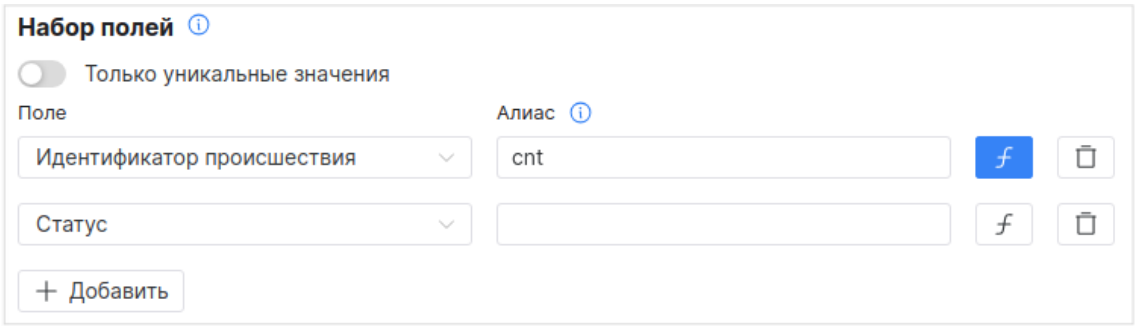


Рис. 208 – Конструктор запросов. Набор полей

4. Выберите необходимое поле датасета из выпадающего списка.
5. При необходимости укажите алиас.
6. При необходимости задайте агрегацию. Для этого нажмите на кнопку добавления агрегации. Откроется окно "Настройки поля" (см. «Рис. 209»).

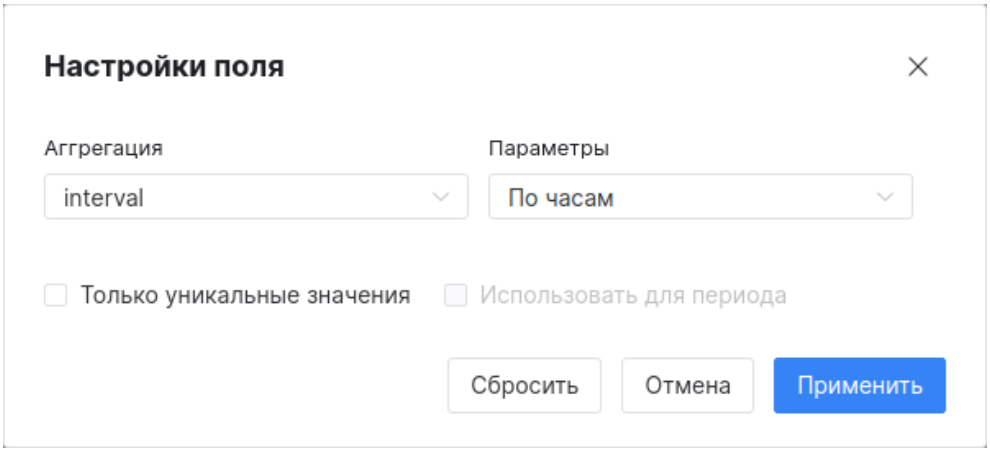


Рис. 209 – Окно "Настройки поля"

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

12.2.1.4 Шаг 4. Условия фильтрации

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

1. Нажмите кнопку + Добавить. Появятся параметры для настройки условия фильтрации (см. «Рис. 210»).

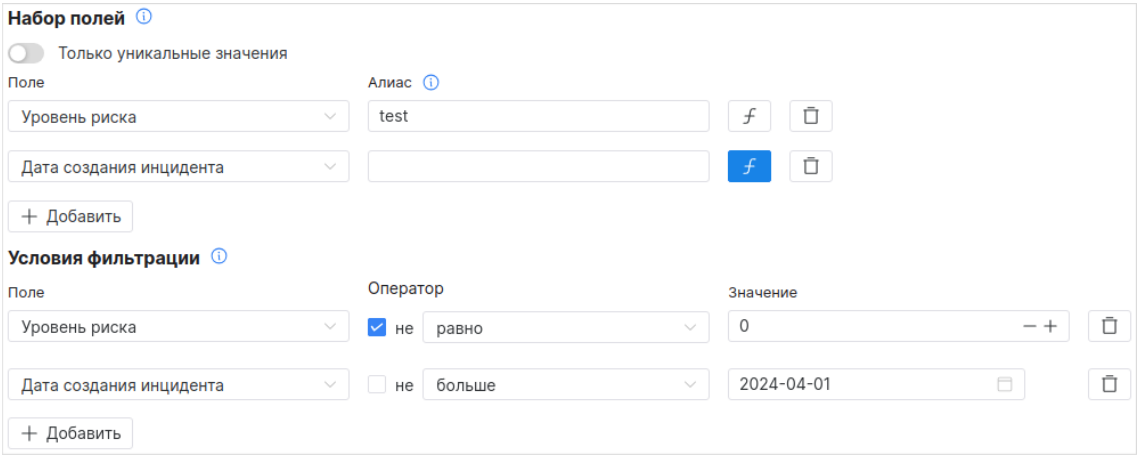


Рис. 210 – Конструктор запросов. Условия фильтрации

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

12.2.1.5 Шаг 5. Группировка и Сортировка

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

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

Для настройки нажмите кнопку + Добавить и выберите поле, по которому вы хотите выполнить группировку (см. «Рис. 211»).

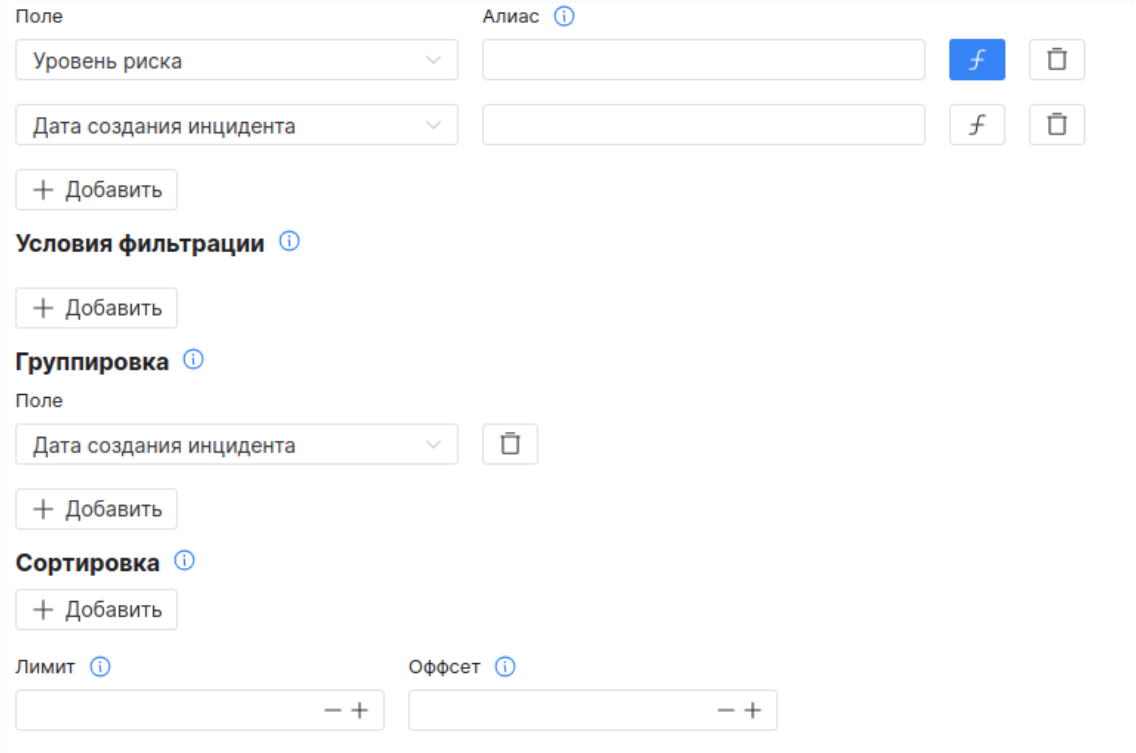


Рис. 211 – Конструктор виджетов. Группировка и сортировка

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

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

Для настройки сортировки выполните следующие действия:

1. Нажмите кнопку Добавить. Появятся параметры для настройки сортировки (см. «Рис. 211»).
2. Выберите поле из выпадающего списка, по которому вы хотите настроить сортировку.
3. Выберите направление сортировки: asc/desc.
4. В поле "Лимит" укажите значение лимита.
5. В поле "Оффсет" укажите значение оффсета.

12.2.2 Копирование запроса

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

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

12.2.3 Дублирование запроса

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

12.2.4 Удаление запроса

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

12.3 Настройка внешнего вида виджета

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

Настройку внешнего вида виджета условно можно разделить на следующие действия:

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

12.3.1 Основные настройки виджета

Блок "Основные настройки" является общим для всех типов виджетов (см. «Рис. 212»).

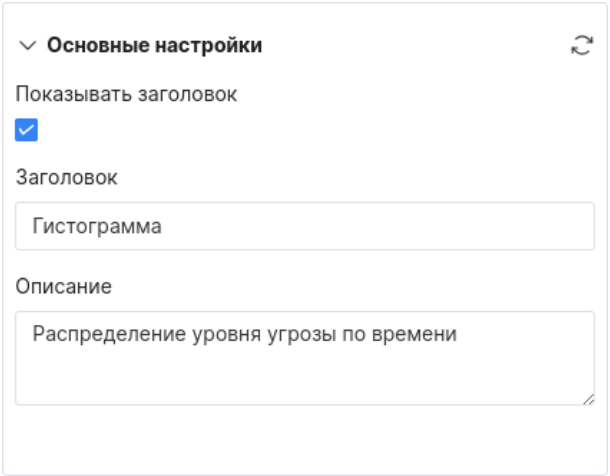


Рис. 212 – Основные настройки виджетов

В блоке доступны следующие настройки:

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

Пример отображения основных настроек приведен на «Рис. 213»

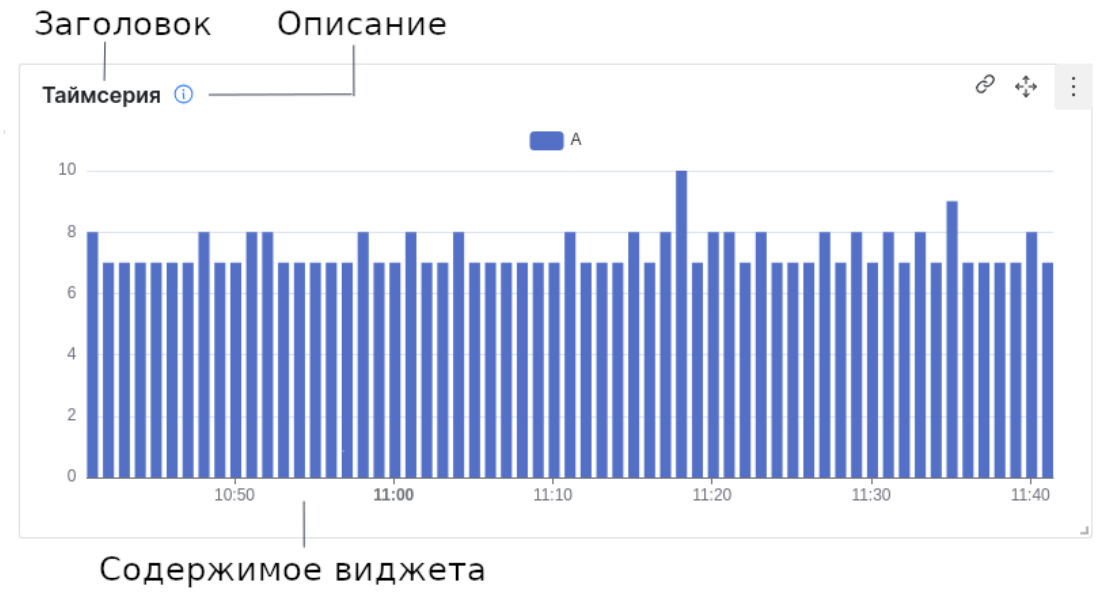


Рис. 213 – Отображение основных настроек на виджете

12.3.2 Временной ряд

Виджет отображает график с группировкой по количеству значений параметра от выбранного источника за определенный период времени. Пример внешнего вида приведен на «Рис. 214».

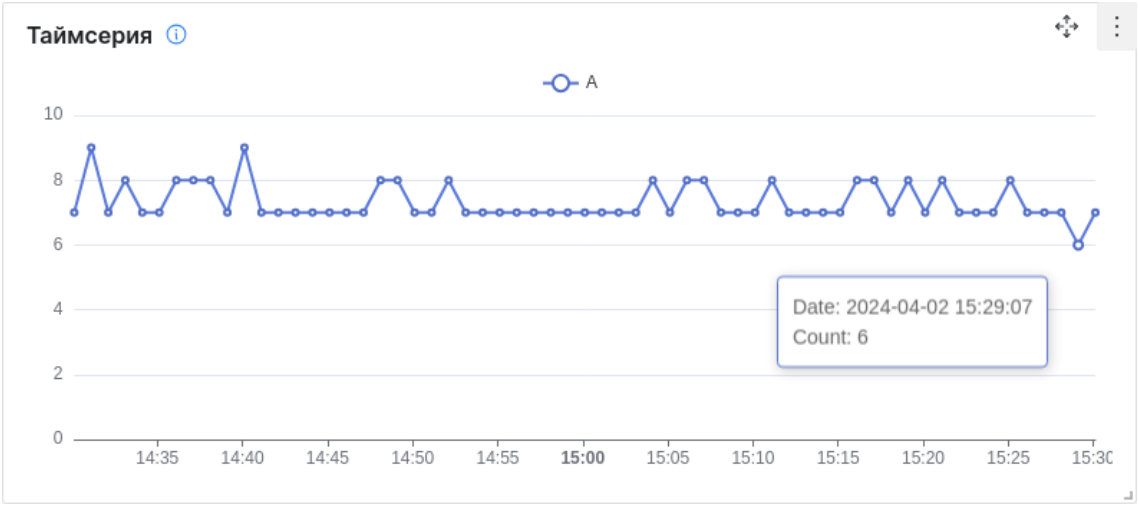


Рис. 214 – Виджет "Временной ряд"

Настройка внешнего вида виджета включает в себя следующие шаги:

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

Пример настроек приведен на «Рис. 215».

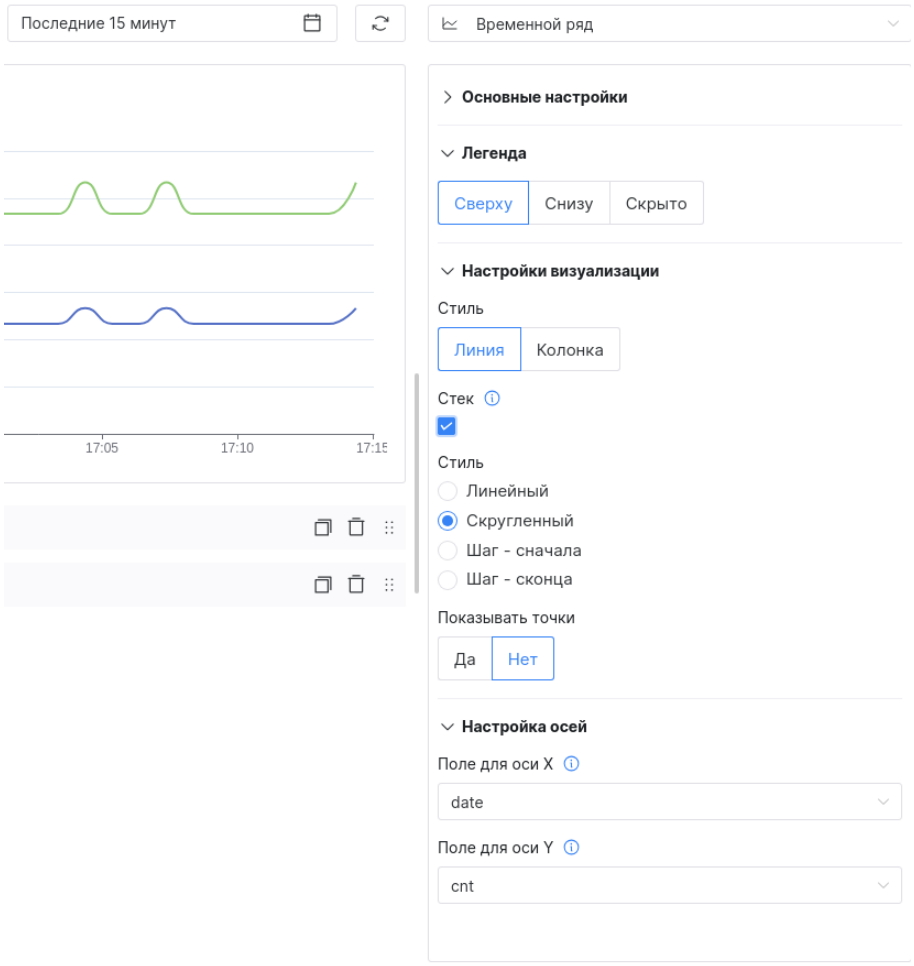


Рис. 215 – Виджет "Временной ряд". Настройки

12.3.2.1 Шаг 1. Настройка осей

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

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

Для настройки осей выполните следующие действия:

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

12.3.2.2 Шаг 2. Настройка визуализации

Настройка позволяет выбрать один из двух стилей графика:

- линия;
- колонка.

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

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

Примеры визуализации графика приведены на «Рис. 216».

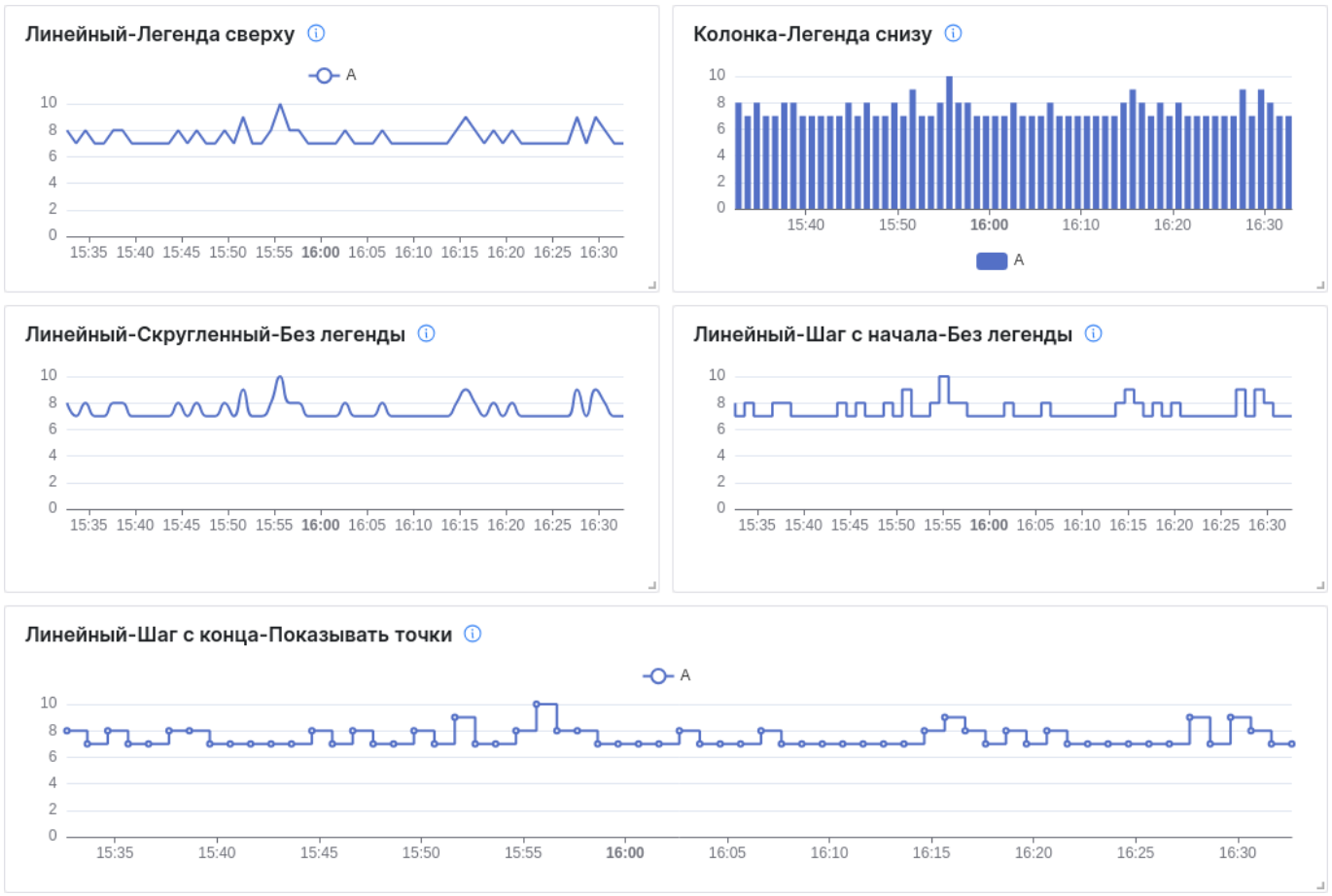


Рис. 216 – Примеры визуализации настроек виджета "Временной ряд"

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

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

Пример отображения с включенным и выключенным стеком приведен на «Рис. 217».

Рис. 217 – Пример визуализации виджета со стеком

Для настройки визуализации выполните следующие действия:

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

12.3.2.3 Шаг 3. Легенда

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

12.3.3 Круговая диаграмма

Виджет отображает группировку по выбранным параметрам с процентным распределением. Пример визуализации приведен на «Рис. 218».

Рис. 218 – Виджет "Круговая диаграмма"

Пример настроек приведен на «Рис. 219».

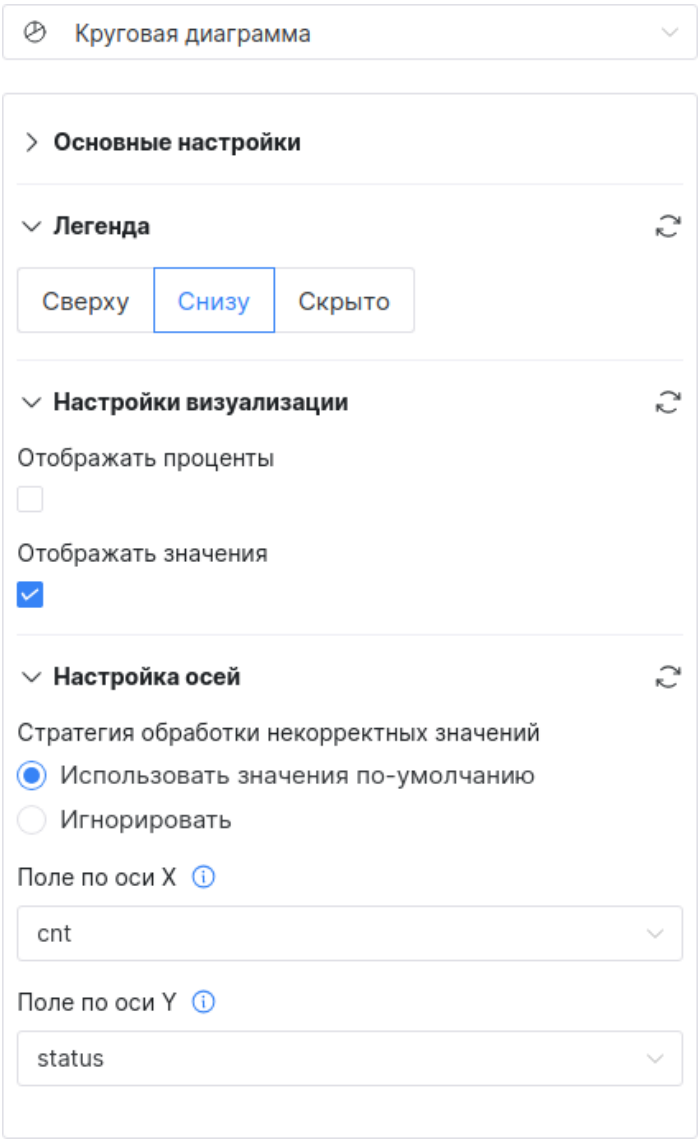


Рис. 219 – Виджет "Круговая диаграмма". Настройки

Для настройки внешнего вида виджета выполните следующие действия:

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

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

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

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

Варианты настроек визуализации приведены на «Рис. 220».

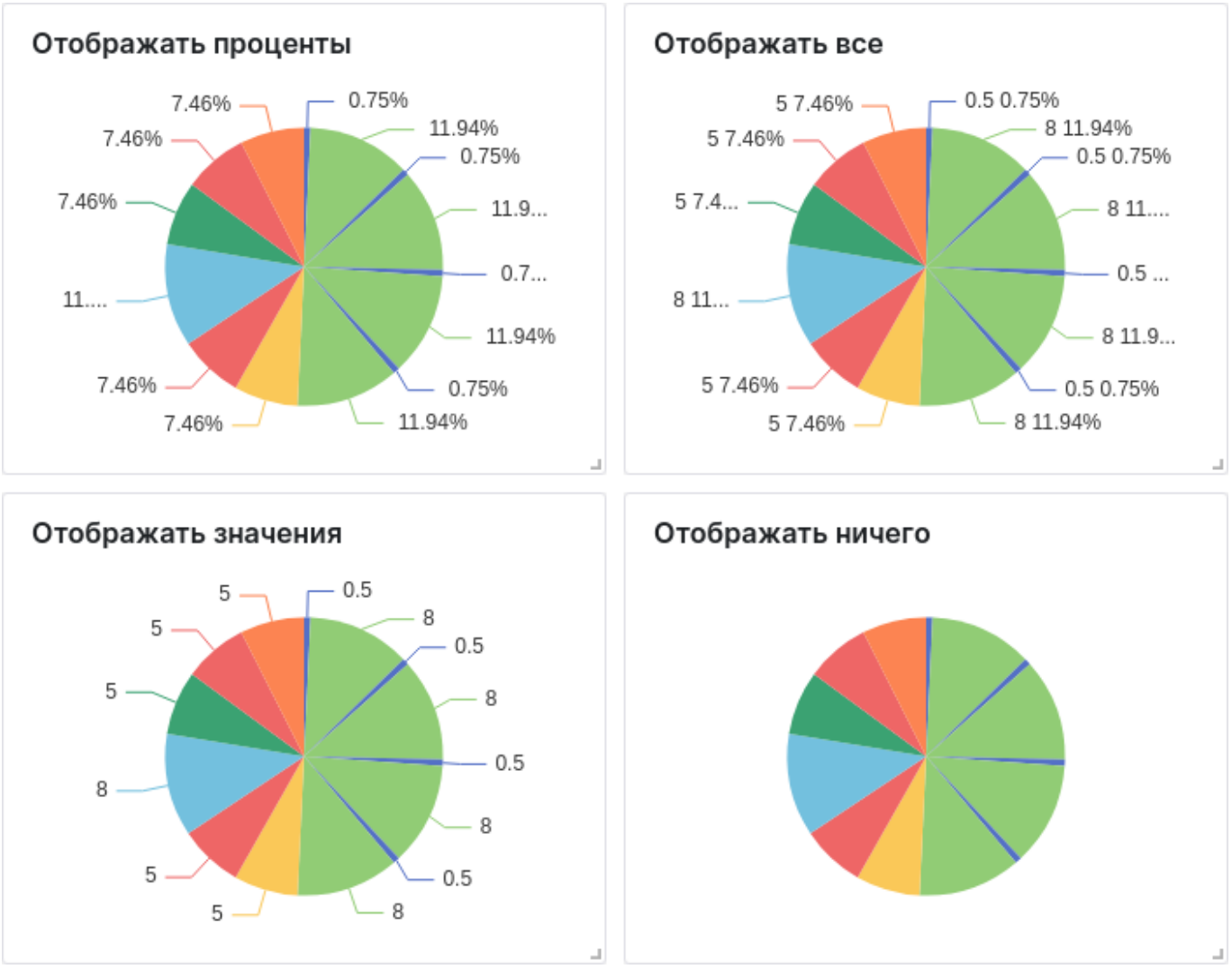


Рис. 220 – Примеры визуализации настроек виджета "Круговая диаграмма"

12.3.4 Таблица

Виджет отображает выбранные показатели в табличном варианте. Пример визуализации приведен на «Рис. 221».

Рис. 221 – Виджет "Таблица"

Пример блока "Настройки" приведен на «Рис. 222».

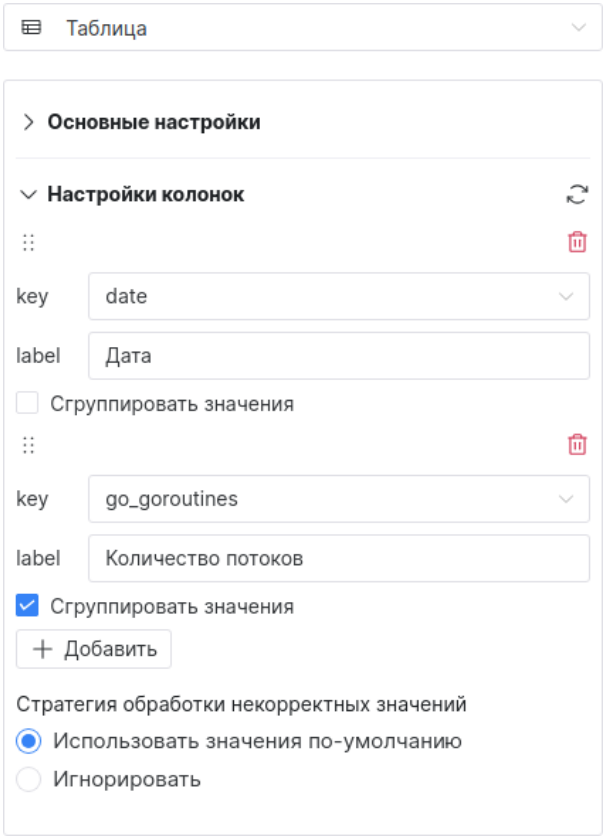
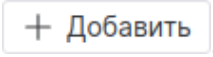


Рис. 222 – Виджет "Таблица". Настройки

Для настройки внешнего вида виджета выполните следующие действия:

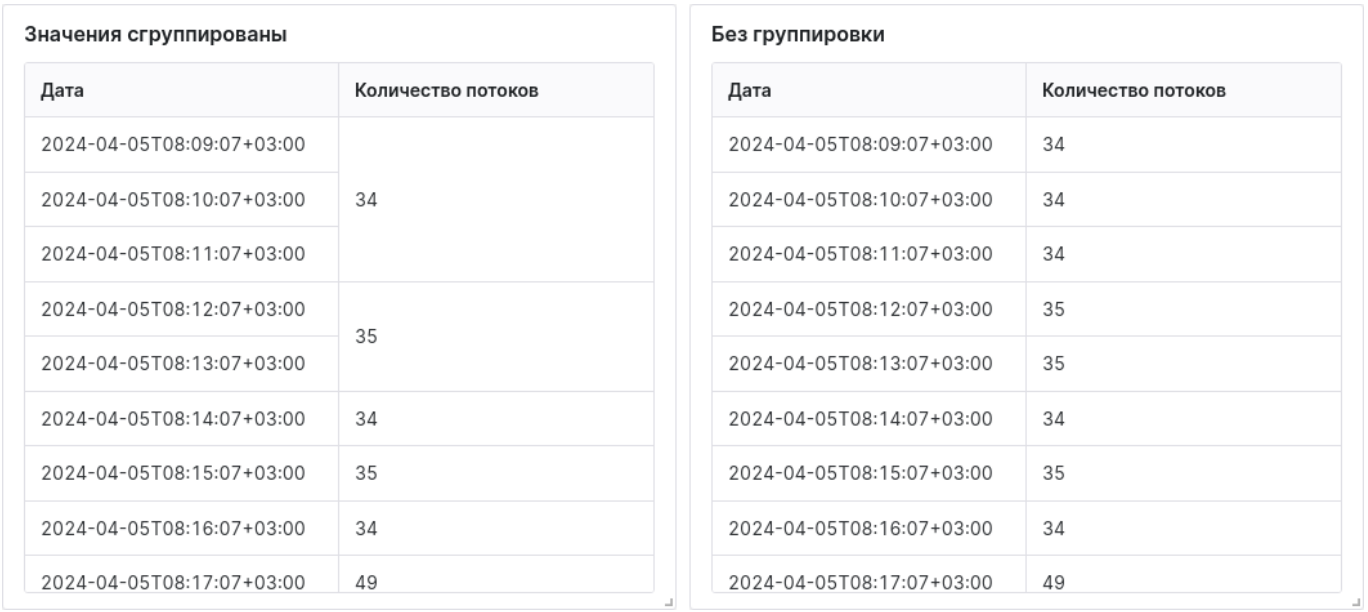
1. Для добавления колонок в таблицу нажмите кнопку 

. Добавьте необходимое количество колонок.
2. В поле "key" из выпадающего списка выберите поле или алиас из набора полей запроса, значения которого будут отображаться в колонке.

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

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

Примеры визуализации настроек приведены на «Рис. 223».



Значения сгруппированы

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

Без группировки

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

Рис. 223 – Примеры визуализации настроек виджета "Таблица"

12.3.5 Текст

Примечание: данный тип виджета не поддерживает серию запросов.

Виджет отображает текст, указанный пользователем.

Пример визуализации приведен на «Рис. 224».

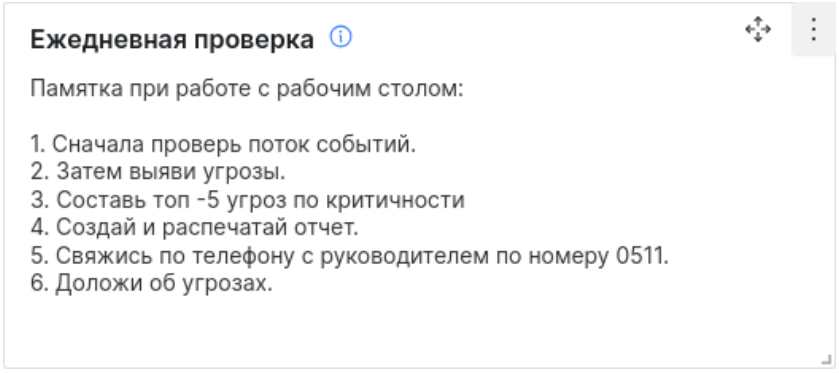


Рис. 224 – Виджет "Текст"

Пример настроек приведен на «Рис. 225».

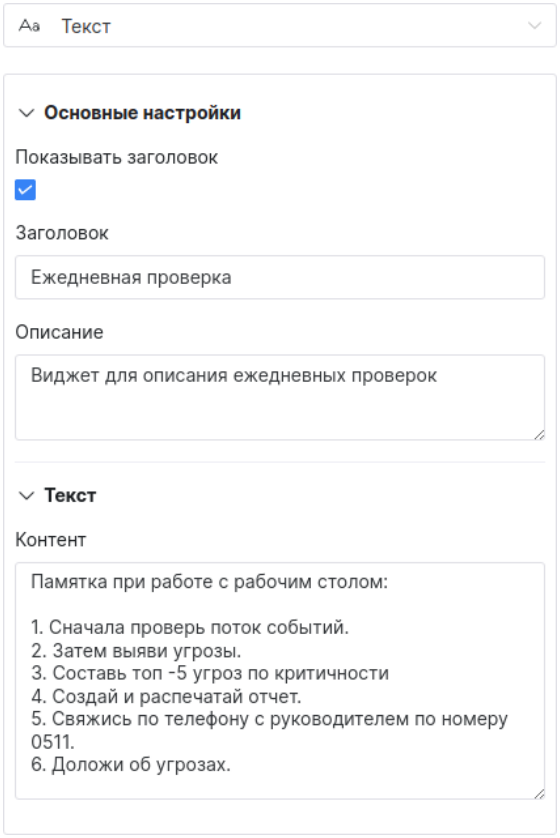


Рис. 225 – Виджет "Текст". Настройки

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

12.3.6 Гистограмма

Виджет отображает столбчатую диаграмму с группировкой по количеству значений параметра от выбранного источника за определенный период времени. Пример внешнего вида приведен на «Рис. 226».

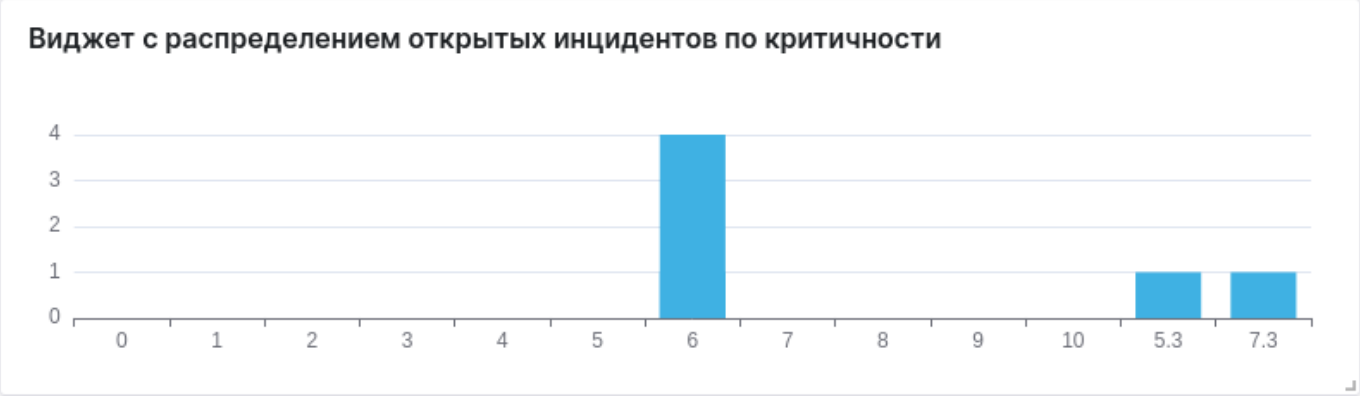


Рис. 226 – Виджет "Гистограмма"

Настройка внешнего вида виджета включает в себя следующие шаги:

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

Пример настроек приведен на «Рис. 227».

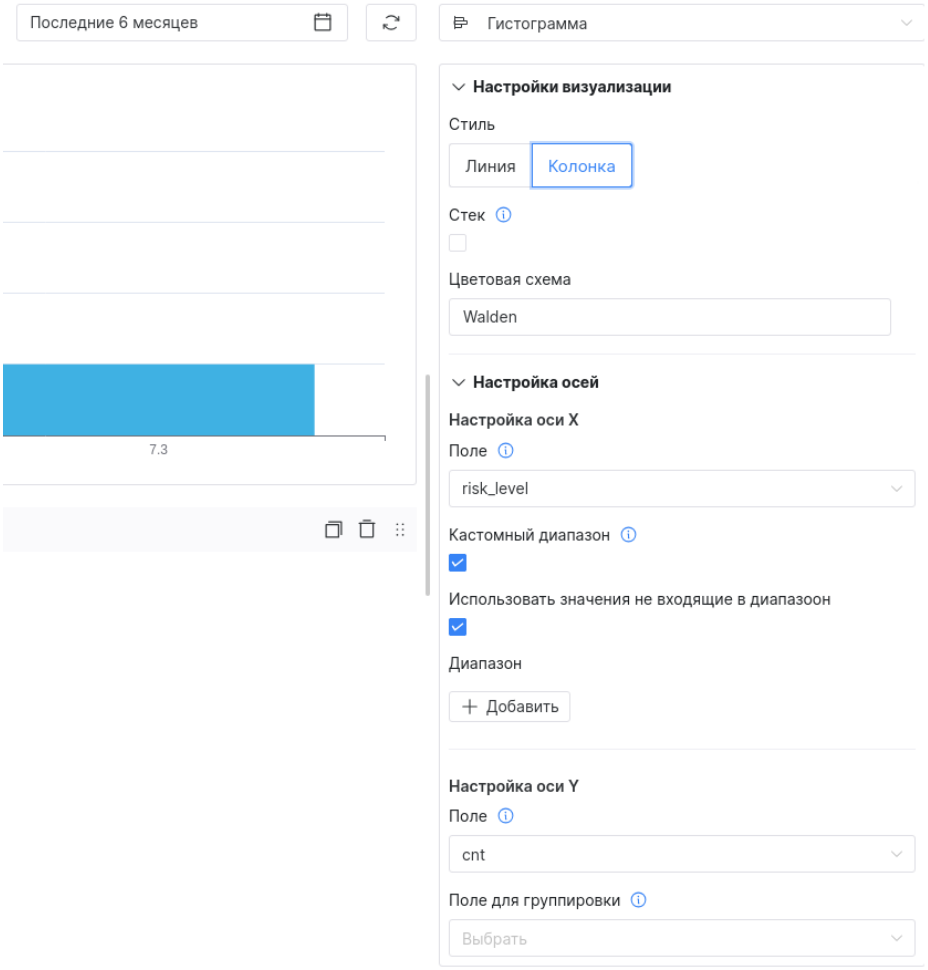


Рис. 227 – Виджет "Гистограмма". Настройки

12.3.6.1 Шаг 1. Настройка осей

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

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

Для настройки осей выполните следующие действия:

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

12.3.6.2 Шаг 2. Настройка визуализации

Настройка позволяет выбрать следующие параметры:

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

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

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

Примеры визуализации графика приведены на «Рис. 228».

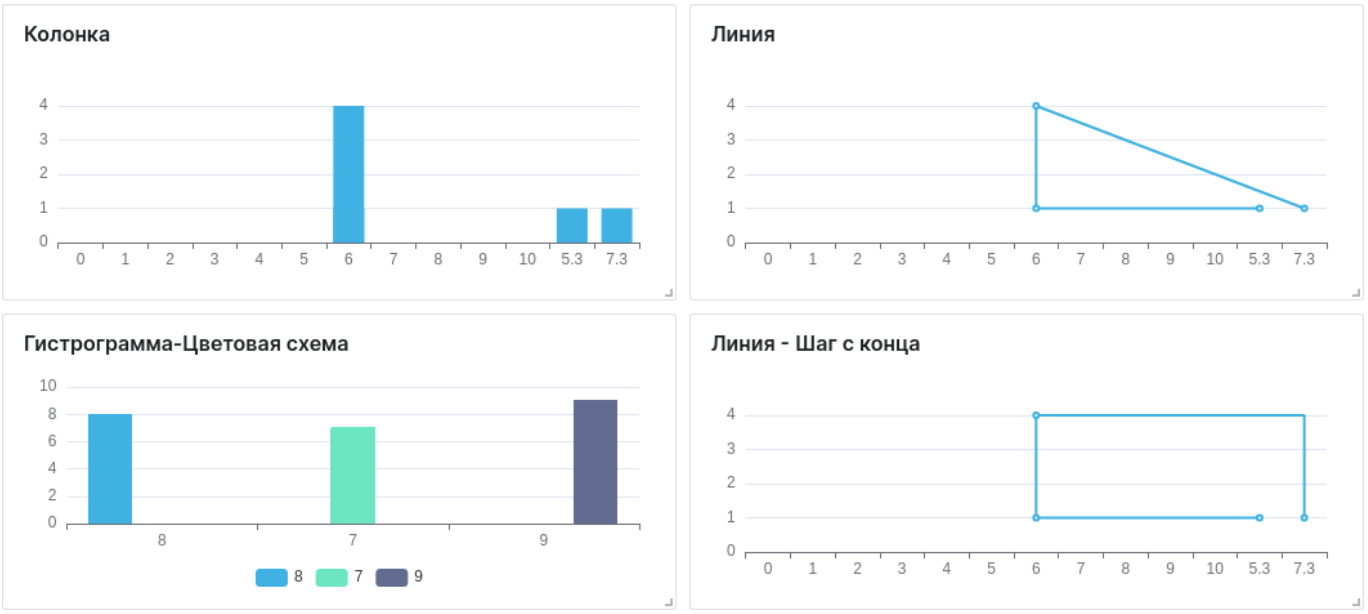


Рис. 228 – Примеры визуализации настроек виджета "Гистаграмма".

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

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

Пример отображения с включенным и выключенным стеком приведен на «Рис. 229».

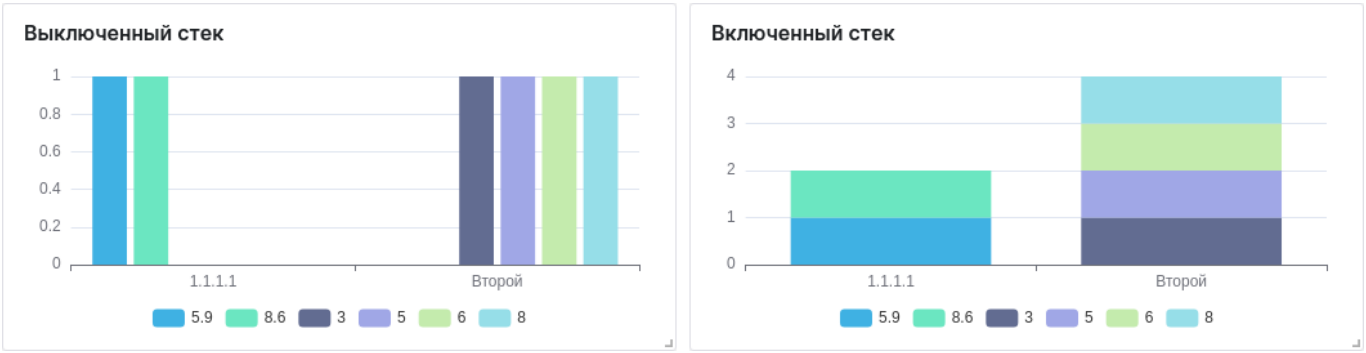


Рис. 229 – Примеры визуализации виджета со стеком

Для настройки визуализации выполните следующие действия:

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

12.3.6.3 Шаг 3. Легенда

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

12.3.7 Метрика

Виджет отображает тренд изменения выбранного показателя за период времени. Пример внешнего вида приведен на «Рис. 230».

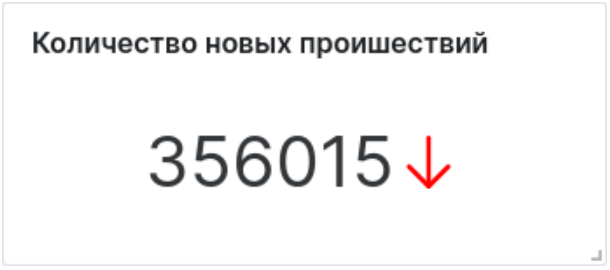


Рис. 230 – Виджет "Метрика"

Пример настроек приведен на «Рис. 231».

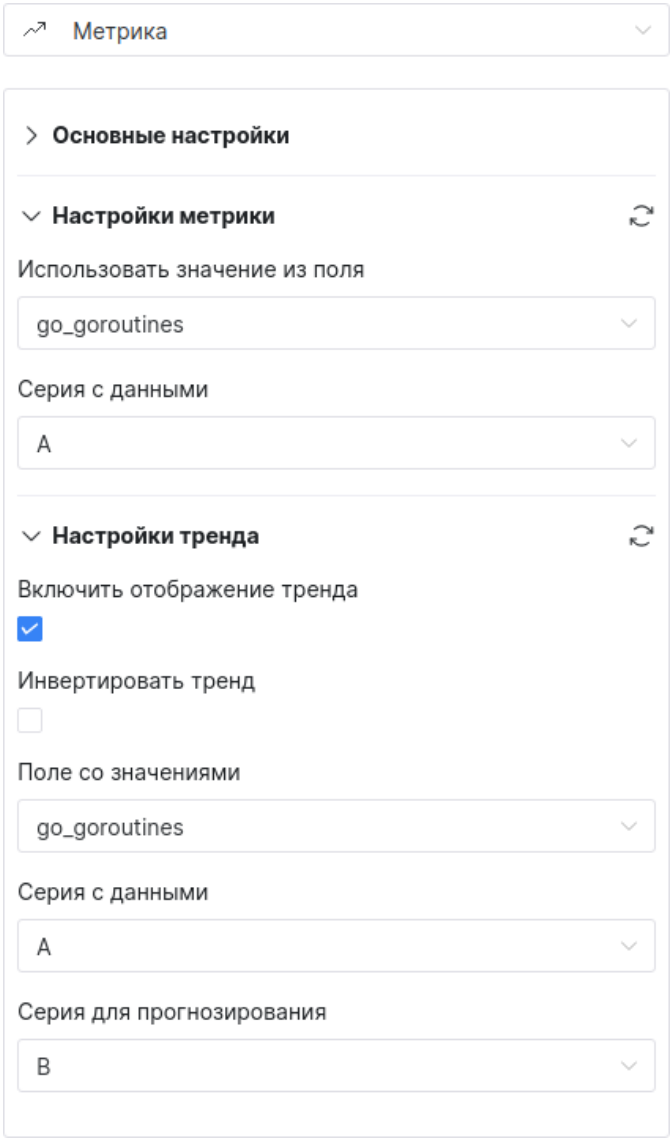


Рис. 231 – Виджет "Метрика". Настройки

Для настройки виджета выполните следующие действия:

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

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

Примеры визуализации виджета приведены на «Рис. 232».

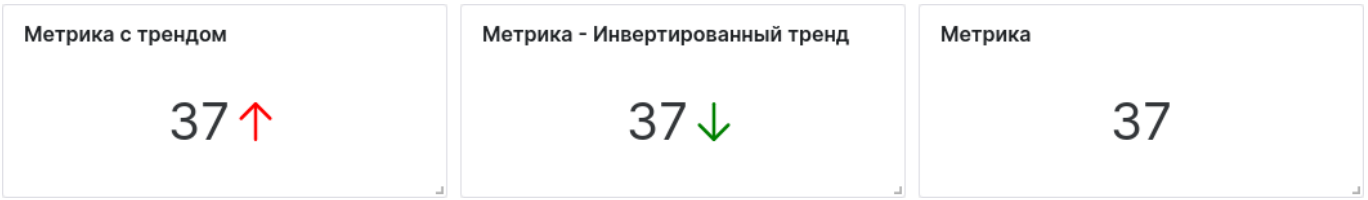


Рис. 232 – Примеры визуализации настроек виджета "Метрика"

12.3.8 Изображение

Виджет отображает изображение, загруженное пользователем.

Пример внешнего вида представлен на «Рис. 233».

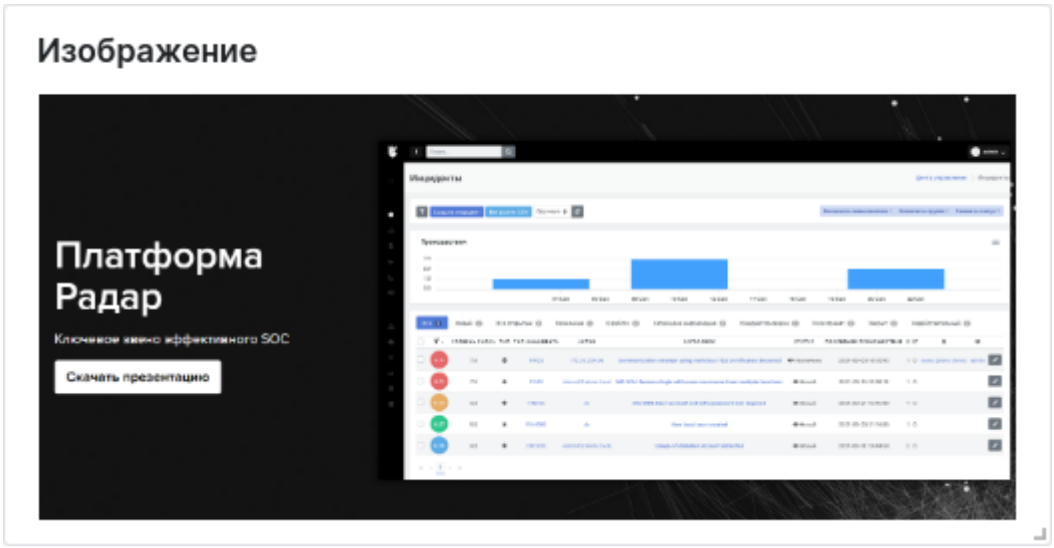


Рис. 233 – Виджет "Изображение"

Пример настроек приведен на «Рис. 234».

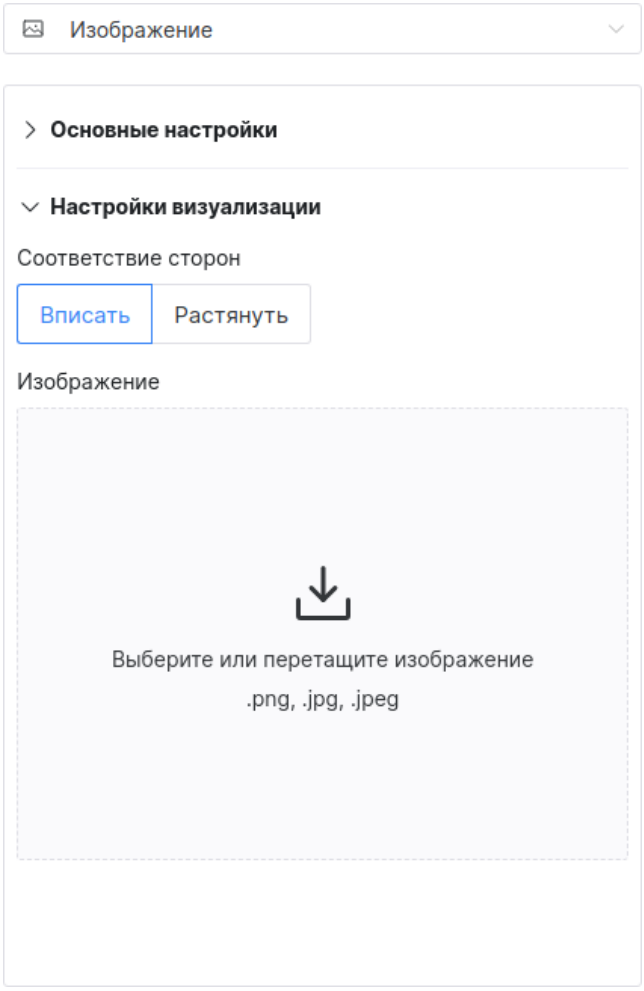


Рис. 234 – Виджет "Изображение". Настройки

Для настройки виджета выполните следующие действия:

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

12.4 Копирование виджета

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

Есть несколько способов для копирования параметров:

- **Способ 1**. В конструкторе виджетов нажмите кнопку . Настройки виджета будут скопированы в буфер обмена.
- **Способ 2**. Перейдите в раздел **Администрирование → Рабочие столы**, выберите виджет, нажмите кнопку и из выпадающего списка выберите пункт **Копировать настройки**.
- **Способ 3**. Перейдите в раздел **Администрирование → Отчеты**, выберите виджет, нажмите кнопку и из выпадающего списка выберите пункт **Копировать настройки**.

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

12.5 Предустановки

Предустановки используются для быстрой настройки виджетов на основе шаблона.

Вы можете добавить собственные шаблоны настроек виджетов в список предустановок.

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

В открывшемся окне "Предустановки" (см. «Рис. 235») выберите предустановку и нажмите кнопку .

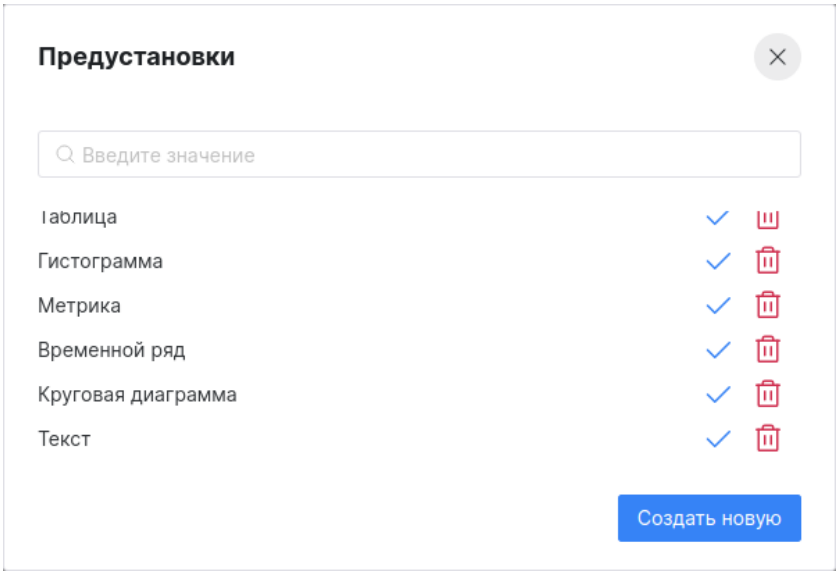


Рис. 235 – Окно "Предустановки"

Для создания предустановки выполните следующие действия:

1. Настройте запросы и визуализацию виджета.
2. Нажмите кнопку и в открывшемся окне "Предустановки" (см. «Рис. 235») нажмите кнопку **Создать новую**.
3. В открывшемся окне укажите название предустановки.
4. Нажмите кнопку **Создать**.

13. Отчеты

13.1 Общие данные

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

Отображение информации выполняется с помощью следующих типов виджетов:

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

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

Работа с отчетами включают в себя следующие процессы:

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

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

Для работы с отчетами перейдите в новый интерфейс и откройте раздел **Администрирование → Отчеты** (см. «Рис. 236»).

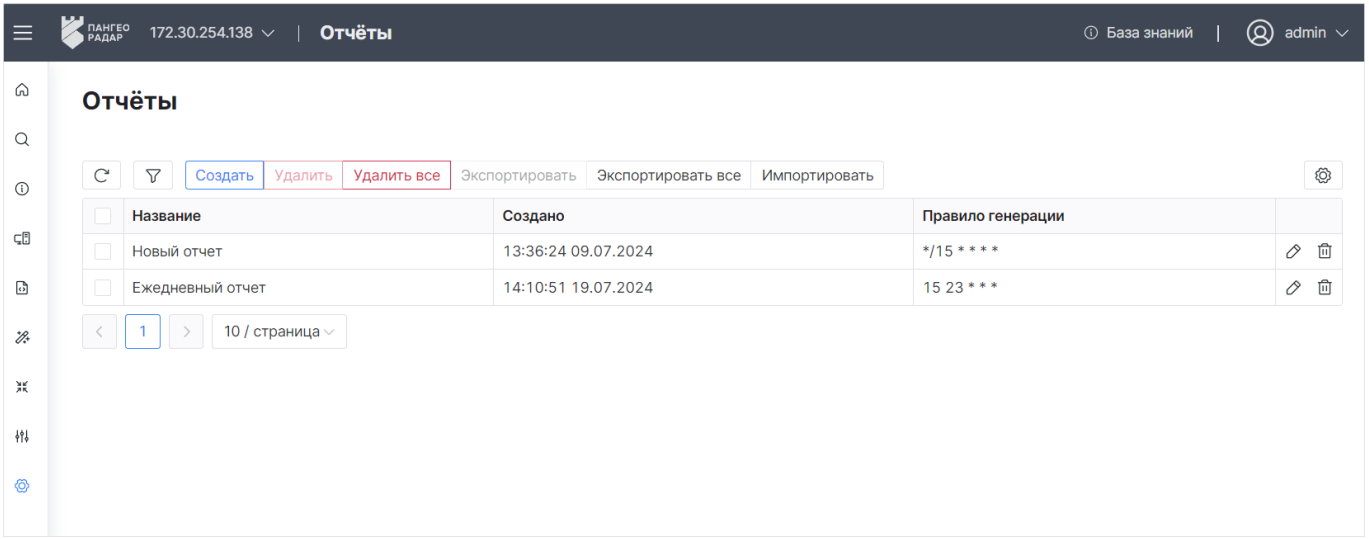


Рис. 236 – Раздел "Отчеты"

В разделе отображается следующая информация:

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

13.2 Создание отчета

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

Откроется окно "Создать отчет" (см. «Рис. 237»).

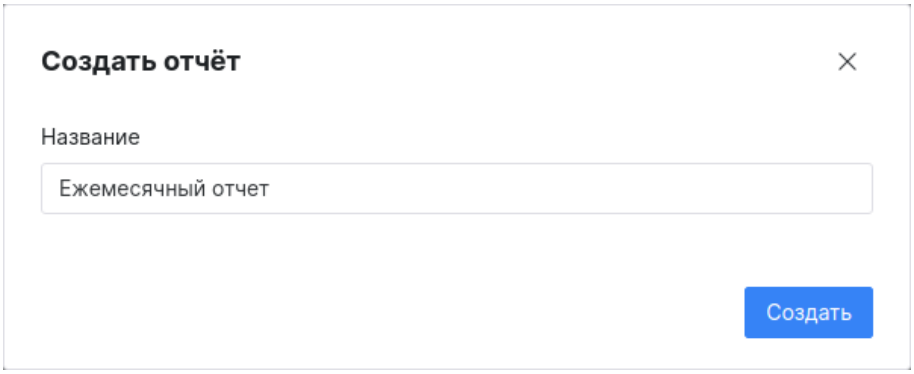


Рис. 237 – Окно "Создать отчет"

Выполните в окне следующие действия:

1. В поле "Название" укажите название отчета.
2. Нажмите кнопку **Создать**.
3. Будет создан отчет и произойдет переход в конструктор отчета (см. «Рис. 238»).

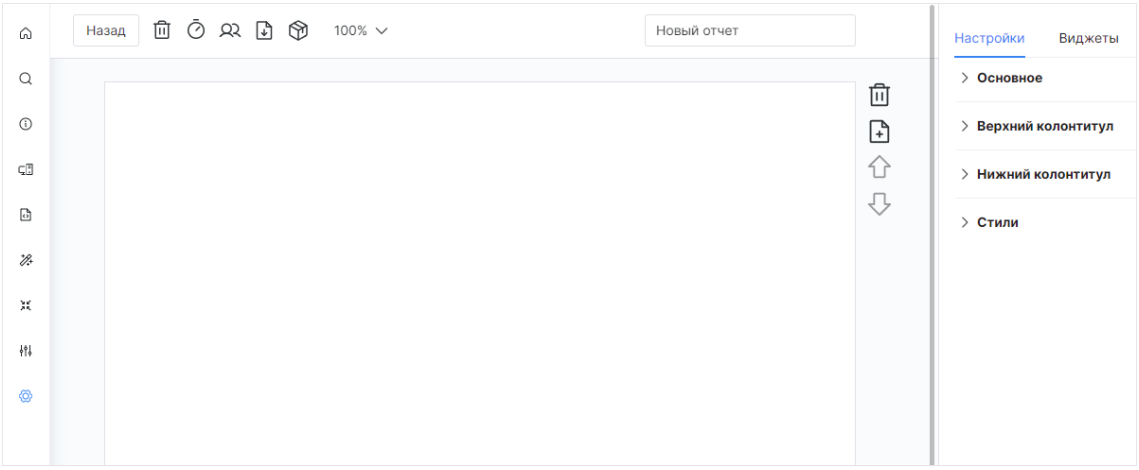


Рис. 238 – Страница "Конструктор отчета"

13.3 Конструктор отчета

Примечание: при настройке отчета все изменения автоматически сохраняются.

Настройка отчета выполняется на странице "Конструктор отчета" (см. «Рис. 239»).

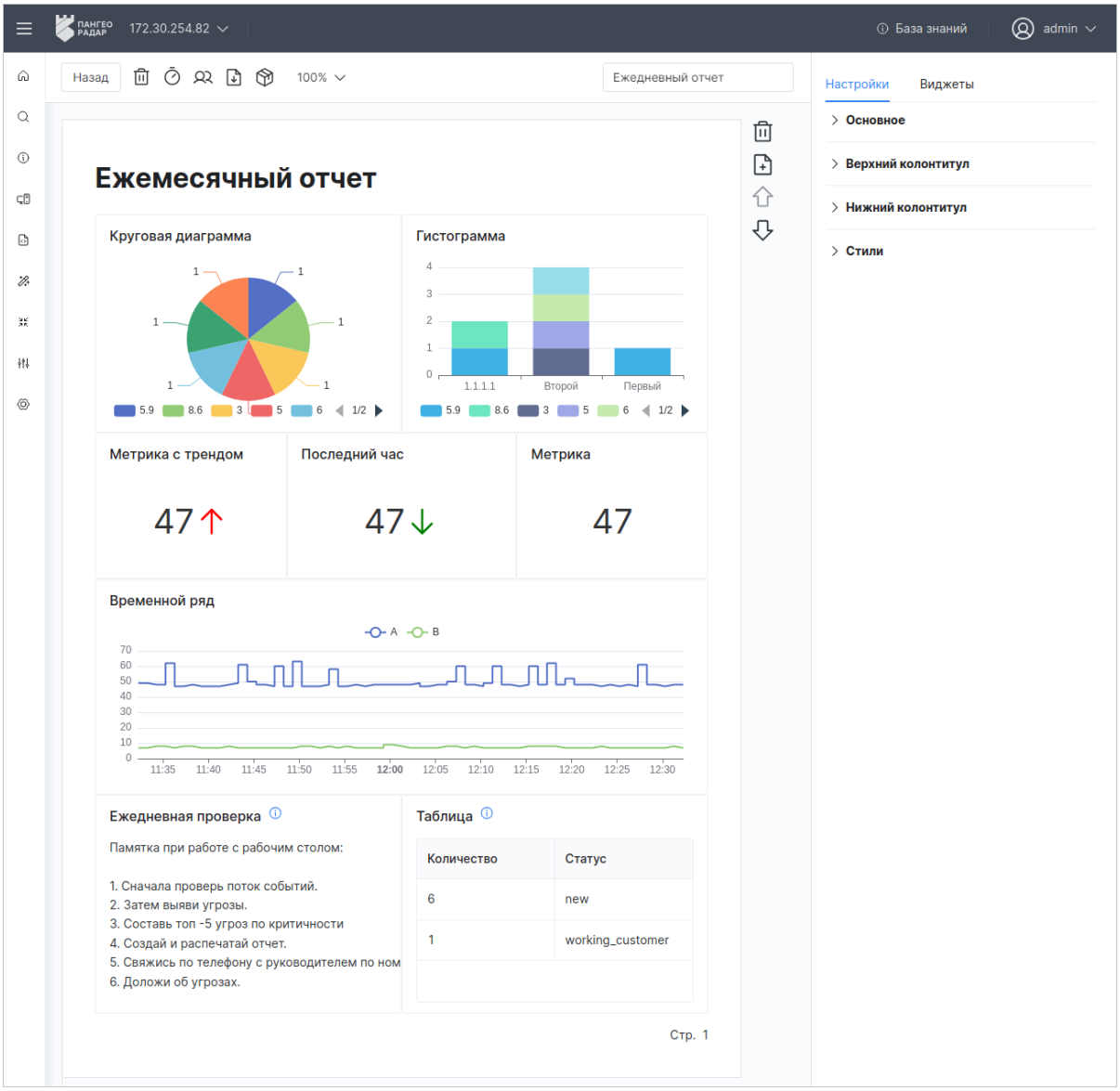


Рис. 239 – Интерфейс страницы "Конструктор отчета"

Страницу можно открыть следующими способами:

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

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

Конструктор состоит из следующих блоков:

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

Панель действий

Блок располагается вверху конструктора (см. «Рис. 240»).

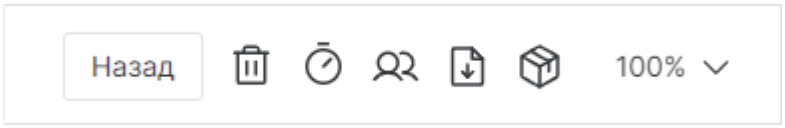


Рис. 240 – Страница "Конструктор отчета". Блок "Панель действий"

На панели действий доступны следующие элементы управления:

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

Рабочая область

Пример внешнего вида блока приведен на «Рис. 241».

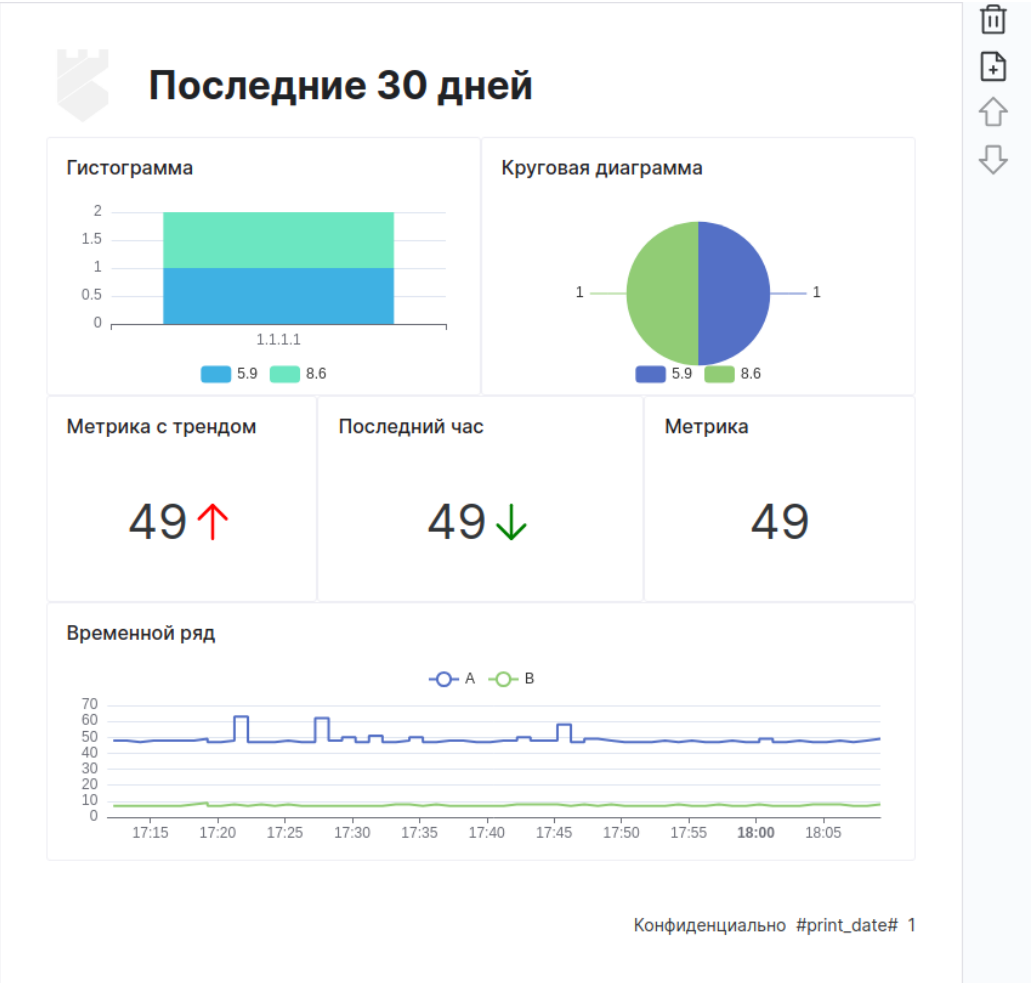


Рис. 241 – Страница "Конструктор отчета". Блок "Рабочая область"

В рабочей области доступны следующие элементы управления:

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

При наведении курсора на виджет становятся доступны следующие элементы управления:

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

Настройка страниц

Блок состоит из двух вкладок:

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

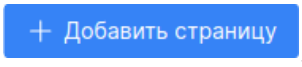
Настройка отчета состоит из следующих процессов:

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

13.3.1 Добавление страницы

На страницах можно расположить виджеты для отображения данных.

Добавление страниц в отчет выполняется следующим образом:

- если в отчете нет страниц, то нажмите кнопку 

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

Добавьте необходимое количество страниц в отчет.

13.3.2 Выбор периода формирования данных виджетов

Выбор периода формирования данных виджетов выполняется в блоке **Настройки** → **Основное** (см. «Рис. 242»).

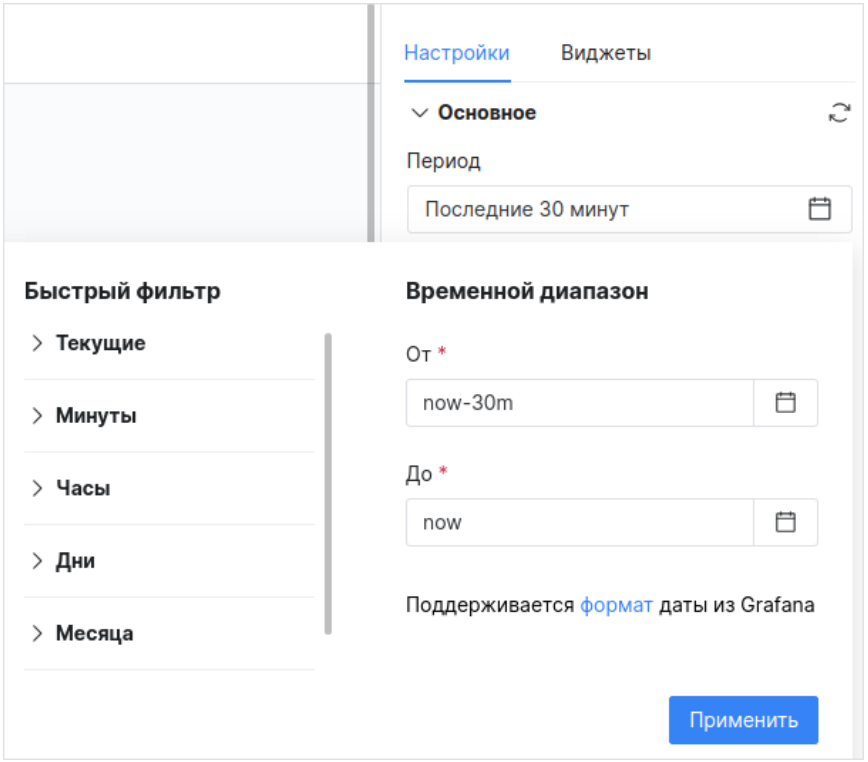


Рис. 242 – Выбор периода формирования данных виджетов

Для настройки периода выполните следующие действия:

1. В поле **Период** нажмите кнопку . Откроется окно выбора временного диапазона (см. «Рис. 242»).
2. Выберите период. Доступные значения:
   - текущие: минута, час, день, месяц, год;
   - последние: минуты, часы, месяца, года;
   - период можно указать вручную в соответствующих полях. Поддерживается формат дат из **Grafana**.
3. Нажмите кнопку **Применить**.

13.3.3 Настройка наименования отчета в момент генерации

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

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

Настройка правила выполняется в блоке **Настройки** → **Основное**. В поле "Маска для генерации названия" укажите необходимую маску (см. «Рис. 243»).

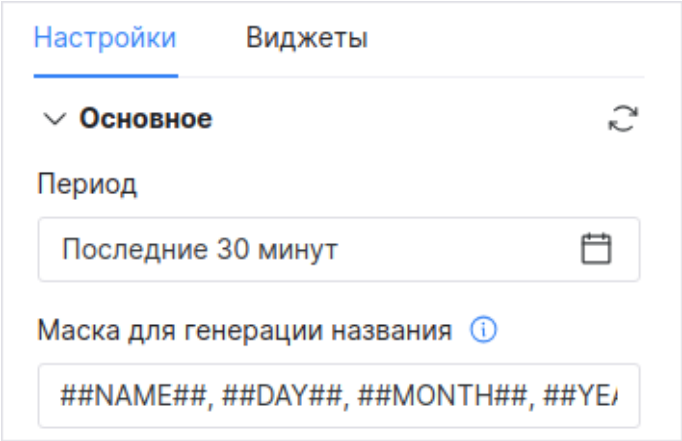


Рис. 243 – Настройка маски для генерации названия

Доступные значения:

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

13.3.4 Настройка страниц

13.3.4.1 Настройка верхнего колонтитула

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

Настройка выполняется в блоке **Настройки → Верхний колонтитул** (см. «Рис. 244»).

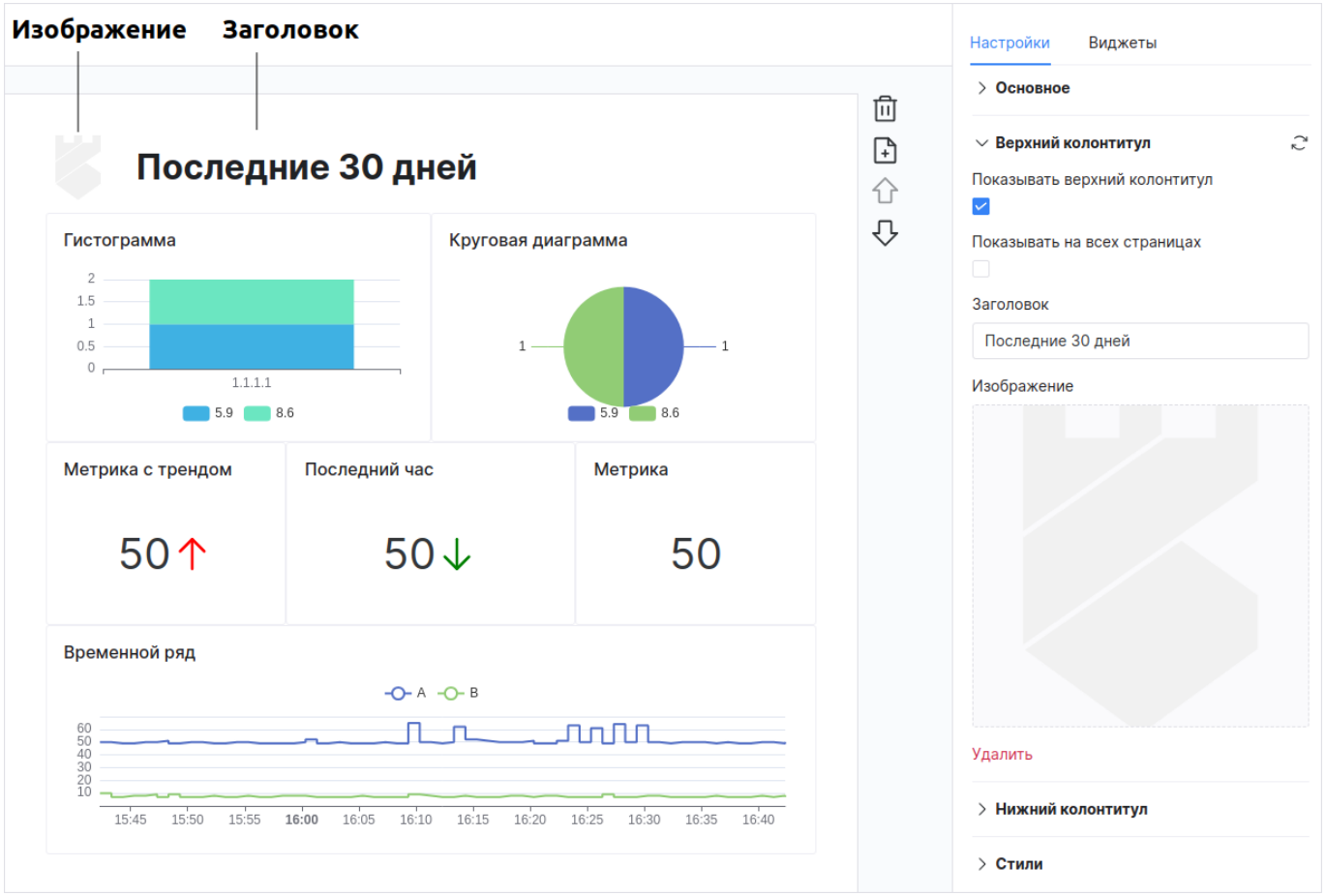


Рис. 244 – Настройка верхнего колонтитула

Для настройки верхнего колонтитула выполните следующие действия:

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

13.3.4.2 Настройка нижнего колонтитула

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

Настройка выполняется в блоке **Настройки → Нижний колонтитул** (см. «Рис. 245»).

Рис. 245 – Настройка нижнего колонтитула

Для настройки нижнего колонтитула выполните следующие действия:

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

13.3.4.3 Настройка стиля шрифта

Вы можете настроить стиль шрифта, отображаемый в виджетах.

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

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

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

13.3.5 Настройка виджетов

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

1. Добавление виджета на страницу отчета.
2. Редактирование виджета.
3. Копирование настроек виджета.

4. Изменение расположения виджета.
5. Изменение размера виджета
6. Удаление виджета.

13.3.5.1 Добавление виджета

Добавление виджета на страницу отчета выполняется из вкладки **Виджеты** (см. «Рис. 246»).

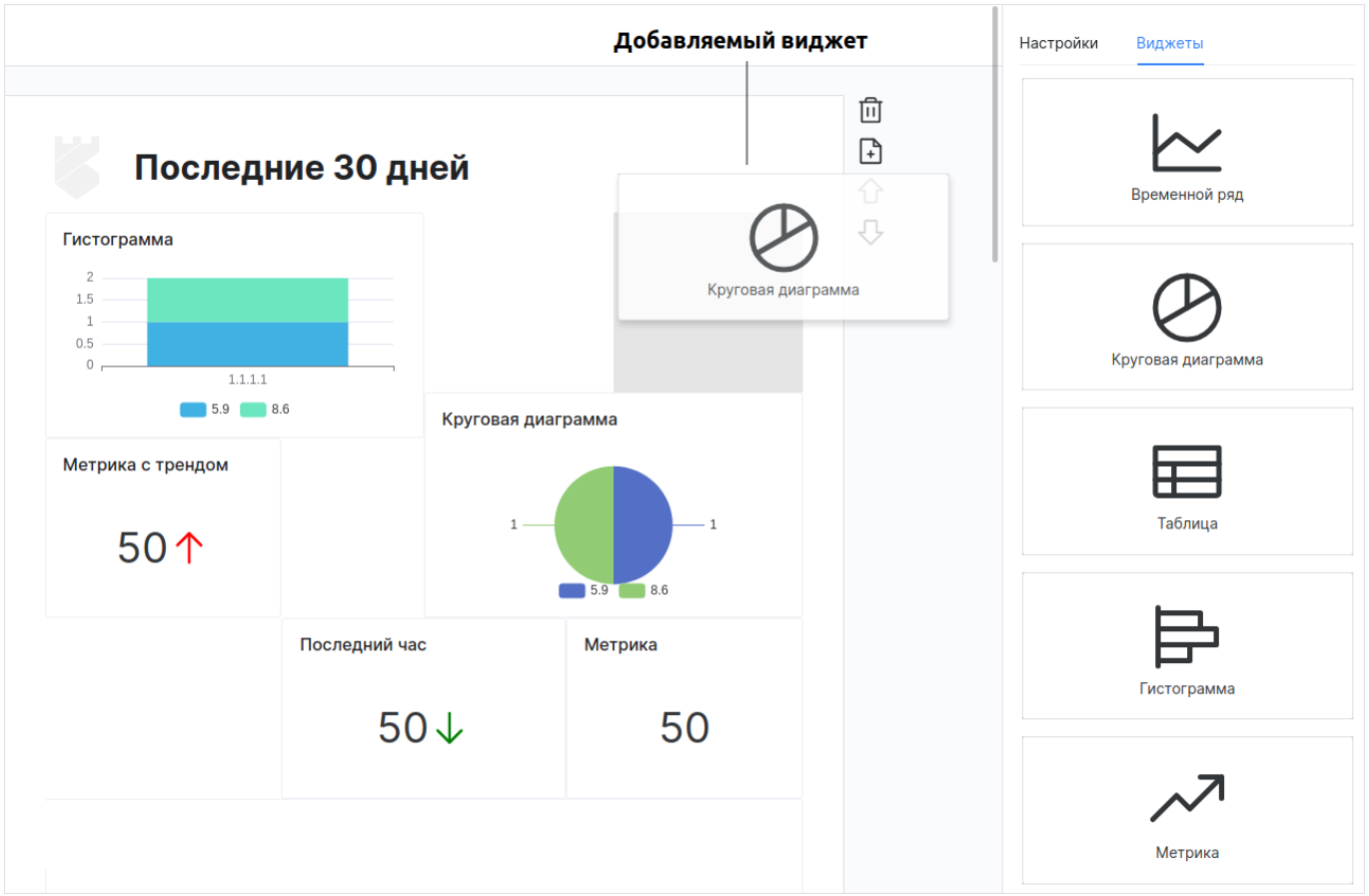


Рис. 246 – Страница "Конструктор отчета". Вкладка "Виджеты"

Для добавления виджета на страницу отчета выполните следующие действия:

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

13.3.5.2 Редактирование виджета

Для редактирования виджета выполните следующие действия:

1. Перейдите на страницу "Конструктор отчета" и выберите виджет.
2. Нажмите кнопку ⋮ и из выпадающего списка выберите пункт **Редактировать**.

3. Выполните настройку виджета в конструкторе (подробнее см. раздел «Конструктор виджетов»).

13.3.5.3 Копирование настроек виджета

Для копирования настроек виджета выполните следующие действия:

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

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

13.3.5.4 Изменение расположения виджета

Для изменения расположения виджета выполните следующие действия:

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

13.3.5.5 Изменение размера виджета

Для изменения размера виджета выполните следующие действия:

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

13.3.5.6 Удаление виджета

Для удаления виджета со страницы отчета выполните следующие действия:

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

13.3.6 Изменение порядка страниц

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

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

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

13.3.7 Удаление страницы

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

13.4 Настройка расписания генерации отчета

Работа с генерацией отчетов по расписанию проходит по следующему сценарию:

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

Для настройки расписания генерации отчета выполните следующие действия:

1. Настройте отчет и нажмите кнопку . Откроется окно "Планировщик" (см. «Рис. 247»).

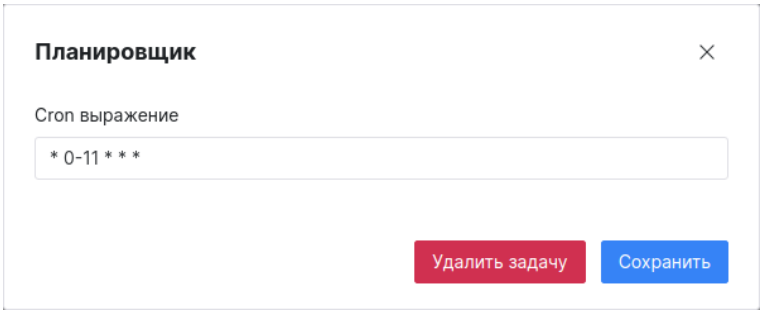


Рис. 247 – Окно "Планировщик"

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

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

13.4.1 Просмотр истории генерации отчета

Для просмотра архива по отчету перейдите на страницу "Конструктор отчета" и нажмите кнопку . Откроется окно "Список отчетов" (см. «Рис. 248»).

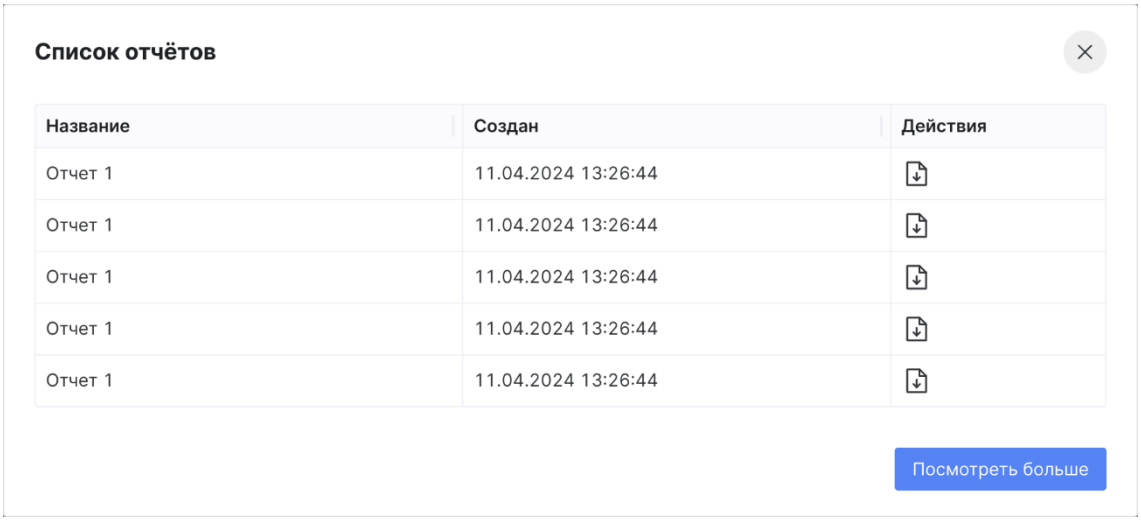


Рис. 248 – Окно "Список отчетов"

В окне отображается следующая информация:

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

Для экспорта отчета нажмите кнопку .

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

13.5 Настройка прав доступа к отчету

Перейдите на страницу "Конструктор отчета" и нажмите кнопку . Откроется окно "Редактирование прав" (см. «Рис. 249»).

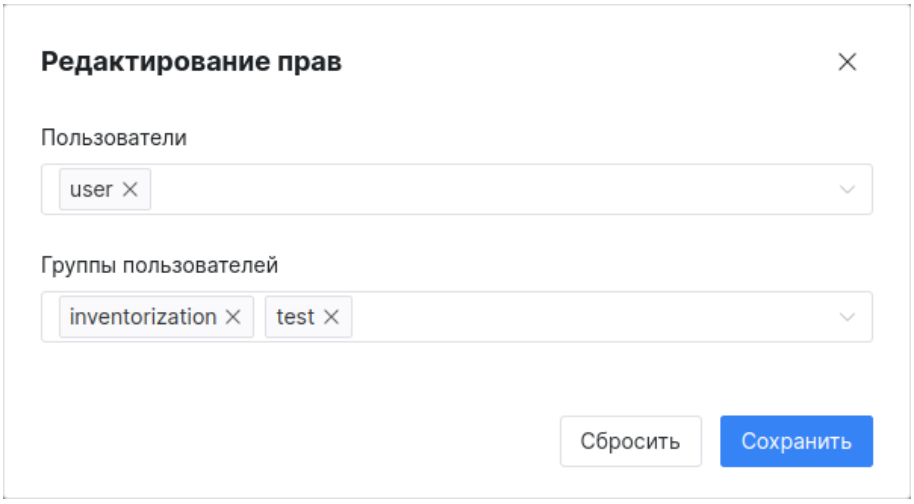


Рис. 249 – Окно "Редактирование прав"

Настройте права доступа одним из следующих способов:

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

13.6 Импорт отчетов

Для импорта отчетов выполните следующие действия:

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

13.7 Экспорт отчетов

Выполнить экспорт отчетов можно двумя способами:

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

Способ 1. Экспорт в файл формата .pdf

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

Способ 2. Экспорт в архив

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

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

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

13.8 Удаление отчета

Удаление отчета можно выполнить следующими способами:

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

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

13.9 Архив отчетов

Отчеты, сгенерированные по расписанию, помещаются в архив (подробнее см. раздел «Настройка расписания генерации отчета»). Для просмотра истории генерации по всем отчетам перейдите в раздел **Администрирование → Архив отчетов** (см. «Рис. 250»).

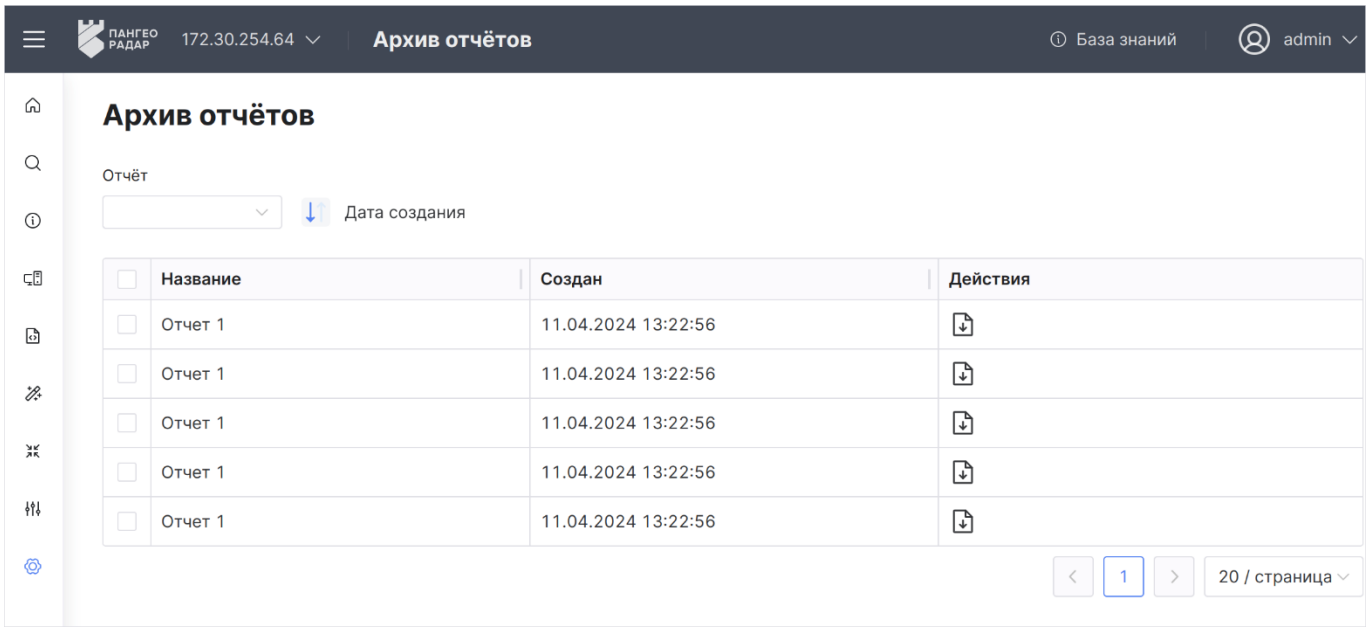


Рис. 250 – Раздел "Архив отчетов"

В разделе отображается следующая информация:

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

Для формирования списка отчетов выполните следующие действия:

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

Для экспорта отчетов выполните следующие действия:

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

14. Сообщения

Платформа Радар поддерживает обмен сообщений между пользователями платформы.

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

Работа с сообщениями включает в себя следующие процессы:

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

Для работы с сообщениями нажмите на наименование учетной записи в правом верхнем углу и выберите пункт **Сообщения**. Откроется страница "Сообщения" (см. «Рис. 251»).

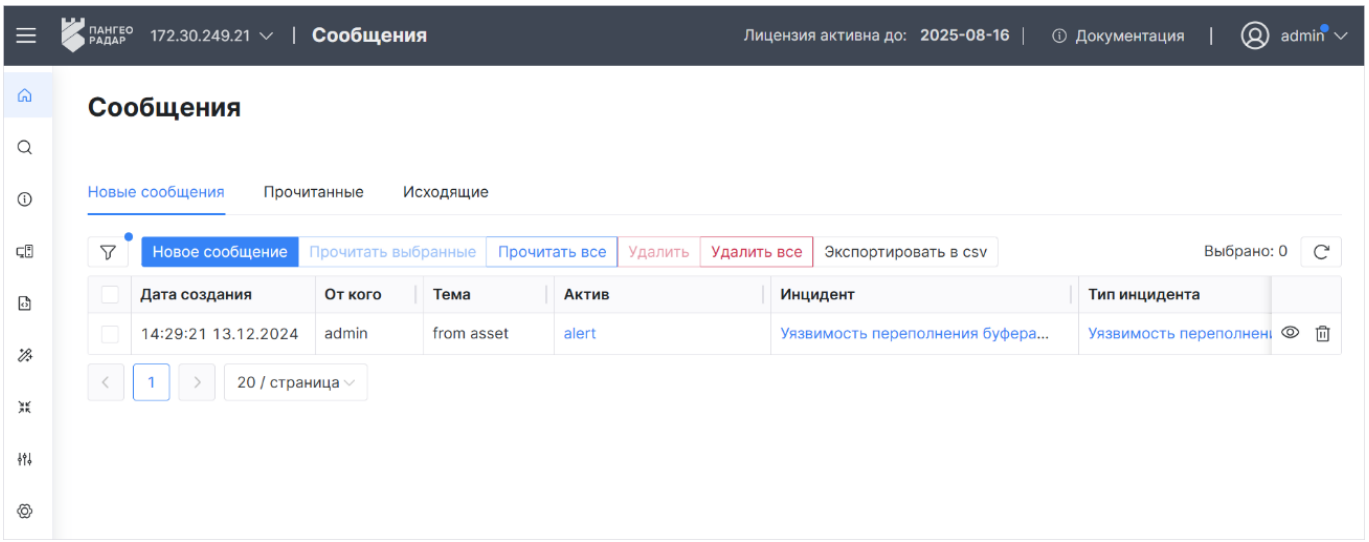


Рис. 251 – Раздел "Сообщения"

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

Сообщения в разделе разделены по следующим вкладкам:

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

На вкладках отображается следующая информация:

- **Дата создания** – дата и время создания сообщения;

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

14.1 Создание сообщения

1. Нажмите кнопку **Новое сообщение**. Откроется окно "Новое сообщение" (см. «Рис. 252»)

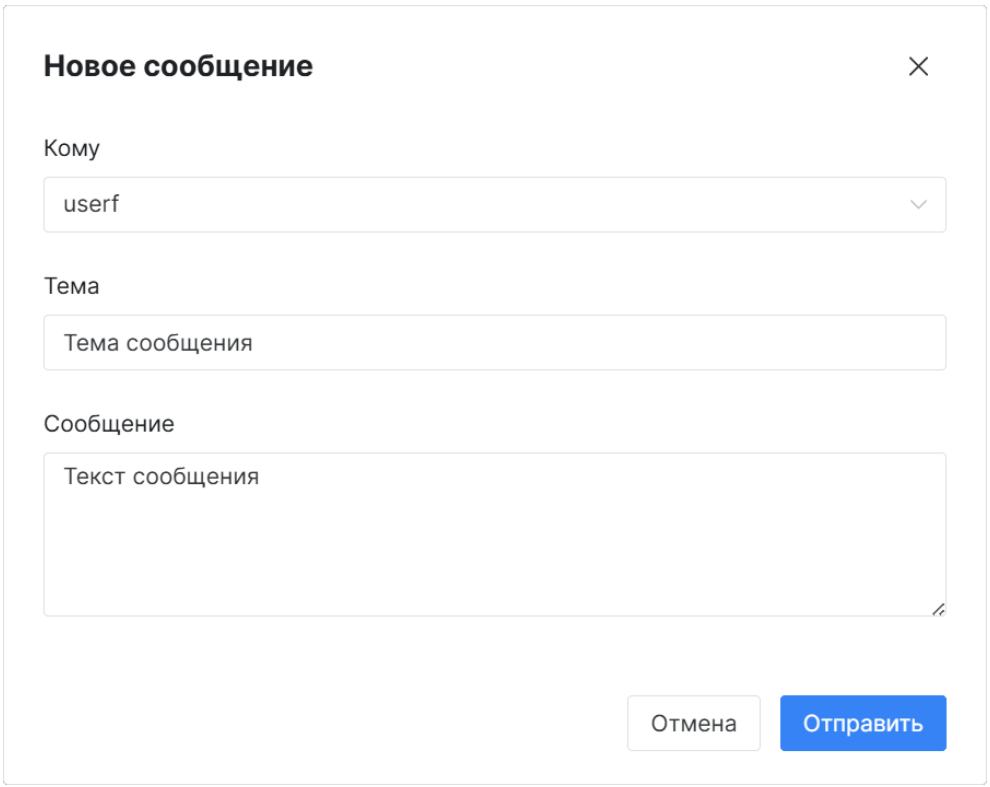


Рис. 252 – Окно "Новое сообщение"

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

14.2 Просмотр сообщения

1. В строке нужного сообщения нажмите кнопку . Откроется окно "Просмотр сообщения" (см. «Рис. 253»).

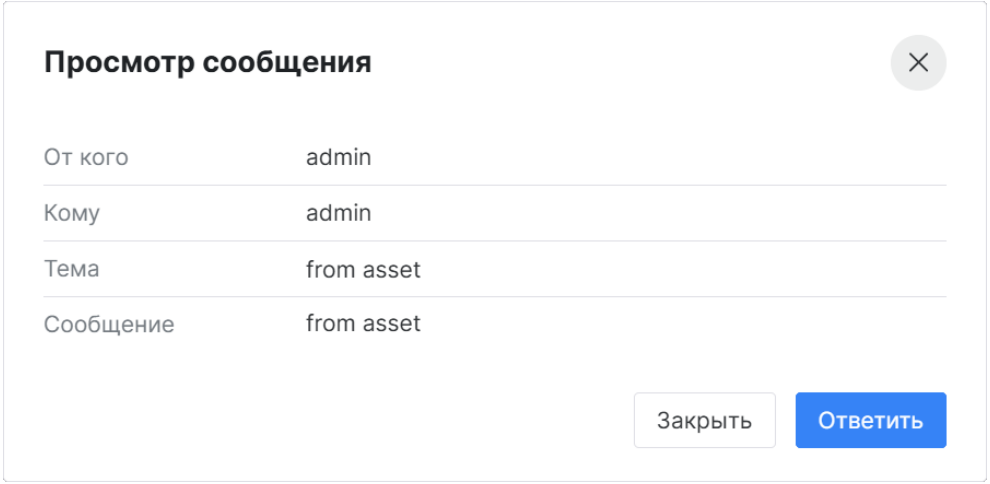


Рис. 253 – Окно "Просмотр сообщения"

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

14.3 Ответ на сообщение

1. Откройте сообщение на просмотр (см. «Рис. 253») и нажмите кнопку **Ответить**. Откроется окно "Новое сообщение" (см. «Рис. 252»).
2. Укажите в окне необходимую информацию и нажмите кнопку **Отправить**.

14.4 Отметить сообщения прочитанными

Действие выполняется на вкладке **Новые сообщения**.

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

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

14.5 Отметить прочитанные сообщения как непрочитанные

Действие выполняется на вкладке **Прочитанные**.

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

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

14.6 Экспорт сообщений

1. Перейдите на нужную вкладку.
2. Нажмите на кнопку **Экспортировать в csv**.
3. Будет сформирован документ в формате .csv.
4. Нажмите кнопку **Скачать** и укажите путь для сохранения файла.

14.7 Удаление сообщений

Для удаления сообщения нажмите кнопку  в соответствующей строке.

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

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

15. Профиль пользователя

В разделе пользователю доступны следующие действия:

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

Для перехода в профиль пользователя нажмите на наименование учетной записи в правом верхнем углу и выберите пункт **Профиль**. Откроется страница "Профиль" (см. «Рис. 254»).

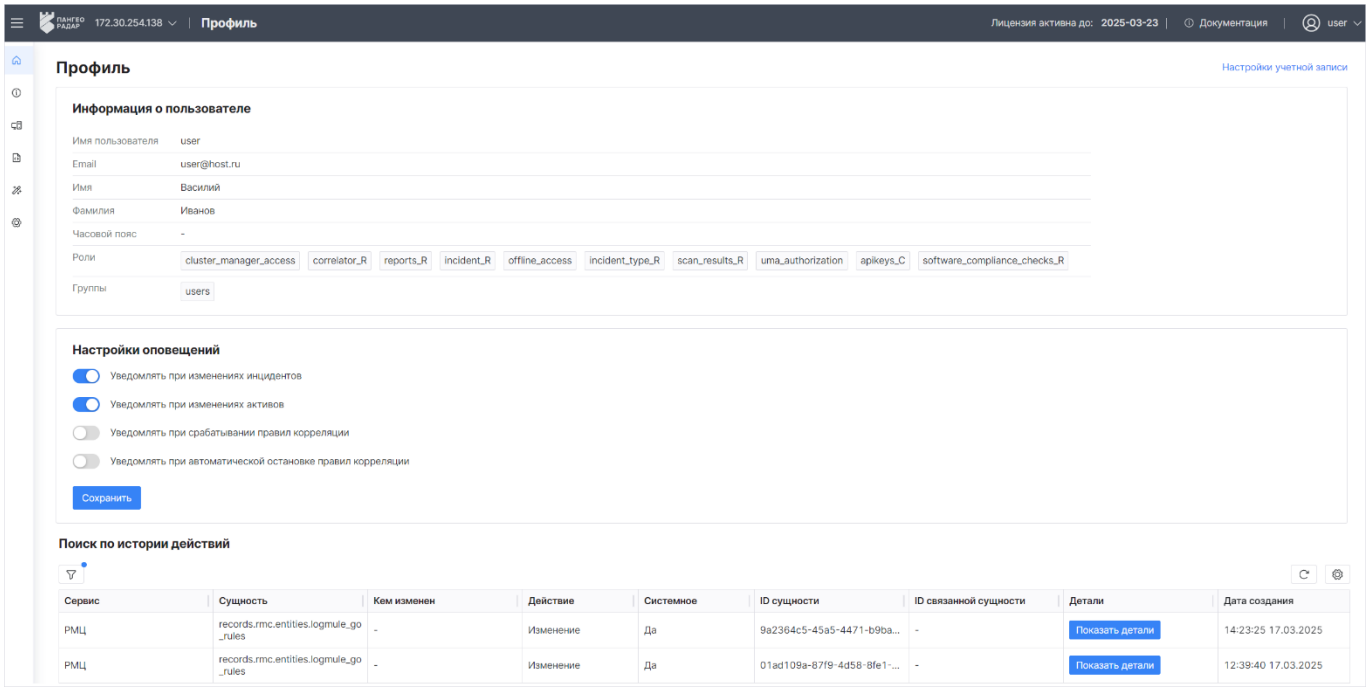


Рис. 254 – Раздел "Профиль"

Информация в разделе отображается в следующих блоках:

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

- список групп, в которые добавлен пользователь.

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

15.1 Изменение информации о своей учетной записи

1. Перейдите в профиль пользователя.
2. Нажмите кнопку **Настройки учетной записи**. Откроется форма "Изменение учетной записи" (см. «Рис. 255»).

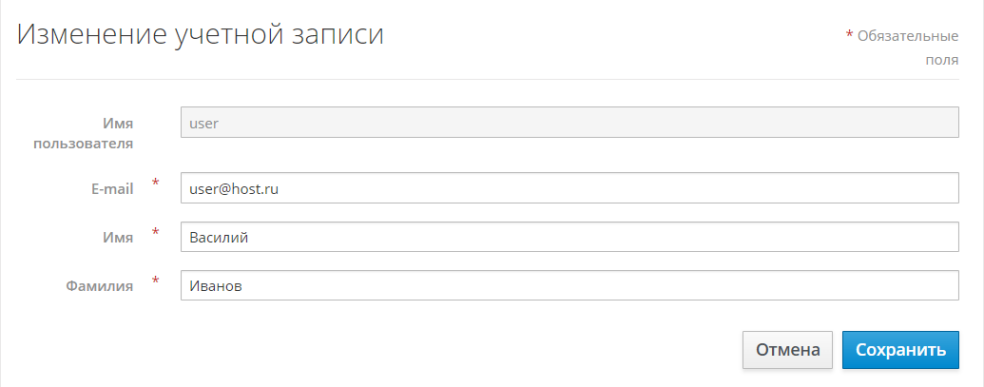


Рис. 255 – Форма "Изменение учетной записи"

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

15.2 Изменение пароля

1. Перейдите в профиль пользователя.
2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Пароль**. Откроется форма "Смена пароля" (см. «Рис. 256»).

Рис. 256 – Форма "Смена пароля"

3. Укажите в окне следующую информацию:

- в поле **Пароль** укажите текущий пароль;
- в полях **Новый пароль** и **Подтверждение пароля** укажите новый пароль.

4. Нажмите кнопку **Сохранить**.

15.3 Подключение аутентификатора

1. Перейдите в профиль пользователя.
2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Аутентификатор**. Откроется форма "Смена пароля" (см. «Рис. 257»).

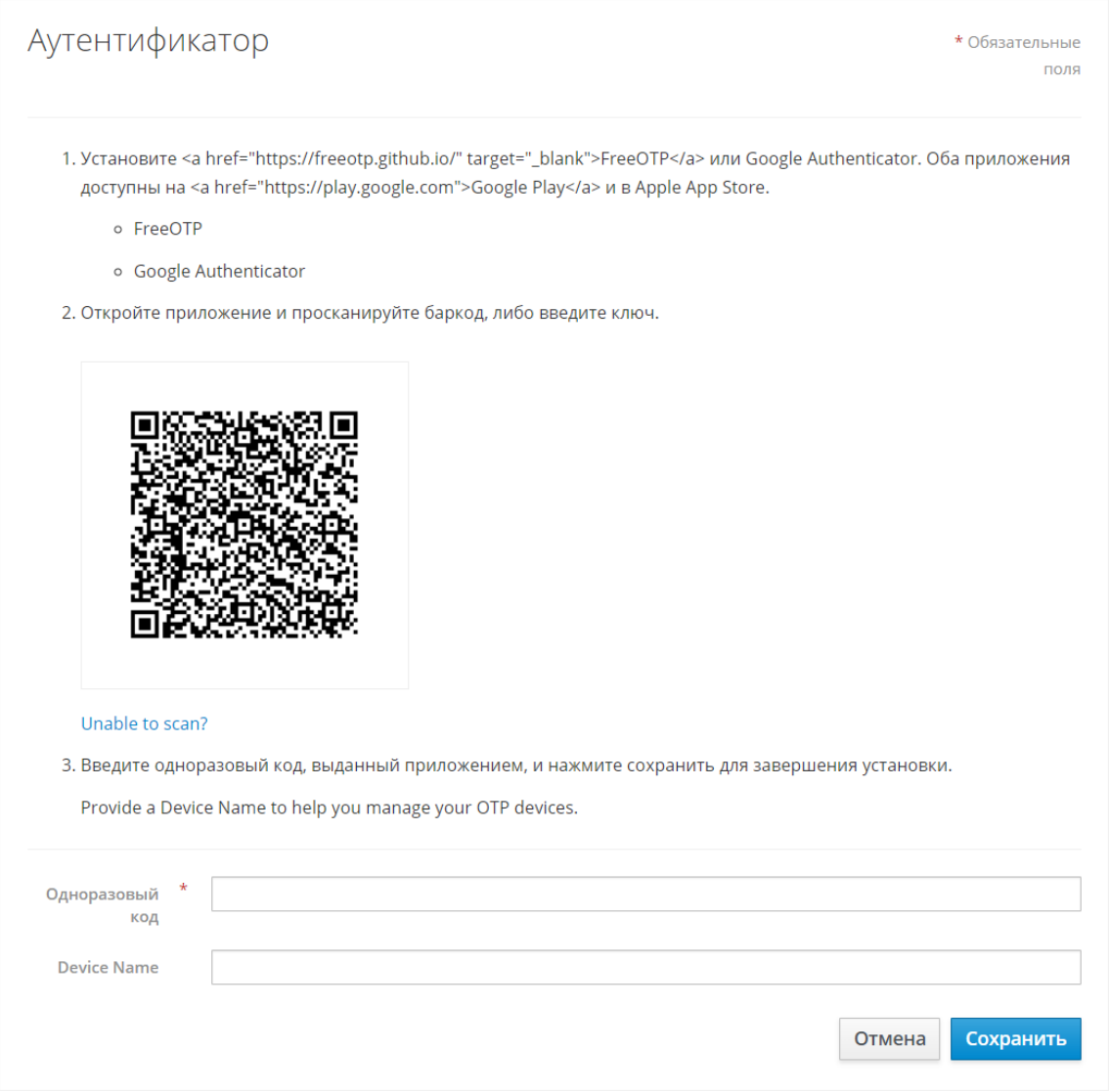


Рис. 257 – Форма "Аутентификатор"

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

15.4 Выход из всех сессий

1. Перейдите в профиль пользователя.

2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Сессии**. Откроется страница "Сессии" (см. «Рис. 258»).

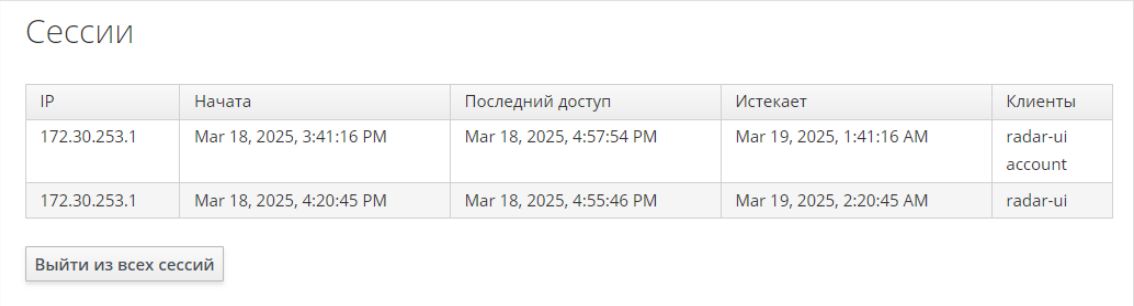


Рис. 258 – Страница "Сессии"

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

15.5 Просмотр журнала изменений учетной записи

1. Перейдите в профиль пользователя.
2. Нажмите кнопку **Настройки учетной записи** и перейдите в раздел **Журнал**. Откроется страница "Лог учетной записи" (см. «Рис. 259»).

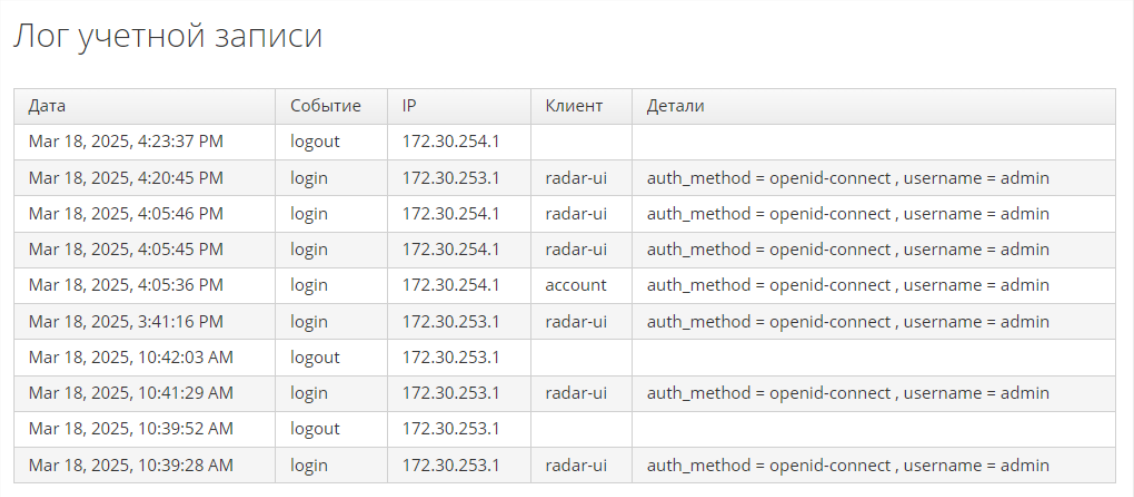


Рис. 259 – Страница "Лог учетной записи"

На странице отображается следующая информация:

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

15.6 Настройка оповещений

1. Перейдите в профиль пользователя.
2. В блоке **Настройка оповещений** включите/выключите уведомления о следующих событиях:

- изменение инцидентов;
- изменение активов;
- произошла "сработка" правила корреляции;
- произошла автоматическая остановка правила корреляции.

3. Нажмите кнопку **Сохранить**.

15.7 Просмотр истории действий в платформе

Пример блока **Поиск по истории действий** приведен на «Рис. 260».

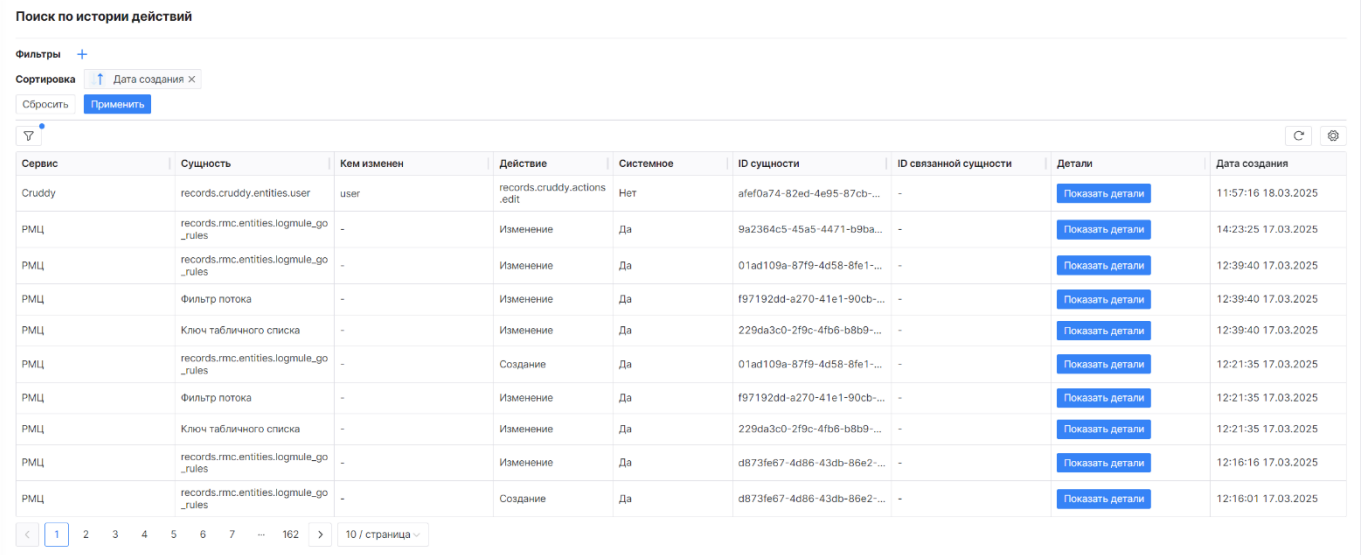


Рис. 260 – Блок "Поиск по истории действий"

В блоке отображается следующая информация:

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

По кнопке **Детали** можно посмотреть подробную информацию о действии (см. «Рис. 261»).

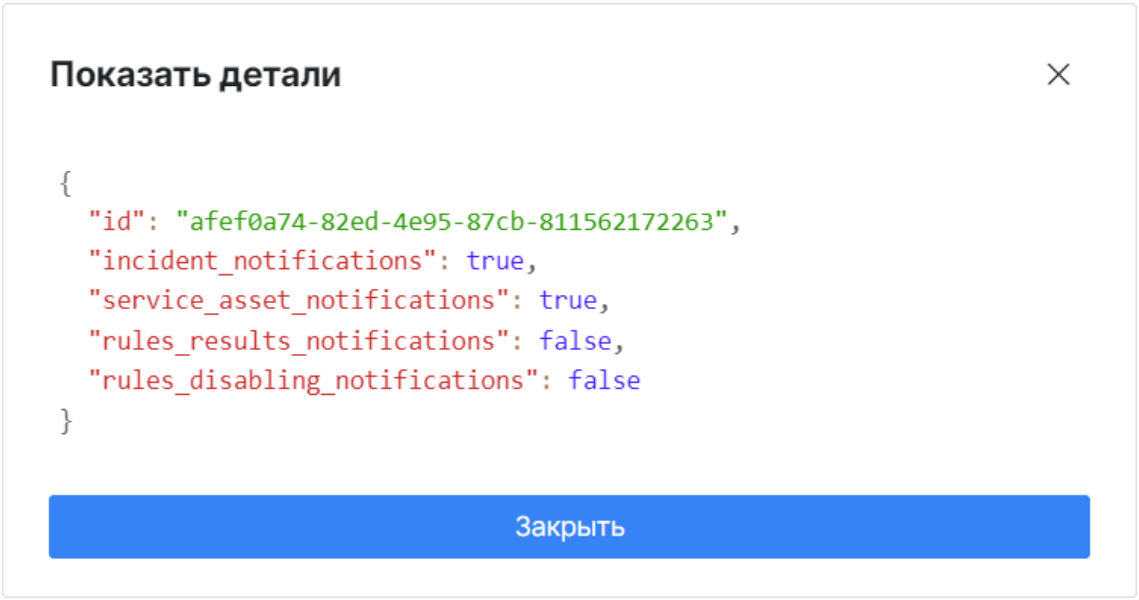


Рис. 261 – Окно "Показать детали"

16. Интеграции

16.1 RT Protect EDR

16.1.1 Общие сведения

16.1.1.1 Характеристики системы

Наименование системы – RT Protect Endpoint Detection and Response (далее RT Protect EDR).

Назначение системы – обнаружение целенаправленных атак и сложных угроз.

Разработчик системы – АО «РТ-Информационная безопасность» — организация прямого управления Государственной корпорации «Ростех».

Сайт – РТ-Информационная безопасность.

Возможности, предоставляемые интеграцией:

- выполнение активных действий на активах;
- импорт активов из RT Protect EDR в **Платформу Радар**;
- синхронизация инцидентов.

Настройка интеграции с системой RT Protect EDR приведена в разделе «Настройка интеграции RT Protect EDR».

Приемы работы с интеграцией приведены в разделе «Работа с интеграцией RT Protect EDR».

16.1.1.2 Активные действия

Система **RT Protect EDR** позволяет выполнять удаленные действия на активе для предотвращения распространения потенциальных угроз.

В рамках интеграции активными действиями являются шаблоны команд для ОС Windows и Linux.

Например, для завершения процесса по его идентификатору, будут использованы следующие команды:

- Linux:

  ```
  # kill -9 {{ .pid }}
  ```

- Windows:

  ```
  # taskkill /PID {{ .pid }} /T /F
  ```

Перечень действий доступных в интеграции по умолчанию:

- **Завершить процесс по PID** – будет завершен процесс по идентификатору процесса на активе;
- **Заблокировать порт** – соответствующий порт будет заблокирован на прием/отправку сообщений;
- **Заблокировать входящий трафик с IP** – будет заблокирован трафик с соответствующего IP-адреса;

- **Включить изоляцию актива** – соответствующий актив будет изолирован в локальной сети;
- **Выключить изоляцию актива** – изоляция актива будет снята;
- **Включить защиту** – включить встроенные в систему **RT Protect EDR** средства защиты на выбранном активе;
- **Выключить защиту** – отключить встроенные в систему **RT Protect EDR** средства защиты на выбранном активе.

Действие над активом может быть выполнено следующими способами:

- автоматически, по результатам сработки правила корреляции;
- вручную, при анализе актива, на котором выявлены инциденты.

Управление активными действия выполняется в разделе «EDR действия».

16.1.1.3 Синхронизация инцидентов и активов

При синхронизации инцидентов выполняется обмен информацией об инцидентах на активах между системами со следующими особенностями:

- для назначения инцидентов в каждой системе должен быть пользователь, имеющий права на работу с инцидентами;
- при возникновении конфликтов при синхронизации приоритет отдается **Платформе Радар**;
- при удалении инцидентов из **Платформы Радар** есть два варианта выбора:
  - удалить также и в RT Protect EDR;
  - отключить синхронизацию инцидента и удалить только в платформе.
- при наличии верхнеуровневой системы, синхронизация будет выполняться по цепочке **Верхнеуровневая система → Платформа Радар → RT Protect EDR**;
- для выполнения синхронизации необходимо настроить периодическую задачу синхронизации (см. раздел «Шаг 2. Настройка задачи синхронизации активов»).

16.1.1.4 Параметры типа интеграции RT Protect EDR

Для просмотра параметров типа интеграции перейдите в раздел **Параметры → Типы интеграций** и нажмите кнопку в строке с наименованием **RT Protect EDR**. Откроется форма просмотра параметров типа интеграции.

Информация на форме отображается на следующих вкладках:

- **Интеграции**. На вкладке отображается список связанных интеграций (см. «Рис. 262»);

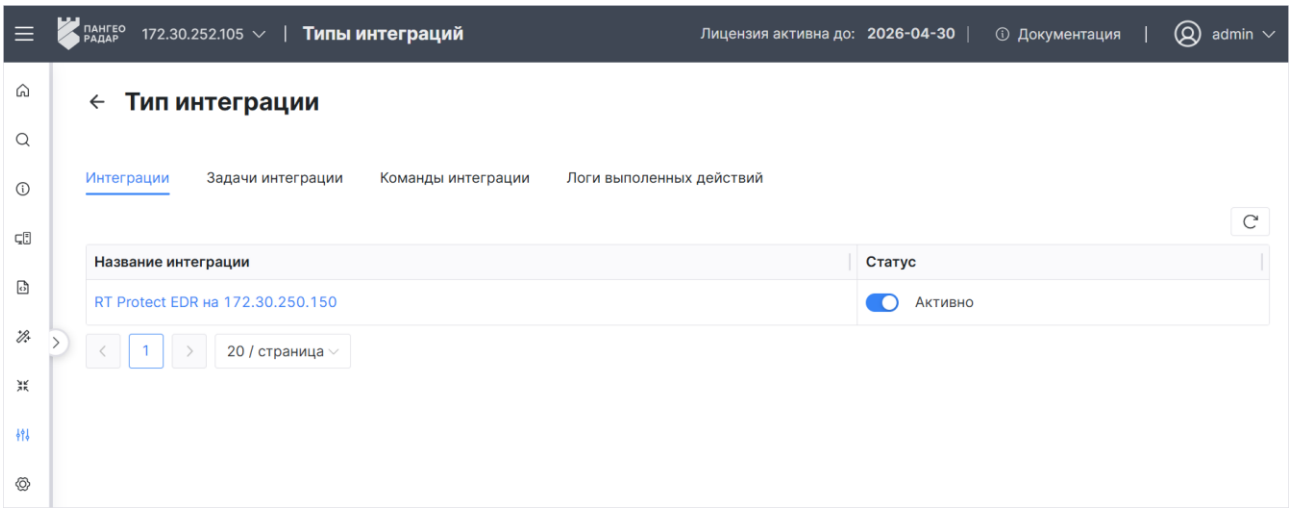


Рис. 262 – Просмотр типа интеграции RT Protect EDR. Вкладка "Интеграции"

- **Задачи интеграции**. Пример вкладки приведен на «Рис. 263».

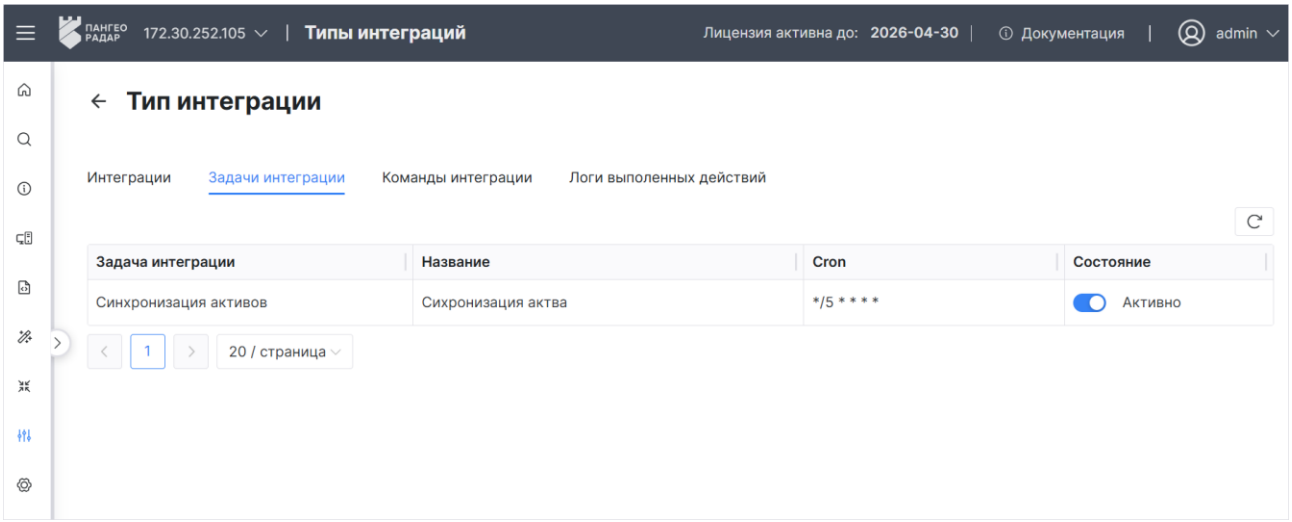


Рис. 263 – Просмотр типа интеграции RT Protect EDR. Вкладка "Задачи интеграции"

На вкладке отображается информация о периодических задачах, выполняемых в рамках всех связанных интеграций:

- **Задача** – тип периодической задачи;
- **Название** – наименование периодической задачи;
- **Cron** – CRON-выражение, описывающее периодичность задачи;
- **Состояние** – состояние задачи: Активно, Неактивно.

- **Команды интеграции**. Пример вкладки приведен на «Рис. 264».

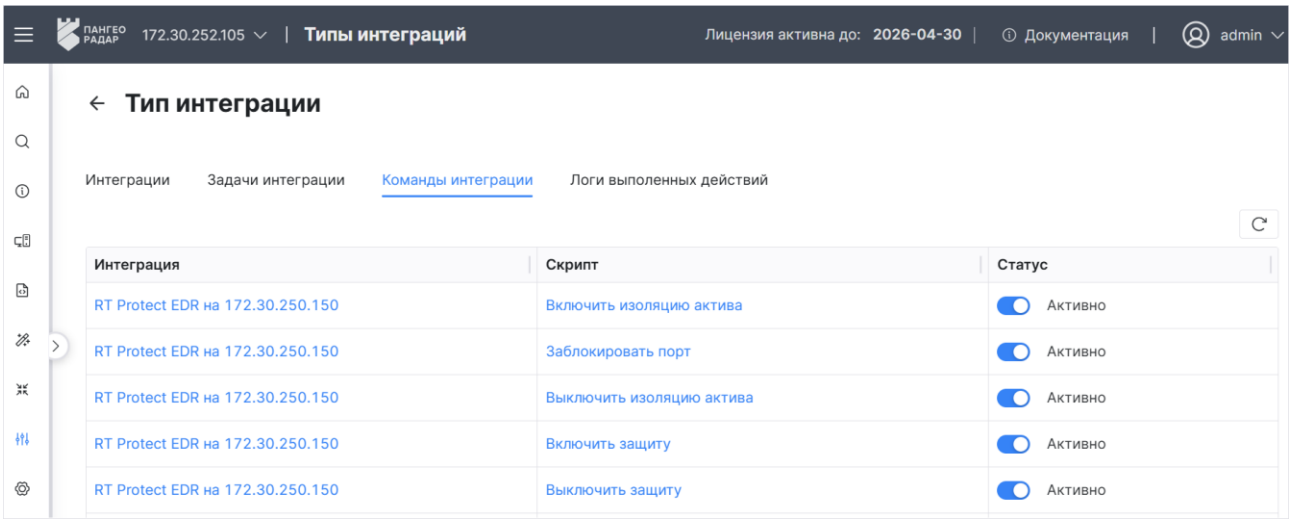


Рис. 264 – Просмотр типа интеграции RT Protect EDR. Вкладка "Команды интеграции"

На вкладке отображается информация об активных действиях, созданных в рамках интеграций:

- **Интеграция** – наименование интеграции, для которой исполняется команда;
- **Скрипт** – наименование команды;
- **Статус** – состояние команды: Активно, Неактивно.

- **Логи выполненных действий**. Пример вкладки приведен на «Рис. 265».

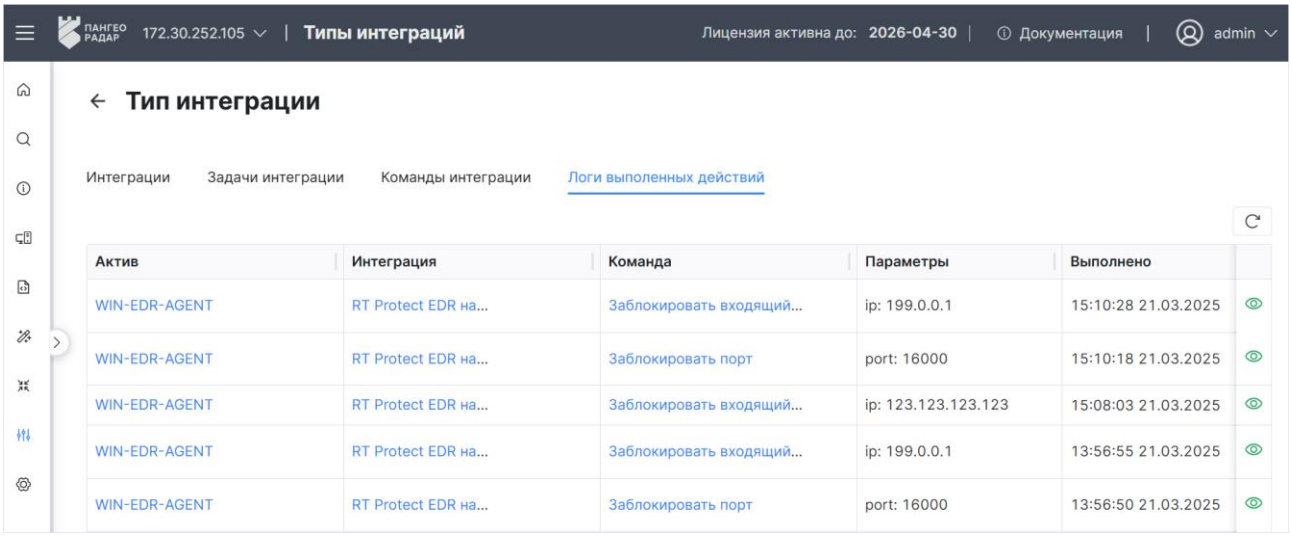


Рис. 265 – Просмотр типа интеграции RT Protect EDR. Вкладка "Логи выполненных действий"

На вкладке отображается журнал выполненных действий:

- **Актив** – наименование актива, на котором выполнено действие;
- **Интеграция** – наименование интеграции, в рамках которой было выполнено действие;
- **Команда** – наименование выполненного действия;
- **Параметры** – информация о параметрах выполненного действия.

Для просмотра результата выполнения действия нажмите кнопку в соответствующей строке. Откроется окно "Результат" (см. «Рис. 266»).

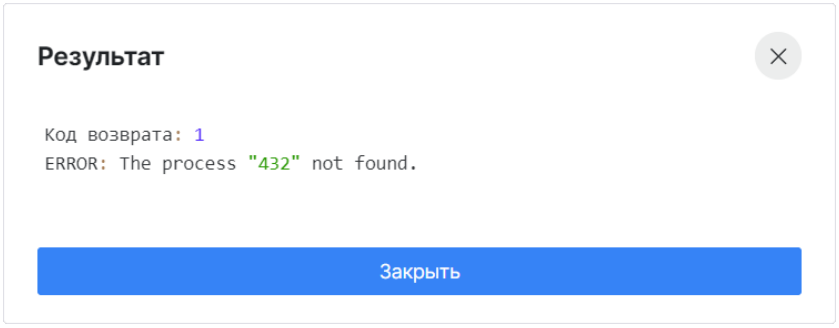


Рис. 266 – Окно "Результат"

16.1.2 EDR действия

О механизме активных действий, доступных в рамках интеграции **RT Protect EDR**, можно ознакомиться в разделе «».

EDR действия могут находиться в следующих состояниях:

- **Активно** – действие становится доступным при настройке правил корреляции и при работе над активами;
- **Неактивно** – действие добавлено в платформу, но не может быть использовано.

Работа с EDR действиями включает в себя следующие процессы:

1. «Создание EDR действия».
2. «Просмотр EDR действия».
3. «Редактирование EDR действия».
4. «Дублирование EDR действия».
5. «Изменение статуса EDR действия».
6. «Экспорт EDR действий».
7. «Импорт EDR действий».
8. «Удаление EDR действий».

Для работы с EDR действиями перейдите в раздел **Параметры → EDR действия** (см. «Рис. 267»).

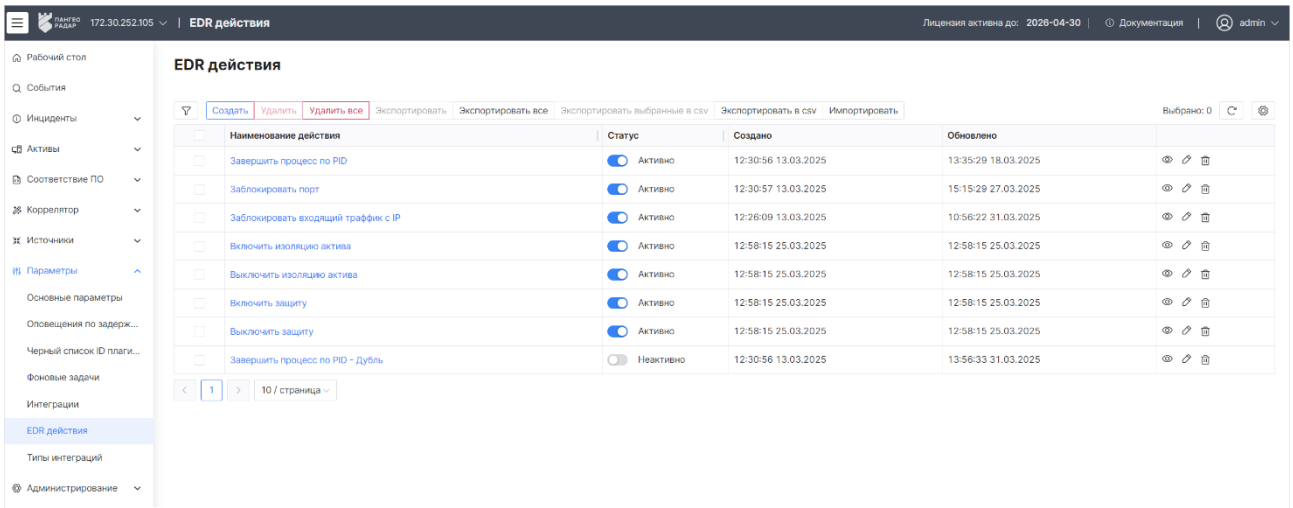


Рис. 267 – Раздел "EDR действия"

16.1.2.1 Создание EDR действия

1. Нажмите кнопку **Создать**. Откроется форма **Создание действия EDR** (см. «Рис. 268»).

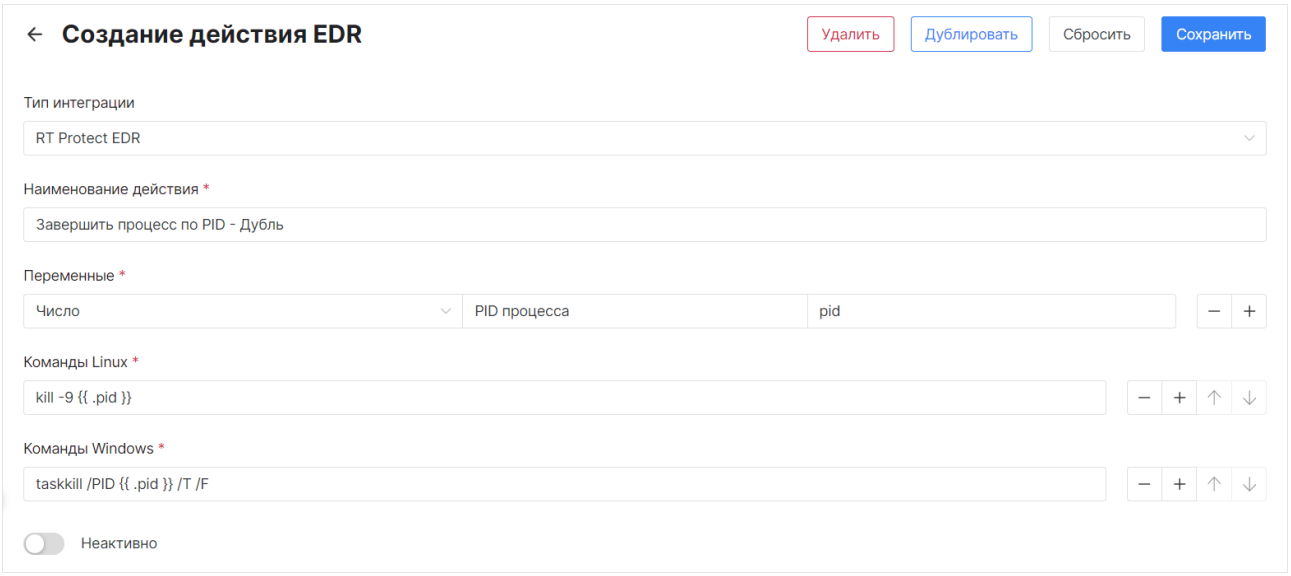


Рис. 268 – Форма "Создание действия EDR"

2. Укажите на форме следующую информацию:
   - в поле **Тип интеграции** из выпадающего списка выберите значение "*RT Protect EDR*";
   - в поле **Наименование действия** укажите наименование EDR действия;
   - в блоке полей **Переменные** добавьте необходимое количество параметров, по которым будет выполнено действие:
     - нажмите кнопку **+**;
     - в поле **Переменная** выберите тип параметра: строка, число, логический;
     - в поле **Название параметра** укажите название параметра для отображения в платформе;
     - в поле **Имя параметра** укажите наименование параметра. По указанному значению будут выполняться команды для ОС Linux и Windows.
   - в блоке полей **Команды Linux** и **Команды Windows** добавьте необходимое количество команд для ОС Linux и Windows. Команды будут исполняться в заданном порядке. Для изменения порядка исполнения команд используйте кнопки ↑, ↓;
   - для активации действия в поле **Статус** установите переключатель в положение "*Включен*".
3. Нажмите кнопку **Сохранить**.

16.1.2.2 Просмотр EDR действия

Для просмотра информации об EDR действии нажмите кнопку в строке нужного действия. Откроется форма "Просмотр действия EDR".

Информация на форме разделена по трем вкладкам:

- **Основные настройки** – информация о параметрах EDR действия;
- **Связанные интеграции** – информация об интеграциях, в которых задействовано действие;
- **Логи выполненных действий** – журнал выполнения действия EDR.

Основные настройки

Пример вкладки "Основные настройки" приведен на «Рис. 269».

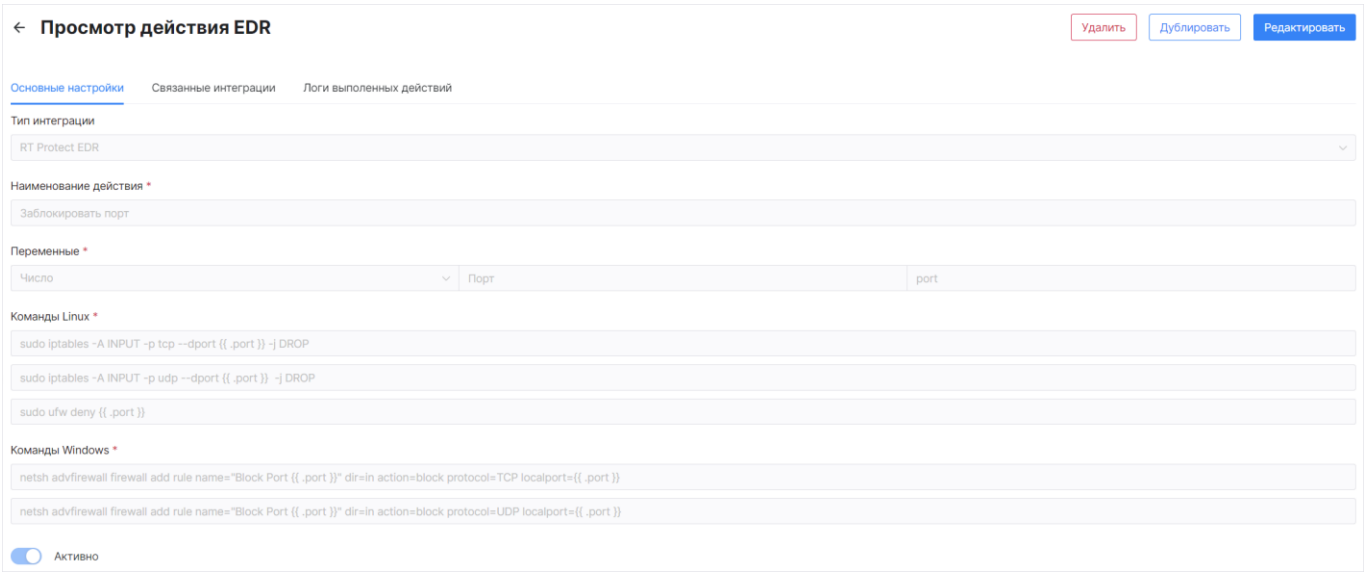


Рис. 269 – Форма "Просмотр действия EDR". Вкладка "Основные настройки"

На вкладке отображается следующая информация:

- **Тип интеграции** – наименование типа интеграции, к которой относится действие;
- **Наименование действия** –название EDR действия в платформе;
- **Переменные** – информация о параметрах EDR действия: Тип переменной, Название действия, Имя действия;
- **Команды Linux** – список команд для ОС Linux;
- **Команды Windows** – список команд для ОС Windows;
- Информация о состоянии EDR действия: Активно, Неактивно.

Связанные интеграции

Пример вкладки "Связанные интеграции" приведен на «Рис. 270».

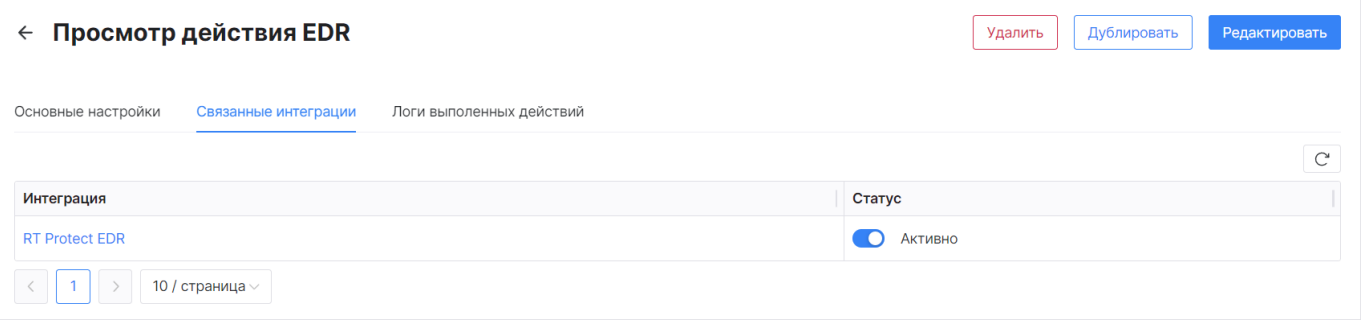


Рис. 270 – Форма "Просмотр действия EDR". Вкладка "Связанные интеграции"

На вкладке отображается список интеграций, в которых используется EDR действие, а также состояние интеграции.

Логи выполненных действий

Пример вкладки "Логи выполненных действий" приведен на «Рис. 271».

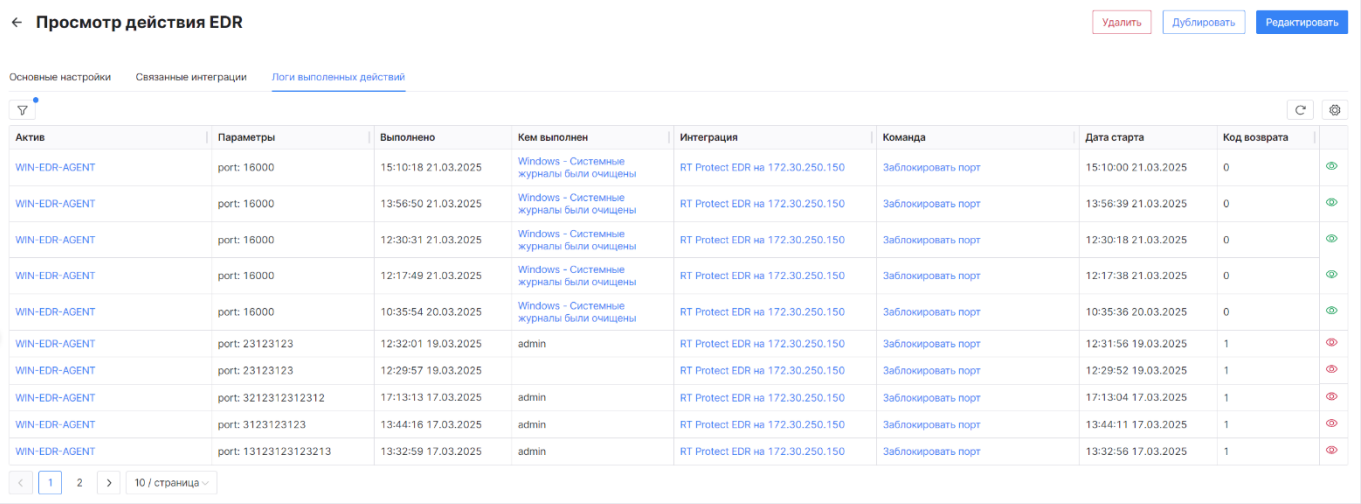


Рис. 271 – Форма "Просмотр действия EDR". Вкладка "Логи выполненных действий"

На вкладке отображается следующая информация:

- **Актив** – наименование актива, на котором выполнено EDR действие;
- **Параметры** – информация о параметрах выполненного действия;
- **Выполнено** – дата и время выполнения действия;
- **Кем выполнено** – информация об инициаторе выполнения действия, например, правило корреляции или пользователь;
- **Интеграция** – наименование интеграции, в рамках которой было выполнено действие;
- **Команда** – наименование EDR действия;
- **Дата старта** – дата и время запуска исполнения действия;
- **Код возврата** – ответ, полученный при выполнении действия:
  - 0 – успешный ответ;
  - 1 – при выполнении действия возникли ошибки.

Для просмотра результата выполнения действия нажмите кнопку в соответствующей строке.

16.1.2.3 Редактирование EDR действия

Открыть EDR действие на редактирование можно двумя способами:

- На главной странице раздела нажмите кнопку в строке нужного EDR действия.
- Перейдите на форму просмотра необходимого EDR действия и нажмите кнопку **Редактировать**.

Для редактирования EDR действия выполните следующие действия:

1. Откройте EDR действие на редактирование.
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

16.1.2.4 Дублирование EDR действия

1. Откройте EDR действие на просмотр.
2. Нажмите кнопку **Дублировать**. Откроется окно "Дублировать действие EDR" (см. «Рис. 272»).

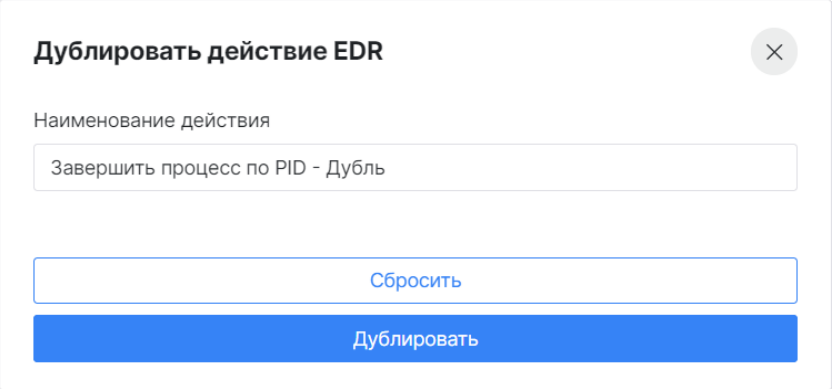


Рис. 272 – Окно "Дублировать действие EDR"

3. При необходимости измените наименование действия и нажмите кнопку **Дублировать**.
4. Будет создано новое EDR действие на основе существующего.

16.1.2.5 Изменение статуса EDR действия

Для изменения статуса EDR действия в графе "Статус" установите переключатель в соответствующее положение.

Примечание: *если у EDR действия есть связанные активные сущности, например правило корреляции или актив, то изменить статус действия будет нельзя*.

16.1.2.6 Экспорт EDR действий

Для массового экспорта EDR действий установите нужные флаги и нажмите кнопку **Экспортировать**. Будет сформирован архив с EDR действиями в формате `.zip`.

Для экспорта всех EDR действий нажмите кнопку **Экспортировать все**.

Для массового экспорта EDR действий в формат CSV нажмите кнопку **Экспортировать выбранные в csv**.

Для экспорта всех EDR действий в формат CSV нажмите кнопку **Экспортировать в csv**.

16.1.2.7 Импорт EDR действий

1. Нажмите кнопку **Импортировать**.
2. В открывшемся окне укажите путь к архиву с EDR действиями.
3. Нажмите кнопку **Открыть**.

16.1.2.8 Удаление EDR действий

Примечание: *для корректной работы интеграций не рекомендуется удалять EDR действия, установленные по умолчанию*.

Для удаления EDR действия нажмите кнопку  в соответствующей строке.

Для массового удаления EDR действий установите нужные флаги и нажмите кнопку **Удалить**.

Для удаление всех EDR действий нажмите кнопку **Удалить все**.

16.1.3 Настройка интеграции RT Protect EDR

Платформа Радар позволяет настроить несколько независимых интеграций с системой **RT Protect EDR**. Например, если используется несколько управляющих серверов системы **RT Protect EDR** с разным списком подчиненных активов, то для каждого управляющего сервера нужно создать экземпляр интеграции с соответствующими настройками.

Все действия над интеграциями выполняются в разделе **Параметры → Интеграции**.

Перед выполнением настройки интеграции с **RT Protect EDR** выполните следующие действия:

1. Активируйте тип интеграции **RT Protect EDR**. Подробнее см. раздел «Типы интеграций».
2. Настройте EDR действия. Подробнее см. раздел «EDR действия».

Процесс настройки интеграции с **RT Protect EDR** включает в себя следующие шаги:

- «Шаг 1. Создание экземпляра интеграции с RT Protect EDR»;
- «Шаг 2. Настройка задачи синхронизации активов»;
- «Шаг 3. Настройка активных действий для интеграции»;
- «Шаг 4. Активация интеграции».

16.1.3.1 Шаг 1. Создание экземпляра интеграции с RT Protect EDR

1. Перейдите в раздел **Параметры → Интеграции**.
2. Нажмите кнопку **Создать**. Откроется окно "Создание интеграции" (см. «Рис. 273»).

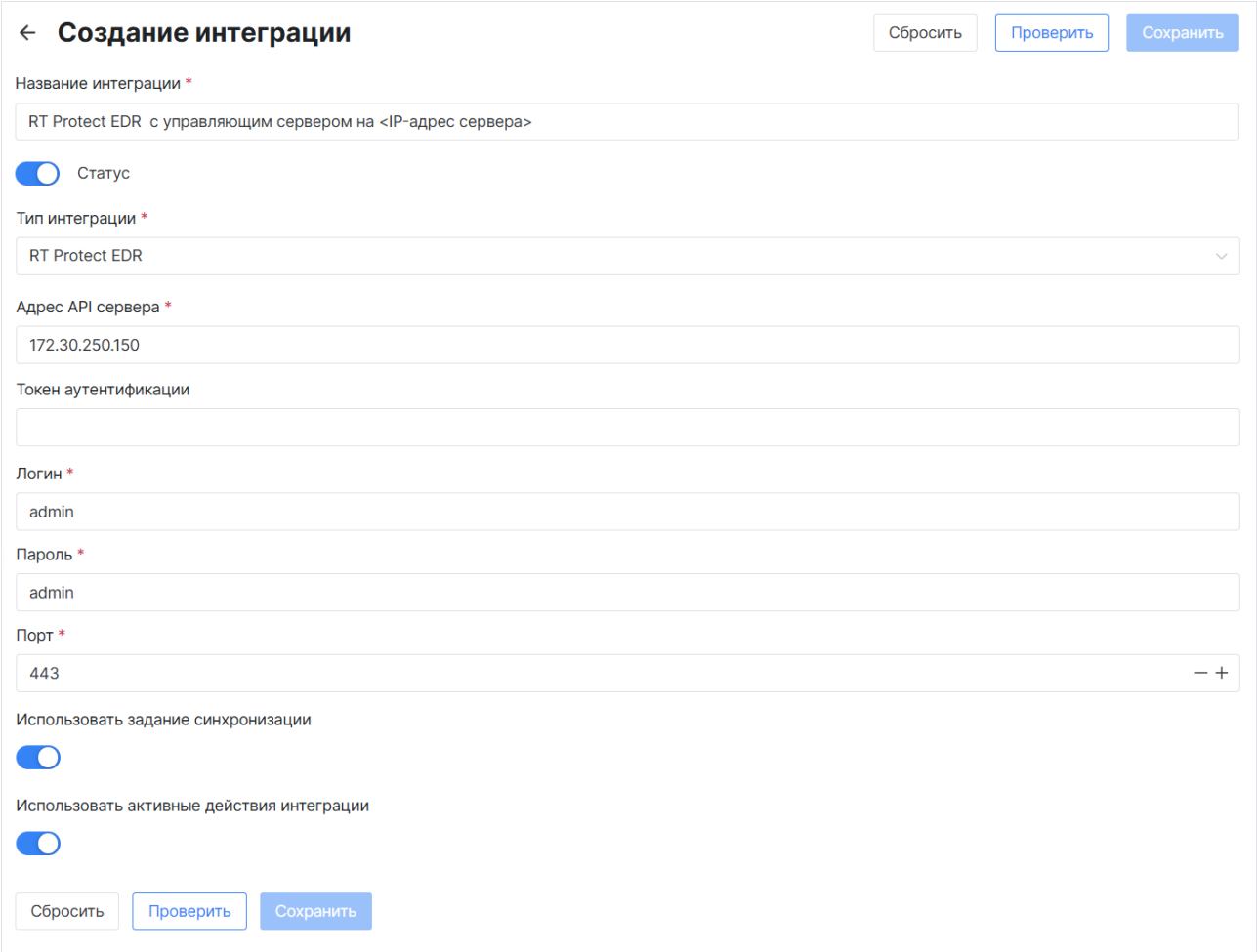


Рис. 273 – Создание интеграции с RT Protect EDR

3. Укажите в окне следующую информацию:
    - **Название интеграции** – укажите наименование интеграции;
    - **Тип интеграции** – из выпадающего списка выберите значение "*RT Protect EDR*". Поля формы автоматически изменятся для настройки выбранного типа интеграции;
    - **Адрес API сервера** – укажите IP-адрес, на котором располагается API сервер **RT Protect EDR**;
    - **Токен аутентификации** – укажите токен, полученный в системе **RT Protect EDR**;
    - **Логин** – укажите логин для доступа к API серверу;
    - **Пароль** – укажите пароль для доступа к API серверу;
    - **Порт** – укажите порт, по которому выполняется подключение к API серверу;
    - **Использовать задание синхронизации** – установите переключатель в положения **Включен** для активации периодических задач синхронизации активов и инцидентов;
    - **Использовать активные действия интеграции** – установите переключатель в положения **Включен** для активации возможности использования активных действий.
4. Нажмите кнопку **Проверить**. Будет выполнена проверка подключения к API серверу.

5. Нажмите кнопку **Сохранить**. Сохранение интеграции будет доступно только после успешной проверки соединения с API сервером.

16.1.3.2 Шаг 2. Настройка задачи синхронизации активов

1. Откройте интеграцию на редактирование (кнопка).
2. Перейдите на вкладку "Задачи интеграции" (см. «Рис. 274»).

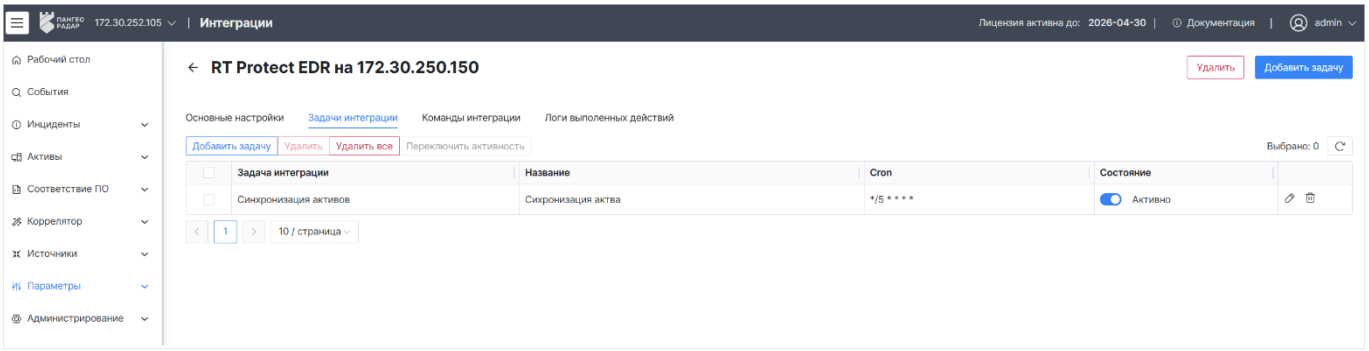


Рис. 274 – Настройка интеграции. Задачи интеграции

3. Нажмите кнопку **Добавить задачу**. Откроется окно "Добавить задачу" (см. «Рис. 275»).

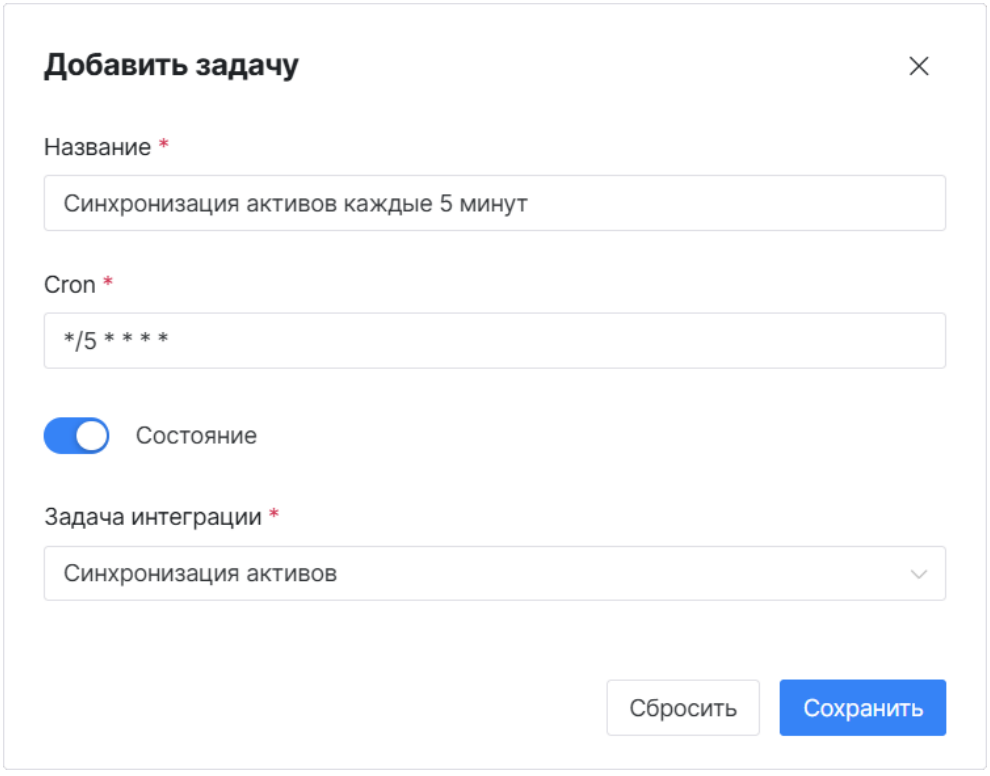


Рис. 275 – Окно "Добавить задачу"

4. Укажите в окне следующую информацию:
   - **Название** – укажите название периодической задачи;
   - **Cron** – укажите CRON-выражение, описывающее периодичность задачи. Подсказу по CRON-выражениям см. на **сайте**;
   - **Состояние** – включите выполнение задачи синхронизации активов, установив переключатель в положение "Включен";

- **Задача интеграции** – из выпадающего списка выберите задачу "Синхронизация активов".

5. Нажмите кнопку **Сохранить**.
6. Журнал выполнения задачи можно посмотреть в разделе **Администрирование → Кластер →** вкладка **Планировщик задач**.

16.1.3.3 Шаг 3. Настройка активных действий для интеграции

1. Откройте интеграцию на редактирование (кнопка).
2. Перейдите на вкладку "Команды интеграции" (см. «Рис. 276»).

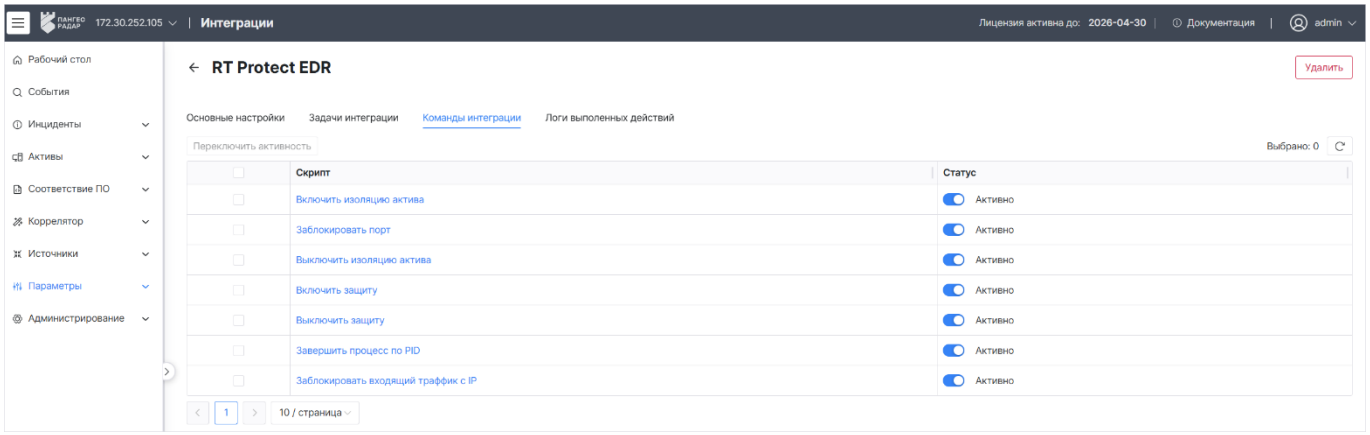


Рис. 276 – Настройка интеграции. Команды интеграции

3. В графе **Статус** включите необходимые действия, которые будут доступны при выявлении инцидентов на активах.

16.1.3.4 Шаг 4. Активация интеграции

Чтобы по интеграции выполнялось взаимодействие с системой **RT Protect EDR**, ее необходимо активировать.

Для активации интеграции перейдите в раздел **Параметры → Интеграции** и в колонке **Статус** установите переключатель в положение "Включен".

16.1.4 Работа с интеграцией RT Protect EDR

После настройки интеграции с **RT Protect EDR** в платформе станут доступны следующие возможности:

- «Работа с правилами корреляции»:
  - настройка активных действий, которые необходимо выполнить при "сработке" правила;
  - просмотр добавленных в правило корреляции активных действий.
- «Настройка правила корреляции. Добавление активных действий

1. Начните процесс создания/редактирования правила корреляции.

   Примечание: *функции по настройке активных действий доступны, как и при создании с помощью визуального конструктора, так и без него.*

2. Перейдите на вкладку Интеграции (см. «Рис. 277»).

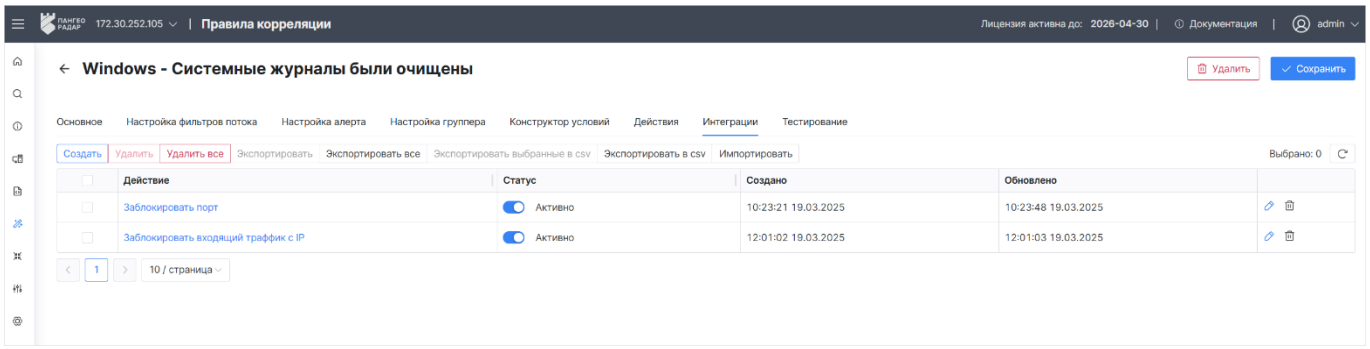


Рис. 277 – Конструктор правила корреляции. Вкладка "Интеграции"

3. Нажмите кнопку Создать. Откроется окно "Действия интеграции" (см. «Рис. 278» - «Рис. 279»).

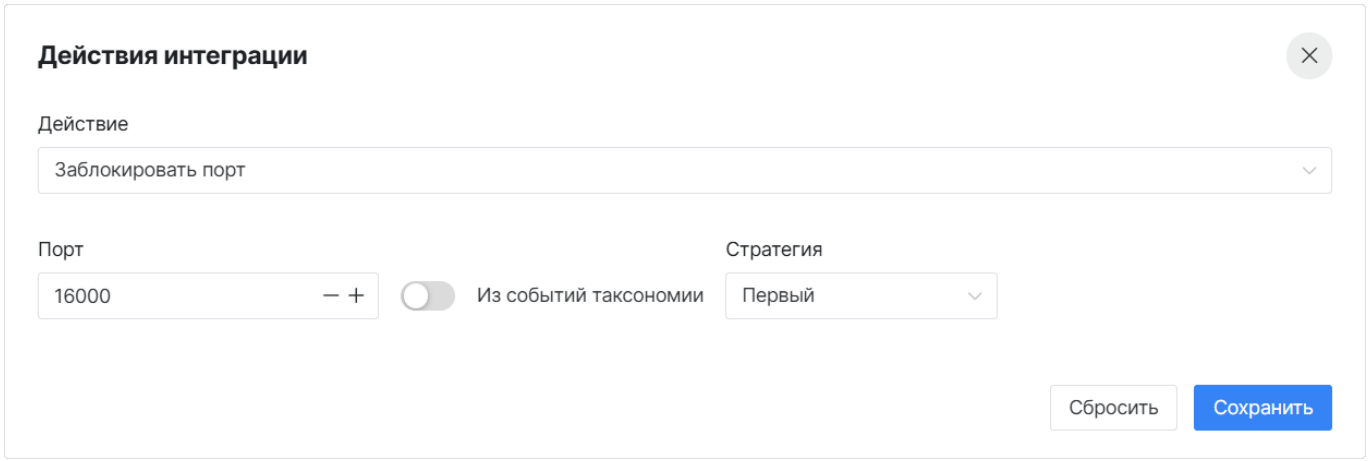


Рис. 278 – Настройка действия интеграции с дополнительными параметрами

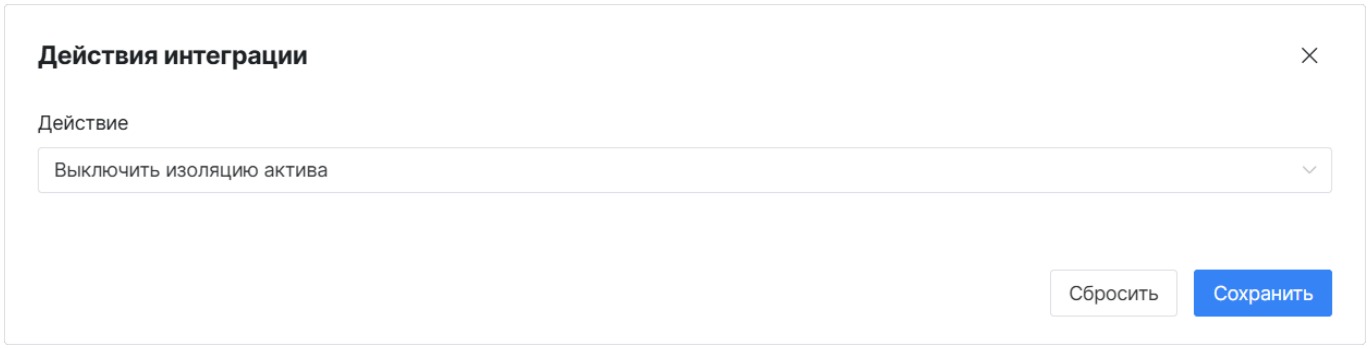


Рис. 279 – Настройка действия интеграции без дополнительных параметров

4. В открывшемся окне выберите действие.
5. В зависимости от выбранного действия поля формы будут автоматически изменены для настройки действия:
    - Для действий Завершить **процесс по PID**, Заблокировать **порт**, Заблокировать **входящий траффик с IP укажите** следующие сведения:
        - в поле Параметр укажите соответствующий параметр: идентификатор процесса, порт или IP-адрес. При необходимости можно выбрать параметр из полей таксономии. Для этого установите переключатель **Из полей**

таксономии в положение "Включен" и в поле Параметр из выпадающего списка выберите поле события;

- в поле **Стратегия** выберите стратегию передачи событий в правиле: передавать только первое событие в интеграцию или последнее;
- нажмите кнопку Сохранить.

- Для действий не требующих дополнительных настроек, нажмите кнопку Сохранить.

6. Активируйте добавленное действие. Для этого в графе Статус установите переключатель в положение "Включен".
7. Добавьте необходимое количество активных действий.
8. Завершите процесс создания/редактирования правила корреляции.

16.1.4.1.1 Просмотр действий интеграции

Для просмотра добавленных в правило действий интеграции откройте его на просмотр и перейдите на вкладку "Интеграции" (см. «Рис. 280»).

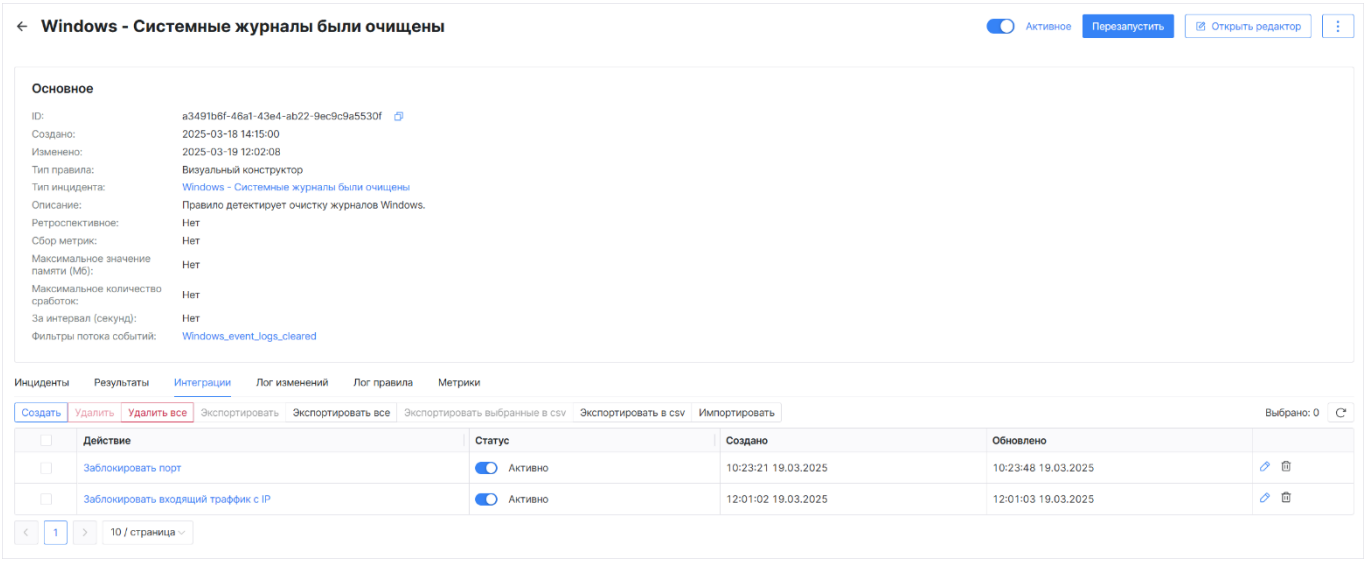


Рис. 280 – Просмотр правила корреляции. Вкладка "Интеграции"

На вкладке отображается следующая информация:

- **Действие** – наименование действия;
- **Статус** – состояние действия: Активно, Неактивно;
- **Создано** – дата и время добавления действия в правило корреляции;
- **Обновлено** – дата и время изменения информации о действии в правиле корреляции.
- Работа с активами»:
  - выполнение активных действий по связанным интеграциям;
  - просмотр журнала выполненных действий на активе.
- «Просмотр связей с интеграциями и журнала выполненных действий

Откройте актив на просмотр (см. «Рис. 281»).

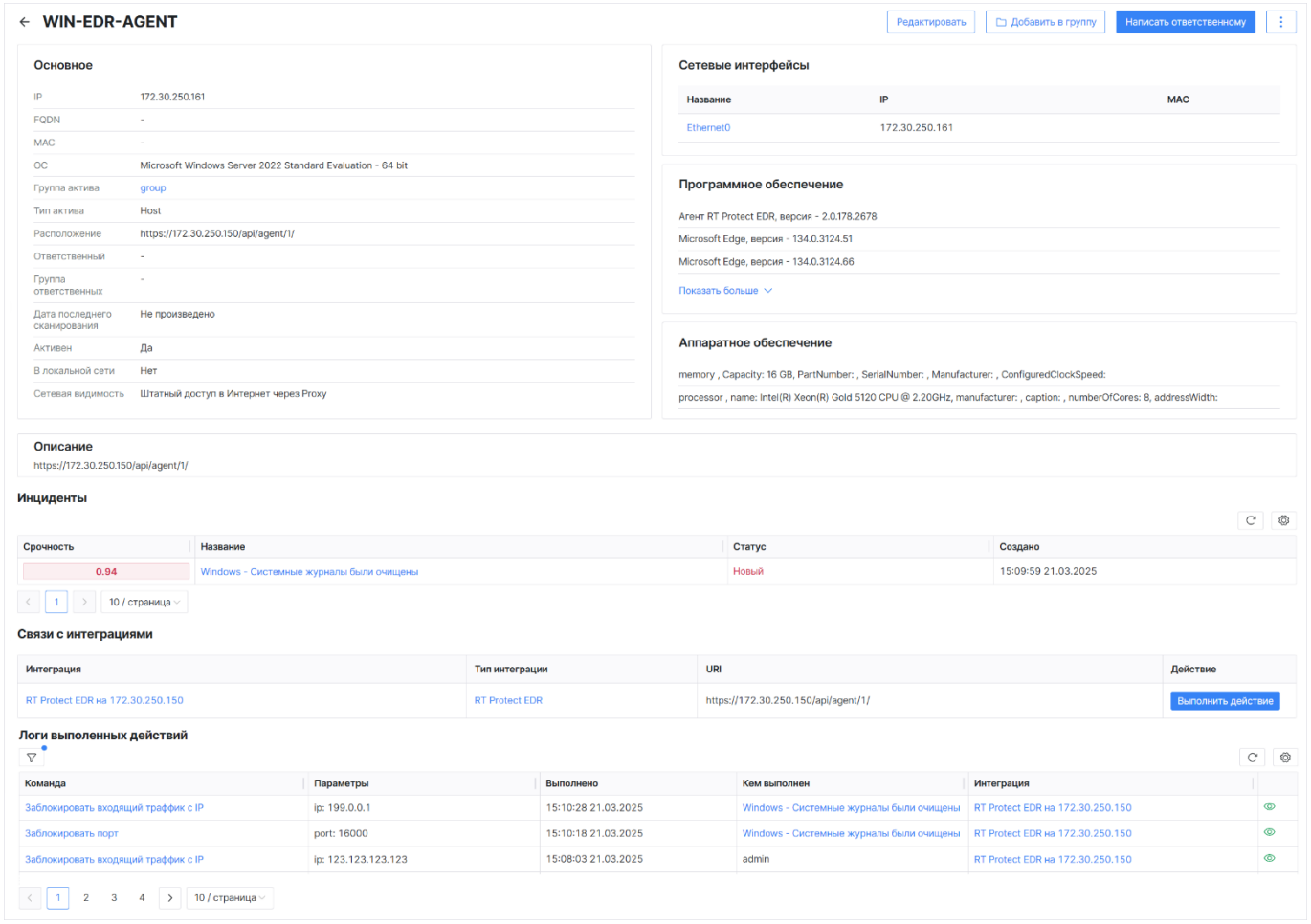


Рис. 281 – Просмотр актива

При интеграции с системой RT **Protect EDR при** анализе актива доступен просмотр следующей дополнительной информации:

- Блок Связи **с интеграциями** – просмотр информации о связанных интеграциях:
  - **Интеграция** – наименование интеграции;
  - **Тип интеграции** – наименование типа интеграции;
  - **URL** – URL адрес API сервера.
- Блок Логи **выполненных действий** – просмотр журнала выполненных действий на активе:
  - **Команда** – наименование выполненного действия;
  - **Параметры** – информация о параметрах выполненного действия;
  - **Выполнено** – дата и время выполнения действия;
  - **Кем выполнено** – информация об инициаторе выполнения действия, например правило корреляции или пользователь;
  - **Интеграция** – наименование интеграции, в рамках которой было выполнено действие;
  - **Актив** – наименование актива, на котором выполнено действие;
  - **Дата старта** – дата и время запуска исполнения действия;

- **Код возврата** – ответ, полученный при выполнении действия:
  - 0 – успешный ответ;
  - 1 – при выполнении действия возникли ошибки.

Для просмотра результата выполнения действия нажмите кнопку в соответствующей строке.

16.1.4.1.2 Выполнение активных действий на активе

1. Откройте актив на просмотр (см. «Рис. 281»).
2. В блоке Связи **с интеграциями нажмите** кнопку Выполнить **действие**. Откроется окно "Выполнить действие" (см. «Рис. 282»).

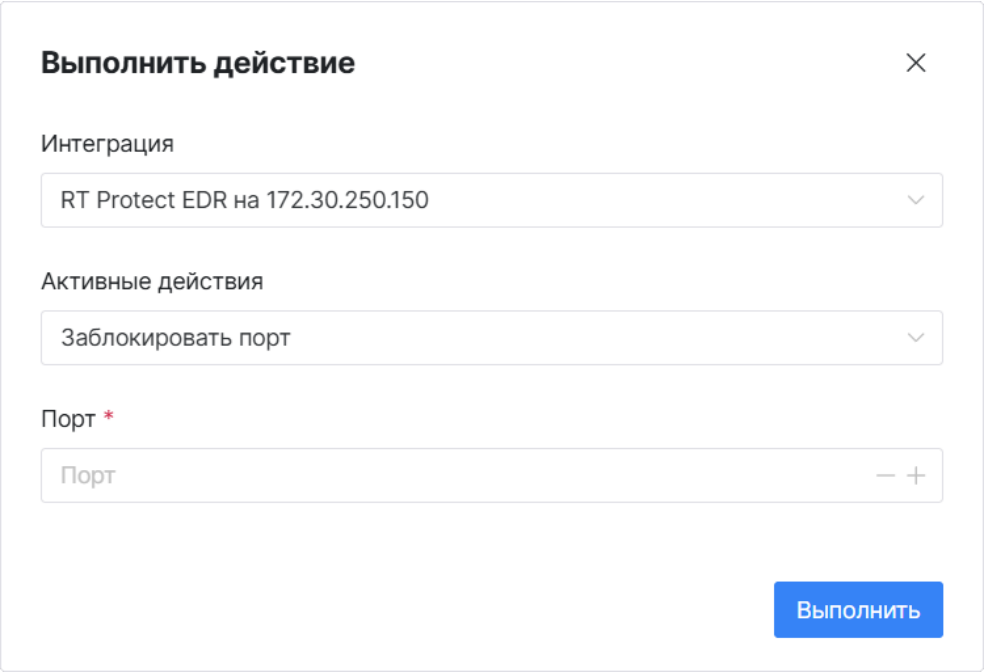


Рис. 282 – Окно "Выполнить действие"

3. Выполните в окне следующие действия:
   - в поле Интеграция выберите необходимую интеграцию с RT **Protect EDR**;
   - в поле Активные **действия из** выпадающего списка выберите действие, которое необходимо выполнить. Поля формы будут автоматически изменены для настройки выбранного действия;
   - при необходимости укажите дополнительные параметры, например идентификатор процесса, IP-адрес или порт;
   - нажмите кнопку Выполнить.

- Работа с инцидентами» – просмотр журнала выполненных действий по инциденту;
- «Просмотр журнала выполнения действий по интеграции».

16.1.4.2 Работа с правилами корреляции

16.1.4.2.1 Настройка правила корреляции. Добавление активных действий

9. Начните процесс создания/редактирования правила корреляции.

Примечание: *функции по настройке активных действий доступны, как и при создании с помощью визуального конструктора, так и без него*.

10. Перейдите на вкладку **Интеграции** (см. «Рис. 277»).

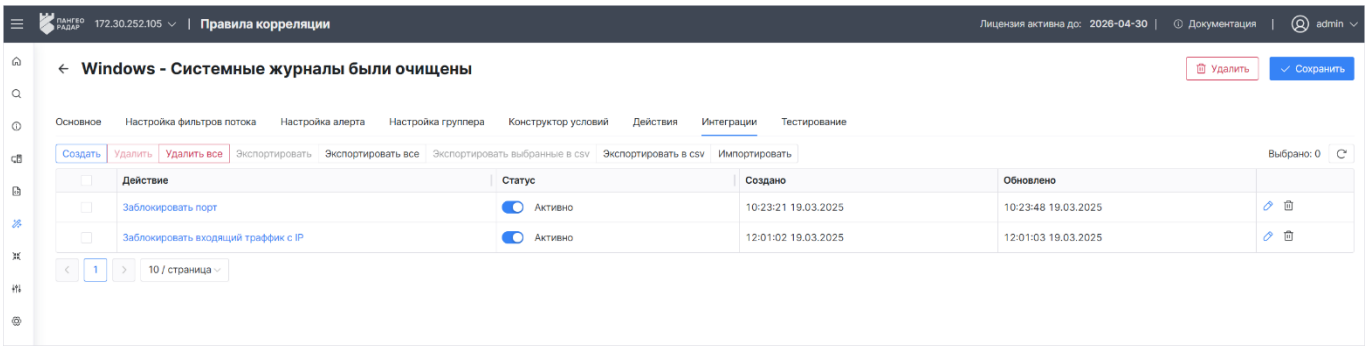


Рис. 277 – Конструктор правила корреляции. Вкладка "Интеграции"

11. Нажмите кнопку **Создать**. Откроется окно "Действия интеграции" (см. «Рис. 278» - «Рис. 279»).

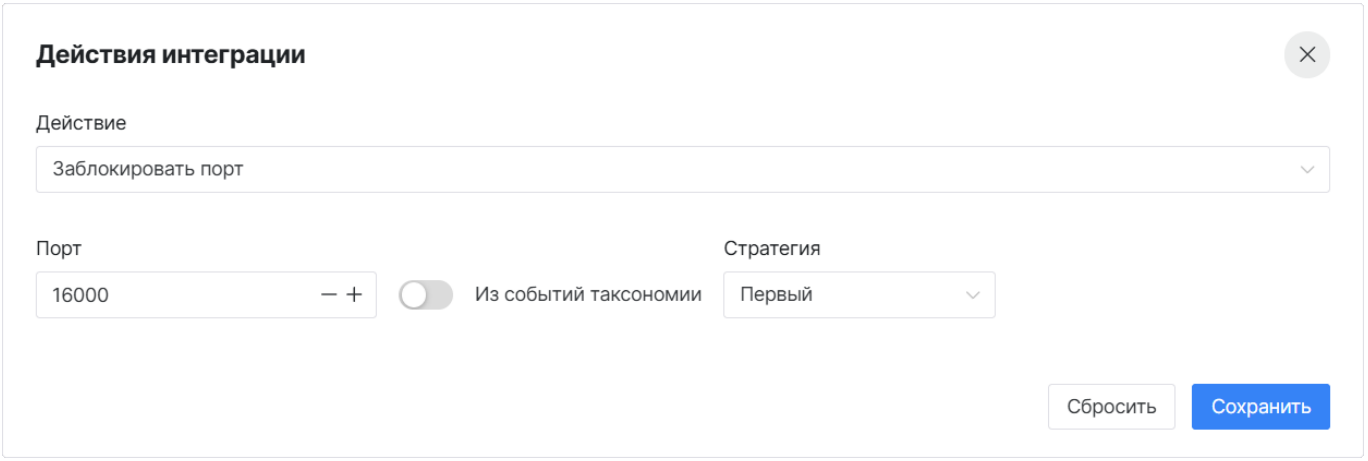


Рис. 278 – Настройка действия интеграции с дополнительными параметрами

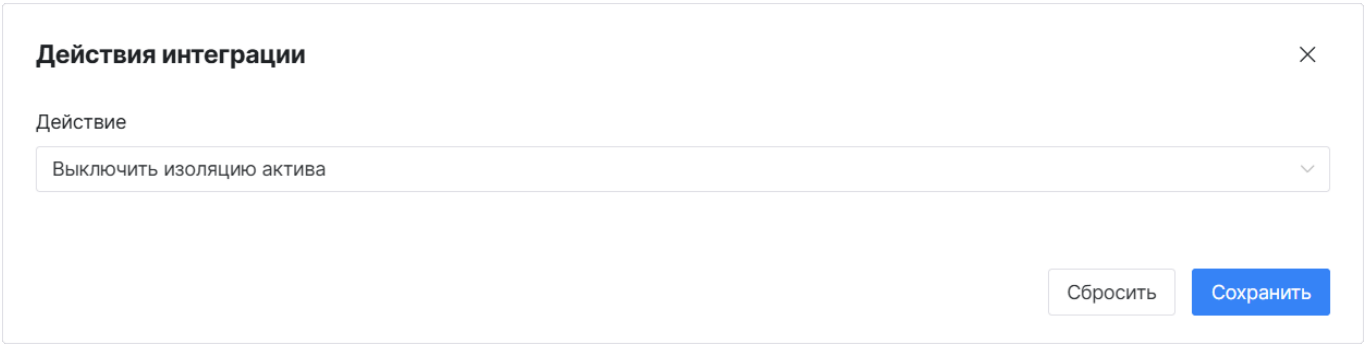


Рис. 279 – Настройка действия интеграции без дополнительных параметров

12. В открывшемся окне выберите действие.
13. В зависимости от выбранного действия поля формы будут автоматически изменены для настройки действия:
    - Для действий **Завершить процесс по PID**, **Заблокировать порт**, **Заблокировать входящий траффик с IP** укажите следующие сведения:

- в поле **Параметр** укажите соответствующий параметр: идентификатор процесса, порт или IP-адрес. При необходимости можно выбрать параметр из полей таксономии. Для этого установите переключатель **Из полей таксономии** в положение "Включен" и в поле **Параметр** из выпадающего списка выберите поле события;
- в поле **Стратегия** выберите стратегию передачи событий в правиле: передавать только первое событие в интеграцию или последнее;
- нажмите кнопку **Сохранить**.

- Для действий не требующих дополнительных настроек, нажмите кнопку **Сохранить**.

14. Активируйте добавленное действие. Для этого в графе **Статус** установите переключатель в положение "Включен".
15. Добавьте необходимое количество активных действий.
16. Завершите процесс создания/редактирования правила корреляции.

16.1.4.2.2 Просмотр действий интеграции

Для просмотра добавленных в правило действий интеграции откройте его на просмотр и перейдите на вкладку "Интеграции" (см. «Рис. 280»).

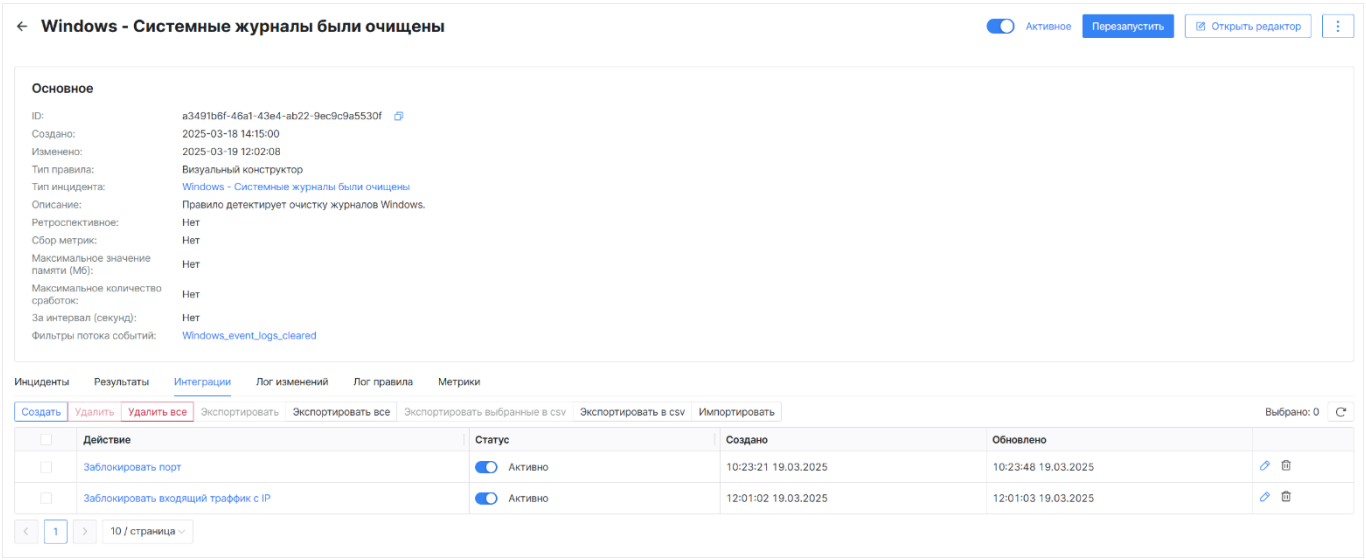


Рис. 280 – Просмотр правила корреляции. Вкладка "Интеграции"

На вкладке отображается следующая информация:

- **Действие** – наименование действия;
- **Статус** – состояние действия: Активно, Неактивно;
- **Создано** – дата и время добавления действия в правило корреляции;
- **Обновлено** – дата и время изменения информации о действии в правиле корреляции.

16.1.4.3 Работа с активами

16.1.4.3.1 Просмотр связей с интеграциями и журнала выполненных действий

Откройте актив на просмотр (см. «Рис. 281»).

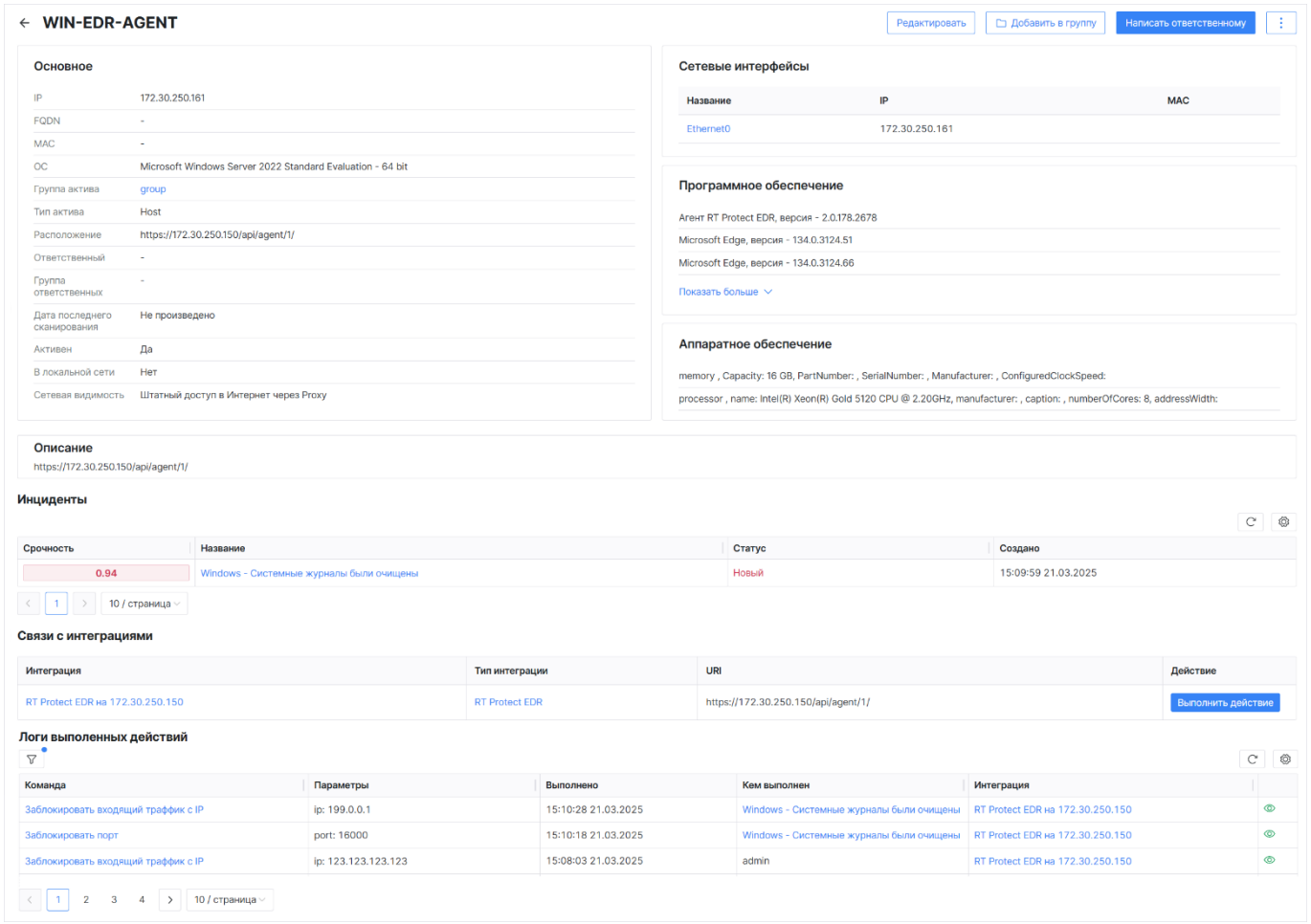


Рис. 281 – Просмотр актива

При интеграции с системой **RT Protect EDR** при анализе актива доступен просмотр следующей дополнительной информации:

- Блок **Связи с интеграциями** – просмотр информации о связанных интеграциях:
  - **Интеграция** – наименование интеграции;
  - **Тип интеграции** – наименование типа интеграции;
  - **URL** – URL адрес API сервера.
- Блок **Логи выполненных действий** – просмотр журнала выполненных действий на активе:
  - **Команда** – наименование выполненного действия;
  - **Параметры** – информация о параметрах выполненного действия;
  - **Выполнено** – дата и время выполнения действия;
  - **Кем выполнено** – информация об инициаторе выполнения действия, например правило корреляции или пользователь;

- **Интеграция** – наименование интеграции, в рамках которой было выполнено действие;
- **Актив** – наименование актива, на котором выполнено действие;
- **Дата старта** – дата и время запуска исполнения действия;
- **Код возврата** – ответ, полученный при выполнении действия:
  - 0 – успешный ответ;
  - 1 – при выполнении действия возникли ошибки.

Для просмотра результата выполнения действия нажмите кнопку в соответствующей строке.

16.1.4.3.2 Выполнение активных действий на активе

4. Откройте актив на просмотр (см. «Рис. 281»).
5. В блоке **Связи с интеграциями** нажмите кнопку **Выполнить действие**. Откроется окно "Выполнить действие" (см. «Рис. 282»).

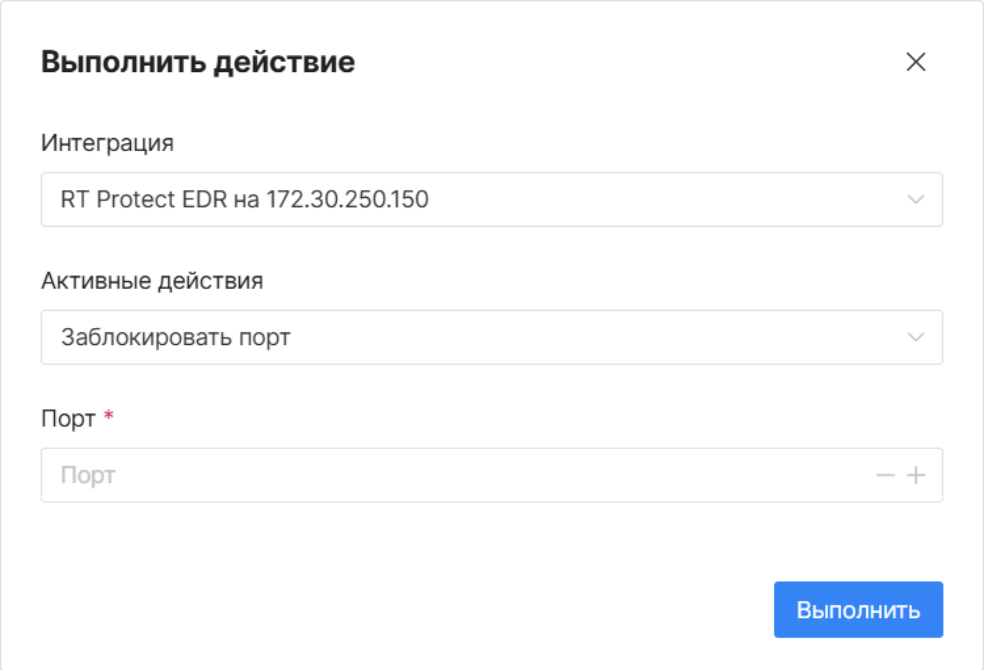


Рис. 282 – Окно "Выполнить действие"

6. Выполните в окне следующие действия:
   - в поле **Интеграция** выберите необходимую интеграцию с **RT Protect EDR**;
   - в поле **Активные действия** из выпадающего списка выберите действие, которое необходимо выполнить. Поля формы будут автоматически изменены для настройки выбранного действия;
   - при необходимости укажите дополнительные параметры, например идентификатор процесса, IP-адрес или порт;
   - нажмите кнопку **Выполнить**.

16.1.4.4 Работа с инцидентами

Откройте инцидент на просмотр (см. «Рис. 283»).

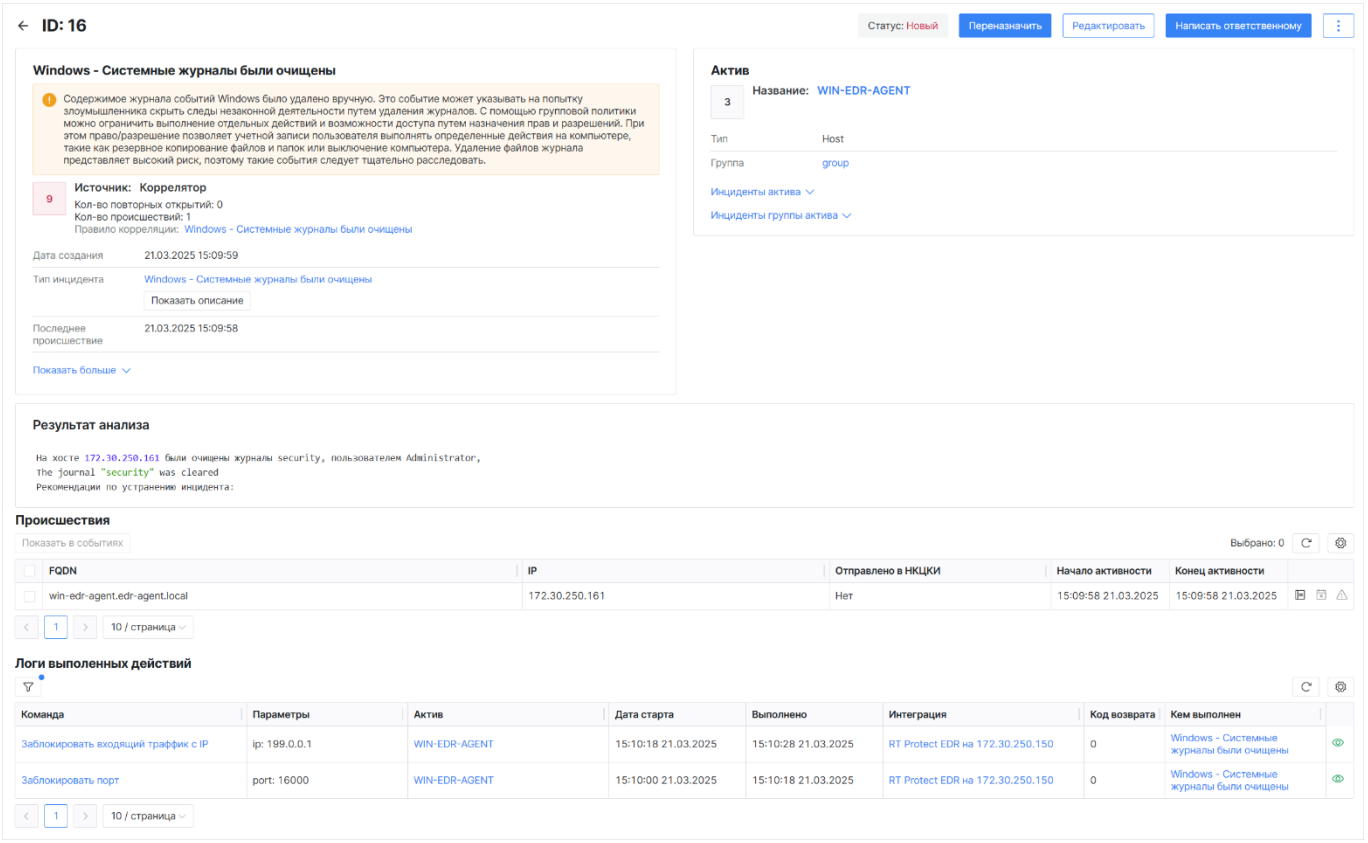


Рис. 283 – Просмотр инцидента

При интеграции с системой **RT Protect EDR** при анализе инцидента в блоке **Логи выполненных действий** доступен просмотр следующей дополнительной информации:

- **Команда** – наименование выполненного действия;
- **Параметры** – информация о параметрах выполненного действия;
- **Актив** – наименование актива, на котором выполнено действие;
- **Дата старта** – дата и время запуска исполнения действия;
- **Выполнено** – дата и время выполнения действия;
- **Кем выполнено** – информация об инициаторе выполнения действия, например правило корреляции или пользователь;
- **Интеграция** – наименование интеграции, в рамках которой было выполнено действие;
- **Код возврата** – ответ, полученный при выполнении действия:
  - 0 – успешный ответ;
  - 1 – при выполнении действия возникли ошибки.

Для просмотра результата выполнения действия нажмите кнопку  в соответствующей строке.

16.1.4.5 Просмотр журнала выполнения действий по интеграции

Для просмотра журнала выполнения действий по экземпляру интеграции перейдите в раздел **Параметры** → **Интеграции**, откройте интеграцию на просмотр и перейдите на вкладку "Логи выполненных действий" (см. «Рис. 284»).

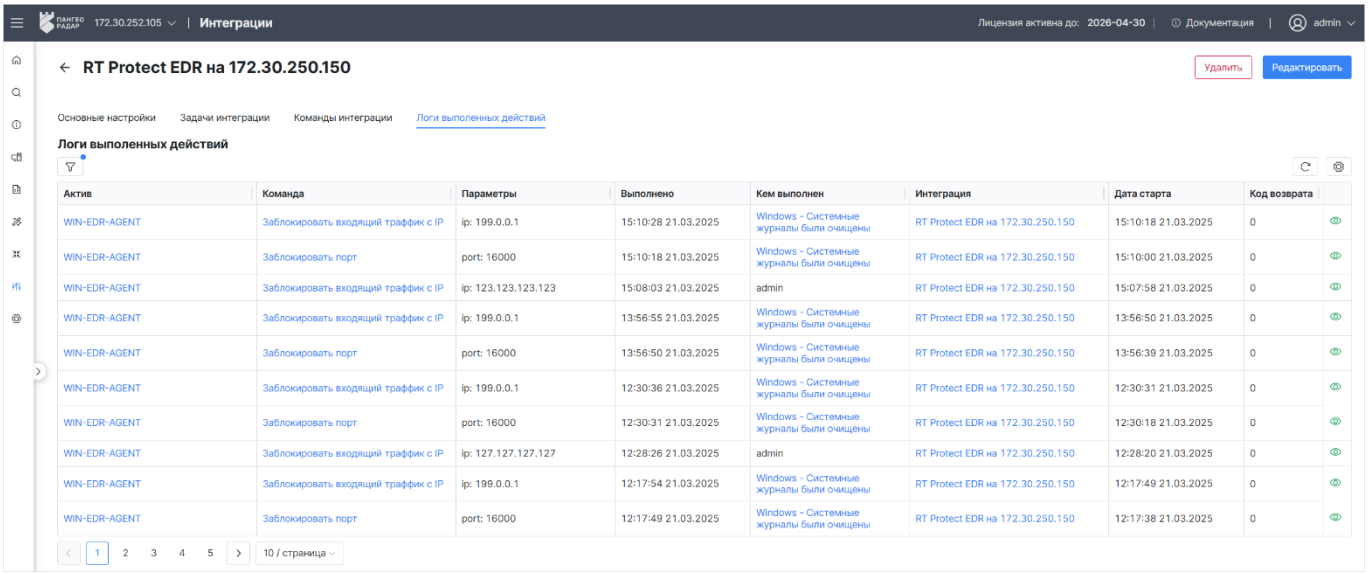


Рис. 284 – Просмотр интеграции. Вкладка "Логи выполненных действий"

На вкладке отображается следующая информация:

- **Актив** – наименование актива, на котором выполнено действие;
- **Команда** – наименование выполненного действия;
- **Параметры** – информация о параметрах выполненного действия;
- **Выполнено** – дата и время выполнения действия;
- **Кем выполнено** – информация об инициаторе выполнения действия, например правило корреляции или пользователь;
- **Интеграция** – наименование интеграции, в рамках которой было выполнено действие;
- **Дата старта** – дата и время запуска исполнения действия;
- **Код возврата** – ответ, полученный при выполнении действия:
  - 0 – успешный ответ;
  - 1 – при выполнении действия возникли ошибки.

Для просмотра результата выполнения действия нажмите кнопку в соответствующей строке.

16.2 Kaspersky Security Center

16.2.1 Характеристики системы

Наименование системы – Kaspersky Security Center (далее KSC).

Назначение системы – универсальная консоль централизованного управления различными решениями, продуктами и сервисами, которые обеспечивают информационную безопасность корпоративной ИТ-инфраструктуры.

Разработчик системы – АО «Лаборатория Касперского».

Сайт – Security Center | Лаборатория Касперского.

Возможности, предоставляемые интеграцией:

- синхронизация активов;
- использование сервиса **Sonar** для сканирования активов. Использование сервиса выполняется в соответствии с параметрами, указанными для экземпляра интеграции.

16.2.2 Настройка интеграции

Перед выполнением настройки интеграции активируйте тип интеграции **KSC**. Подробнее см. раздел «Типы интеграций».

Процесс настройки интеграции с **KSC** включает в себя следующие шаги:

- «Шаг 1. Создание экземпляра интеграции с KSC»;
- «Шаг 2. Создание задачи по синхронизации активов»;
- «Шаг 3. Активация экземпляра интеграции с KSC».

16.2.2.1 Шаг 1. Создание экземпляра интеграции с KSC

1. Перейдите в раздел **Параметры → Интеграции**.
2. Нажмите кнопку **Создать**. Откроется окно "Создание интеграции" (см. «Рис. 285»).

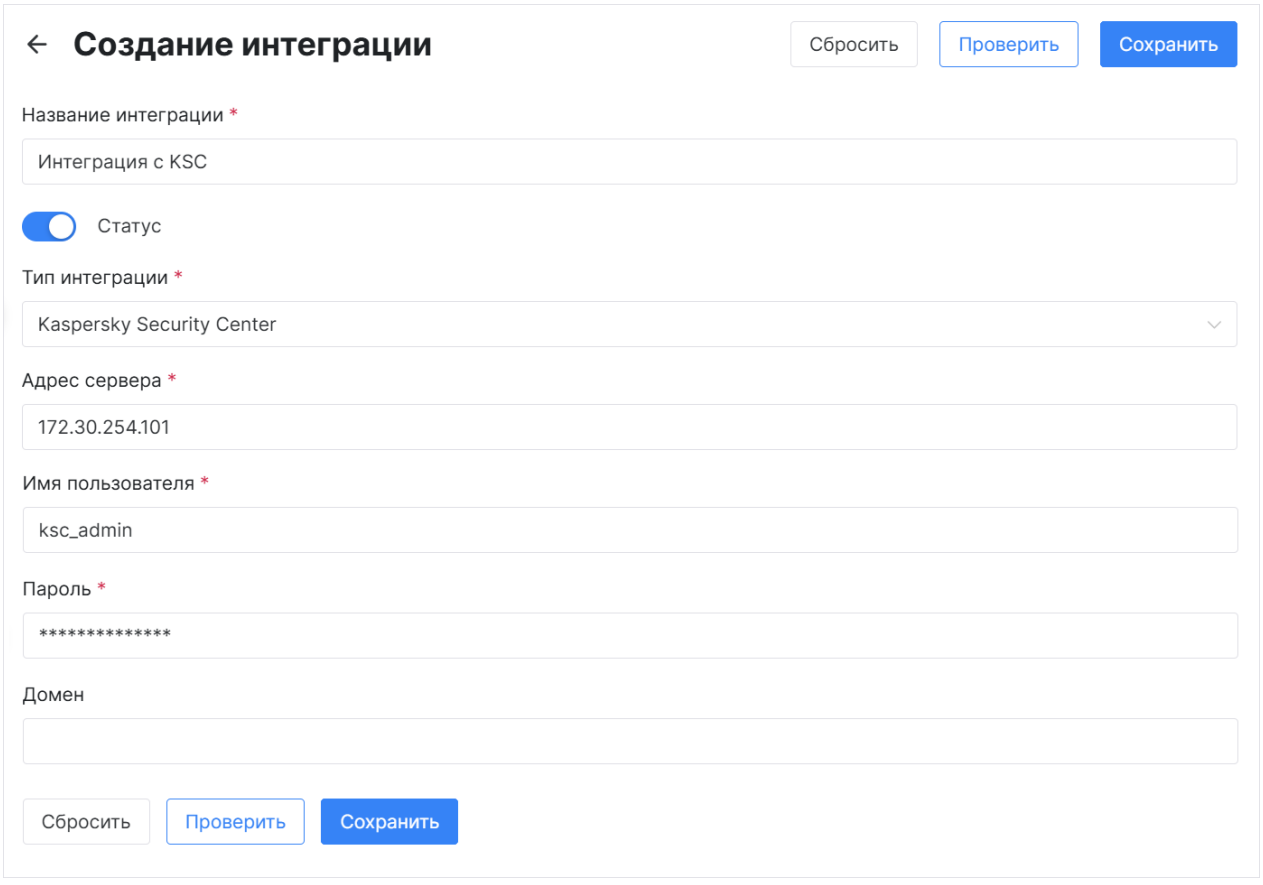


Рис. 285 – Создание интеграции с KSC

3. Укажите в окне следующую информацию:
    - **Название интеграции** – укажите наименование интеграции;

- **Тип интеграции** – из выпадающего списка выберите значение "*Kaspersky Security Center*". Поля формы автоматически изменятся для настройки выбранного типа интеграции;
- **Адрес сервера** – укажите IP-адрес, на котором развернут API сервер KSC;
- **Имя пользователя** – укажите имя пользователя для доступа к API серверу KSC. Убедитесь, что пользователь обладает необходимым набором прав для выполнения запросов к API серверу KSC;
- **Пароль** – укажите пароль пользователя;
- **Домен** – при необходимости укажите домен, в котором располагается API сервер KSC.

4. Нажмите кнопку **Проверить**. Будет выполнена проверка подключения к API серверу. После успешной проверки соединения с API сервером станет доступно сохранение экземпляра интеграции.
5. Нажмите кнопку **Сохранить**.

16.2.2.2 Шаг 2. Создание задачи по синхронизации активов

1. Откройте экземпляр интеграции на редактирование (кнопка).
2. Перейдите на вкладку "Задачи интеграции" (см. «Рис. 286»).

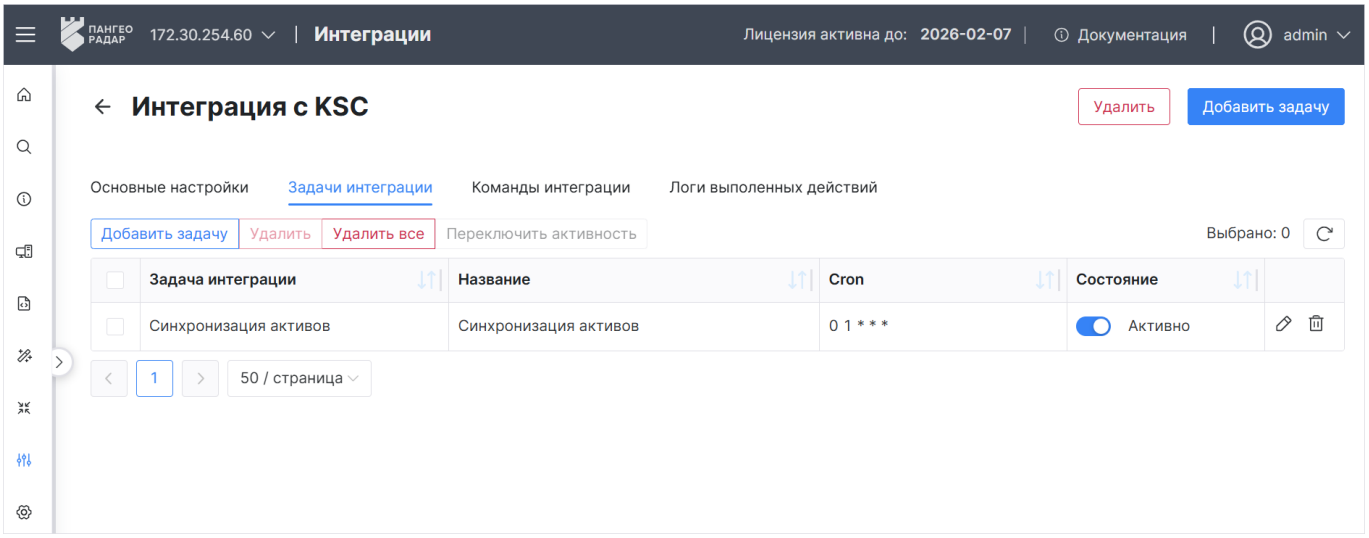


Рис. 286 – Настройка интеграции. Вкладка "Задачи интеграции"

3. Нажмите кнопку **Добавить задачу**. Откроется окно "Добавить задачу" (см. «Рис. 287»).

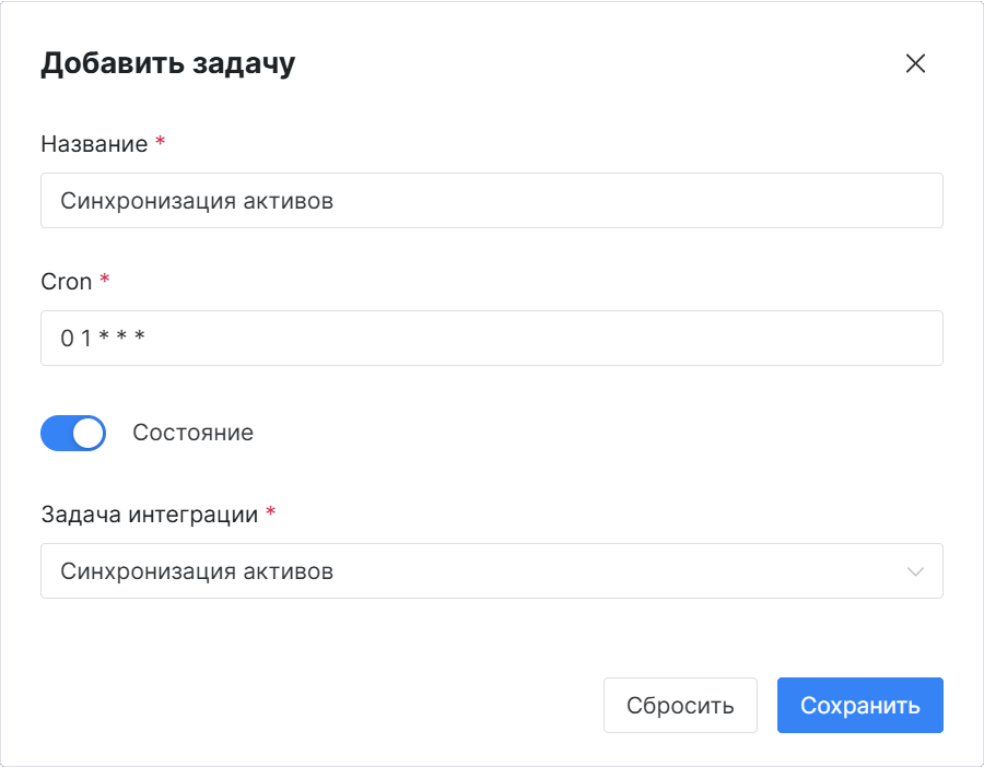


Рис. 287 – Окно "Добавить задачу"

4. Укажите в окне следующую информацию:
   - **Название** – укажите название периодической задачи;
   - **Cron** – укажите CRON-выражение, описывающее периодичность задачи. Подсказу по CRON-выражениям см. на **сайте**;
   - **Состояние** – включите выполнение задачи синхронизации активов, установив переключатель в положение "Включен";
   - **Задача интеграции** – из выпадающего списка выберите задачу "Синхронизация активов".
5. Нажмите кнопку **Сохранить**.
6. Журнал выполнения задачи можно посмотреть в разделе **Администрирование** → **Кластер** → вкладка **Планировщик задач**.

16.2.2.3 Шаг 3. Активация экземпляра интеграции с KSC

Чтобы по экземпляру интеграции выполнялось взаимодействие с системой **KSC**, ее необходимо активировать.

Для активации интеграции перейдите в раздел **Параметры** → **Интеграции** и в колонке **Статус** установите переключатель в положение "Включен".

16.2.3 Работа с интеграцией

В ходе работы интеграции будет выполняться сканирование активов в соответствии с параметрами периодической задачи:

1. Запускается периодическая задача.

2. **Платформа Радар** запрашивает у KSC информацию об агентах (активах).
3. Информация об активах добавляется в платформу.
4. На форме просмотра актива появляется дополнительная информация:
    - наименование экземпляра интеграции, в рамках которой получены сведение об активе;
    - наименование агента в системе KSC, на основании которого создан актив;
    - ссылка для просмотра агента непосредственно в системе KSC.

Для просмотра журнала выполнения действий по конкретной интеграции перейдите в раздел **Параметры → Интеграции**, откройте интеграцию на просмотр (кнопка ) и перейдите на вкладку "Логи выполненных действий".