



Платформа Радар

Руководство оператора

Версия 4.2.4

ООО «Пангео Радар»

Оглавление

1.	Общие сведения о «Платформе Радар»	12
2.	Требования	13
3.	Вход в платформу	14
4.	Интерфейс платформы	15
4.1	Шапка сайта	16
4.2	Панель разделов	16
4.3	Универсальные таблицы	19
4.3.1	Текстовый поиск	20
4.3.2	Настройка сортировки и фильтрации записей таблицы	21
4.3.3	Настройки отображения полей	22
4.3.4	Быстрая сортировка	22
4.4	Боковая панель	23
4.4.1	Поиск сущности в списке	24
4.4.2	Сортировка и фильтрация сущностей в списке	24
4.4.3	Массовые действия	25
4.5	Папки контента	26
4.6	Формы работы с сущностями	28
4.7	Шаблоны сущностей	29
4.7.1	Создание шаблона	29
4.7.2	Использование шаблона	31
4.8	Визуализации	32
4.9	Синхронизация пользовательского контента	32
5.	События	35
5.1	Общие данные	35
5.1.1	График "Поток событий"	36
5.1.2	Топ-10 значений по выделенной области потока событий	37
5.1.2.1	Масштабирование графика потока событий	39
5.1.3	Список событий	39
5.2	Работа с фильтрами	43
5.2.1	Настройка запросов	45
5.2.1.1	Добавление запроса в условия фильтра	45
5.2.1.2	Сохранение конфигурации запроса	48
5.2.2	Настройка агрегации	49
5.2.2.1	Добавление агрегации	50
5.2.2.2	Добавление подагрегации	52
5.2.2.3	Сохранение агрегации	52
5.2.3	Работа с пресетами	53
5.2.3.1	Создание пресета	54
5.2.3.2	Применение пресета	55

5.2.3.3	Удаление пресета	55
5.2.4	История поиска	55
5.3	Работа с событиями.....	56
5.3.1	Поиск инцидента	57
5.3.1.1	Создание инцидента	58
5.3.1.2	Добавление события в инцидент	59
5.3.2	Экспорт списка событий.....	60
5.3.3	Вспомогательные инструменты для анализа событий.....	61
5.3.3.1	Поиск событий	61
5.3.3.2	Просмотр событий по сформированной агрегации	62
5.3.3.3	Настройка плотности отрисовки потока событий	63
5.3.3.4	Сортировка событий.....	64
5.3.3.5	Настройка набора полей для табличного вида.....	65
6.	Инциденты ИБ.....	67
6.1	Инциденты	67
6.1.1	Общие данные.....	67
6.1.2	Создание инцидента	70
6.1.3	Просмотр инцидента	72
6.1.3.1	Общая информация об инциденте.....	73
6.1.3.2	Информация об активе	75
6.1.3.3	Результат анализа.....	76
6.1.3.4	Информация о происшествиях	77
6.1.3.5	История коммуникации.....	79
6.1.4	Назначение инцидента	79
6.1.5	Изменение статуса инцидента	80
6.1.6	Добавление комментария к инциденту.....	80
6.1.7	Редактирование инцидента.....	80
6.1.8	Просмотр истории изменения инцидента	80
6.1.9	Удаление инцидента.....	81
6.2	Типы инцидентов	81
6.2.1	Общие сведения.....	81
6.2.2	Просмотр и анализ типа инцидента	83
6.2.3	Создание типа инцидента	84
6.2.4	Редактирование типа инцидента	85
6.2.5	Написать ответственному	85
6.2.6	Дублирование типа инцидента.....	86
6.2.7	Импорт типов инцидентов	86
6.2.8	Экспорт типов инцидентов	86
6.2.9	Экспорт типов инцидентов в CSV	86
6.2.10	Удаление типа инцидента	86
6.3	Группы инцидентов	87
6.3.1	Просмотр группы инцидентов.....	88

6.3.2	Создание группы инцидентов	89
6.3.3	Редактирование группы инцидентов	90
6.3.4	Назначение группы инцидентов пользователю	90
6.3.5	Назначение группы инцидентов группе пользователей	90
6.3.6	Добавление инцидентов в группу	90
6.3.7	Массовое закрытие инцидентов через группу	90
6.3.8	Открепление инцидентов от группы	90
6.3.9	Удаление группы инцидентов	91
6.4	Происшествия на отправку	91
6.5	Дополнительные поля	91
6.5.1	Просмотр значений дополнительного поля	92
6.5.2	Создание дополнительного поля	93
6.5.3	Редактирование дополнительного поля	94
6.5.4	Добавление дополнительного поля в инцидент	94
6.5.5	Удаление дополнительного поля	94
7.	Активы	95
7.1	Активы	95
7.1.1	Общие данные	95
7.1.2	Просмотр и анализ актива	97
7.1.3	Создание актива	99
7.1.4	Редактирование актива	100
7.1.5	Добавление актива в группу	100
7.1.6	Написать ответственному	100
7.1.7	Экспорт активов	101
7.1.8	Объединение активов	101
7.1.9	Активация/деактивация активов	102
7.1.10	Настройка параметров активов	102
7.1.11	Удаление актива	104
7.2	Группы активов	104
7.2.1	Создание группы активов	105
7.2.2	Просмотр группы активов	107
7.2.3	Редактирование группы активов	108
7.2.4	Настройка автоматического добавления актива в группу	108
7.2.5	Написать ответственному	109
7.2.6	Удаление группы активов	109
7.3	Настройки идентификации активов	110
7.3.1	Создание стратегии идентификации активов	111
7.3.2	Редактирование стратегии идентификации активов	111
7.3.3	Удаление стратегии идентификации активов	111
7.4	Сетевые интерфейсы	111
7.4.1	Просмотр сетевого интерфейса	112
7.4.2	Создание сетевого интерфейса	113
7.4.3	Редактирование сетевого интерфейса	114
7.4.4	Удаление сетевого интерфейса	114
7.5	Результаты сканирования	115

7.5.1	Импорт результатов сканирования	115
7.5.2	Просмотр списка результатов сканирования	116
7.5.3	Просмотр результата сканирования.....	117
7.5.3.1	Основная информация о результате сканирования	117
7.5.3.2	Информация о просканированных хостах	118
7.5.4	Сравнение результатов сканирования	119
7.5.4.1	Создание инцидентов по результатам сравнения	121
7.5.4.2	Закрытие инцидентов по результатам сравнения	121
7.5.5	Изменение статуса результата сканирования	121
7.6	Обнаружение хостов	122
7.7	Обнаружение сервисов	123
7.8	Сбор данных	124
8.	Соответствие ПО	126
8.1	Общие сведения.....	126
8.2	Результаты соответствия ПО.....	126
8.2.1	Запуск процесса проверки соответствия ПО	127
8.2.2	Просмотр информации о результате соответствия ПО	128
8.2.3	Удаление результатов соответствия ПО	128
8.3	Список ПО	129
8.3.1	Просмотр информации о ПО	130
8.3.2	Просмотр информации об активах, на которых установлено ПО.....	131
8.3.3	Редактирование записи о ПО.....	131
8.3.4	Удаление записи о ПО из платформы	131
8.4	Список групп ПО	132
8.4.1	Создание группы ПО.....	133
8.4.2	Просмотр группы ПО	134
8.4.3	Редактирование группы ПО	134
8.4.4	Удаление группы ПО	134
8.5	Правила соответствия ПО	135
8.5.1	Создание правила соответствия ПО	136
8.5.2	Просмотр правила соответствия ПО.....	137
8.5.3	Редактирование правила соответствия ПО	137
8.5.4	Удаление правила соответствия ПО	137
8.6	Наборы правил соответствия ПО.....	138
8.6.1	Создание политики соответствия ПО	139
8.6.2	Просмотр политики соответствия ПО	139
8.6.3	Редактирование политики соответствия ПО	140
8.6.4	Удаление политики соответствия ПО.....	140
9.	Коррелятор	142
9.1	Общие данные	142
9.2	Правила корреляции	142
9.2.1	Просмотр статистики работы правил	144
9.2.1.1	Вкладка "Инциденты"	144

9.2.1.2	Вкладка "Результаты"	146
9.2.1.3	Вкладка "Лог изменений"	146
9.2.1.4	Вкладка "Лог правила"	147
9.2.1.5	Вкладка "Метрики"	147
9.2.2	Создание и настройка правила	149
9.2.2.1	Создание правила с помощью визуального конструктора	149
9.2.2.2	Создание правила с помощью скриптового языка Lua	163
9.2.3	Редактирование правила	169
9.2.4	Активация правила	169
9.2.5	Перезапуск правила	170
9.2.6	Дублирование правила	170
9.2.7	Конвертирование правила в код Lua	170
9.2.8	Импорт правил	170
9.2.9	Экспорт правил	171
9.2.10	Удаление правила	171
9.2.11	Массовые действия над правилами из боковой панели	171
9.2.12	Массовое изменение настроек правил корреляции	172
9.2.13	Действия над результатами сработок правила	173
9.2.13.1	Создание инцидента	173
9.2.13.2	Просмотр события	173
9.3	Пересылка событий	174
9.3.1	Общие данные	174
9.3.2	Включение пересылки событий	175
9.3.3	Просмотр фильтра для пересылки событий	177
9.3.4	Создание фильтра для пересылки событий	178
9.3.5	Редактирование фильтра для пересылки событий	179
9.3.6	Дублирование фильтра для пересылки событий	180
9.3.7	Импорт фильтров	180
9.3.8	Экспорт фильтров	180
9.3.9	Удаление фильтра	180
9.4	Фильтры потока событий	181
9.4.1	Общие данные	181
9.4.2	Просмотр фильтра потока событий	181
9.4.3	Создание фильтра потока событий	182
9.4.4	Редактирование фильтра потока событий	184
9.4.5	Дублирование фильтра потока событий	184
9.4.6	Импорт фильтров потока событий	184
9.4.7	Экспорт фильтров потока событий	185
9.4.8	Удаление фильтра потока событий	185
9.5	Макросы	185
9.5.1	Общие данные	185
9.5.2	Просмотр макроса	186
9.5.3	Создание макроса	186

9.5.4	Редактирование макроса	187
9.5.5	Дублирование макроса	187
9.5.6	Импорт макросов	187
9.5.7	Экспорт макросов	187
9.5.8	Удаление макроса	187
9.6	Шаблоны алертов	188
9.6.1	Общие данные	188
9.6.2	Просмотр шаблона "алерта"	188
9.6.3	Создание шаблона "алерта"	189
9.6.4	Редактирование шаблона "алерта"	190
9.6.5	Дублирование шаблона "алерта"	190
9.6.6	Удаление шаблона "алерта"	191
9.7	Шаблоны группировки	191
9.7.1	Общие данные	191
9.7.2	Просмотр шаблона группировки	192
9.7.3	Создание шаблона группировки	192
9.7.4	Редактирование шаблона группировки	194
9.7.5	Дублирование шаблона группировки	194
9.7.6	Удаление шаблона группировки	195
9.8	Табличные списки	195
9.8.1	Общие данные	195
9.8.2	Просмотр табличного списка	196
9.8.3	Создание табличного списка	197
9.8.4	Работа с записями табличного списка	198
9.8.4.1	Добавление записи	198
9.8.4.2	Редактирование записи	198
9.8.4.3	Дублирование записи	198
9.8.4.4	Экспорт записей	199
9.8.4.5	Импорт записей	199
9.8.4.6	Удаление записи	199
9.8.4.7	Массовое удаление записей	200
9.8.5	Редактирование табличного списка	200
9.8.6	Дублирование табличного списка	200
9.8.7	Импорт табличных списков	201
9.8.8	Экспорт табличных списков	201
9.8.9	Синхронизация табличных списков	201
9.8.10	Удаление табличного списка	202
9.9	Ретроспективная корреляция	202
9.9.1	Общие данные	202
9.9.2	Добавление задачи для ретроспективной корреляции	203
9.9.3	Остановка задачи	204
9.9.4	Перезапуск задачи	204
9.9.5	Удаление задачи	204

9.9.6	Массовые действия над задачами	204
10.	Параметры	205
10.1	Основные параметры	205
10.2	Оповещения по задержкам	209
10.3	Черный список ID плагинов	212
10.4	Фоновые задачи	213
10.5	Интеграции	214
10.6	Типы интеграций	214
10.7	Папки контента	215
10.8	Шаблоны	216
11.	Рабочие столы	218
11.1	Общие данные	218
11.2	Создание рабочего стола	220
11.3	Редактирование рабочего стола	221
11.4	Управление виджетами	222
11.4.1	Установка периода и обновление данных виджетов	223
11.4.2	Добавление виджета на рабочий стол	223
11.4.3	Переход к табличному представлению данных	223
11.4.4	Редактирование виджета	223
11.4.5	Копирование настроек виджета	224
11.4.6	Изменение расположения виджета	224
11.4.7	Изменение размера виджета	224
11.4.8	Удаление виджета	224
11.5	Копирование рабочего стола	225
11.6	Создание отчета	225
11.7	Удаление рабочего стола	226
11.8	Grafana. Единицы измерения и временной диапазон	226
12.	Конструктор виджетов	228
12.1	Особенности работы в конструкторе	232
12.2	Конструктор запросов	232
12.2.1	Добавление запроса	233
12.2.1.1	Шаг 1. Выбор источника данных и датасета	233
12.2.1.2	Шаг 2. Выбор периода формирования запроса	234
12.2.1.3	Шаг 3. Настройка набора полей	234
12.2.1.4	Шаг 4. Условия фильтрации	236
12.2.1.5	Шаг 5. Группировка и Сортировка	236
12.2.2	Копирование запроса	237
12.2.3	Дублирование запроса	238
12.2.4	Удаление запроса	238
12.3	Настройка внешнего вида виджета	238
12.3.1	Основные настройки виджета	238
12.3.2	Временной ряд	239
12.3.2.1	Шаг 1. Настройка осей	240

12.3.2.2	Шаг 2. Настройка визуализации	240
12.3.2.3	Шаг 3. Легенда	242
12.3.3	Круговая диаграмма	242
12.3.4	Таблица.....	245
12.3.5	Текст	246
12.3.6	Гистограмма.....	247
12.3.6.1	Шаг 1. Настройка осей	248
12.3.6.2	Шаг 2. Настройка визуализации	251
12.3.7	Метрика	252
12.3.8	Изображение	254
12.4	Копирование виджета.....	255
12.5	Предустановки	256
13.	Отчеты	257
13.1	Общие данные	257
13.2	Создание отчета	258
13.3	Конструктор отчета	259
13.3.1	Добавление страницы	262
13.3.2	Выбор периода формирования данных виджетов	263
13.3.3	Настройка наименования отчета в момент генерации	263
13.3.4	Настройка страниц	264
13.3.4.1	Настройка верхнего колонтитула	264
13.3.4.2	Настройка нижнего колонтитула	265
13.3.4.3	Настройка стиля шрифта.....	266
13.3.5	Настройка виджетов.....	266
13.3.5.1	Добавление виджета	267
13.3.5.2	Редактирование виджета	267
13.3.5.3	Копирование настроек виджета.....	268
13.3.5.4	Изменение расположения виджета	268
13.3.5.5	Изменение размера виджета	268
13.3.5.6	Удаление виджета.....	268
13.3.6	Изменение порядка страниц	268
13.3.7	Удаление страницы	269
13.4	Настройка расписания генерации отчета.....	269
13.4.1	Просмотр истории генерации отчета	269
13.5	Настройка прав доступа к отчету	270
13.6	Импорт отчетов	271
13.7	Экспорт отчетов	271
13.8	Удаление отчета	271
13.9	Архив отчетов	272
14.	Сообщения.....	273
14.1	Создание сообщения.....	274
14.2	Просмотр сообщения.....	274

14.3	Ответ на сообщение	275
14.4	Отметить сообщения прочитанными	275
14.5	Отметить прочитанные сообщения как непрочитанные	275
14.6	Экспорт сообщений	275
14.7	Удаление сообщений	276
15.	Профиль пользователя	277
15.1	Изменение информации о своей учетной записи	278
15.2	Изменение пароля	278
15.3	Подключение аутентификатора	279
15.4	Выход из всех сессий	279
15.5	Просмотр журнала изменений учетной записи	280
15.6	Настройка оповещений	280
15.7	Просмотр истории действий в платформе	281
16.	Интеграции	283
16.1	RT Protect EDR	283
16.1.1	Общие сведения	283
16.1.1.1	Характеристики системы	283
16.1.1.2	Активные действия	283
16.1.1.3	Синхронизация инцидентов и активов	284
16.1.1.4	Параметры типа интеграции RT Protect EDR	284
16.1.2	EDR действия	287
16.1.2.1	Создание EDR действия	288
16.1.2.2	Просмотр EDR действия	289
16.1.2.3	Редактирование EDR действия	291
16.1.2.4	Дублирование EDR действия	291
16.1.2.5	Изменение статуса EDR действия	291
16.1.2.6	Экспорт EDR действий	291
16.1.2.7	Импорт EDR действий	292
16.1.2.8	Удаление EDR действий	292
16.1.3	Настройка интеграции RT Protect EDR	292
16.1.3.1	Шаг 1. Создание экземпляра интеграции с RT Protect EDR	292
16.1.3.2	Шаг 2. Настройка задачи синхронизации активов	294
16.1.3.3	Шаг 3. Настройка активных действий для интеграции	295
16.1.3.4	Шаг 4. Активация интеграции	295
16.1.4	Работа с интеграцией RT Protect EDR	295
16.1.4.1	Работа с правилами корреляции	296
16.1.4.2	Работа с активами	298
16.1.4.3	Работа с инцидентами	300
16.1.4.4	Просмотр журнала выполнения действий по интеграции	301
16.2	Kaspersky Security Center	301

16.2.1	Характеристики системы	301
16.2.2	Настройка интеграции	302
16.2.2.1	Шаг 1. Создание экземпляра интеграции с KSC.....	302
16.2.2.2	Шаг 2. Создание задачи по синхронизации активов	303
16.2.2.3	Шаг 3. Активация экземпляра интеграции с KSC	304
16.2.3	Работа с интеграцией	304
16.3	Active Directory	305
16.3.1	Характеристики системы	305
16.3.2	Настройка интеграции	305
16.3.2.1	Шаг 1. Создание экземпляра интеграции с AD.....	305
16.3.2.2	Шаг 2. Создание задачи по синхронизации активов	307
16.3.2.3	Шаг 3. Активация экземпляра интеграции с AD	308
16.3.3	Работа с интеграцией	309

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](#)»).

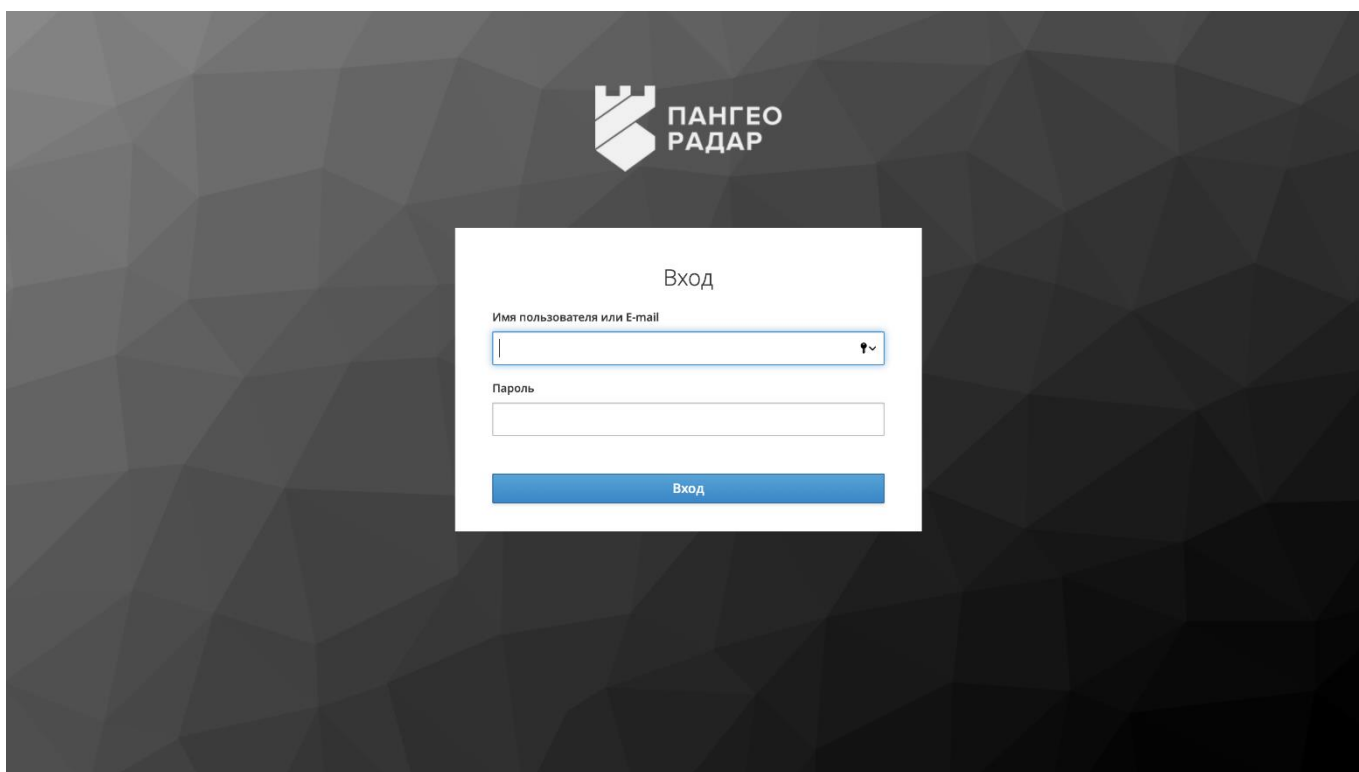


Рис. 1 – Окно входа в платформу

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 сущностями (просмотр, создание, редактирование).

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

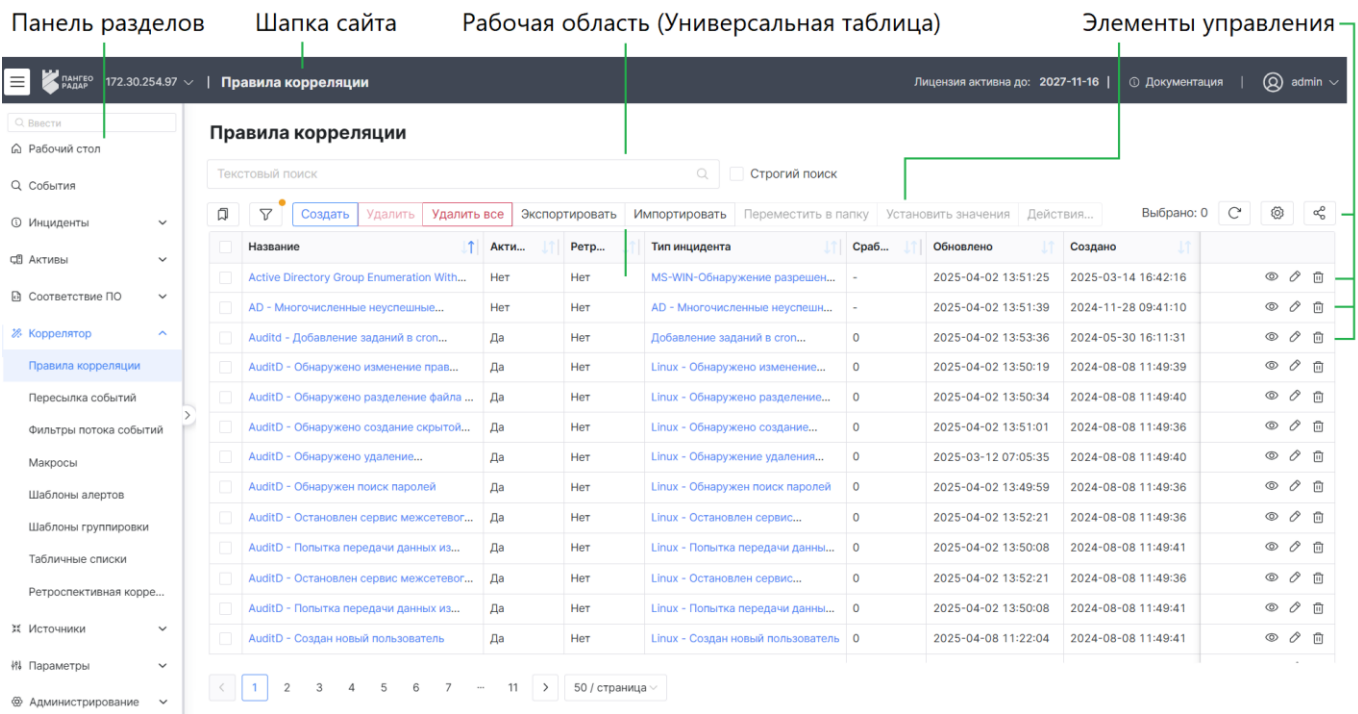


Рис. 2 – Интерфейс Платформы Радар. Табличное представление

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 выбранной сущности (см. «Рис. 3»).

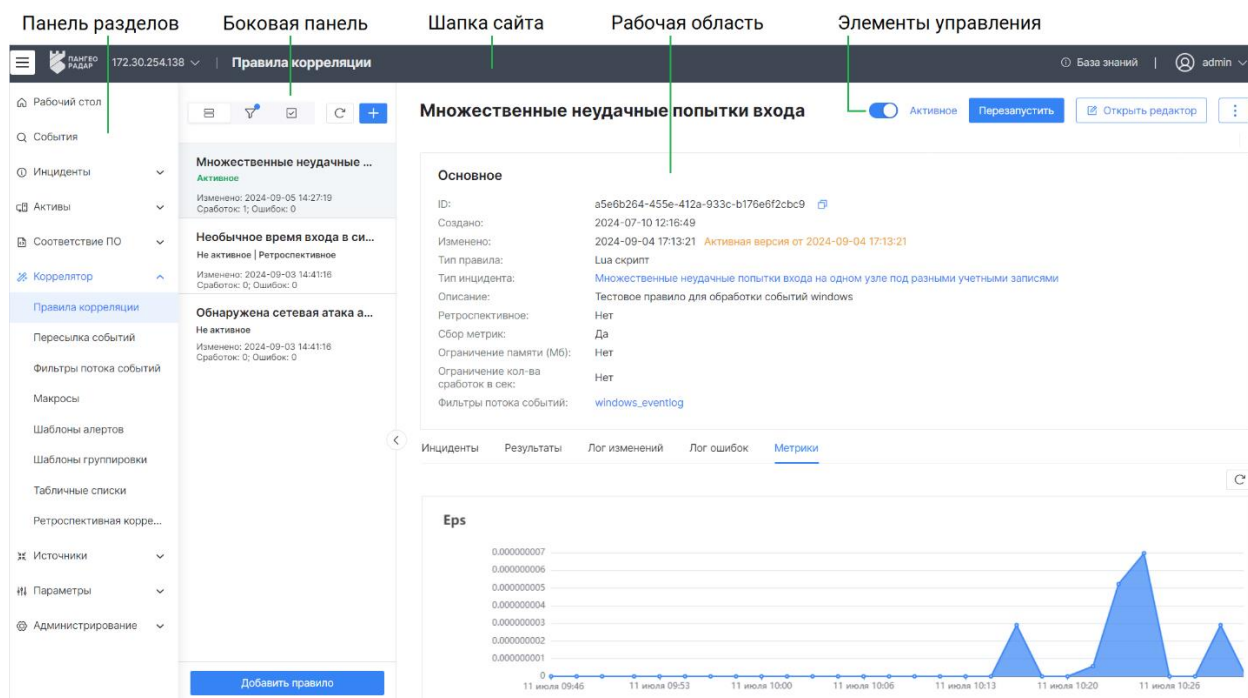







Рис. 3 – Интерфейс Платформы Радар. Представление через боковую панель и формы сущностей

4.1 Шапка сайта

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

Кнопка	Действие
 / 	показать/скрыть панель разделов
 master ▾	выбор инстанса
 База знаний	доступ к базе знаний платформы
 admin ▾	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.

По разделам интерфейса доступен текстовый поиск. Для поиска нужного раздела укажите значение или часть значения в поле **Ввести**. По мере ввода текста в поле поиска, в панели разделов будут формироваться подходящие данные.

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 параметров **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 сущностей, представленных в табличном виде и имеющие единые элементы управления (см. «Рис. 4»).

Срочно...	ID	Название	Статус	Создано	Результат анализа	Актив
0.95	323	Установка SUID флага на заданный файл	Новый	2025-08-13 12:30:45	Обнаружена установка SUL...	blb-minkar-tst
0.95	1261	Установка SUID флага на заданный файл	Новый	2025-08-14 13:02:54	Обнаружена установка SUL...	dap-mirach-mgmt
0.98	1070	Linux: Обнаружение изменений правил iptables...	Новый	2025-08-14 05:08:45	Обнаружена подозрительн...	vs-alkaid-dev
0.95	1074	Установка SUID флага на заданный файл	Новый	2025-08-14 05:14:53	Обнаружена установка SUL...	vs-phact-dev
0.95	1551	Установка SUID флага на заданный файл	Новый	2025-08-15 13:31:58	Обнаружена установка SUL...	fas-skat-mgmt





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/сущности в таблице

Кнопка	Действие
Удалить	удаление выбранной записи/сущности из таблицы
Удалить все	удаление всех показанных записей/сущностей. Будут удалены все записи/объекты, попавшие под параметры сортировки и фильтрации
Экспортировать	экспорт выбранной записи/сущности
Экспортировать все	экспорт всех показанных записей/сущностей. Будут выгружены в архив все записи/объекты, попавшие под параметры сортировки и фильтрации
Экспортировать выбранные в csv	массовый экспорт выбранных записей/сущностей в формат CSV
Экспортировать в csv	экспорт всех показанных записей/сущностей в формат CSV. Будут выгружены в файлы формата CSV все записи/объекты, попавшие под параметры сортировки и фильтрации
Синхронизировать	Синхронизация изменений между инстансами. Кнопка доступна в режиме мультиарендности и предоставляет доступ к следующим действиям: - Синхронизировать выбранные - синхронизация выбранных изменений на подчиненных инстансах; - Синхронизировать все - синхронизация всех изменений на подчиненных инстансах.
Импортировать	импорт записей/сущностей в таблицу
Переместить в папку	переместить выбранные объекты в папку
	настройка столбцов таблицы
	поделиться параметрами фильтрации и сортировки. При нажатии на кнопку текущие параметры будут скопированы в буфер обмена

В колонках таблицы могут располагаться следующие кнопки:

Кнопка	Действие
	выбор направления сортировки выбранной колонки
	просмотр подробных сведений о сущности
	изменение информации о сущности
	удаление сущности


4.3.1 Текстовый поиск

Для поиска сущностей укажите значение или часть значения в поле **Текстовый поиск**. По мере ввода текста в поле поиска, в таблице будут формироваться подходящие данные.

Для поиска сущностей по точному соответствию введенному запросу, установите флаг **Строгий поиск**.

4.3.2 Настройка сортировки и фильтрации записей таблицы

Для поиска необходимого сущности 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»).

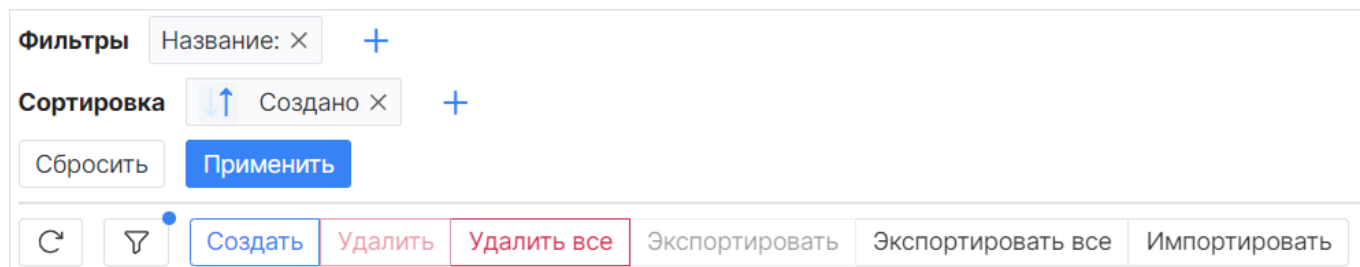


Рис. 5 – Универсальная таблица. Блоки для настройки фильтров и сортировки

2. В блоке **Фильтры** нажмите кнопку «+» для добавления столбца, по которому будет выполняться фильтрация.

Можно выполнить фильтрацию по значения нескольких столбцов.

Для каждого столбца предусмотрена настройка дополнительных параметров фильтрации. Для вызова настройки необходимо добавить столбец в блок фильтры и нажать по нему ЛКМ. Откроется окно дополнительных настроек (см. «Рис. 6»).

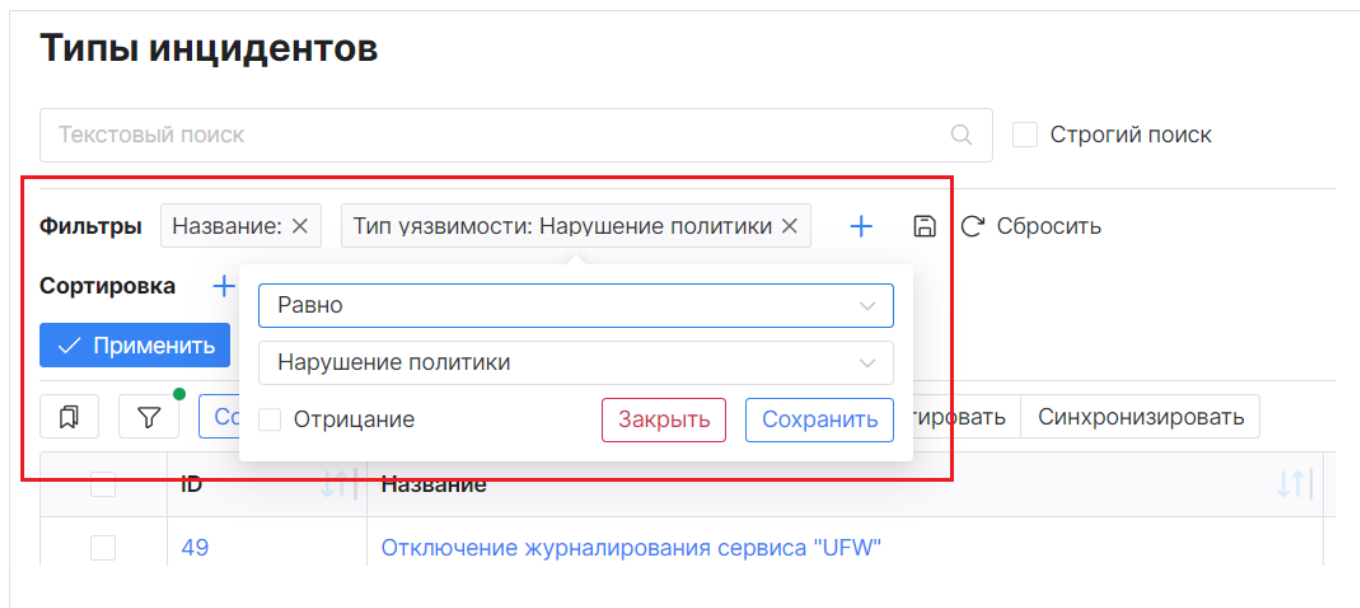



Рис. 6 – Универсальная таблица. Окно для дополнительных настроек параметров фильтрации

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**.

При необходимости можно сохранить параметры фильтрации и сортировки в "Шаблон". Подробнее см. раздел «[Шаблоны сущностей](#)».

4.3.3 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. 7»).

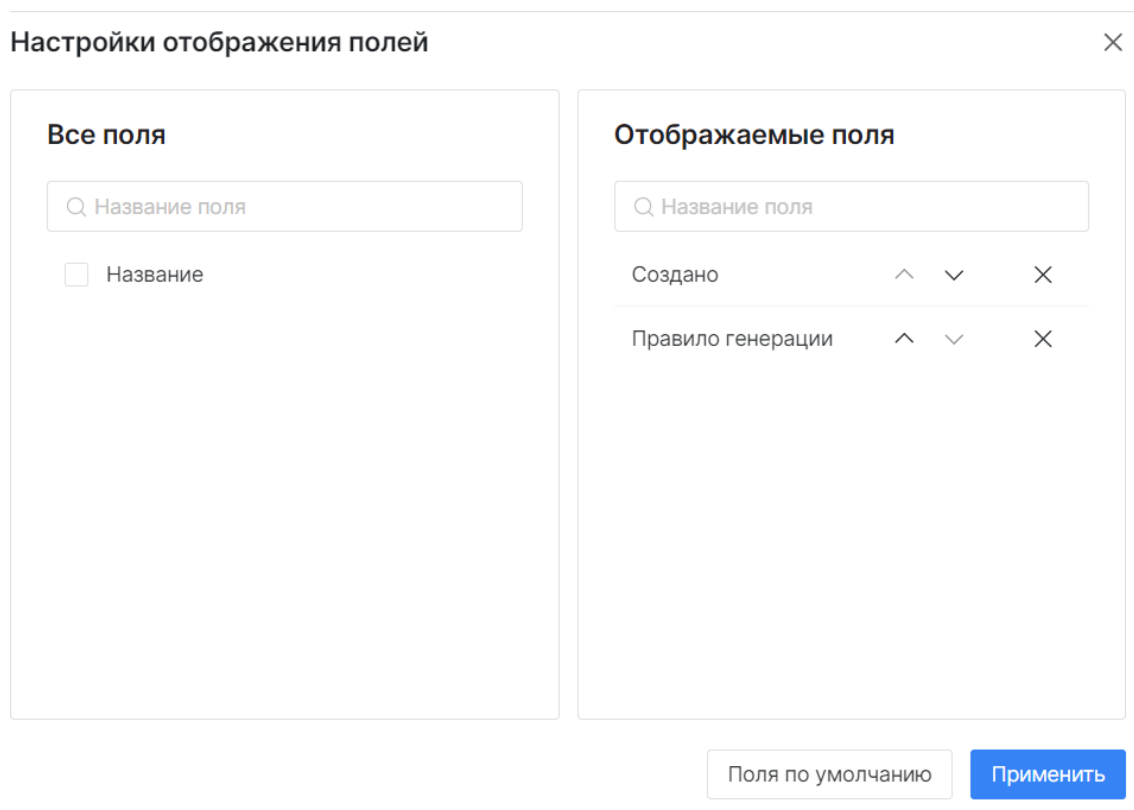


Рис. 7 – Настройки отображения полей

4.3.4 Быстрая сортировка

Универсальные таблицы позволяют выполнять быструю сортировку с помощью нажатия ЛКМ на заголовок столбца таблицы. Быстрая сортировка работает следующим образом:

- При нажатии на заголовок столбца таблицы добавляется сортировка по этому полю:
 - при первом клике добавляется сортировка от последней записи к первой;
 - при втором клике – от первой записи к последней.
- При нажатии на другой заголовок столбца, сортировка будет переключена на указанное поле. Предыдущие сортировки сбрасываются;
- При нажатии на другой заголовок с зажатой клавишей **CTRL/CMD** будет добавлено новое поле в текущую сортировку. Повторное нажатие на заголовок с зажатой клавишей **CTRL/CMD** уберёт выбранное поле из сортировки;
- При добавлении сортировки по любому столбцу, в соответствующем заголовке будет отображено направление сортировки (стрелочкой) и приоритет сортировки (цифрой) рядом с заголовком;

- При нажатии на цифру, обозначающую приоритет сортировки, с зажатым **CTRL/CMD**, приоритет сортировки будет соответственно повышен или понижен;
- Нажатие ПКМ на заголовок столбца таблицы, который не участвует в сортировке, предоставляет доступ к следующим функциям:
 - Добавить выбранное поле в сортировку по убыванию;
 - Добавить выбранное поле в сортировку по возрастанию;
 - Скрыть столбец.
- Нажатие ПКМ на заголовок столбца таблицы, который участвует в сортировке, предоставляет доступ к следующим функциям:
 - Включить сортировку по убыванию;
 - Включить сортировку по возрастанию;
 - Повысить приоритет сортировки по выбранному полю;
 - Понизить приоритет сортировки по выбранному полю;
 - Убрать поле из сортировки;
 - Скрыть столбец.

4.4 Боковая панель

В общем случае боковая панель предназначена для поиска, сортировки, фильтрации и выбора сущности, для вывода информации о нем в рабочей области (см. «Рис. 8»).

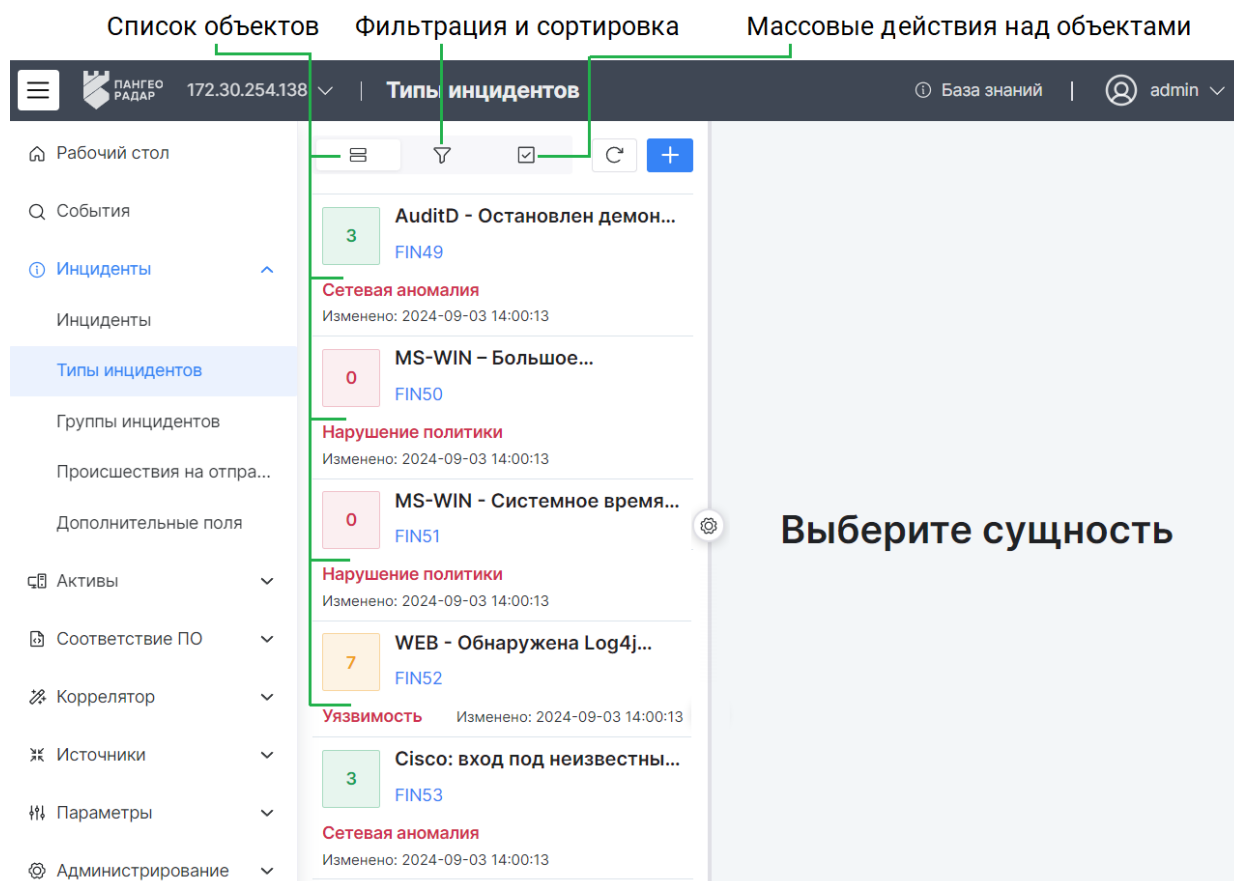







Рис. 8 – Боковая панель. Список сущностей

На боковой панели доступны следующие элементы управления:


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

4.4.1 Поиск сущности в списке

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

Для поиска сущностей по точному соответствию введенному запросу, установите флаг **Строгий поиск**.

4.4.2 Сортировка и фильтрация сущностей в списке

1. Нажмите кнопку . Откроется блок для настройки сортировки и фильтрации сущностей в списке (см. «Рис. 9»).

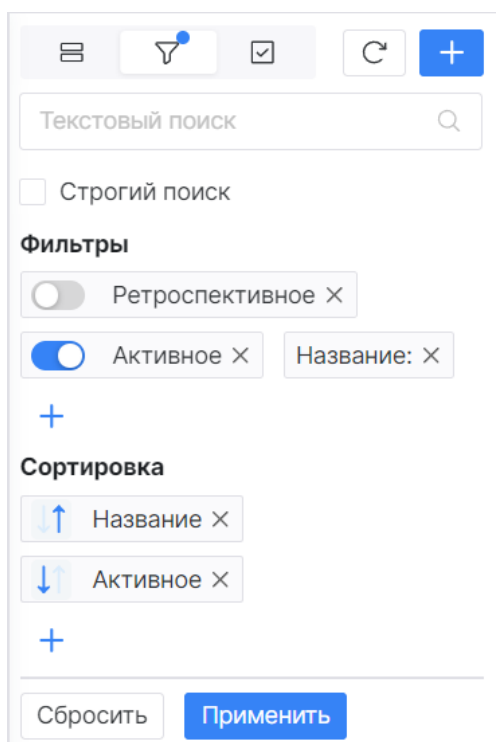


Рис. 9 – Боковая панель. Сортировка и фильтрация

2. Если для сущности доступна фильтрация по конкретным полям (для некоторых сущностей фильтрация недоступна), то в блоке **Фильтрация** укажите необходимые значения полей.

Можно выполнить фильтрацию по значениям нескольких полей.

Для каждого поля предусмотрена настройка дополнительных параметров фильтрации. Для вызова настройки необходимо добавить поле в блок фильтры и нажать по нему ЛКМ. Откроется окно дополнительных настроек (см. «Рис. 10»).

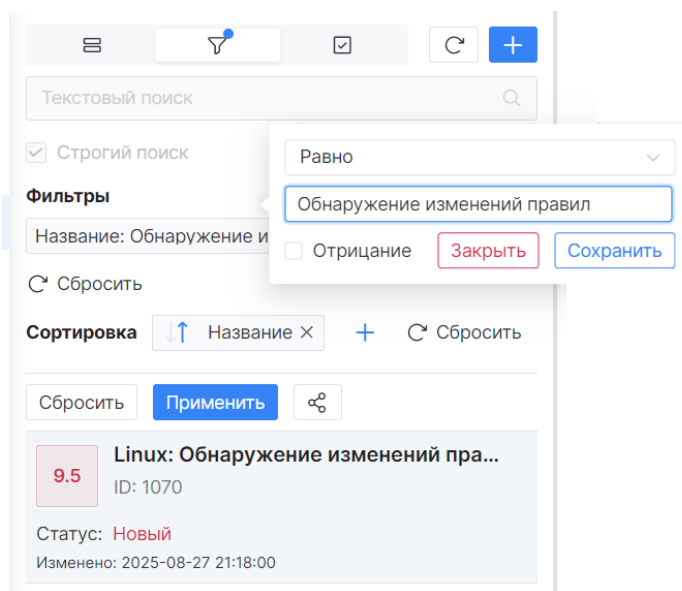


Рис. 10 – Боковая панель. Окно для дополнительных настроек параметров фильтрации

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 сущностями в разделах платформы, может отличаться.

В общем случае над сущностями доступны следующие массовые действия:

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


- **Удалить все** - удаление всех отфильтрованных сущностей. Будут удалены все объекты, попавшие под параметры сортировки и фильтрации.

В режиме мультиарендности появляются дополнительные массовые действия:

- **Синхронизировать выбранные** - синхронизация выбранных изменений на подчиненных инстансах;
- **Синхронизировать все** - синхронизация всех изменений на подчиненных инстансах.

Подробнее о процессе синхронизации см. раздел «Синхронизация пользовательского контента».

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. 11»).

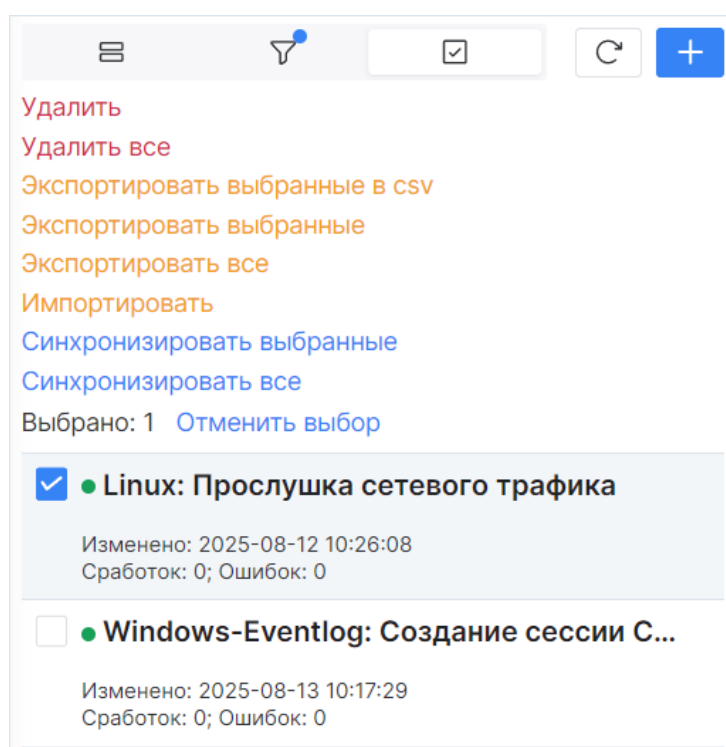


Рис. 11 – Массовые действия над табличными списками

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. 12»).

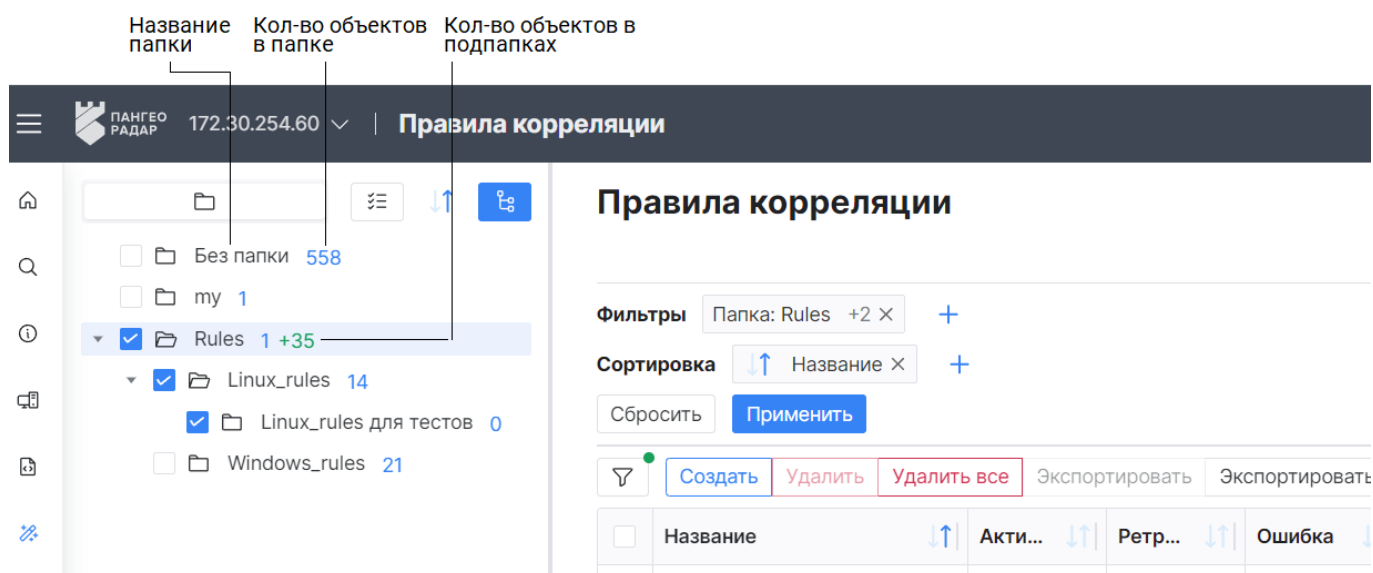


Рис. 12 – Боковая панель. Папки контента

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 сущностями

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

- Создание;
- Просмотр;
- Редактирование.

Форма работы с сущностями имеет различный вид в зависимости от сущности и выполняемого действия (см. «Рис. 13»).

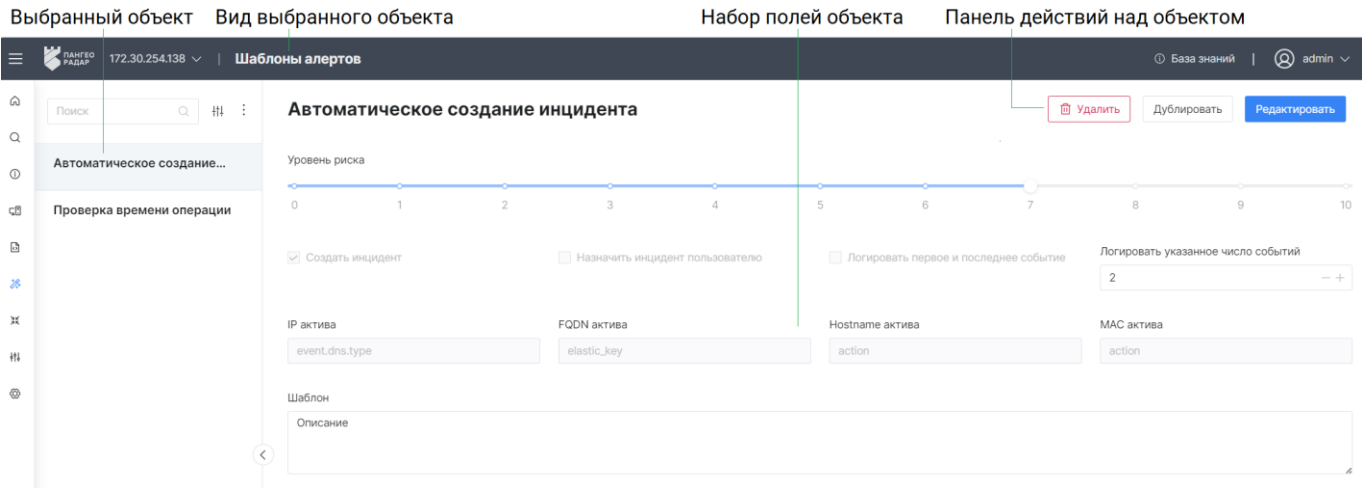







Рис. 13 – Рабочая область. Форма сущности

В общем случае страница состоит из следующих элементов:

- **Поля формы** – содержит поля для указания сведений и выполнения настроек сущности;
- **Панель действий** – содержит кнопки для работы с сущностями. 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 сущности	Действие
Редактировать / 	Просмотр	Изменение информации о сущности
Дублировать	Просмотр	Создание новой сущности на основе существующего

Кнопка	Тип формы сущности	Действие
Назначить пользователю / 	Просмотр	Выдача прав на работу с сущностью выбранному пользователю
Назначить группе пользователей / 	Просмотр	Выдача прав на работу с сущностью выбранной группе пользователей
Написать ответственному	Просмотр	Написать сообщение ответственному пользователю. История сообщений доступна в профиле пользователя
Добавить в группу	Просмотр	Добавление сущности в выбранную группу
Опубликовать	Просмотр	Публикация изменений на всех подчиненных инстансах
Сохранить	Создание / Редактирование	Сохранение сведений о сущности
Сбросить	Создание / Редактирование	Сброс введенных сведений о сущности
Создать	Создание	Создание сущности
	Все	Возврат на предыдущую страницу

4.7 Шаблоны сущностей

Для упрощения поиска, создания/редактирования сущностей в платформе используется механизм **шаблонов**.

В платформе шаблоны делятся на два типа:

- **Редактирование** – шаблон будет определять структуру данных, внешний вид и поведение форм создания/редактирования сущностей;
- **Фильтр** – шаблон будет определять параметры фильтрации и сортировки выбранных сущностей в универсальной таблице.

4.7.1 Создание шаблона

Тип "Редактирование":

1. Откройте необходимую сущность 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](#)».

Тип "Фильтр":

1. Перейдите в раздел для работы с нужной сущностью, например **Инциденты**.
2. Выполните настройку сортировки и фильтрации записей таблицы (см. «[Рис. 14](#)»).

Инциденты

Текстовый поиск ☐ Строгий поиск

Servers **Все закрытые** Все открытые По происшествиям

Фильтры Название: Windows X Уровень риска: 5 X + 🗑️ ↺ Сбросить

Сортировка ↕ Срочность X + 🗑️ ↺ Сбросить

Рис. 14 – Пример настроенных параметров фильтрации и сортировки

Примечание: Обратите внимание, что в примере фильтрации и сортировки включены два шаблона фильтрации: **Server** и **Все закрытые**.

- Нажмите кнопку . Откроется окно **Сохранение шаблона** (см. «Рис. 15»).

Сохранение шаблона ✕

Название

Настройки

- ☒ Учитывать выбранные шаблоны
- ☒ Сохранять фильтры ☒ Сохранять сортировку

Итоговый шаблон

Фильтры

Название: Windows Уровень риска: 5 Группа активов: Servers

Статус: Закрыт +2

Сортировка

↕ Срочность

Рис. 15 – Окно "Сохранение шаблона"


- Выполните в окне следующие действия:
 - в поле **Название** укажите название шаблона;
 - в блоке **Настройки** выберите параметры сохранения шаблона:
 - Учитывать выбранные шаблоны** – опция включает/выключает сохранение параметров шаблонов, которые были применены при настройке фильтрации и сортировки. В примере это шаблоны **Server** и **Все закрытые**;
 - Сохранить фильтры** – опция включает/выключает сохранение параметров фильтрации, которые были применены при настройке фильтрации и сортировки;
 - Сохранить сортировку** – опция включает/выключает сохранение параметров сортировки, которые были применены при настройке фильтрации и сортировки.
 - в блоке **Итоговый шаблон** проверьте правильность заданных параметров фильтрации и сортировки в шаблоне перед сохранением.
- Нажмите кнопку **Сохранить**.
- Шаблон будет сохранен в платформе. Информацию о шаблоне можно посмотреть в разделе **Параметры** → «[Шаблоны](#)».

4.7.2 Использование шаблона

Тип "Редактирование":

1. Откройте форму необходимой сущности 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.

Тип "Фильтр":

1. Перейдите в раздел для работы с нужной сущностью, например **Инциденты**.
2. Нажмите кнопку . Откроется окно "Настройка отображения шаблонов" (см. «Рис. 16»).

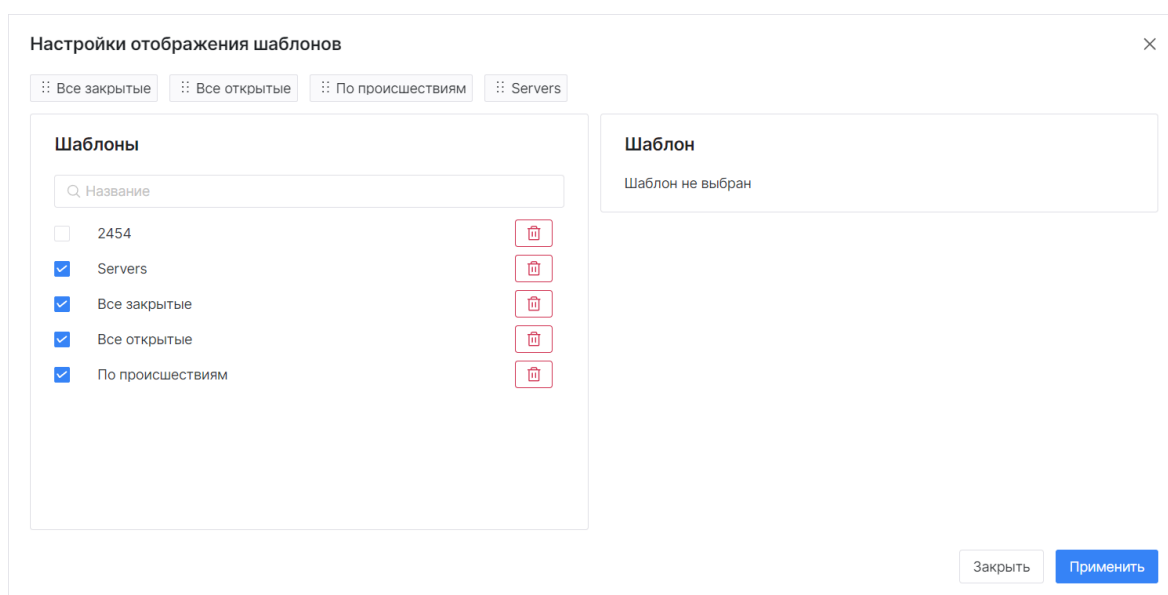


Рис. 16 – Применение шаблона фильтрации и сортировки

3. Выберите шаблоны, которые должны отображаться над универсальной таблицей, установив соответствующие флаги.
4. Нажмите кнопку **Применить**. Над универсальной таблицей будут доступны выбранные шаблоны для фильтрации и сортировки.
5. Для включения/выключения шаблона необходимо нажать по нему ЛКМ.
6. Выбранный шаблон будет автоматически применен (см. «Рис. 17»).

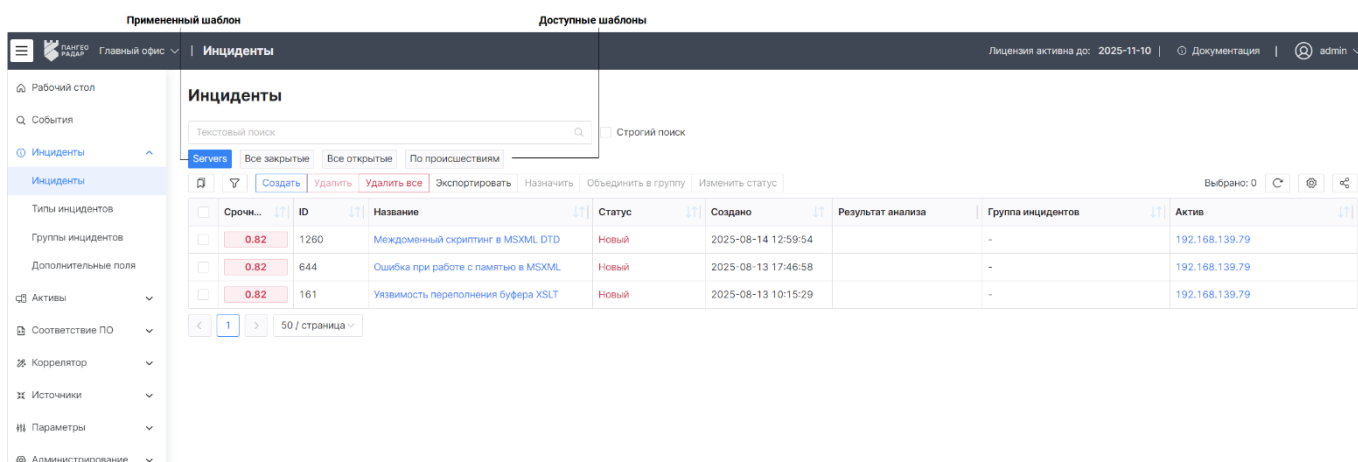


Рис. 17 – Применение шаблона фильтрации и сортировки

4.8 Визуализации

Визуализации – это графики, виджеты, метрики и т.д. (см. «Рис. 18»).

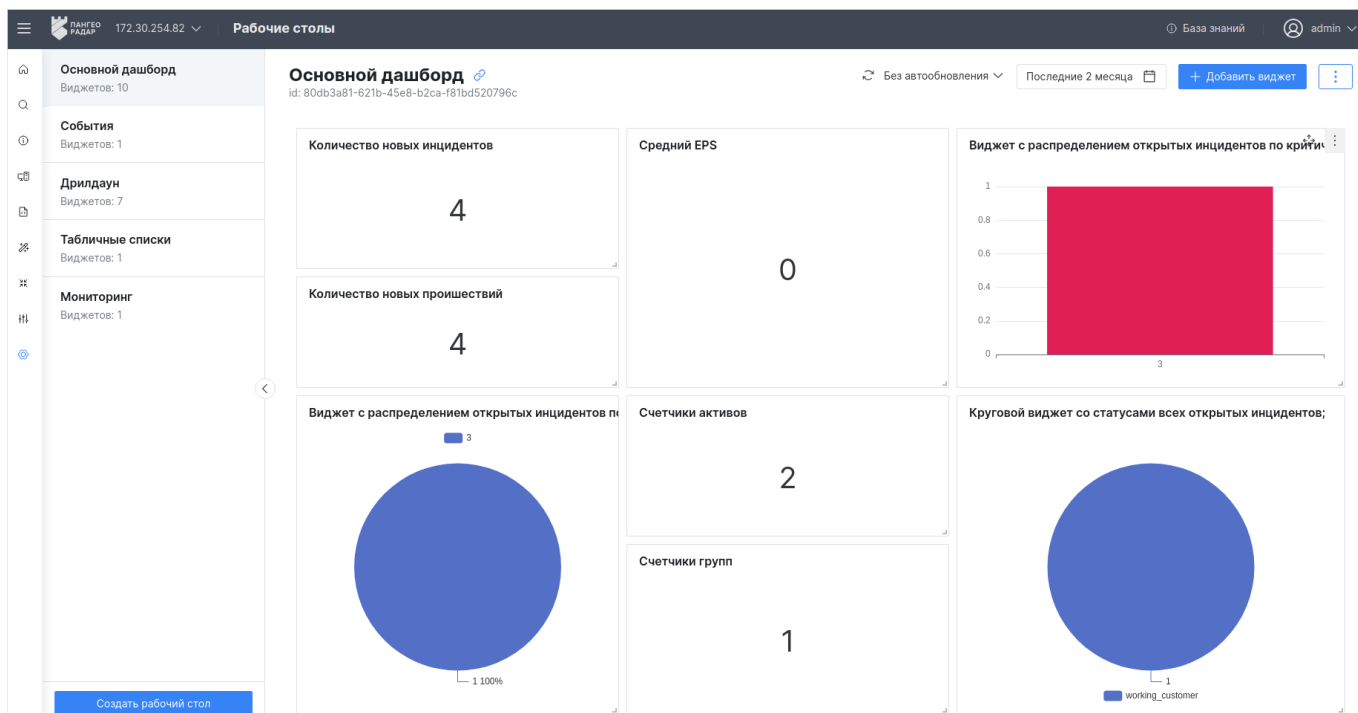


Рис. 18 – Рабочая область. Визуализации

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

4.9 Синхронизация пользовательского контента

Пользовательским контентом являются следующие сущности, создаваемые пользователями в платформе:

- Правила корреляции;
- Фильтры потока событий;
- Табличные списки;

- Макросы;
- Типы инцидентов;
- Источники;
- Правила разбора;
- Правила обогащения;
- Профили сбора.

Если **Платформа Радар** работает в режиме мультиарендности, то пользовательский контент при необходимости можно синхронизировать между подчиненными инстансами.

Синхронизацию можно выполнить в двух режимах:

- добавление – в этом режиме пользовательский контент будет добавлен на подчиненный инстанс, а весь контент, который был на инстансе, останется без изменений;
- перезапись – в этом режиме пользовательский контент будет перезаписан на подчиненном инстансе.

Внимание! *Перезапись контента может вызвать потерю данных на подчиненных инстансах.*

Для выполнения синхронизации выполните следующие действия:

1. Начините процесс синхронизации контента через [универсальную таблицу](#) или [боковую панель](#). Откроется окно "Синхронизация контента" (см. «[Рис. 19](#)»).

Синхронизация контента

Выберите инстансы

Выбрать все

☒ Филиал 2

☐ Филиал 3

☐ Перезаписать

Перезапись контента может вызвать потерю данных на подчиненных инстансах

Закрыть Синхронизировать

Рис. 19 – Окно "Синхронизация контента"

2. В открывшемся окне выберите инстансы, на которые необходимо внести изменения.
3. При необходимости включите режим перезаписи данных на подчиненном инстансе, установив переключатель **Перезаписать** в положение "Включен".
4. Нажмите кнопку **Синхронизировать**.

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;
- просмотр событий на выбранном инстансе, если платформа работает в режиме мультиарендности.

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. 20](#)»).

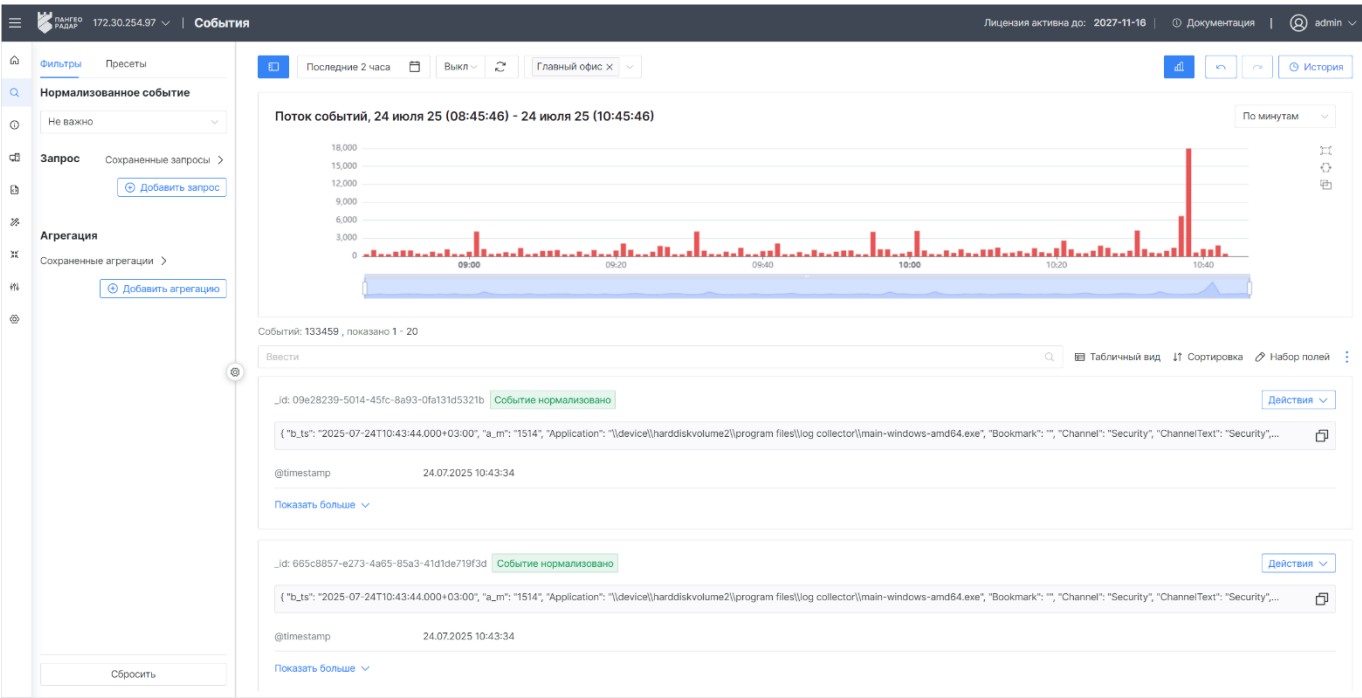


Рис. 20 – Страница "События"

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. 21».

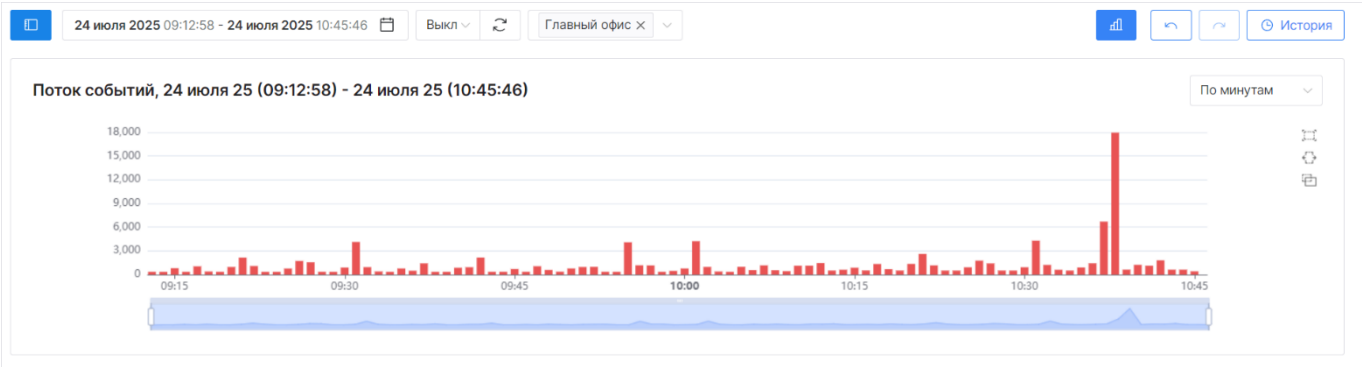











Рис. 21 – Страница "События". График "Поток событий"

В блоке доступны следующие элементы управления:




Кнопка	Действие
	показать / скрыть боковую панель

Кнопка	Действие
	выбор периода
Автообновление данных	из выпадающего списка выбирается режим автоматического обновления списка событий. Доступные значения: - выключен; - по секундам: каждые 5, 10, 30 секунд; - по минутам: каждые 1, 5, 10, 30 минут.
Выбор инстанса	из выпадающего списка выбирается инстанс, поток событий с которого необходимо отобразить на графике. Возможность доступна только если платформа работает в режиме мультиарендности
	показать / скрыть график потока событий
	обновить список событий
	просмотр предыдущего запроса из истории поиска событий
	просмотр следующего запроса из истории поиска событий
 История	просмотр 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. 22](#)».

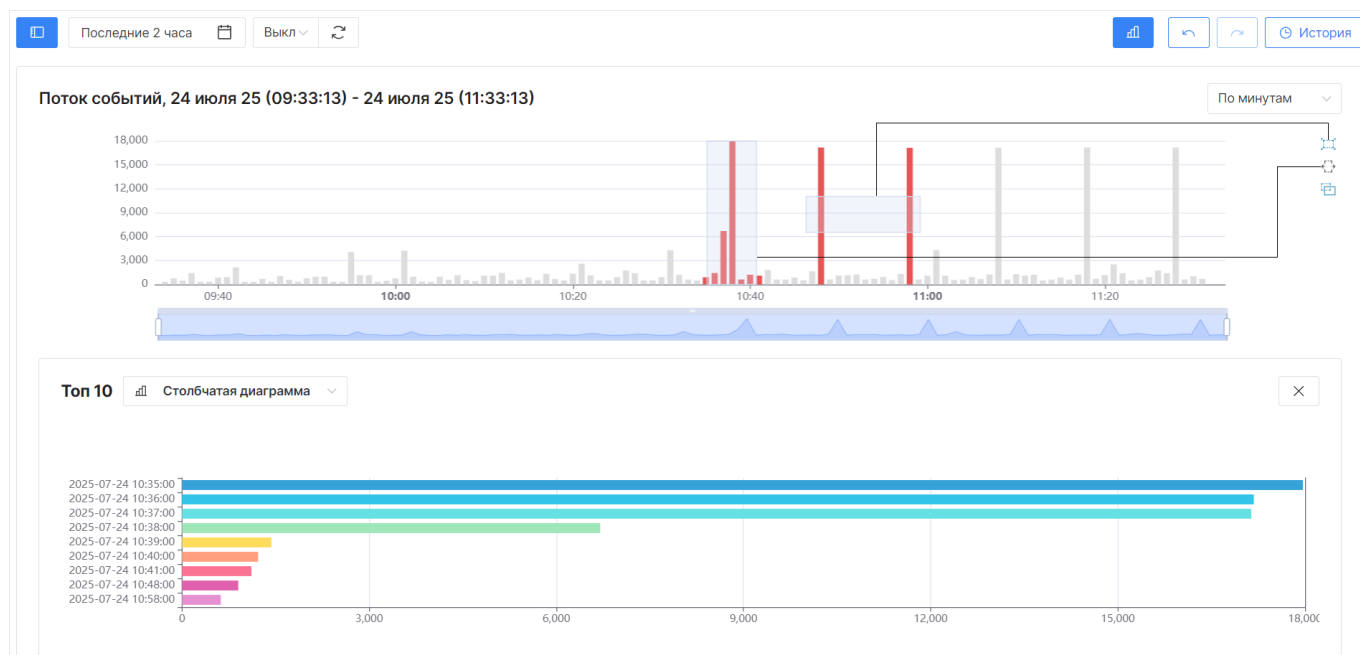


Рис. 22 – Страница "События". Блок "Топ-10"

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. 22](#)»);
- таблица;
- круговая диаграмма (см. «[Рис. 23](#)»).

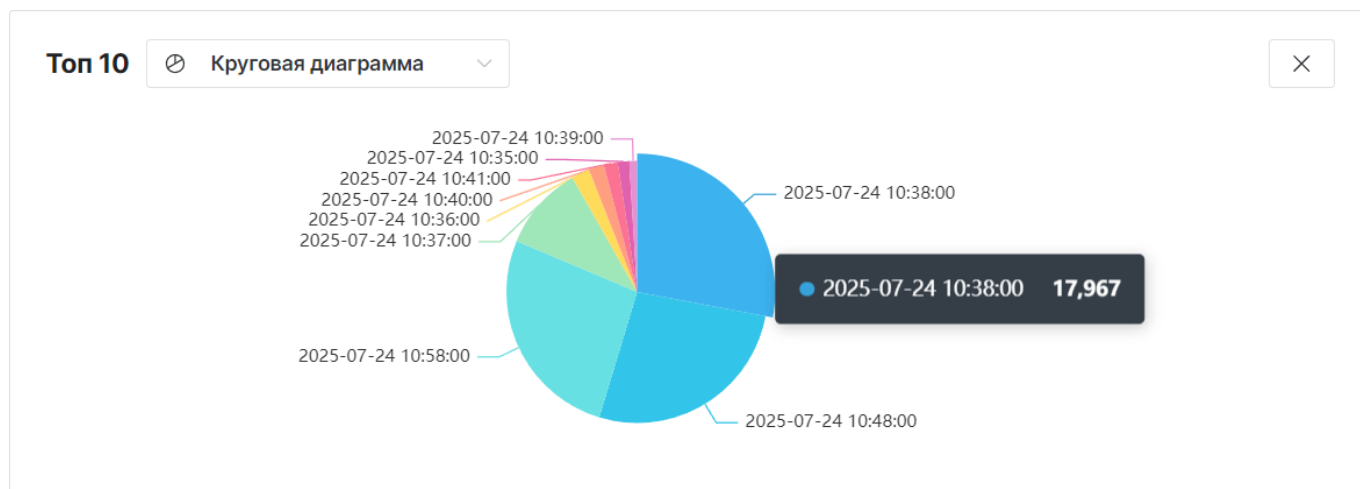


Рис. 23 – Блок "Топ-10". Круговая диаграмма

Для закрытия блока нажмите кнопку **X**.

5.1.2.1 Масштабирование графика потока событий

Для более подробной детализации графика потока событий используйте инструмент "Масштабирование" (см. «Рис. 24»).

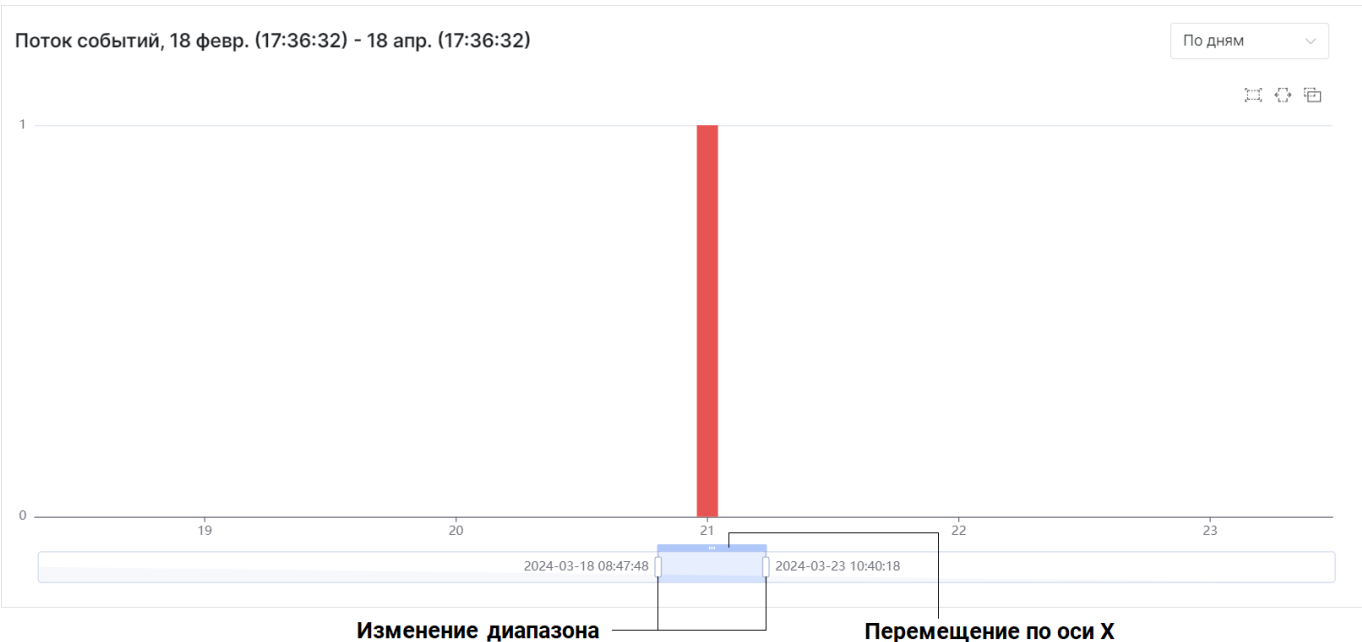


Рис. 24 – Элементы управления масштабом

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.




Карточный вид

Панель располагается над списком событий (см. «Рис. 25»).



Рис. 25 – Панель управления списком событий

На панели доступны следующие элементы управления:

Кнопка	Действие
Поиск	поиск по значениям полей события
 Табличный вид	включить табличный вид
 Сортировка	настроить параметры сортировки событий в списке
Набор полей	выбрать поля для отображения в таблице (только для табличного вида)
	доступ к следующим действиям над событиями: <ul style="list-style-type: none">– экспортировать страницу в CSV;– экспортировать в CSV.

Пример отображения событий в карточном виде (см. «Рис. 26»).

Событий: 19037, показано 1 - 20

Ввести

Табличный вид

Сортировка

Набор полей

_id: e88233d4-1a9e-4125-a6f1-2172158f42ae

Событие нормализовано

Действия

{ "b_ts": "2025-07-24T11:09:54.000+03:00", "a_m": "1514", "Application": "\\device\\harddiskvolume2\\program files\\log collector\\main-windows-amd64.exe", "Bookmark": "", "Channel": "Security", "ChannelText..." }

@timestamp24.07.2025 11:09:44

Показать больше

_id: 02c12c3c-a730-4012-9355-3456b04f6258

Событие нормализовано

Действия

{ "b_ts": "2025-07-24T11:09:54.000+03:00", "a_m": "1514", "Application": "\\device\\harddiskvolume2\\program files\\log collector\\main-windows-amd64.exe", "Bookmark": "", "Channel": "Security", "ChannelText..." }

@timestamp24.07.2025 11:09:44

Показать больше

Рис. 26 – Список событий в карточном виде

По кнопкам **Показать больше** / **Показать меньше** можно открыть/скрыть отображение всех полей события (см. «Рис. 27»).

_id: 5d8c1675-1c82-40a6-8c98-d0aea0edf1af

Событие нормализовано

Действия

{ "b_ts": "2025-07-24T12:27:21.000+03:00", "a_m": "1514", "Bookmark": "", "Channel": "Security", "ChannelText": "Security", "EventData": "", "EventDataErr": null, "EventID": 4634, "EventTime": "2025-07-..." }

@timestamp	24.07.2025 12:27:12
action	disconnect
event.category	communication
event.description	An account was logged off
event.input.source	1514-microsoft_windows_eventlog
event.logsource.input	mseven6_input
event.logsource.name	security
event.logsource.product	operating_system
event.logsource.vendor	microsoft
event.opcode.value	0
event.record.id	296013521
event.severity	4
event.subcategory	session_connection
event.thread.id	5188
event.uuid	5d8c1675-1c82-40a6-8c98-d0aea0edf1af
target.user.name	vadim

Показать меньше

Рис. 27 – 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
<div>Действия</div>	<div>доступ к следующим действиям над событием:<ul style="list-style-type: none">- скопировать событие- найти инцидент, в котором присутствует событие.</div> <div>Если после выполнения функции Найти инцидент не были найдены подходящие инциденты, то становятся доступны следующие действия:<ul style="list-style-type: none">- создать инцидент;- добавить к инциденту.</div>

Табличный вид

Для переключения списка событий в табличный вид нажмите кнопку Табличный вид.

Панель управления располагается над таблицей (см. «Рис. 28»).

Событий: 167929 , показано 1 - 20

Ввести

Карточки








Сортировка

Набор полей














Рис. 28 – Панель управления табличным представлением списка событий

В табличном виде на панели доступны следующие элементы управления:

Кнопка	Действие
--------	----------


Кнопка	Действие
Поиск	поиск по значениям полей события
 Карточки	включить карточный вид
	включить/выключить возможность изменения столбцов. После включения функции в заголовках столбцов появятся кнопки  /  , которые позволяют изменять порядок столбцов
	включить/выключить отображение полного наименования заголовков столбцов таблицы
 Сортировка	настроить параметры сортировки событий в списке
Набор полей	выбрать поля для отображения в таблице
	доступ к следующим действиям над событиями: <ul style="list-style-type: none"> – экспортировать страницу в CSV; – экспортировать в CSV.

Пример табличного представления данных приведен на «Рис. 29».

<input type="checkbox"/>	@timestamp	action	event.category	event.description	event.severity	event.record.id	event.uuid	target.user.name	
<input type="checkbox"/>	24 июля 2025,...	disconnect	communication	An account was logged off	4	296013521	5d8c1675-1c82-40a6-8c98-...	vadim	
<input type="checkbox"/>	24 июля 2025,...	execute	system	This event generates if an...	5	296013522	d226bbf0-9a9d-4024-a2c8-...		
<input type="checkbox"/>	24 июля 2025,...	close	system	The handle to an object was...	2	296013523	64a47567-f075-4054-920f-...		
<input type="checkbox"/>	24 июля 2025,...	access	system	A handle to an object was...	3	296013524	6c7547af-db2b-4eb4-a6f6-...		
<input type="checkbox"/>	24 июля 2025,...	execute	system	This event generates if an...	5	296013525	b015015e-ef5f-4f95-b6c9-...		
<input type="checkbox"/>	24 июля 2025,...	close	system	The handle to an object was...	2	296013526	e6ed99a2-ceba-4f65-9a85-...		
<input type="checkbox"/>	24 июля 2025,...	access	system	A handle to an object was...	3	296013527	77e5363b-6b6f-4315-8b93-...		
<input type="checkbox"/>	24 июля 2025,...	access	system	An attempt was made to acces...	3	296013528	e6deb77d-bc5b-4848-9f3c-...		
<input type="checkbox"/>	24 июля 2025,...	close	system	The handle to an object was...	2	296013529	265b388a-8cc8-4bb1-b2a4-...		
<input type="checkbox"/>	24 июля 2025,...	close	system	The handle to an object was...	2	296013530	924c381a-7793-4a1c-aff6-...		
<input type="checkbox"/>	24 июля 2025,...	execute	system	This event generates if an...	5	296013531	8b49495e-b0c7-4578-8140-...		
<input type="checkbox"/>	24 июля 2025,...	close	system	The handle to an object was...	2	296013532	258dbb71-5c49-4013-ab84-...		
<input type="checkbox"/>	24 июля 2025,...	close	system	The handle to an object was...	2	296013506	537b6d79-9fea-4f45-8211-...		

<
1
2
3
4
5
6
7
...
8397
>
20

Рис. 29 – Список событий в табличном виде

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

При клике на строку таблицы откроется блок **Просмотр события**, в котором отображается выбранное событие в карточном виде (см. «Рис. 30»).

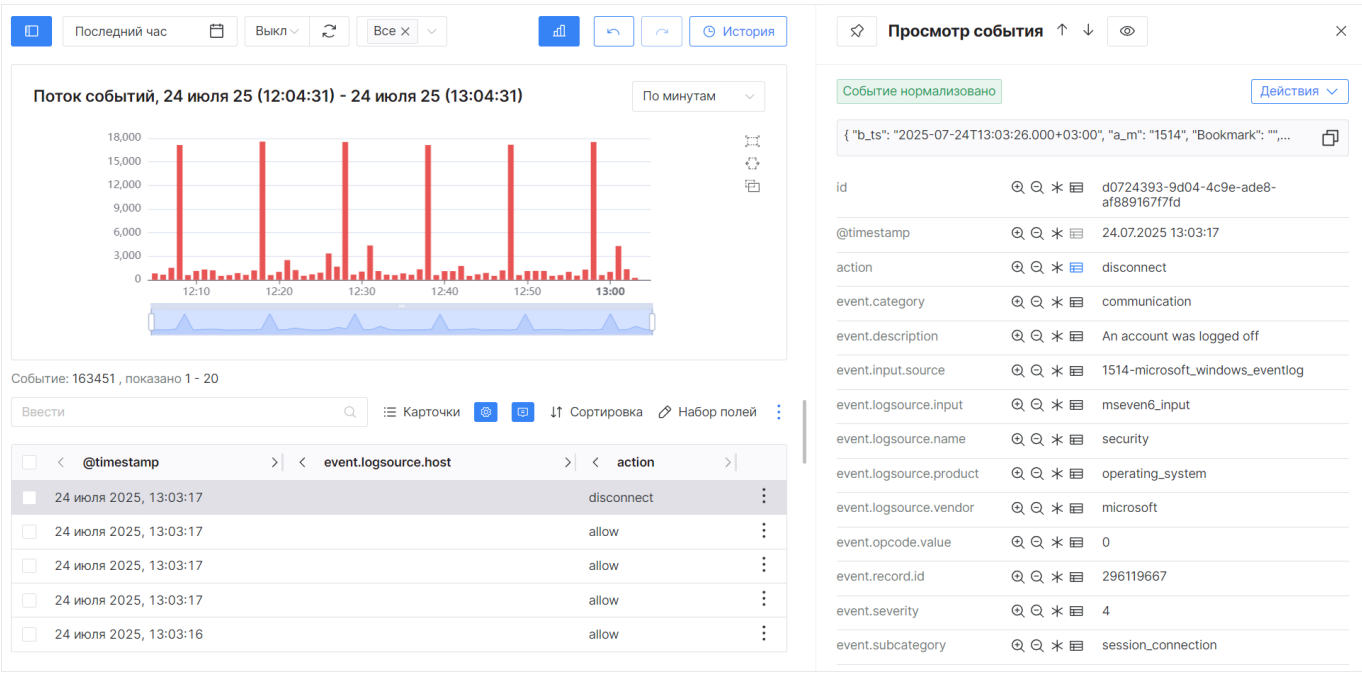


Рис. 30 – Список событий в табличном виде. Просмотр события

В блоке **Просмотр события** доступны следующие элементы управления:

Кнопка	Действие
	закрепить выбранное событие в блоке Просмотр события
	открыть следующее / предыдущее событие из списка
	включить / выключить отображение кнопок по установке фильтров и добавления поля в набор столбцов таблицы
	установить фильтр "Равно". В параметры запроса фильтра добавится условие поиска событий по значению равным в указанном поле. Элемент управления появляется при наведении курсора мыши на соответствующую область
	установить фильтр "Не равно". В параметры запроса фильтра добавится условие поиска событий по всем значениям, кроме того, что указано в поле. Элемент управления появляется при наведении курсора мыши на соответствующую область
	установить фильтр "Существует". В параметры запроса фильтра добавится условие поиска событий по всем событиям, в которых существует выбранное поле. Элемент управления появляется при наведении курсора мыши на соответствующую область
	добавить/исключить поле из набора столбцов таблицы
<div>Действия </div>	<div>доступ к следующим действиям над событием:</div> <div>- скопировать событие</div> <div>- найти инцидент, в котором присутствует событие.</div> <div>Если после выполнения функции Найти инцидент не были найдены подходящие инциденты, то становятся доступны следующие действия:</div> <div>- создать инцидент;</div> <div>- добавить к инциденту.</div>

5.2 Работа с фильтрами

Настройка фильтра выполняется на вкладке "Фильтры" (см. «Рис. 31»).

Фильтры

Пресеты

Нормализованное событие

Событие нормализовано

▼

Запрос

Сохраненные запросы >

📄

Сохранить выбор как

⊕

Добавить запрос

action равен disconnect

✎

✖

Агрегация

Сохраненные агрегации >

📄

Сохранить выбор как

⊕

Добавить агрегацию

@timestamp min

✎

✖


Рис. 31 – Страница "События". Вкладка "Фильтры"

При работе с фильтрами доступны следующие элементы управления:

Кнопка	Действие
Добавить запрос	добавление запроса в условия фильтра
Добавить агрегацию	добавление агрегаций в условия фильтра
✎	редактирование запроса/агрегации
✖	удаление запроса/агрегации
Сбросить	очистить условия фильтра

Настройку условий фильтра можно поделить на два этапа.

Первый этап – настройка периода и автообновления данных. Для этого в блоке **График потока событий** выполните следующие действия:

- 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.
- 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**.

Второй этап – настройка запросов и агрегаций. Для этого в боковой панели на вкладке **Фильтры** выполните следующие действия:

1. 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.
2. В поле **Запрос** добавьте необходимое количество запросов (см. раздел «[Настройка запросов](#)»).
3. В поле **Агрегация** добавьте необходимое количество агрегаций (см. раздел «[Настройка агрегации](#)»).
4. При необходимости вы можете сохранить условия фильтра как пресет (см. раздел «[Работа с пресетами](#)»).

Также 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. 32](#)»).

Запрос Сохраненные запросы >

Сохранить выбор как

+ Добавить запрос

@timestamp НЕ равен	✎	✕
2024-03-22T13:21:17.998015077+03:00		
elastic_key существует	✎	✕
ip равен	✎	✕
192.168.203.167		
@timestamp равен	✎	✕
1712178000000		

Рис. 32 – 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. 33»).

Добавить запрос ✕

Поле

@timestamp ▾

Действие

равен ▾

Значение

2024-04-04 📅

Сбросить Сохранить

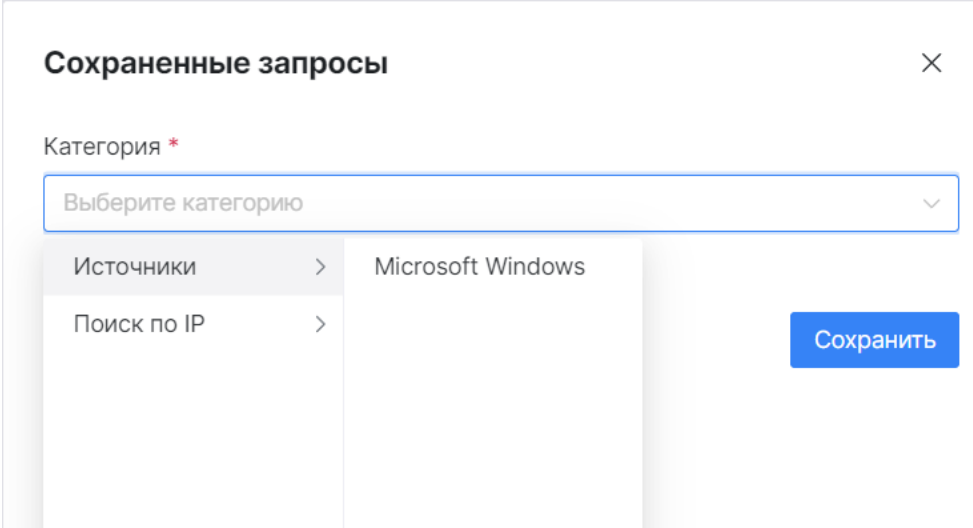
Рис. 33 – Окно "Добавить запрос"

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. 34](#)»).



Сохраненные запросы

Категория *

Выберите категорию

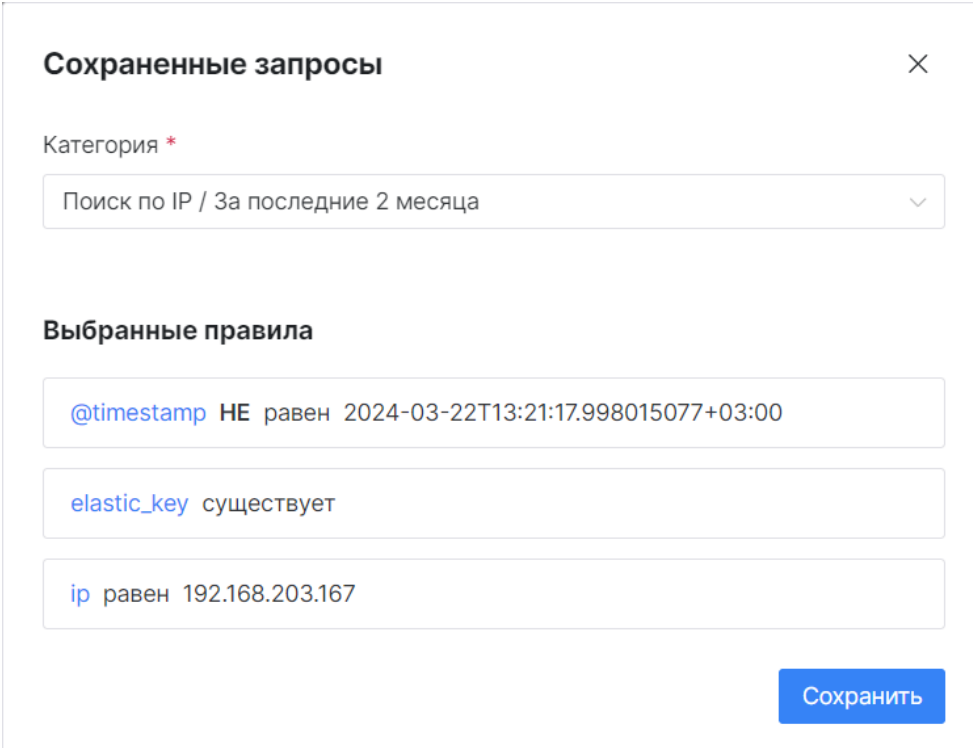
Источники > Microsoft Windows

Поиск по IP >

Сохранить

Рис. 34 – Окно "Сохраненные запросы"

2. В поле "Категория" выберите сохраненную категорию, а затем необходимый запрос. Отобразится структура запроса (см. «[Рис. 35](#)»).



Сохраненные запросы

Категория *

Поиск по IP / За последние 2 месяца

Выбранные правила

@timestamp НЕ равен 2024-03-22T13:21:17.998015077+03:00

elastic_key существует

ip равен 192.168.203.167

Сохранить




Рис. 35 – 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 таким способом запросов, приведен на «[Рис. 36](#)».

Нормализованное событие

Не важно

Запрос

Сохраненные запросы >

Сохранить выбор как

Добавить запрос

@timestamp равен 2024-03-22T13:21:17.998015077+03:00































elastic_key существует

Агрегация

Сохраненные агрегации >

Добавить агрегацию

_id: pZnbxtEXMTljuFwRTqowMjsjZrOxrWSQ Событие нормализовано

@timestamp	  	22.03.2024 13:21:17
elastic_key	  	normalized
fqdn	  	["MVV-4269", "2"]
hostname	  	["MVV-4269"]
id	  	pZnbxtEXMTljuFwRTqowMjsjZrOxrWSQ
initiator.host.internal	  	false
initiator.host.test	  	testtest
initiator.host.test-ip	  	192.168.236.223
ip	  	["192.168.236.223"]
target.host.internal	  	false

Показать меньше ^

Рис. 36 – 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. 37](#)»).

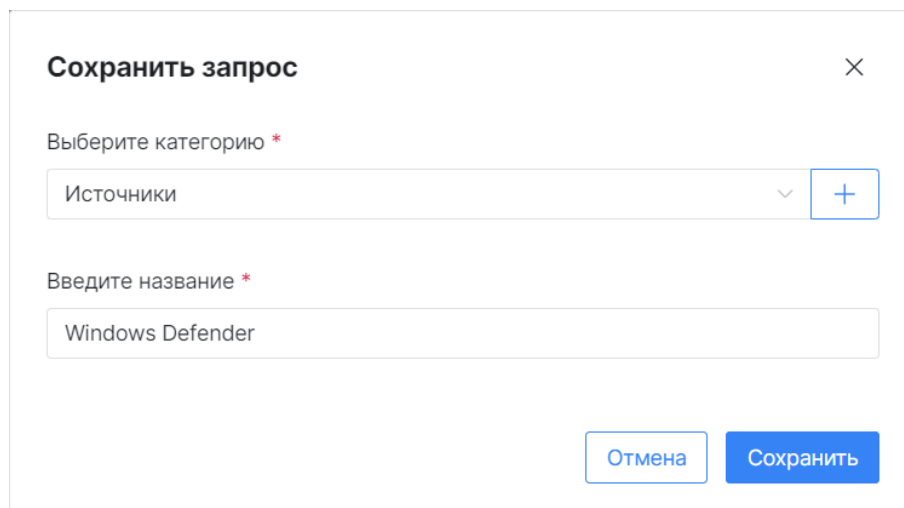


Рис. 37 – Окно "Сохранить запрос"

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. 38»).

Фильтры

Пресеты

Нормализованное событие

Не важно

Запрос

Сохраненные запросы

Добавить запрос

Агрегация

Сохраненные агрегации

Сохранить выбор как

Добавить агрегацию

@timestamp stats

_id terms

Сбросить

Агрегация

Поле и функция

Подагрегация

@timestamp stats

count

min

max

avg

sum

2020

21.03.2024 15:45:08

22.03.2024 13:21:17

21.03.2024 16:56:58

3456279426358658

_id terms

_id

doc_count

ADGgCMWYTKGMMsnMHADP\$iegwLyWdvWZ

1

ADKCbBkQqkUxplmbdxrucbpQAEGLLnO

1

AFVeWLpkrededbQufeRekTOQWSigoQtK

1

AJXkJuOkvaYibjGgsxeROzmLEjdqogq

1

AJddpwpfpoGbrDYBbPrvtvAmuxiRbbGZ

1

elastic_key_terms

elastic_key

doc_count

normalized

1

error

1

@timestamp_avg

value

1711026709729

1711026757794

1711025215595

1711025622258

_id_terms

_id

doc_count

ADGgCMWYTKGMMsnMHADP\$iegwLyWdvWZ

1

ADKCbBkQqkUxplmbdxrucbpQAEGLLnO

1

AFVeWLpkrededbQufeRekTOQWSigoQtK

1

AJXkJuOkvaYibjGgsxeROzmLEjdqogq

1

Событий: 2020, показано 1 - 20

Ввести

Сортировка

Набор полей

Выбрать несколько

_id: pZnbxtEXMTIjuFwRTqowMjsjZrOxrWSQ

Событие нормализовано

Действия

@timestamp

22.03.2024 13:21:17

Показать больше

Рис. 38 – 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. 39»).

Добавить агрегацию

Действие

Stats

Поле

@timestamp

Сбросить

Сохранить

Рис. 39 – Окно "Добавить агрегацию"

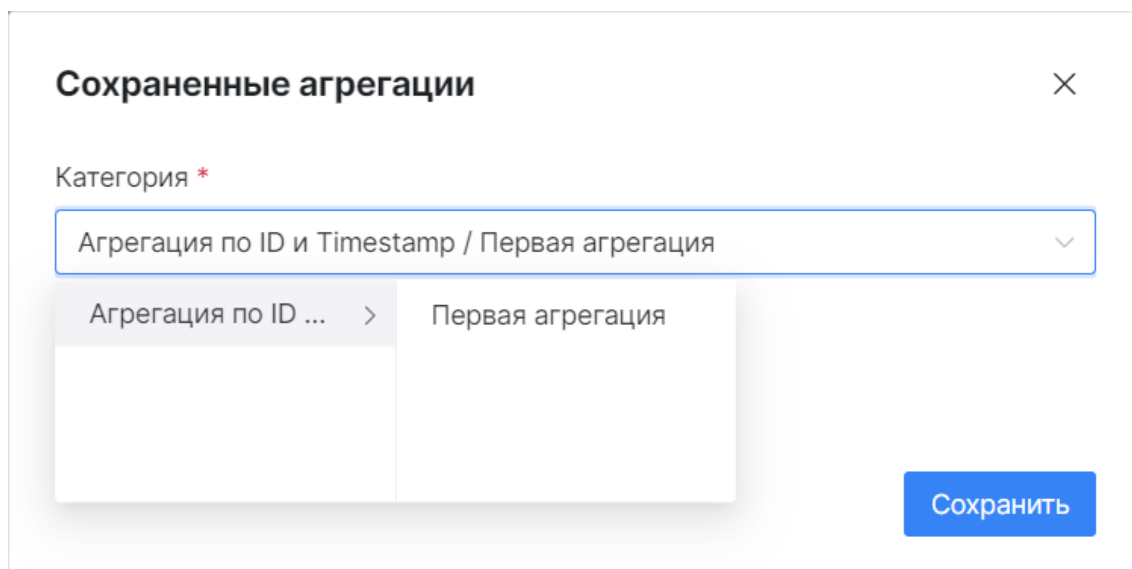
2. Укажите следующие данные:
 - в поле "Действие" из выпадающего списка выберите функцию агрегации;
 - из выпадающего списка выберите поле, по которому будет выполняться функция агрегации.
3. Нажмите кнопку **Сохранить**.

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 **Агрегации** нажмите кнопку **Сохраненные агрегации**. Откроется окно "Сохраненные агрегации" (см. «[Рис. 40](#)»).



Сохраненные агрегации ×

Категория *

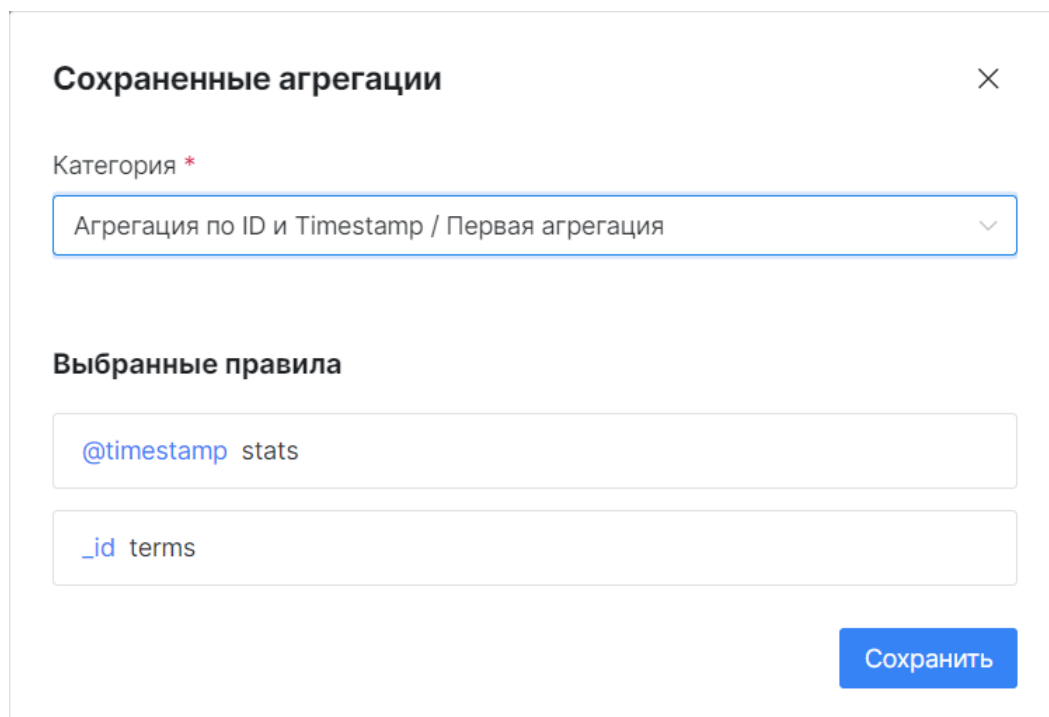
Агрегация по ID и Timestamp / Первая агрегация

Агрегация по ID ...	>	Первая агрегация
---------------------	---	------------------

Сохранить

Рис. 40 – Окно "Сохраненные агрегации"

2. В поле "Категория" выберите сохраненную категорию, а затем необходимую агрегацию. Отобразятся параметры агрегации (см. «[Рис. 41](#)»).



Сохраненные агрегации ×

Категория *

Агрегация по ID и Timestamp / Первая агрегация

Выбранные правила

@timestamp stats

_id terms

Сохранить

Рис. 41 – 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. 42»).

Добавить агрегацию [X]

Действие: Terms [v] Поле: _id [v]

Ограничение количества: 10 [– +]

[Добавить подагрегацию]

_id terms	[edit] [X]
elastic_key terms	[edit] [X]
@timestamp avg	[edit] [X]

[Сбросить] [Сохранить]

Рис. 42 – 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. 43»).

Сохранить агрегацию ×

Выберите категорию *

Агрегация по ID и Timestamp ▼ +

Введите название *

Первая агрегация

Отмена Сохранить

Рис. 43 – 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. 45](#)»).

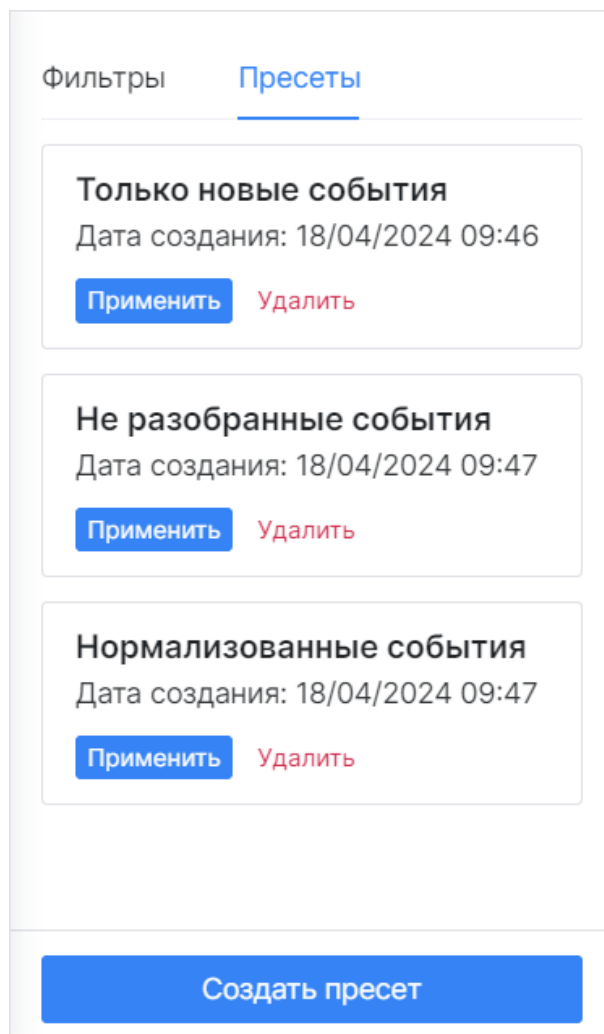


Рис. 44 – Страница "События". Вкладка "Пресеты"

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. 45»).

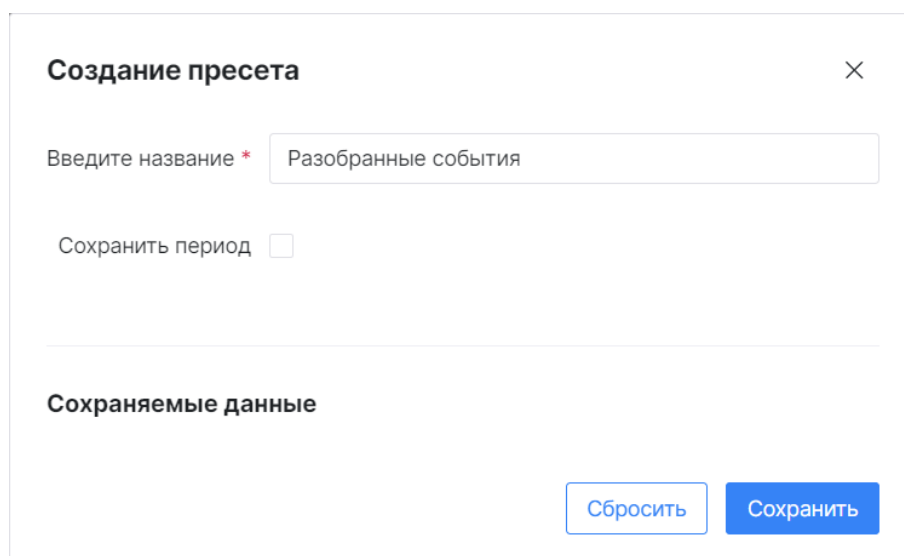


Рис. 45 – Окно "Создание пресета"

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  **История**. Откроется окно "История поиска" (см. «Рис. 46»).

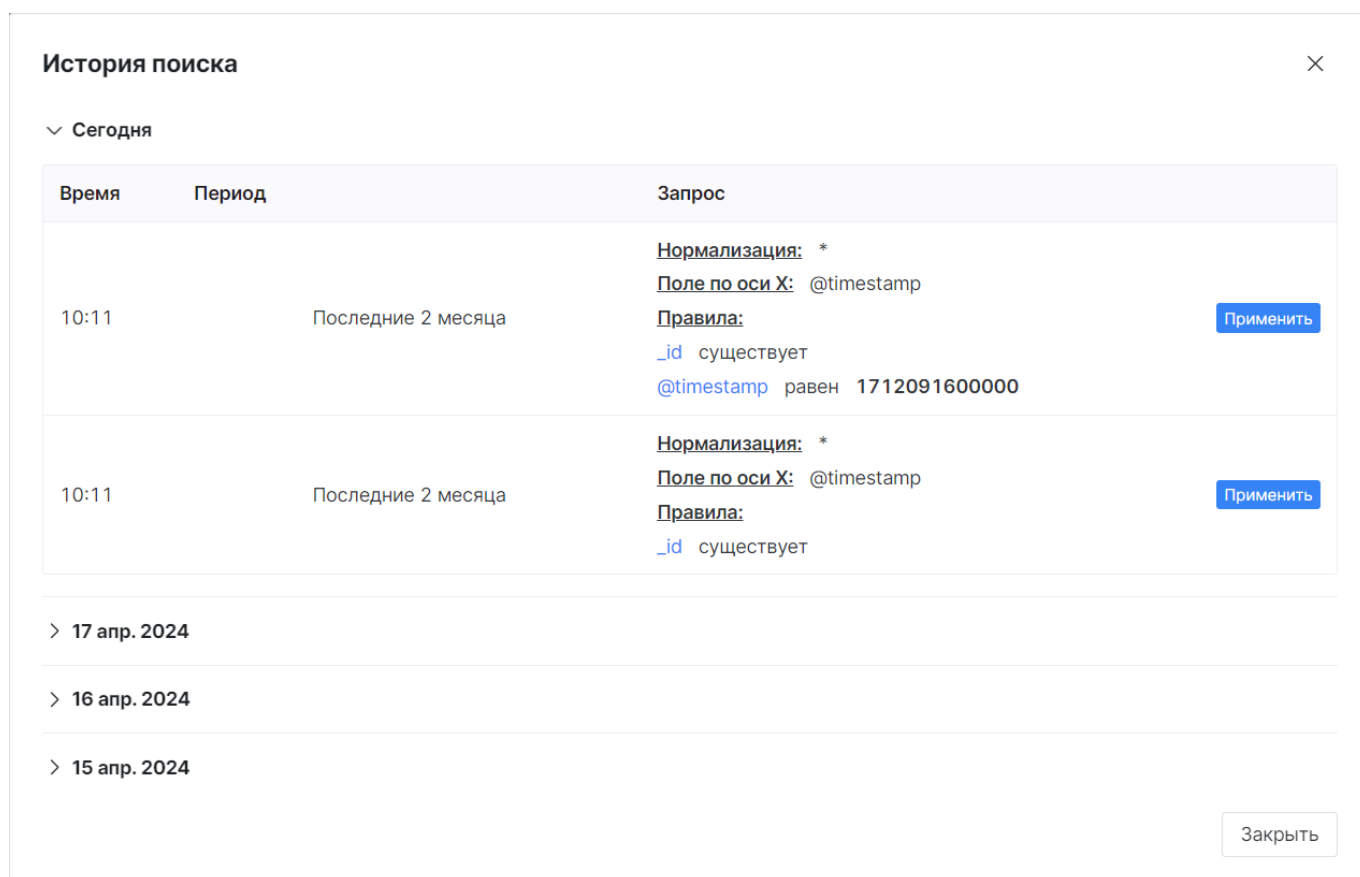


Рис. 46 – Окно "История поиска"

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. 47](#)».



Рис. 47 – Страница "События". Сформированный список событий

Работа с событиями включает в себя следующие процессы:

1. Поиск инцидента. Если результат поиска не дал результатов, то становятся доступны следующие действия:
 - Создание инцидента;
 - Добавление в инцидент.
2. 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 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. 48](#)»).

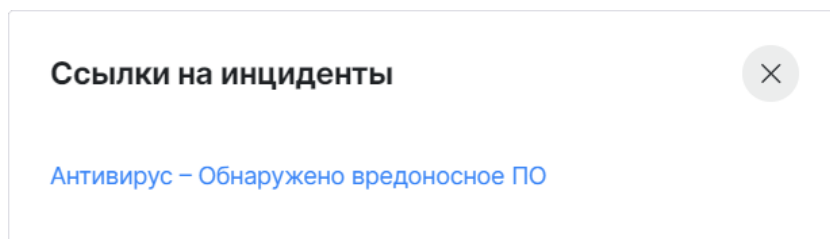


Рис. 48 – Список найденных инцидентов по событию

3. Для открытия инцидента нажмите на нужную ссылку.



5.3.1.1 Создание инцидента

Действие доступно только после выполнения действия **Найти инцидент**.

Примечание. Подробнее об инцидентах см. раздел «[Инциденты](#)».

Платформа Радар позволяет создать инцидент на основе подозрительного события.

Для этого 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 **Создать инцидент**. Откроется окно **Быстрое создание инцидента** (см. «Рис. 49»).

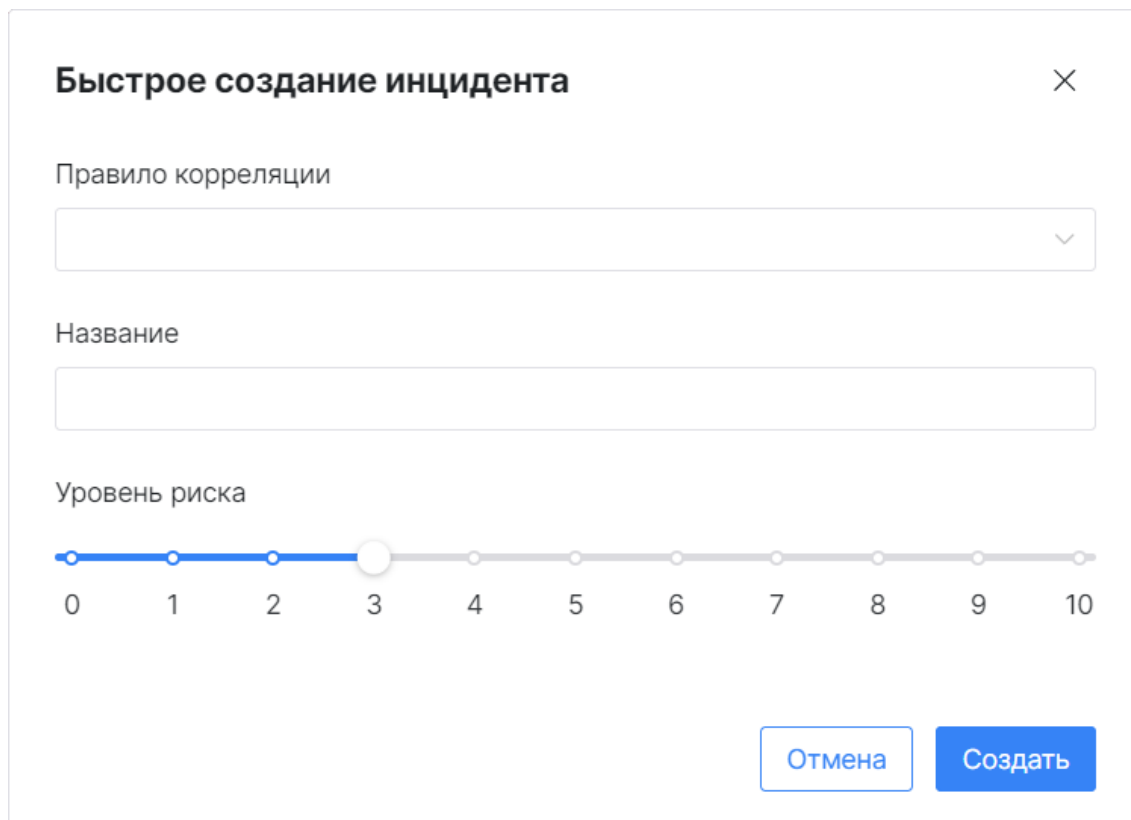


Рис. 49 – Окно "Быстрое создание инцидента"

3. Выполните в окне следующие действия:

- в поле **Правило корреляции** из выпадающего списка выберите правила корреляции, на основе которого будет создан инцидент;
- в поле **Название** укажите наименование инцидента;
- в поле **Уровень риска** выберите цифровое обозначение уровня риска создаваемого инцидента.

4. Нажмите кнопку **Создать**.



5.3.1.2 Добавление события в инцидент

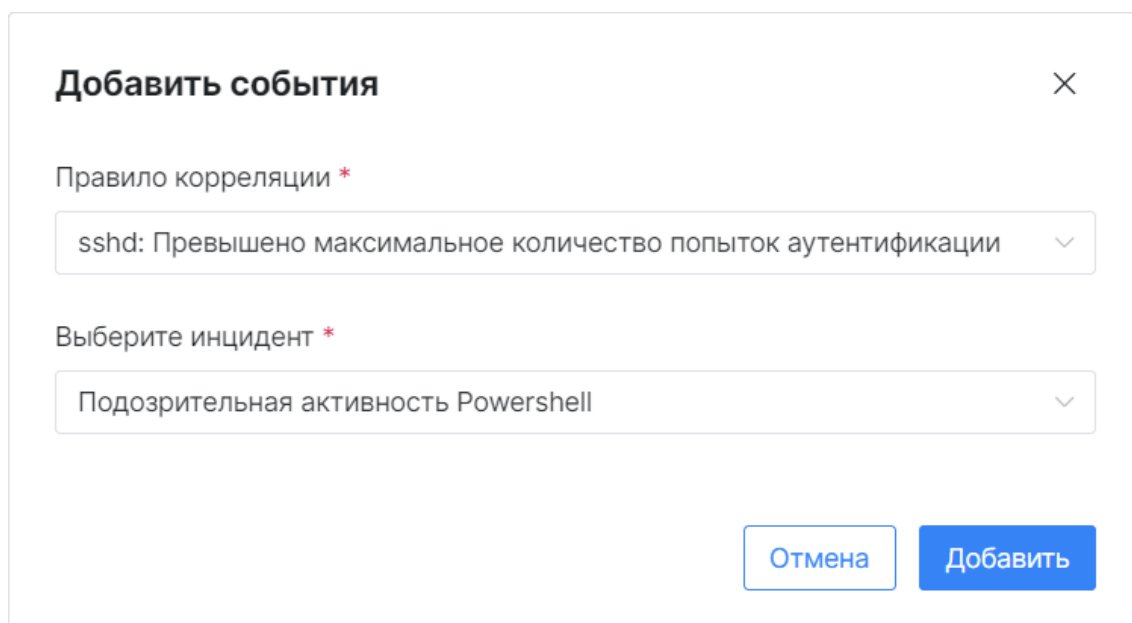
Действие доступно только после выполнения действия **Найти инцидент**.

Примечание. Подробнее об инцидентах см. раздел «[Инциденты](#)».

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

Для этого 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 **Добавить к инциденту**. Откроется окно **Быстрое создание инцидента** (см. «[Рис. 50](#)»).



Добавить события

Правило корреляции *

ssh: Превышено максимальное количество попыток аутентификации

Выберите инцидент *

Подозрительная активность Powershell

Отмена Добавить

Рис. 50 – Окно "Добавить события"


3. Выполните в окне следующие действия:

- в поле **Правило корреляции** из выпадающего списка выберите соответствующее правило корреляции;


- в поле **Инцидент** выберите инцидент, в который будет добавлено событие.
4. Нажмите кнопку **Добавить**. После успешного добавления события в инцидент платформа предложит вам открыть соответствующий инцидент.

5.3.2 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**.

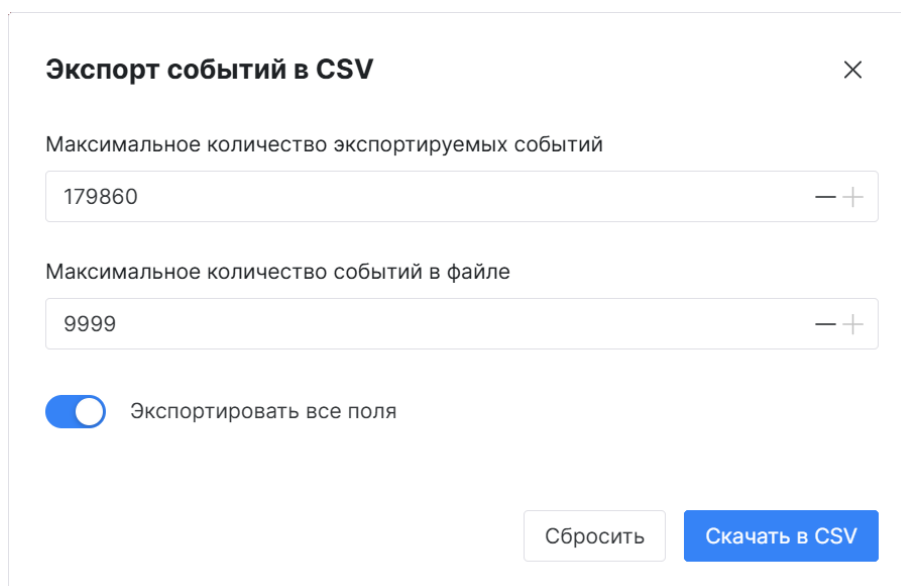


Рис. 51 – Окно "Экспорт событий в CSV"

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.

5.3.3 Вспомогательные инструменты для анализа событий

5.3.3.1 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. 52](#)»).

Синтаксис `elastic_key: (parsed)`.

The screenshot shows the OpenSearch search results for the query `elastic_key: (parsed)`. The interface includes a search bar with the query, a toolbar with options like 'Сортировка', 'Набор полей', and 'Выбрать несколько', and a list of results. Two results are shown, each with a table of fields and values. The `elastic_key` field is highlighted in orange and labeled 'Событие разобрано'.

Field	Value
id	AAAAAGYT2ItDRkTEh/iJdNk35NfcQJx1
@timestamp	08.04.2024 02:44:11
event.logsource.host	172.30.254.155:9992
elastic_key	parsed
epoch	1712576651.792
event.logsource.application	parsed
event.logsource.input	1514-microsoft_windows_eventlog

Field	Value
id	AAAAAGYT2IvCJ+3ZFfhcbyb4gDKmc6CI
@timestamp	08.04.2024 02:44:11
event.logsource.host	172.30.254.155:9992
elastic_key	parsed
epoch	1712576651.792
event.logsource.application	parsed
event.logsource.input	1514-microsoft_windows_eventlog

Рис. 52 – 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. 53](#)»).

Синтаксис: elastic_key: (NOT parsed)

Событий: 831098, показано 1 - 20

elastic_key: (NOT parsed) 🔍

Сортировка ⚙️ Набор полей 🗑️ Выбрать несколько ⋮

id: AAAAGYhIKExpLOT+IEEUluk4y88tszW Не разобрано Действия ▾

@timestamp	🔍 🔍 *	18.04.2024 04:31:13
event.logsource.host	🔍 🔍 *	172.30.254.155:9992
elastic_key	🔍 🔍 *	error
error	🔍 🔍 *	Traceback (most recent call last): File "<frozen termite.daemon.worker>", line 364, in _process_events File "<frozen termite.pipeline>", line 228, in execute File "<frozen termite.pipeline>", line 69, in parse File "<frozen termite.parsers.json_parser>", line 28, in parse rapidjson.JSONDecodeError: Parse error at offset 206: Missing a name for object member.
event.logsource.input	🔍 🔍 *	1514-microsoft_windows_eventlog
event.uuid	🔍 🔍 *	AAAAGYhIKExpLOT+IEEUluk4y88tszW
id	🔍 🔍 *	AAAAGYhIKExpLOT+IEEUluk4y88tszW
raw	🔍 🔍 *	{"rs_collector_hostname":"v-back-com-05","rs_relay_fqdn":"172.30.254.169","rs_relay_ip":"172.30.254.169","rs_collector_ts":"2024-04-18T16:31:13.073681+03:00","__rs_module":"1514-microsoft_windows_eventlog",

Показать меньше ^

id: AAAAGYhIKUSp4wUxuwLpyfJNklxZnsF Событие нормализовано Действия ▾

@timestamp	🔍 🔍 *	18.04.2024 04:31:12
event.logsource.host	🔍 🔍 *	172.30.254.155:9992
action	🔍 🔍 *	detect
elastic_key	🔍 🔍 *	normalized
epoch	🔍 🔍 *	1713447072.324

Рис. 53 – Поиск всех событий, в которых поле elastic_key имеет значение отличное от "Разобрано"

Пример 3. Поиск по конкретному значению поля (см. «Рис. 54»).

Событие: 1, показано 1 - 1

AAAAGYhJrxHuWzqY3i2p6mx31fkltnu 🔍

Сортировка ⚙️ Набор полей 🗑️ Выбрать несколько ⋮

id: AAAAGYhJrxHuWzqY3i2p6mx31fkltnu Событие нормализовано Действия ▾

@timestamp	🔍 🔍 *	18.04.2024 04:57:10
event.logsource.host	🔍 🔍 *	172.30.254.155:9992

Показать больше ▾

< 1 > 20 / страница ▾

Рис. 54 – Поиск по конкретному значению

5.3.3.2 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. 55»).

_id terms		Ссылки на страницу просмотра выбранного события		
_id	doc_count	elastic_key__terms		@timestamp_avg
ADGgCMWYTKGMMsnMHADPsiegwLyWdvWZ	1	elastic_key	doc_count	value
		normalized	1	1711026709729
ADKCbBkQqpkUxplmbdxrucbpQAEGLLnO	1	elastic_key	doc_count	value
		error	1	1711026757794
AFVeWLpkrededbQufeRekTOQWSigoQtK	1	elastic_key	doc_count	value

Рис. 55 – Просмотр результатов агрегации

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

5.3.3.3 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. 56»).

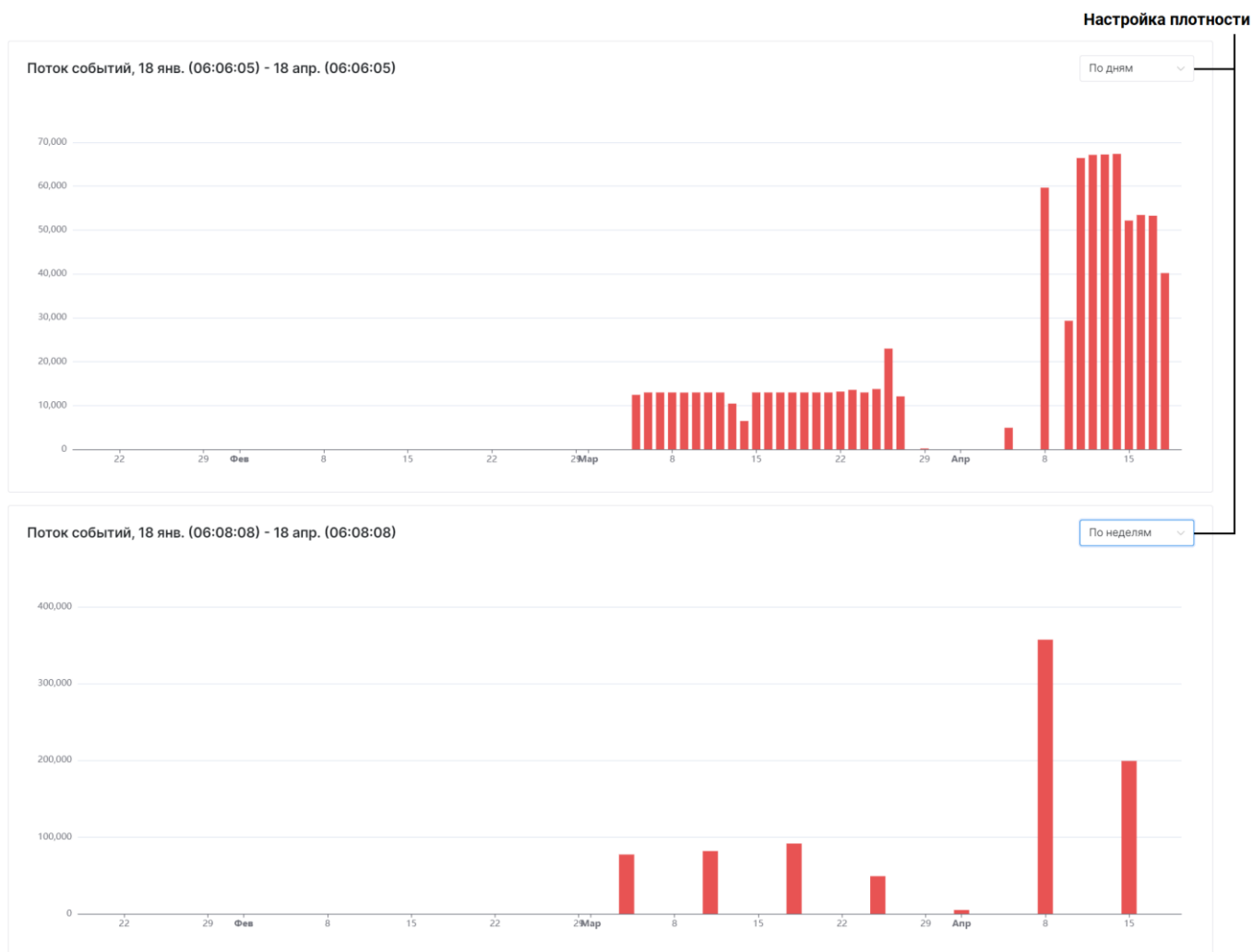


Рис. 56 – Настройка плотности отрисовки потока событий

5.3.3.4 Сортировка событий

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

Для этого нажмите кнопку **Сортировка**. Откроется окно настройки сортировки (см. «Рис. 57»).

Событий: 17 , показано 1 - 17

Ввести

Событие нормализовано

@timestamp	🔍 🔍 *	17.04.2024 17:28:36
event.logsource.host	🔍 🔍 *	172.30.254.68:9992

Показать больше ▾

Событие нормализовано

@timestamp	🔍 🔍 *	17.04.2024 11:28:36
event.logsource.host	🔍 🔍 *	172.30.254.68:9992

Показать больше ▾

Выбранные поля

- ☒ @timestamp
- ☒ _id

Все поля

Введите значение

- ☐ _index
- ☐ access
- ☐ action
- ☐ application.name.keyword
- ☐ createdTimeMs
- ☐ elastic_key
- ☐ epoch

Действия ▾

Рис. 57 – 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 / ;
- для полей, по которым выполняется сортировка, можно задать направление сортировки:
 - ↓ - от последнего к первому;
 - ↑ - от первого к последнему.

5.3.3.5 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. 58»).

Выбор набора полей

Q Введите название поля

☒ @timestamp

^

v

☒ event.logsource.host

^

v

☒ elastic_key

^

v

☒ action

^

v

☐ _doc_count

☐ _id

☐ _index

☐ _source

☐ epoch

☐ error

Применить

Рис. 58 – 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 ^ / v.
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;
- **Закрит** – работы по расследованию инцидента завершены;
- **Недействительный** – инцидент был создан по ошибке, закрыт без разбора.

Процесс изменения стадии обработки инцидента приведен на «Рис. 59».

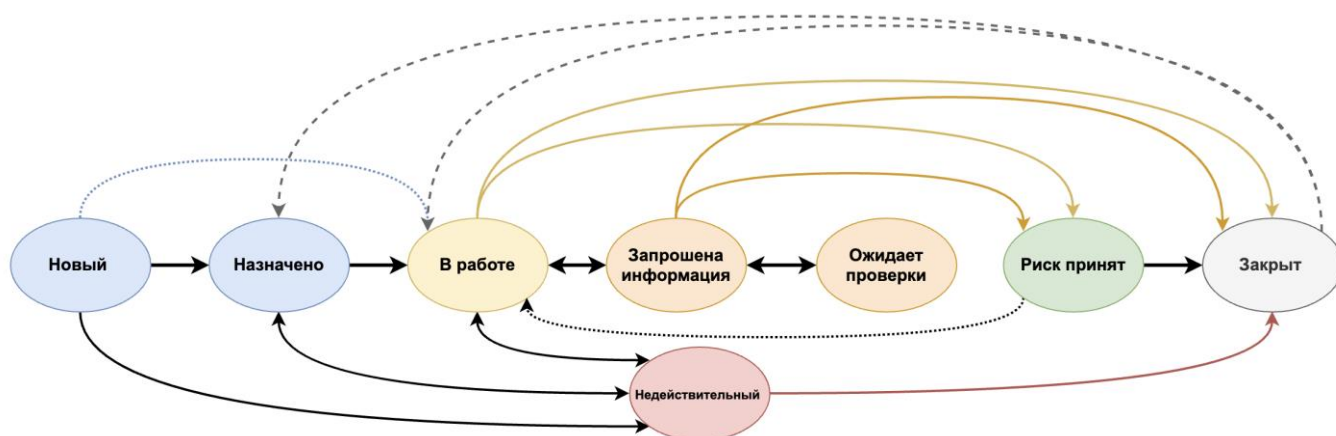


Рис. 59 – Процесс изменения статусов инцидентов

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. 60»).

Срочность	ID	Название	Статус	Создано	Результат анализа	Группа инцидентов	Актив
0.49	51	Попытка модификации процесса...	Новый	2025-09-23 03:30:23	Обнаружение модификации...	-	dc1
0.22	50	Маскировка	Новый	2025-09-22 23:04:34	На узле, Hostname: [dc1], ...	-	dc1
0.95	49	Windows-AD: Многочисленные неуспешные...	Новый	2025-09-22 13:58:52	Обнаружены множественн...	Администраторский доступ	dc1
0.49	48	Сканирование портов	Новый	2025-09-22 10:53:41	С устройства 172.30.254...	-	199.232.210.172
0.49	47	Сканирование портов	Новый	2025-09-22 10:51:15	С устройства 172.30.254...	-	172.30.254.58
0.15	46	Множественные запросы с внутреннего коста...	Новый	2025-09-22 10:47:40	Обнаружены множественн...	-	172.30.249.42
0.15	45	Обнаружены множественные запросы внутри...	Новый	2025-09-22 10:47:07	Обнаружены множественн...	-	172.30.249.42
0.15	4	Множественные запросы с внешнего "IP" на...	Новый	2025-09-19 09:17:43	Обнаружены множественн...	-	172.30.249.63

Рис. 60 – Раздел "Инциденты"

В разделе отображается следующая информация об инцидентах:

- **Срочность** – цветное 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 «[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. 61](#)» и «[Рис. 62](#)»).

←

Создание инцидента

Сбросить

Создать

Тип инцидента

Множественные неудачные попытки входа на одном узле

Актив

stand-x.pgr.local

Создать актив

Уровень риска

2

Категория

☒ Нарушение политики

☐ Сетевая аномалия

☐ Уязвимость

Результат анализа

Внутреннее примечание

Группа инцидентов

Группа "Множественные неудачные попытки входа"

Рис. 61 – Создание инцидента. Общие сведения

Подробности по типу инцидента

Сводка

Один целевой узел сообщает о превышении установленного предела количества ошибок входа в систему под различными именами пользователя.

Описание

Обнаружено превышение установленного предела количества ошибок входа в систему с одного узла-источника под различными именами пользователей. Большое количество таких ошибок может указывать на попытку получения учетных данных пользователя в целевой системе методом подбора. Атака методом подбора предполагает поиск решения путем постоянного перебора множества возможных вариантов паролей, расшифрованных ключей и т. д.

Последствия реализованной угрозы

Множественные ошибки аутентификации могут указывать на попытку взлома учетной записи. Риск будет зависеть от источника входа в систему. В случае успеха злоумышленника наиболее опасными являются следующие риски:

* Раскрытие информации: Уязвимость, которая может привести к раскрытию учетных данных жертвы. В результате киберпреступник может получить действительные учетные данные пользователя, а с их помощью – доступ к конфиденциальной информации.

* Повышение привилегий: Злоумышленник, успешно воспользовавшийся этой уязвимостью, может запустить произвольный код от имени администратора. В этом случае он также получает возможность устанавливать программы, просматривать, изменять и удалять данные, создавать новые учетные записи с полными правами пользователя.

* Удаленное выполнение кода: Эта уязвимость позволяет злоумышленнику получить доступ к чужому вычислительному устройству и вносить изменения, независимо от географического расположения этого устройства.

* Распространение вредоносного контента или спама, а также перенаправление доменов на страницы с вредоносным контентом и выдача себя за владельцев учетных записей с целью распространения фальшивого контента или вредоносных ссылок.

* Сбор учетных данных для продажи третьим сторонам.

Рекомендации по устранению угрозы

* Изолируйте узел от сети. Просканируйте узел с помощью антивирусной программы на предмет наличия угроз и устраните их в случае выявления.

* Если узел-источник является внутренним узлом, проверьте его на предмет взлома.

* Если узел-источник является внешним узлом, проверьте политику брандмауэра, чтобы убедиться, что доступ ко внутренним системам можно получить только с IP-адресов доверенных диапазонов.

Рекомендации по уменьшению риска

Профилактика угрозы эффективнее, чем устранение ее последствий. Далее приведен список основных рекомендаций по повышению безопасности системы:

* Используйте сложные пароли или требуйте их использования.

* Определите «нормальное» количество неудачных попыток входа в систему.

* Используйте тесты CAPTCHA.

* Настройте задержку между попытками входа.

* Используйте контрольные вопросы.

* Активируйте двухфакторную аутентификацию.

* Используйте несколько URL-адресов входа.

* Перехитрите ПО злоумышленников (некоторые боты обучены распознавать ошибки, но в случае одновременных неудачных попыток входа в систему можно использовать перенаправление на разные страницы ошибок. Из-за этого злоумышленнику потребуется как минимум перейти на более продвинутое ПО).

Рис. 62 – 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". При создании инцидента вручную, данное поле также будет являться и его названием. В дальнейшем для смены названия инцидента можно воспользоваться функцией **Редактирование**;
- в поле **Актив** из выпадающего списка выберите устройство, на котором был обнаружен инцидент. Если нужного актива нет в платформе, то вы можете его создать вручную. Для этого нажмите кнопку **Создать актив** и следуйте инструкциям из раздела «[Создание актива](#)»;
- 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. 63](#)»).

ID: 1

Расширенное многовекторное обнаружение угроз VNC

1

Правило корреляции выявило подозрительную активность VNC-процессов (UltraVNC, TightVNC, RealVNC, VNC4) с анализом системных событий Windows Security Log (4656/4658/4663/4624/4625/4648/4672). Обнаруженные типы угроз: • APT (Advanced Persistent Threat) - долгосрочная компрометация с установкой постоянства и сбором учетных данных • Брутфорс-атаки - интенсивная активность с подозрительными масками доступа к системным объектам • Латеральное движение - распространение угрозы по множественным хостам инфраструктуры • Повышение привилегий - несанкционированный доступ к критическим системным компонентам • Установка постоянства - модификация автозагрузки, служб и системных компонентов Анализ включает: - Мониторинг доступа к 24+ критическим объектам реестра (LSA, SAM, службы, сетевые параметры) - Классификацию пользователей по уровню привилегий (система, администраторы, службы) - Корреляцию событий в 3-минутном временном окне - Детекцию опасных операций записи с масками доступа 0x2, 0x4, 0x20019 Техника MITRE ATT&CK: T1021.005 (Remote Services: VNC) + смежные техники T1110, T1078, T1134, T1547, T1543, T1055, T1082.

9.1

Источник: Коррелятор

Кол-во повторных открытий: 0
Кол-во происшествий: 1
Правило корреляции: Windows - VNC Multi-Vector Detection

Дата создания

15.09.2025 12:47:04

Тип инцидента

Расширенное многовекторное обнаружение угроз VNC

Показать описание

Последнее происшествие

15.09.2025 12:47:03

Показать больше

Актив

3

Название: dc1

Тип

Host

Группа

-

Инциденты активна

Текстовый поиск

Строгий поиск

Срочность

Название

Обновлено

0.15

Перебор паролей

2025-09-17 15:24:24

0.95

Расширенное многовекторное обнаружение угроз VNC

2025-09-15 12:47:04

0.98

Расширенное многовекторное обнаружение угроз VNC

2025-09-15 12:47:05

0.49

Попытка модификации процесса аутентификации в системе

2025-09-15 19:03:20

0.95

Windows-AD: Многочисленные неуспешные аутентификации с...

2025-09-17 15:11:03

1

50 / страница

Результат анализа

VNC подозрительная активность: VNC_LATERAL_MOVEMENT

Пользователь: dc1\$@ru

Узел: dc1

Происшествия

Показать в событиях

Выбрано: 0

FQDN

dc1

IP

127.0.0.1

Отправлено в...

Нет

Начало...

2025-09-19 08:56:11

Конец...

2025-09-19 08:56:11

ID

6f8e2a42-9f40-48dc...

MAC

-

1

50 / страница

Дополнительные поля

Название

Значение

user_privilege_level

2

vnc_type

ultravnc

1

50 / страница

История коммуникации

Добавить комментарий

1 комментарий

Сортировка

↑

Время

23.09.2025 08:19:32

Тестовый комментарий

admin

1

Рис. 63 – 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.
- Дополнительные поля – список дополнительных полей, добавленных в 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. 64».

Расширенное многовекторное обнаружение угроз VNC

! Правило корреляции выявило подозрительную активность VNC-процессов (UltraVNC, TightVNC, RealVNC, VNC4) с анализом системных событий Windows Security Log (4656/4658/4663/4624/4625/4648/4672). Обнаруженные типы угроз: • APT (Advanced Persistent Threat) - долгосрочная компрометация с установкой постоянного и сбором учетных данных • Брутфорс-атаки - интенсивная активность с подозрительными масками доступа к системным объектам • Латеральное движение - распространение угрозы по множественным хостам инфраструктуры • Повышение привилегий - несанкционированный доступ к критическим системным компонентам • Установка постоянного - модификации автозагрузки, служб и системных компонентов Анализ включает: - Мониторинг доступа к 24+ критическим объектам реестра (LSA, SAM, службы, сетевые параметры) - Классификацию пользователей по уровню привилегий (система, администраторы, службы) - Корреляцию событий в 3-минутном временном окне - Детекцию опасных операций записи с масками доступа 0x2, 0x4, 0x20019 Техника MITRE ATT&CK: T1021.005 (Remote Services: VNC) + смежные техники T1110, T1078, T1134, T1547, T1543, T1055, T1082.

9.6

Источник: Коррелятор

Кол-во повторных открытий: 0

Кол-во происшествий: 1

Правило корреляции: [Windows - VNC Multi-Vector Detection](#)

Дата создания	19.09.2025 08:56:13
Тип инцидента	Расширенное многовекторное обнаружение угроз VNC
	Показать описание
Последнее происшествие	19.09.2025 08:56:11
Группа инцидентов	VNC_Advanced_Bruteforce_Attack
Назначенный пользователь	-
Назначенная группа пользователей	-
Категория	Сетевая аномалия
Время повторного открытия	-
Техники Mitre (для группы инцидентов)	https://attack.mitre.org/techniques/T1021/005 https://attack.mitre.org/techniques/T1110 https://attack.mitre.org/techniques/T1082
Краткое описание	Обнаружена многовекторная угроза через VNC-подключения с признаками APT-активности, брутфорс-атак, латерального движения или повышения привилегий.

[Показать меньше](#) ^

Рис. 64 – 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 значения: 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.
 - Группа инцидентов – наименование группы инцидентов, к которой принадлежит инцидент.
 - Назначенный пользователь / Назначенная группа пользователей – информация о пользователях / группе пользователей, которым назначен инцидент.
 - Категория – категория, к которой относится инцидент: нарушение политики, сетевая аномалия, уязвимость.
 - Дата и время повторного открытия.
 - Перечень техник Mitre, которые могут быть применены злоумышленниками для реализации данной угрозы (указываются для группы инцидентов).
 - Краткое описание угрозы.

6.1.3.2 Информация об активе

Пример блока с информацией об активе приведен на «[Рис. 65](#)».

Актив

3

Название: **dc1**

Тип

Host

Группа

-

Инциденты актива ^

Текстовый поиск

☐ Строгий поиск

Срочность <div>↓↑</div>	Название <div>↓↑</div>	Обновлено <div>↓↑</div>
0.49	Попытка модификации процесса аутентификации в системе	2025-09-23 03:30:28
0.22	Маскировка	2025-09-22 23:04:39
0.98	Расширенное многовекторное обнаружение угроз VNC	2025-09-19 08:56:13
0.92	Расширенное многовекторное обнаружение угроз VNC	2025-09-19 08:56:14
0.95	Расширенное многовекторное обнаружение угроз VNC	2025-09-19 08:56:14
0.95	Windows-AD: Многочисленные неуспешные аутентификации с...	2025-09-22 13:58:52

<

1

>

50 / страница

Рис. 65 -- 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.
- Перечень инцидентов, выявленных на активе.

6.1.3.3 Результат анализа

Пример блока с информацией о результатах анализа приведен на рисунке «Рис. 66».

Результат анализа

VNC расширенная брутфорс-атака обнаружена!

Пользователь: dc1\$@spy (regular)

Процесс: C:\Program Files\uvnc bvba\UltraVNC\winvnc.exe (ultravnc)

Узел: dc1

Активность: 56 событий за 3m

Handle операций: 48

Опасных операций: 0

Критических объектов: 24

Индикаторы: high_frequency, handle_operations, registry_access, network_scanning

Рекомендация: Немедленная блокировка VNC доступа

Рис. 66 – Просмотр инцидента. Результат анализа

В блоке отображается информация, заполненная ответственным специалистом при ручном создании инцидента.

6.1.3.4 Информация о происшествиях

Пример блока с информацией о происшествиях приведен на «Рис. 67».








Происшествия								
Показать в событиях					Выбрано: 0			
<input type="checkbox"/>	FQDN	IP	MAC	ID	Отправлено в...	Начало активности	Конец активности	
<input type="checkbox"/>	dc1	127.0.0.1	-	6f8e2a42-9f40-48dc-aaf8-10fb893feb1c	Нет	2025-09-19 08:56:11	2025-09-19 08:56:11	  
<input type="checkbox"/>	dc1	127.0.0.1	-	10fb893feb1c0-aaf8-9f40-10fb6f8e2a42	Нет	2025-09-19 08:56:11	2025-09-19 08:56:11	  
<div>< 1 > 50 / страница</div>								

Рис. 67 – Просмотр инцидента. Информация о происшествиях

В блоке отображается следующая информация:

- FQDN – FQDN актива, на котором выявлено происшествие;
- IP – IP-адрес актива, на котором выявлено происшествие;
- MAC – MAC-адрес актива, на котором выявлено происшествие;
- ID – уникальный идентификатор происшествия;
- Отправлено в ... – признак отправки происшествия во внешнюю систему реагирования на компьютерные инциденты (подробнее см. раздел «[Происшествия на отправку](#)»);
- Начало активности – дата и время начала активности происшествия;
- Конец активности – дата и время 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. 68»).



Рис. 68 – 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. 69»).

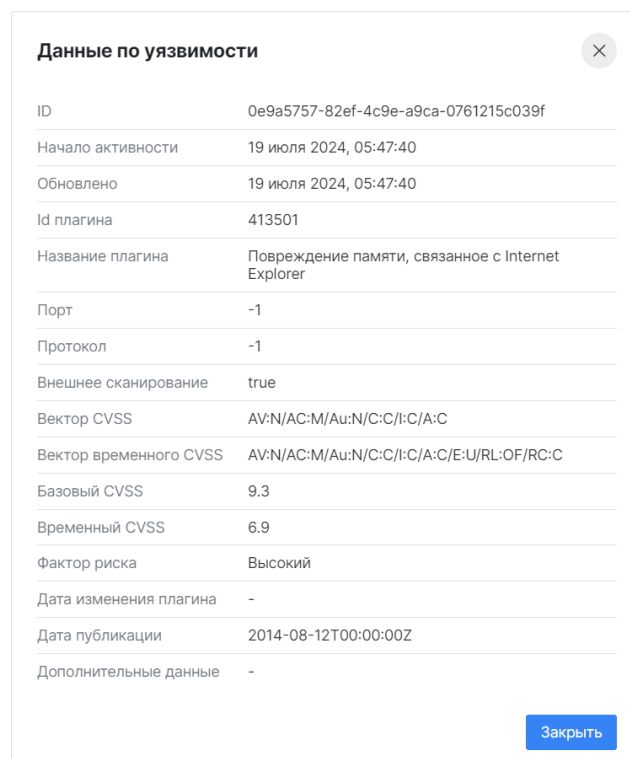


Рис. 69 – Окно "Данные по уязвимости"

6.1.3.5 История коммуникации

Пример блока с информацией об истории коммуникации приведен на «Рис. 70».

История коммуникации Добавить комментарий 2 комментария ^

12 сент. 2024, 12:09:31 Инцидент взять в работу
admin

12 сент. 2024, 12:09:48 Инцидент передан. Итоги в файле
admin

2024-09-12T12:06:48+03:00_итор.pdf

Рис. 70 -- 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. 71»).

Назначить ✕

☒ Назначить пользователю ☐ Назначить группе

admin ▾

Сохранить

Рис. 71 – 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. 72»)

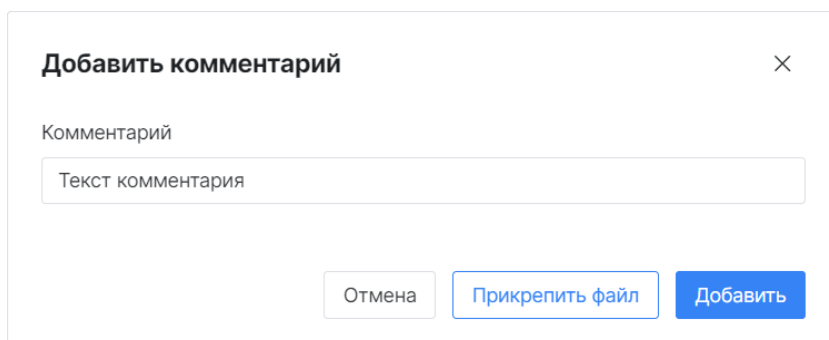



Рис. 72 – Окно "Добавить комментарий"

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 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. 73»).

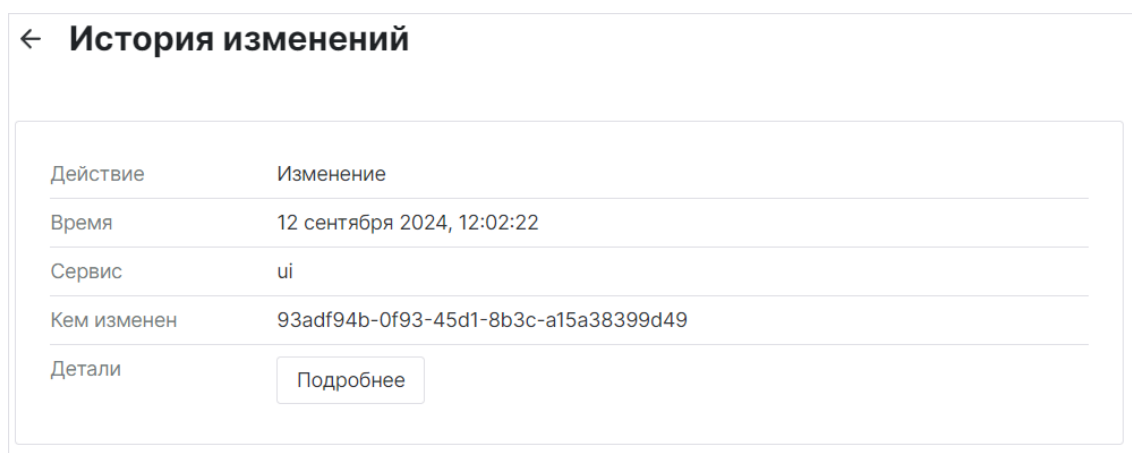


Рис. 73 – История изменений"

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.

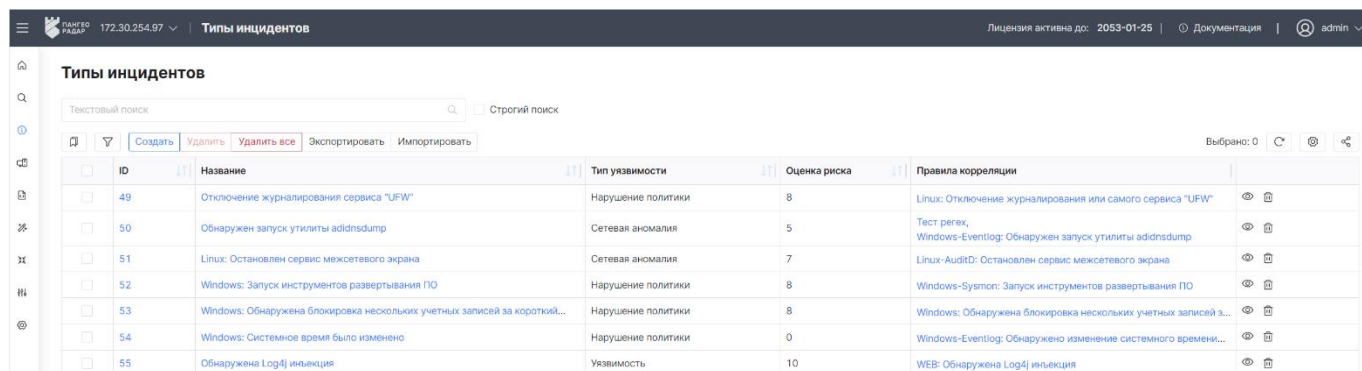
Тип инцидента всегда принадлежит к одному из трех типов уязвимостей:

- 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. [«Импорт типов инцидентов»](#).
7. [«Экспорт типов инцидентов»](#).
8. [«Экспорт типов инцидентов в CSV»](#).
9. [«Удаление типа инцидента»](#).

Для работы с типами инцидентов перейдите в раздел **Инциденты → Типы инцидентов** (см. «Рис. 74»).



ID	Название	Тип уязвимости	Оценка риска	Правила корреляции
49	Отключение журналирования сервиса "UFW"	Нарушение политики	8	Linux: Отключение журналирования или самого сервиса "UFW"
50	Обнаружен запуск утилиты adidnsdump	Сетевая аномалия	5	Test regex, Windows-Eventlog: Обнаружен запуск утилиты adidnsdump
51	Linux: Остановлен сервис межсетевого экрана	Сетевая аномалия	7	Linux-AuditD: Остановлен сервис межсетевого экрана
52	Windows: Запуск инструментов развертывания ПО	Нарушение политики	8	Windows-Sysmon: Запуск инструментов развертывания ПО
53	Windows: Обнаружена блокировка нескольких учетных записей за короткий...	Нарушение политики	8	Windows: Обнаружена блокировка нескольких учетных записей з...
54	Windows: Системное время было изменено	Нарушение политики	0	Windows-Eventlog: Обнаружено изменение системного времени...
55	Обнаружена Log4j инъекция	Уязвимость	10	WEB: Обнаружена Log4j инъекция

Рис. 74 – 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. 75](#)»).

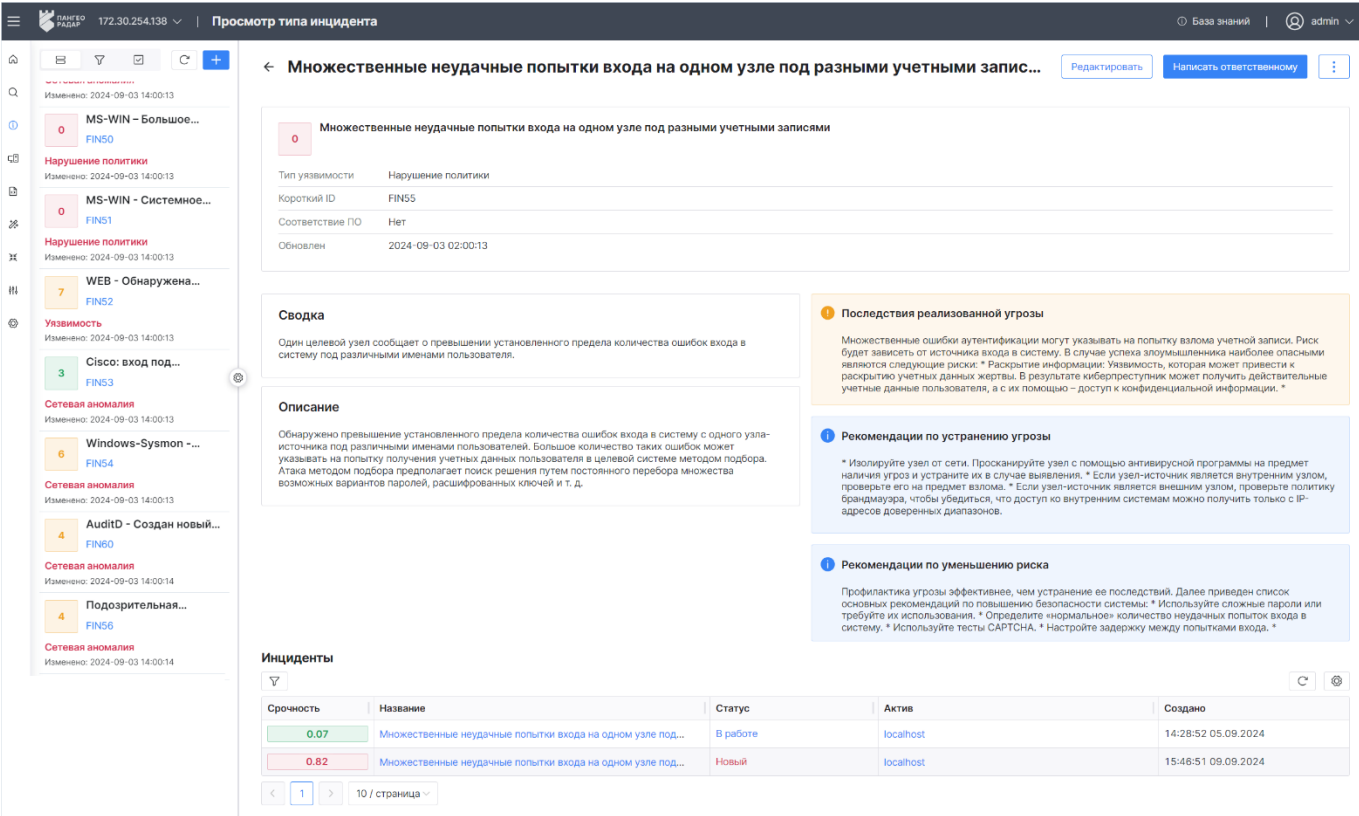


Рис. 75 – Форма просмотра типа инцидента

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 определяется 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.

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. 76](#)»).

Создание типа инцидента Сбросить Создать

Название *

Тип уязвимости *

☐ Использовать для создания инцидентов при оценке соответствия ПО

Краткое описание *

Описание

Последствия реализованной угрозы

Рекомендации по устранению угрозы *

Рекомендации по уменьшению риска

Внутренняя заметка

Оценка риска

Комментарий

Рис. 76 – 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 относиться 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 **Краткое описание** 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. 77»](#)).

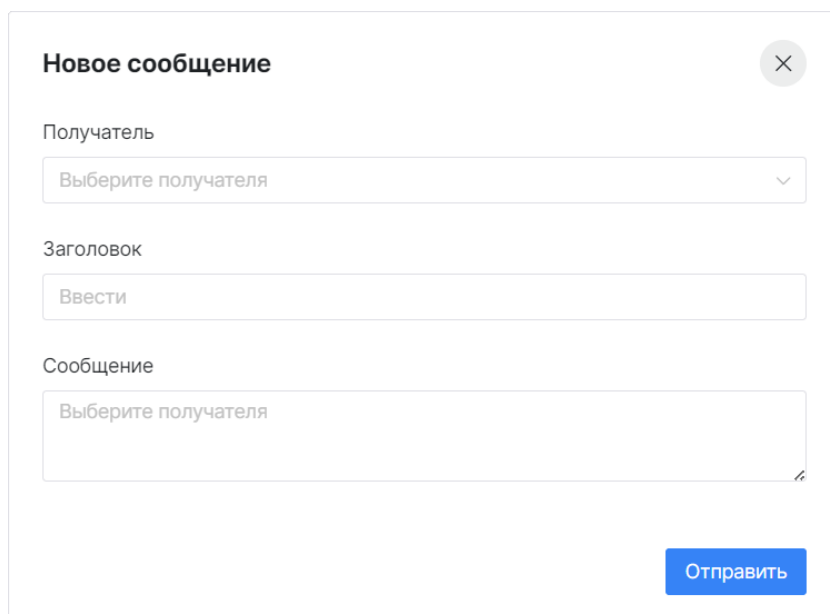


Рис. 77 – Окно "Новое сообщение"

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

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.

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.

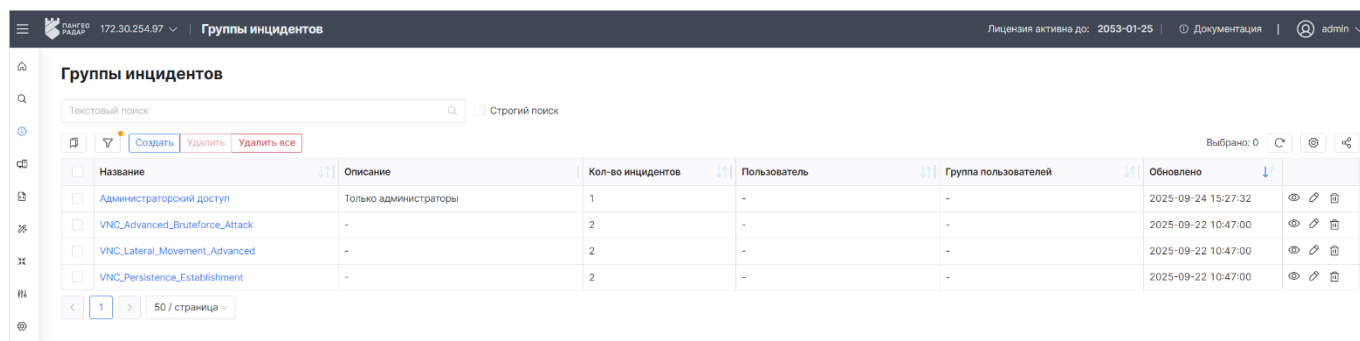
Группа инцидентов может быть создана одним из следующих способов:

- 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. 78»).




Группы инцидентов						
Текстовый поиск						
Создать Удалить Удалить все						
Выбрано: 0						
<input type="checkbox"/>	Название	Описание	Кол-во инцидентов	Пользователь	Группа пользователей	Обновлено
<input type="checkbox"/>	Администраторский доступ	Только администраторы	1	-	-	2025-09-24 15:27:32
<input type="checkbox"/>	VNC_Advanced_BruteForce_Attack	-	2	-	-	2025-09-22 10:47:00
<input type="checkbox"/>	VNC_Lateral_Movement_Advanced	-	2	-	-	2025-09-22 10:47:00
<input type="checkbox"/>	VNC_Persistence_Establishment	-	2	-	-	2025-09-22 10:47:00

Рис. 78 – 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. 79»).

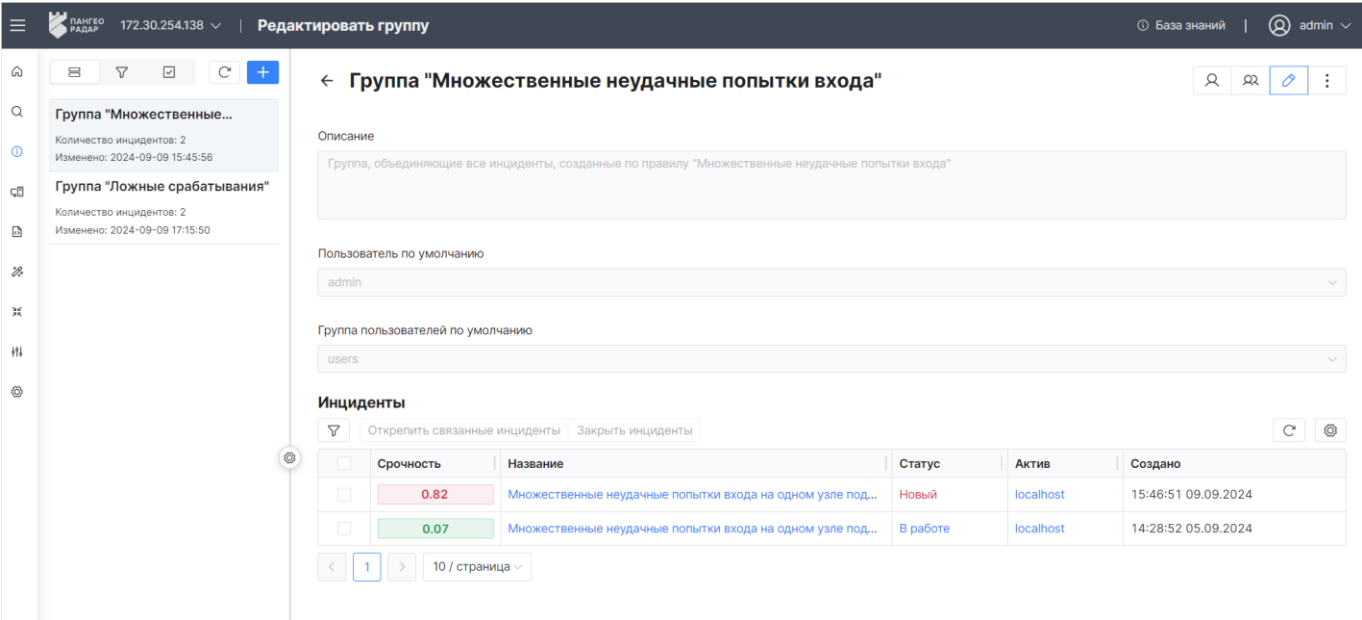


Рис. 79 – Форма просмотра группы инцидентов

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** – цветное 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. 80](#)»).

Создать группу инцидентов Сбросить Создать

Название
Ложные срабатывания

Описание
Здесь помещаются инциденты, признанные как "Ложное срабатывание"

Пользователь по умолчанию
admin

Группа пользователей по умолчанию
users

Рис. 80 – 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. [Просмотр значений дополнительного поля.](#)
2. [Создание дополнительного поля.](#)
3. [Редактирование дополнительного поля.](#)
4. [Добавление дополнительного поля в инцидент.](#)
5. [Удаление дополнительного поля.](#)

Для работы с дополнительными полями перейдите в раздел **Инциденты** → **Дополнительные поля** (см. «[Рис. 81](#)»).

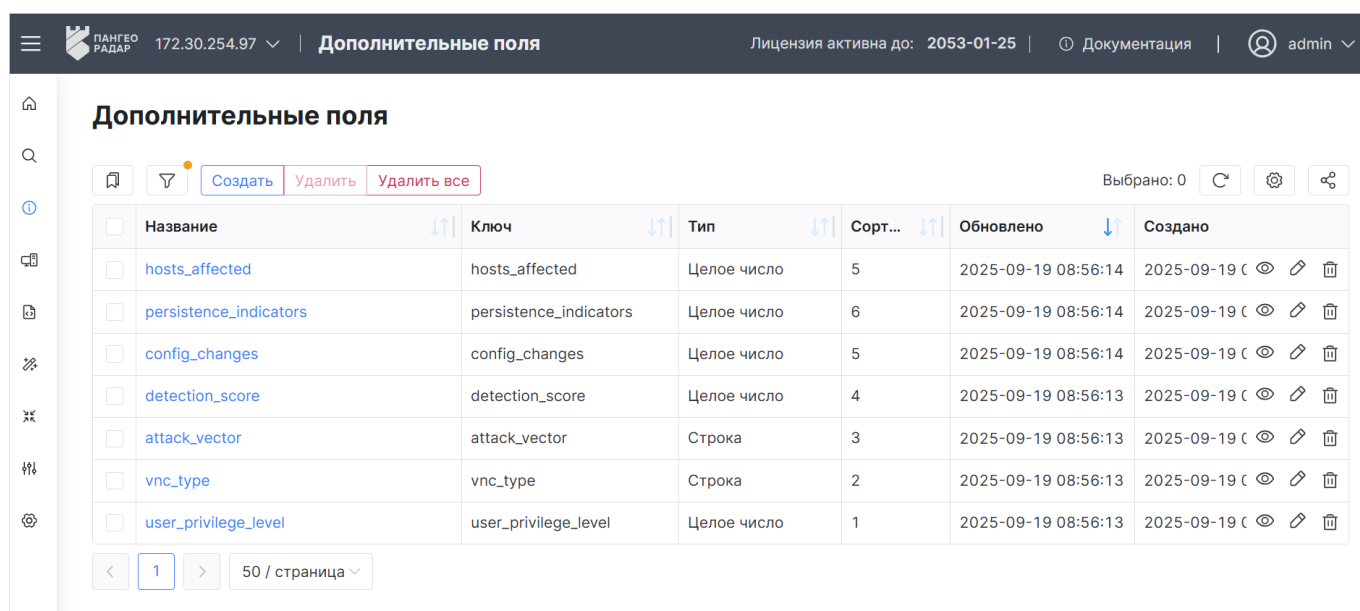



Рис. 81 – Раздел "Дополнительные поля"

В разделе отображается следующая информация:

- **Название** – название дополнительного поля. По ссылке произойдет переход на страницу просмотра дополнительного поля;
- **Ключ** – уникальный ключ, идентифицирующий поле. Данный ключ можно использовать при ручной настройке правил корреляции в секции alert (см. руководство «Описание редактора Lua для правил корреляции»);
- **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.

6.5.1 Просмотр значений дополнительного поля

Для просмотра дополнительного поля нажмите кнопку  в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного дополнительного поля (см. «Рис. 82»).

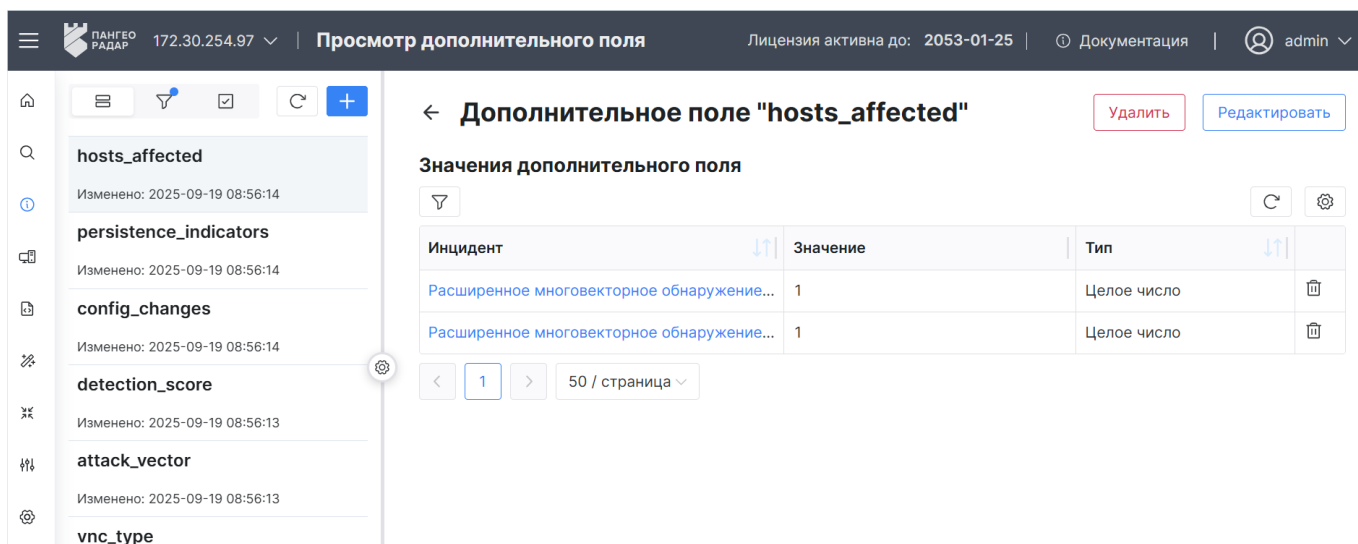



Рис. 82 – Страница просмотра дополнительного поля

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;
- **Тип** – тип данных, который указан в поле.

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

6.5.2 Создание дополнительного поля

1. Нажмите на кнопку **Создать**. Откроется форма "Создание дополнительного поля" (см. «Рис. 83»).

Рис. 83 – 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**.

6.5.3 Редактирование дополнительного поля

1. Начните процесс редактирования дополнительного поля через «[универсальные таблицы](#)» или инструмент «[боковая панель](#)».
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

6.5.4 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.

6.5.5 Удаление дополнительного поля

1. Начните процесс удаления дополнительного поля через «[универсальные таблицы](#)» или инструмент «[боковая панель](#)».
2. Подтвердите удаление в открывшемся окне.
3. Группа инцидентов будет удалена из платформы.

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 трафик, 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.

В зависимости от способа передачи трафика, активы делятся на следующие типы:

- Node – актив, который является частью платформы. Создается при добавлении новых узлов к платформе;
- Host – актив, который не является частью платформы. Может быть соединен с другими устройствами компании как часть компьютерной сети, так и предоставлять сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам.

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 – не критичный. 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. «[Экспорт активов](#)».
7. «[Объединение активов](#)».
8. «[Активация/деактивация активов](#)».
9. «[Настройка параметров активов](#)».
10. «[Удаление актива](#)».

Для работы с активами перейдите в раздел **Активы** → **Активы** (см. «[Рис. 84](#)»).

Уров...	Тип	Название	Сетевые интерфейсы	Операциона...	Группы активов	Располо...	Открыт...	Риск...	Закры...	Обновлено	Создано	
9.60	Host	dc1	dc1	Linux 5.0 - 5.4	-	-	7	0	0	2025-09-19 08:56:13	2025-09-19 08:56:13	
9.60	Host	dc1	dc1	Linux 5.0 - 5.4	-	-	6	0	0	2025-09-22 10:47:00	2025-09-22 10:47:00	
9.60	Host	z	z	Linux 5.0 - 5.4	-	-	2	0	0	2025-09-19 09:39:22	2025-09-19 09:39:22	
9.60	Host	172.30.252.109	172.30.252.109	Linux 5.0 - 5.4	-	-	2	0	0	2025-09-24 11:37:58	2025-09-24 11:37:58	
9.60	Host	172.30.254.151	172.30.254.151	Linux 5.0 - 5.4	-	-	2	0	0	2025-09-19 09:21:59	2025-09-19 09:21:59	
9.60	Host	172.30.250.107	172.30.250.107	Linux 5.0 - 5.4	-	-	2	0	0	2025-09-19 15:16:21	2025-09-19 15:16:21	


Рис. 84 – 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. 85»).

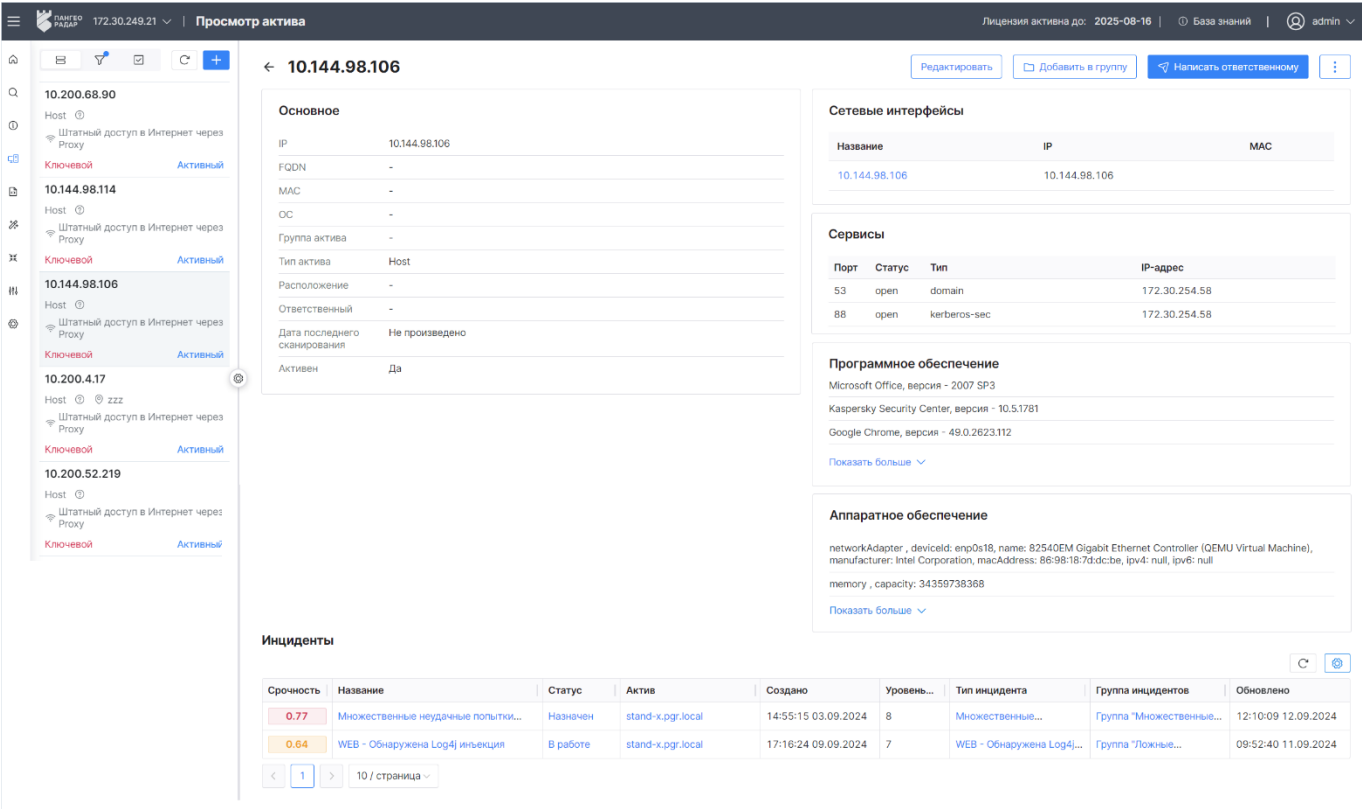


Рис. 85 – Форма просмотра актива

В боковой панели отображается следующая информация об активах:

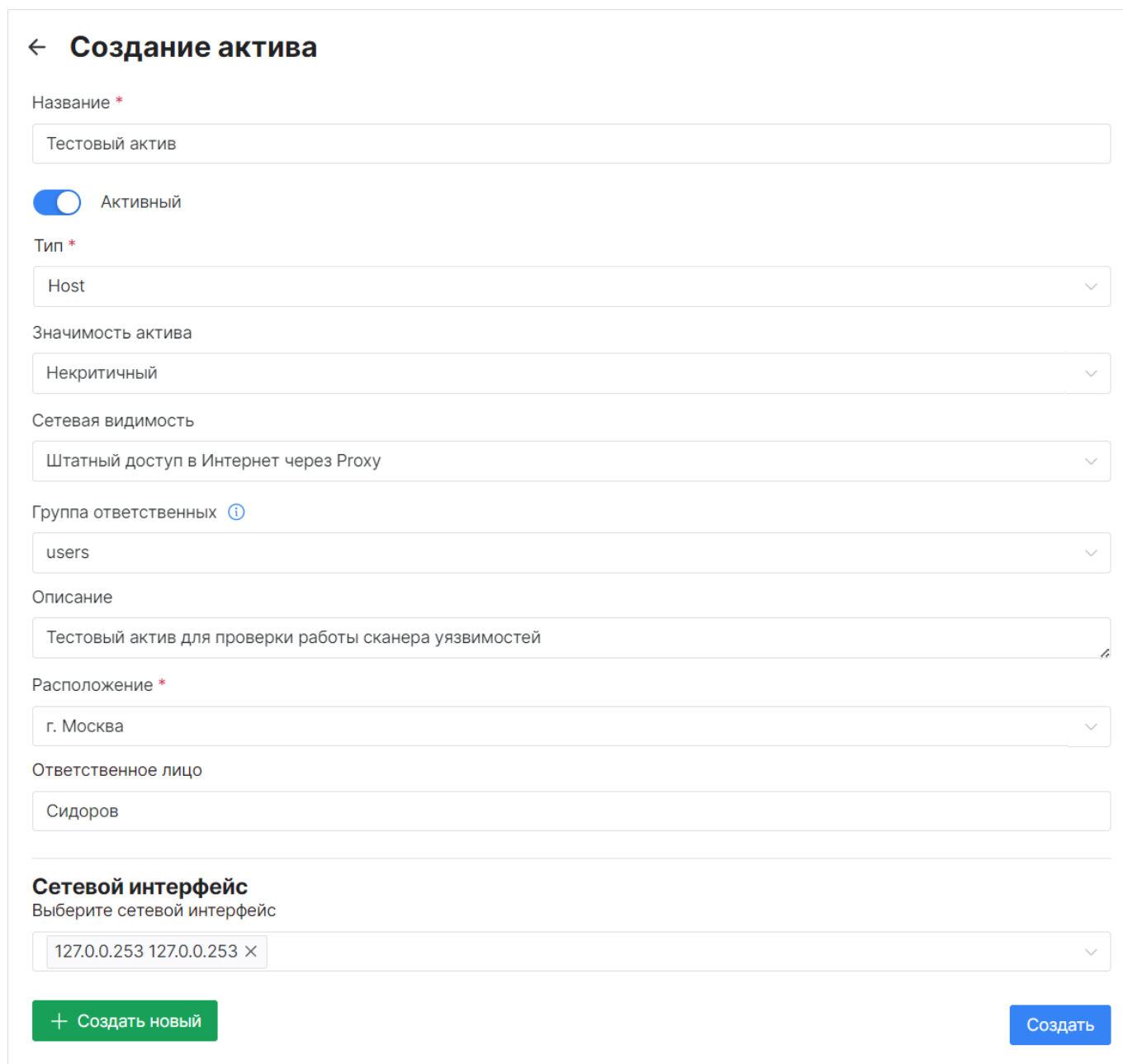
- Наименование актива;
- Тип актива;
- Расположение актива;
- Сетевая видимость актива;
- Значимость актива;
- Состояние актива.

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 **Сервисы** отображается информация о сервисах, обнаруженных на активе:
 - Номер порта, который использует сервис;
 - Статус сервиса (open, close и т.д.);
 - Тип сервиса (ldap, domain, msrpc и т.д.);
 - IP-адрес, на котором обнаружен сервис.
- 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. 86](#)»).



← **Создание актива**

Название *

Тестовый актив

☒ Активный

Тип *

Host

Значимость актива

Некритичный

Сетевая видимость

Штатный доступ в Интернет через Proxy

Группа ответственных ⓘ

users

Описание

Тестовый актив для проверки работы сканера уязвимостей

Расположение *

г. Москва

Ответственное лицо

Сидоров

Сетевой интерфейс
Выберите сетевой интерфейс

127.0.0.253 127.0.0.253 ×

+ Создать новый

Создать

Рис. 86 – 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** из выпадающего списка выберите тип актива: Host, Node;
 - 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** из выпадающего списка выберите 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. 87](#)»).

Новое сообщение

Получатель

Выберите получателя

Заголовок

Ввести

Сообщение

Выберите получателя

Отправить

Рис. 87 – 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 Экспорт активов

1. Начните процесс экспорта активов через [«универсальные таблицы»](#) или инструмент [«боковая панель»](#).
2. Будет сформирован файл с информацией об активах в формате CSV.
3. Укажите путь для сохранения файла и нажмите кнопку **Сохранить**.

7.1.8 Объединение активов

Данная функция позволяет объединить несколько активов, информация о которых была получена из различных источников, в один. Выполните следующие действия:

1. В универсальной таблице раздела выберите необходимые активы, установив флаги в соответствующих строках таблицы.
2. Нажмите кнопку **Объединить**.
3. Подтвердите действие в открывшемся окне.

Будет выполнено объединение активов по следующим правилам:

- основным активом считается актив, у которого более ранняя дата создания;
- остальные активы считаются активами дублерами;
- в случае наличия значения в поле у одной карточки актива и отсутствия в другой карточке актива – записывается значение из карточки, где значение присутствует;
- в случае, если значение в поле присутствует в обеих карточках активов, создаётся конфликт и добавляется соответствующая запись в таблицу конфликтов при объединении активов;
- при объединении активов будут объединены и соответствующие сетевые интерфейсы;
- все созданные инциденты будут перепривязаны к основному активу;
- основной актив будет добавлен во все группы, в которых находились активы дублеры;
- результирующая сетевая видимость основного актива будет равна наиболее высокой сетевой видимости активов дублеров;
- результирующая значимость основного актива будет равна наиболее высокой значимости активов дублеров;
- все результаты сканирований активов-дублёров сменят привязку на основной актив;
- списки программного и аппаратного обеспечения активов-дублёров будут добавлены в соответствующие списки основного актива.

7.1.9 Активация/деактивация активов

1. В универсальной таблице раздела выберите необходимые активы, установив флаги в соответствующих строках таблицы.
2. Нажмите кнопку **Активация/деактивация** и из выпадающего списка выберите необходимое действие.
3. Подтвердите действие в открывшемся окне. Состояние актива будет изменено.

7.1.10 Настройка параметров активов

Данная функция позволяет массово изменить следующие параметры активов:

- **Значимость** – в платформе значимость актива может принимать следующие значения:
 - **Ключевой** – актив обеспечивает функционирование бизнеса;
 - **Важный** – актив обеспечивает штатную работу компании;
 - **Некритичный** – актив не влияет на штатную работу компании;
 - **Распределенный** – актив находится в составе распределенной системы, которая не задействована в бизнес-процессах;
 - **Тестовый** – актив располагается в тестовой среде. Недоступность данного актива не влияет ни на бизнес-процессы, ни на штатную работу компании.
- **Сетевая видимость** – тип сетевой видимости актива. Может принимать следующие значения:

- **Прямое подключение к интернету** – актив напрямую подключен к сети Интернет;
- **DMZ, частичный доступ из Интернета** – актив располагается в демилитаризованной зоне (DMZ);
- **Штатный доступ в Интернет через Proxy** – актив подключен к сети Интернет через Proxy-сервер;
- **Ограниченный доступ в Интернет** – актив имеет ограниченный доступ к сети Интернет и к ограниченному набору онлайн-сервисов. Например, тонкие клиенты, POS-терминалы, удаленные офисы;
- **Нет подключения к сети** – актив не подключен к сети.
- **Расположение** – информация о физическом расположении актива (например, *Москва*).

Выполните следующие действия:

1. В универсальной таблице раздела выберите необходимые активы, установив флаги в соответствующих строках таблицы.
2. Нажмите кнопку **Установить значение**. Откроется окно "Установка значений" (см. «[Рис. 88](#)»).

Установка значений ×

☒ Установить значимость

Значимость актива

Важный ▼

☒ Установить сетевую видимость

Сетевая видимость

DMZ, частичный доступ из Интернета ▼

☐ Установить расположение

Расположение

Выбрать ▼

Сбросить Сохранить

Рис. 88 – Окно "Установка значений"

3. Выполните в окне следующие действия:
 - включите переключатель у параметра, значение которого необходимо изменить. Значение остальных параметров, изменены не будут;

- из выпадающих списков **Значимость актива**, **Сетевая видимость** или **Расположение** выберите необходимое значение;
- нажмите кнопку **Сохранить**.

7.1.11 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. 89](#)»).

Название	Маски подсетей	Регулярное...	Кол-во...	Группа ответственных	Связанные группы...	Создано	Обновлено	КИИ
КИИ	170.30.254.0/24	-	1	users	admin, inventORIZATION	2025-09-24 15:37:23	2025-09-24 15:45:01	Да
Группа Линукс		-	1	admin	-	2025-09-24 15:36:59	2025-09-24 15:42:40	Нет

Рис. 89 – 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 ли 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. 90](#)»).

←

Создание группы актива

Сбросить

Создать

Название

Распределенные активы

Настройки автоматического добавления активов в группу ⓘ

Маски подсетей в CIDR-нотации (например 192.168.0.0/24)

+ Создать

Регулярное выражение для FQDN

Regex

Справка по регулярным выражениям

Группы пользователей

Группа ответственных ⓘ

users

Связанные группы пользователей

admin × inventORIZATION ×

ID объекта

534

ID субъекта

45

ID системы

55

☐ КИИ

Ответственное лицо

Смирнов

Технический специалист

Афанасьев

Ассоциации

Актив

localhost ×

Набор правил

Выбрать

Рис. 90 –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 внешней системой, 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. 91](#)»).

← Fully Qualified Domain Names

Редактировать Написать ответственному

Основное

Название Fully Qualified Domain Names

Маска подсети -

Группа ответственных admin

Активы Инциденты

Уровень риска	Название	Обновлено	Создано
0.77	localhost	14:55:13 03.09.2024	14:55:13 03.09.2024
0.77	stand-x.pgr.local	14:55:15 03.09.2024	14:55:15 03.09.2024

1 10 / страница

Рис. 91 – 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. 92](#)»).

← Fully Qualified Domain Names

Редактировать

Написать ответственному

Основное

Название

Fully Qualified Domain Names

Маска подсети

-

Группа ответственных

admin

Активы

Инциденты

↺

⚙

Срочность	Название	Статус	Актив	Создано	Уровень...	Группа инцидентов	Тип инцидента	Обновлено
0.00	AuditD - Остановлен демо...	Закрыт	localhost	16:32:09 12.09.2024	3	-	AuditD - Остановлен демон...	11:08:01 13.09.2024
0.64	WEB - Обнаружена Log4j...	В работе	stand-x.pgr.local	17:16:24 09.09.2024	7	Группа "Ложные срабатывания"	WEB - Обнаружена Log4j...	09:52:40 11.09.2024
0.00	Множественные неудачны...	Новый	localhost	15:46:51 09.09.2024	9	-	Множественные неудачные...	09:53:12 11.09.2024
0.07	Множественные неудачны...	В работе	localhost	14:28:52 05.09.2024	0.5	Группа "Множественные...	Множественные неудачные...	12:21:18 12.09.2024
0.00	MS-WIN - ...	Новый	localhost	17:17:01 09.09.2024	0	Группа "Ложные срабатывания"	MS-WIN - непривилегированный...	09:51:26 11.09.2024
0.07	MS-WIN - Для учетной...	В работе	localhost	14:37:16 05.09.2024	0.5	-	MS-WIN - Для учетной записи...	10:56:31 09.09.2024
0.77	Множественные неудачны...	Назначен	stand-x.pgr.local	14:55:15 03.09.2024	8	Группа "Множественные...	Множественные неудачные...	12:10:09 12.09.2024

<

1

>

10 / страница

Рис. 92 – 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. 93»).

Настройки автоматического добавления активов в группу ⓘ

Маски подсетей в CIDR-нотации (например 192.168.0.0/24)

192.168.0.0/24

−

+

Поля должны быть допустимыми cidr-адресами

Регулярное выражение для FQDN

(?:\V)(?=[1,255]\$)(([1,63]\.){1,127}(?![0-9]*\$)[a-z0-9-]+\.)?

Справка по регулярным выражениям

Рис. 93 – 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. 94»).

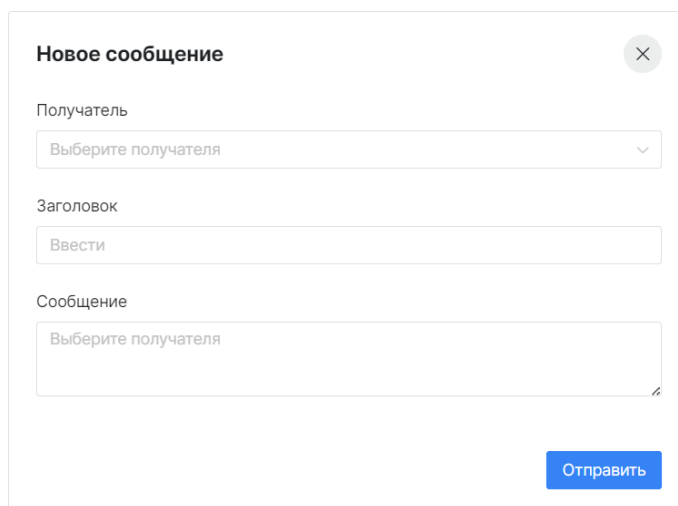


Рис. 94 – Окно "Новое сообщение"

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 удаления 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.

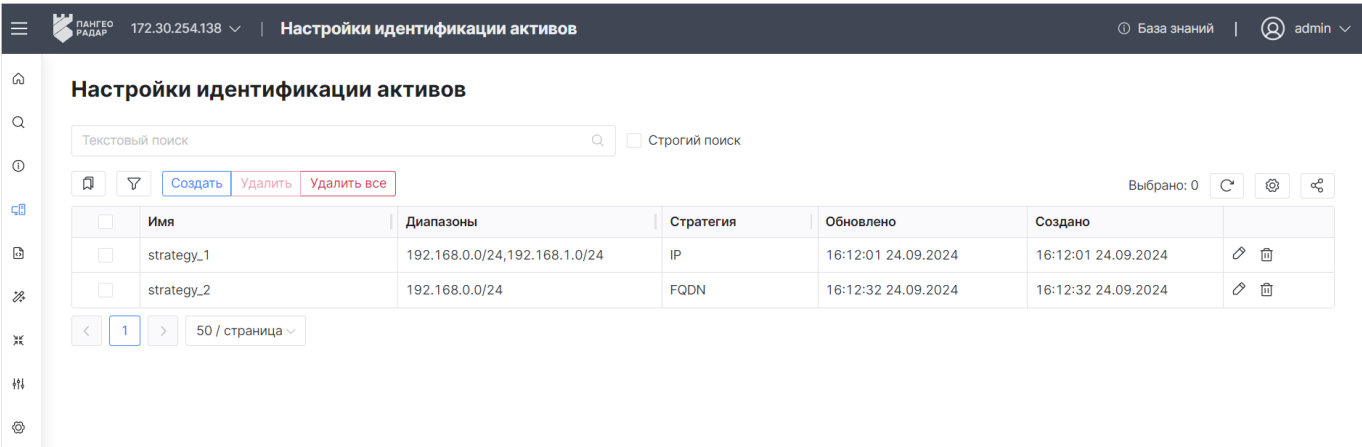
Стратегию сравнения можно настроить по следующим идентификаторам:

- **FQDN** – по полному доменному имени актива;
- **MAC** – по Мас-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. 95](#)»).







Имя	Диапазоны	Стратегия	Обновлено	Создано	
strategy_1	192.168.0.0/24,192.168.1.0/24	IP	16:12:01 24.09.2024	16:12:01 24.09.2024	 
strategy_2	192.168.0.0/24	FQDN	16:12:32 24.09.2024	16:12:32 24.09.2024	 

Рис. 95 – 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. 96»).

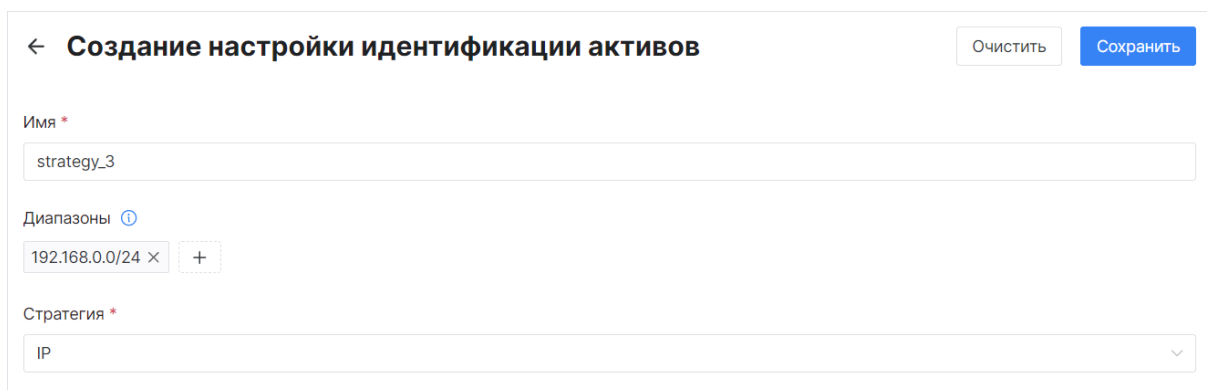



Рис. 96 – Окно "Создание настройки идентификации активов"

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 удаления 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. 97](#)»).


Название	MAC-адрес	IP-адрес	FQDN	Операционная...	Актив	Обновлено	Создано
172.30.252.109	-	172.30.252.109	-	-	172.30.252.109	2025-09-24 11:37:58	2025-09-24 11:37:58
199.232.210.172	-	199.232.210.172	-	-	199.232.210.172	2025-09-22 10:53:41	2025-09-22 10:53:41
172.30.252.105	f2:ed:6f:b4:e4:4e	172.30.252.105	-	Linux 5.0 - 5.4	172.30.252.105	2025-09-22 17:55:27	2025-09-22 10:47:05
172.30.249.42	-	172.30.249.42	-	-	172.30.249.42	2025-09-22 10:47:05	2025-09-22 10:47:05
dc1	-	-	dc1	-	dc1	2025-09-22 10:47:00	2025-09-22 10:47:00
172.30.253.105	-	172.30.253.105	-	-	172.30.253.105	2025-09-21 14:48:56	2025-09-21 14:48:56

Рис. 97 – 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. 98](#)»).

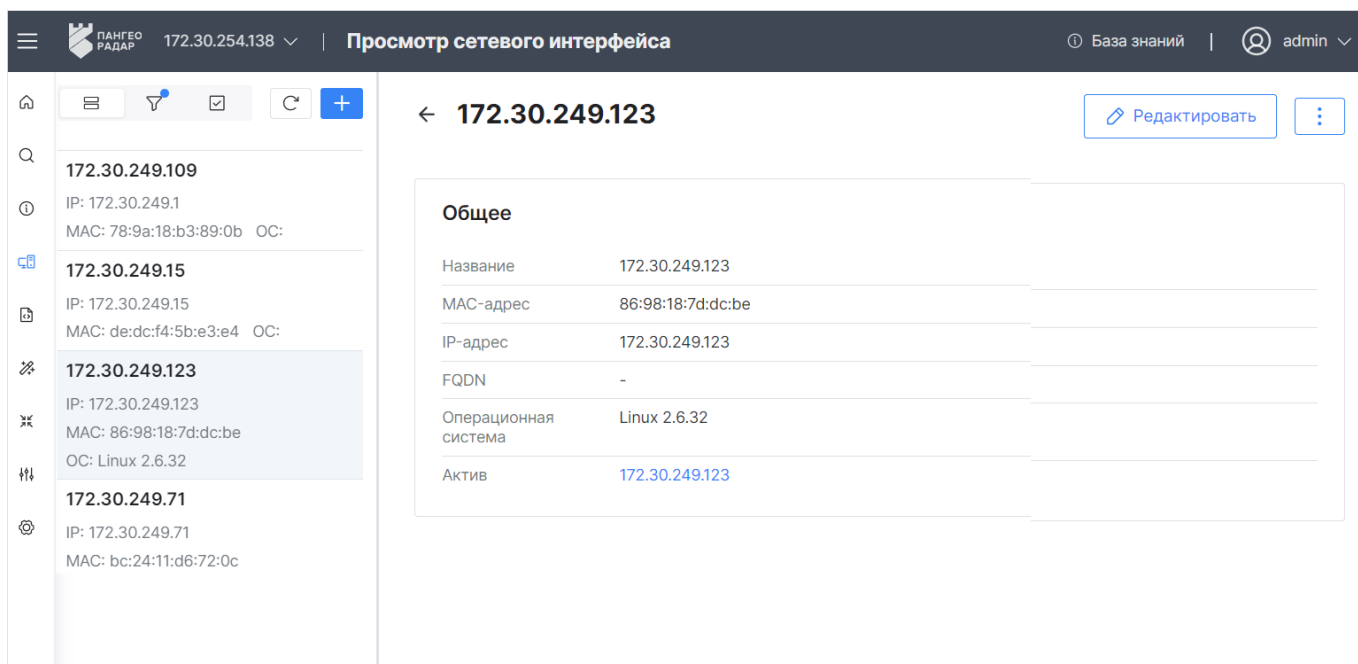


Рис. 98 – Форма просмотра сетевого интерфейса

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. 99](#)»).

← **Создание сетевого интерфейса** Сбросить Создать

Название *
test

MAC-адрес *
de:dc:f4:5b:e3:e4

IP-адрес *
172.30.249.15

FQDN *
stand-x.pgr.local × +

Операционная система
Windows

Активы
172.30.249.15

Рис. 99 – 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

1. Начните процесс удаления сетевого интерфейса через «[универсальные таблицы](#)» или инструмент «[боковая панель](#)».
2. Подтвердите удаление в открывшемся окне.
3. 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. 100](#)»).

Имя файла	Тип отчета	Создано	Обновлено	
2024-08-...	redcheck	11:06:07 29.08.2024	11:06:07 29.08.2024	⬇️ ⌂
2024-09-12T18:39:49+03:00_scan-rep.xml	redcheck	18:39:49 12.09.2024	18:39:49 12.09.2024	⬇️ ⌂
2024-09-13T14:55:41+03:00_scan-rep.xml	redcheck	14:55:41 13.09.2024	14:55:41 13.09.2024	⬇️ ⌂
2024-09-13T14:56:31+03:00_MP8_Audit.xml_parsing_error	redcheck	14:56:31 13.09.2024	14:56:31 13.09.2024	⬇️ ⌂

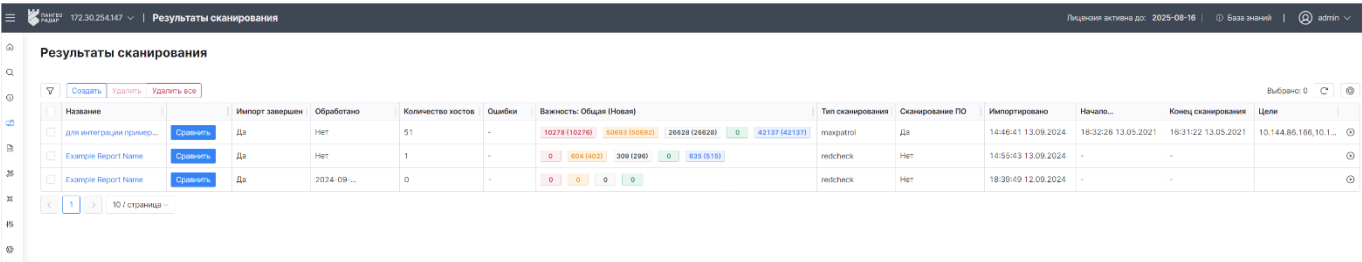
Рис. 100 – Форма импорта результатов сканирования

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. 101»).




Название	Импорт завершен	Обработано	Количество хостов	Ошибки	Важность: Общая (Новая)	Тип сканирования	Сканирование ПО	Импортировано	Начало...	Конец сканирования	Цели
для интеграции пример...	Да	Нет	51	-	10278 (10278) 30683 (30683) 26828 (26828) 42137 (42137)	maxpatrol	Да	14:46:41 13.09.2024	18:32:28 13.05.2021	18:31:22 13.05.2021	10.144.86.186, 10.1...
Example Report Name	Да	Нет	1	-	0 604 (604) 309 (309) 0 639 (639)	redcheck	Нет	14:55:43 13.09.2024	-	-	
Example Report Name	Да	2024-09...	0	-	0 0 0 0	redcheck	Нет	18:30:49 12.09.2024	-	-	

Рис. 101 – 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. 102»).

← пример xml отчета Audit

Основное

Тип сканирования:

maxpatrol

Начало сканирования:

2021-05-13 18:32:26

Конец сканирования:

2021-05-13 16:31:22

Обработано:

Импорт завершен:

Да

Наличие уязвимостей:

Да

Сканирование ПО:

Да

Путь сканирования:

/opt/pangeoradar/cruddy/imports/maxpatrol/archive/2024-09-13T14:58:50+03:00_MP8_Audit.xml

Найдено уязвимостей:

129736

Количество хостов:

51

Уязвимости по важности:

10278 (10276)

50693 (50692)

26628 (26628)

0

42137 (42137)

Хосты

Хосты с ошибкой

С

⚙

FQDN	IP	MAC	Количество уязвимостей	Важность 4	Важность 3	Важность 2	Важность 1	Важность 0	Установле...	Начало сканирования	Конец сканирования
	10.144.86.166		0	0	0	0	0	0	0	16:03:14 13.05.2021	16:31:22 13.05.2021
	10.144.87.122		0	0	0	0	0	0	0	16:03:56 13.05.2021	16:48:04 13.05.2021
	10.144.96.216		0	0	0	0	0	0	0	16:07:13 13.05.2021	16:56:22 13.05.2021
	10.144.87.131		0	0	0	0	0	0	0	16:15:11 13.05.2021	17:00:01 13.05.2021
	10.144.87.177		0	0	0	0	0	0	0	16:16:01 13.05.2021	16:59:44 13.05.2021
cta-belav2.main.oao.rzd	10.200.70.148		0	0	0	0	0	0	0	16:24:47 13.05.2021	17:02:52 13.05.2021
cta-milshnikov.main.oao.rzd	10.200.70.182		0	0	0	0	0	0	0	16:25:10 13.05.2021	16:49:42 13.05.2021
ctech-apolosov.main.oao.rzd	10.200.31.50		0	0	0	0	0	0	0	16:26:22 13.05.2021	16:55:22 13.05.2021
ctim-lukashkina.main.oao.rzd	10.200.229.159		0	0	0	0	0	0	0	16:30:38 13.05.2021	16:48:34 13.05.2021
ctib-burenko.main.oao.rzd	10.222.9.145		0	0	0	0	0	0	0	16:31:37 13.05.2021	17:22:43 13.05.2021

<

1

2

3

4

5

6

>

10 / страница

Рис. 102 – 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. 103».

Основное	
Тип сканирования:	maxpatrol
Начало сканирования:	2021-05-13 18:32:26
Конец сканирования:	2021-05-13 16:31:22
Обработано:	
Импорт завершен:	Да
Наличие уязвимостей:	Да
Сканирование ПО:	Да
Путь сканирования:	/opt/pangeoradar/cruddy/imports/maxpatrol/archive/2024-09-13T14:58:50+03:00_MP8_Audit.xml
Найдено уязвимостей:	129736
Количество хостов:	51
Уязвимости по важности:	<div>10278 (10276)</div> <div>50693 (50692)</div> <div>26628 (26628)</div> <div>0</div> <div>42137 (42137)</div>

Рис. 103 – 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. 104».

Хосты

Хосты с ошибкой

FQDN	IP	MAC	Количество уязвимостей	Важность 4	Важность 3	Важность 2	Важность 1	Важность 0	Установле...	Начало сканирования	Конец сканирования
	10.144.86.166		0	0	0	0	0	0	0	16:03:14 13.05.2021	16:31:22 13.05.2021
	10.144.87.122		0	0	0	0	0	0	0	16:03:56 13.05.2021	16:48:04 13.05.2021
	10.144.96.216		0	0	0	0	0	0	0	16:07:13 13.05.2021	16:56:22 13.05.2021
	10.144.87.131		0	0	0	0	0	0	0	16:15:11 13.05.2021	17:00:01 13.05.2021
	10.144.87.177		0	0	0	0	0	0	0	16:16:01 13.05.2021	16:59:44 13.05.2021
cta-belav2.main.oao.rzd	10.200.70.148		0	0	0	0	0	0	0	16:24:47 13.05.2021	17:02:52 13.05.2021
cta-milshnikov.main.oao.rzd	10.200.70.182		0	0	0	0	0	0	0	16:25:10 13.05.2021	16:49:42 13.05.2021
ctech-apolosov.main.oao.rzd	10.200.31.50		0	0	0	0	0	0	0	16:26:22 13.05.2021	16:55:22 13.05.2021
ctim-lukashkina.main.oao.rzd	10.200.229.159		0	0	0	0	0	0	0	16:30:38 13.05.2021	16:48:34 13.05.2021
ctib-burenko.main.oao.rzd	10.222.9.145		0	0	0	0	0	0	0	16:31:37 13.05.2021	17:22:43 13.05.2021

<

1

2

3

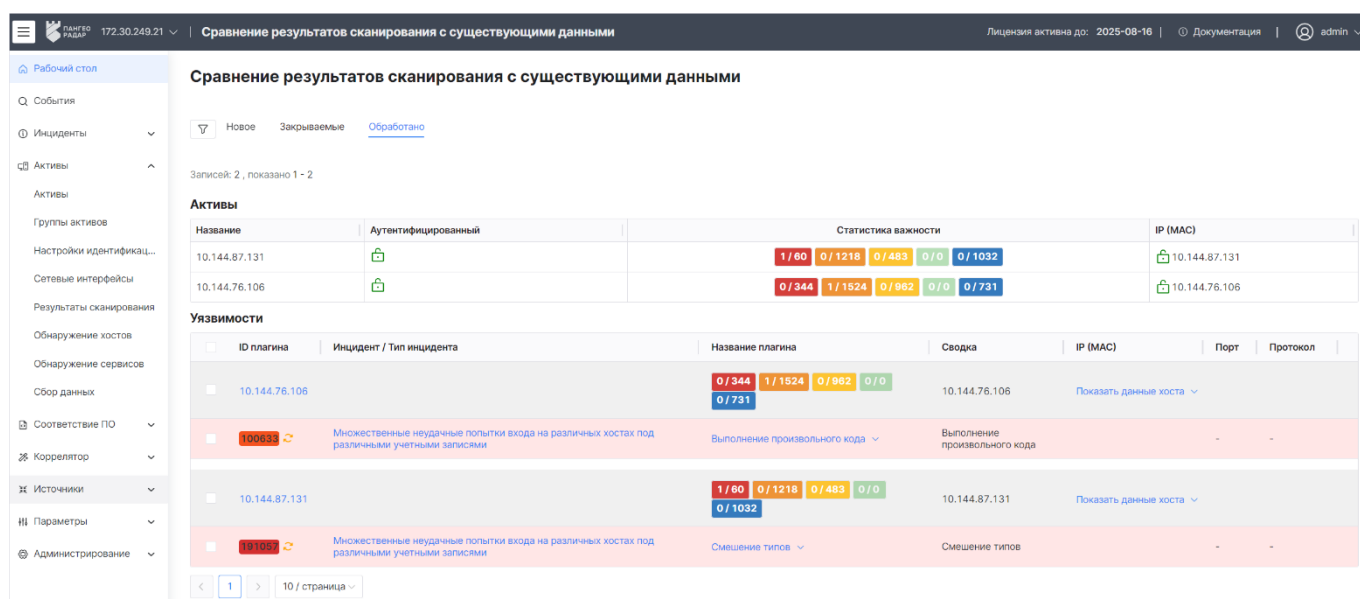
4

5

6

>

10 / страница



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

- **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.

- **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. 106](#)».

Рис. 106 – Таблица "Уязвимости". Строка с информацией об активе

Пример приведен на «[Рис. 107](#)».

Рис. 107 – 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. «[Заккрытие 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 Заккрытие инцидентов по результатам сравнения

1. Откройте результаты сравнения и перейдите на вкладку "Закрываемые".
2. Выберите уязвимости, установив соответствующие флаги.
3. Нажмите кнопку **Заккрытие 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. 108](#)»).

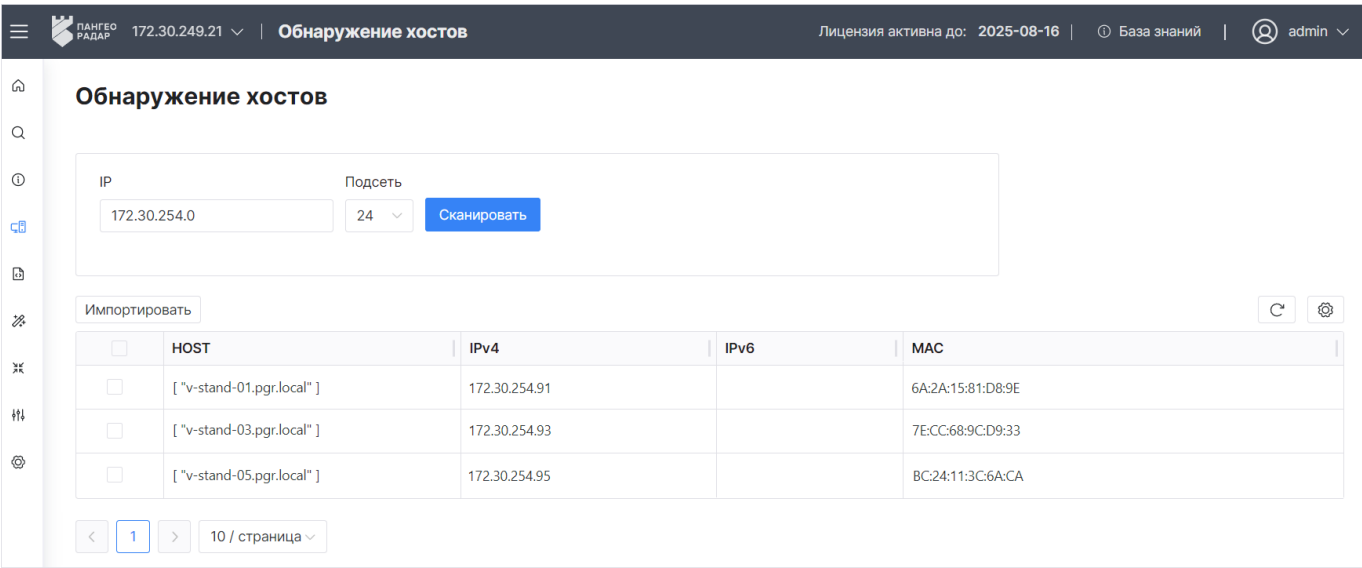


Рис. 108 – Раздел «Обнаружение хостов»

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** – Мас-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. 109».

172.30.249.21 | Обнаружение сервисов

Лицензия активна до: 2025-08-16 | Документация | admin

Обнаружение сервисов

Текстовый поиск

Строгий поиск

Сканировать сервисы

Выбрано: 1

	Название	Операционная...	Сетевые...	Сервисы	Тип	Обновлено	Создано	Значимост...	Сетевая...	Группа ответственных	Уровень риска
<input type="checkbox"/>	Актив с сетевы...			PostgreSQL DB	Host	11:36:46 04.12.2024	11:36:46 04.12.2024	Некритичн...	Нет...	-	0
<input type="checkbox"/>	111.111.111.11		111.111.111.11	nginx	Host	13:05:42 02.12.2024	13:05:42 02.12.2024	Ключевой	Штатный...	-	0
<input type="checkbox"/>	10.11.0.205		10.11.0.205	nginx	Host	11:53:17 28.11.2024	11:53:17 28.11.2024	Ключевой	Штатный...	-	0
<input type="checkbox"/>	172.30.254.97		172.30.254.97	nginx	Host	13:57:45 30.10.2024	13:57:45 30.10.2024	Ключевой	Штатный...	-	0
<input type="checkbox"/>	10.200.68.90	Microsoft Windows	10.200.68.90	nginx	Host	13:37:02 17.10.2024	15:02:02 13.09.2024	Ключевой	Штатный...	users	0
<input checked="" type="checkbox"/>	10.144.98.114	Microsoft Windows	10.144.98.114	nginx	Host	15:01:58 13.09.2024	15:01:58 13.09.2024	Ключевой	Штатный...	-	0
<input type="checkbox"/>	10.144.98.106	Microsoft Windows	10.144.98.106	-	Host	15:01:54 13.09.2024	15:01:54 13.09.2024	Ключевой	Штатный...	-	0
<input type="checkbox"/>	10.200.4.17	Microsoft Windows	1.2.1.12 10.200.4.17	-	Host	15:53:55 17.09.2024	15:01:52 13.09.2024	Ключевой	Штатный...	-	0
<input type="checkbox"/>	10.200.52.219	Microsoft Windows	10.200.52.219	-	Host	15:01:50 13.09.2024	15:01:50 13.09.2024	Ключевой	Штатный...	-	0

Рис. 109 – 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. 110](#)».

Название	Тип	Сетевые интерфейсы	Аппаратное...	Программное...	Создано	Обновлено	Значимос...	Сетевая...	Уров...	Группы активов
<input checked="" type="checkbox"/> 172.30.252.109	Host	172.30.252.109	×	×	2025-09-24 11:37:58	2025-09-24 11:37:58	Некритичный	Штатный доступ в...	0	-
<input type="checkbox"/> 199.232.210.172	Host	199.232.210.172	×	×	2025-09-22 10:53:41	2025-09-22 10:53:41	Некритичный	Штатный доступ в...	0	-
<input type="checkbox"/> 172.30.252.105	Host	172.30.252.105	✓	✓	2025-09-22 10:47:05	2025-09-22 10:47:05	Некритичный	Штатный доступ в...	0	-
<input type="checkbox"/> 172.30.249.42	Host	172.30.249.42	×	×	2025-09-22 10:47:05	2025-09-22 10:47:05	Некритичный	Штатный доступ в...	0	-
<input type="checkbox"/> dc1	Host	dc1	×	×	2025-09-22 10:47:00	2025-09-22 10:47:00	Некритичный	Штатный доступ в...	9.6	-
<input type="checkbox"/> 172.30.253.105	Host	172.30.253.105	×	×	2025-09-21 14:48:56	2025-09-21 14:48:56	Некритичный	Штатный доступ в...	0	-
<input type="checkbox"/> 172.30.254.255	Host	172.30.254.255	×	×	2025-09-20 18:45:03	2025-09-20 18:45:03	Некритичный	Штатный доступ в...	0	-

Рис. 110 – 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. 111»).

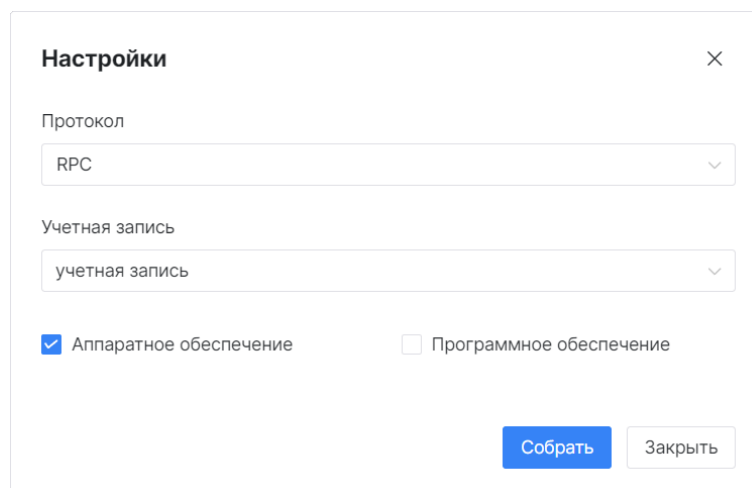


Рис. 111 – Окно "Настройки"

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. 112»](#)).

172.30.254.155

Результаты соответствия ПО

Лицензия активна до: 2024-12-25 | Документация | admin

Результаты соответствия ПО

Удалить

Удалить все

Выбрано: 0

ID	Группа активов	Соответствует	Выполнено	
68a36d96-ec9c-4067-83af-a75970534389	Servers	Нет	12:18:50 06.10.2023	
84185d45-f8e7-4e3f-ac16-5fd60b2fb41c	Servers	Нет	12:49:51 04.10.2024	
e45a1829-6262-4244-ad9b-3be6671da52b	Servers	Нет	12:50:29 04.10.2024	
edc94644-118d-4e44-832f-7b6c5472da58	Servers	Нет	11:21:55 02.11.2024	
79fe0e3e-ce11-4442-85fe-a5c8220b8afc	Servers	Нет	11:21:57 02.11.2024	
e40579a6-9263-4195-b225-13cc91e68e7d	Servers	Нет	11:21:57 02.11.2024	
39a6a63e-3c20-4d90-ac8f-81b09affc427	Servers	Нет	11:21:57 02.11.2024	
6ec88f35-2401-42dd-a687-96c5670fbc01	Servers	Нет	11:21:59 02.11.2024	
3af3de75-2052-4d83-a257-7bbb5f2197f2	Servers	Нет	11:22:00 02.11.2024	
c3d08bef-212f-42fd-ae46-8a2b088811a6	Servers	Нет	11:22:00 02.11.2024	

1

2

3

10 / страница

Рис. 112 – 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. 113»).


Группы активов

Создать

Удалить

Удалить все

Выбрано: 0

Название	Регулярное выражение	Кол-во активов	Группа ответственных	
Servers	.*AD.*	256	admin	

1


10 / страница

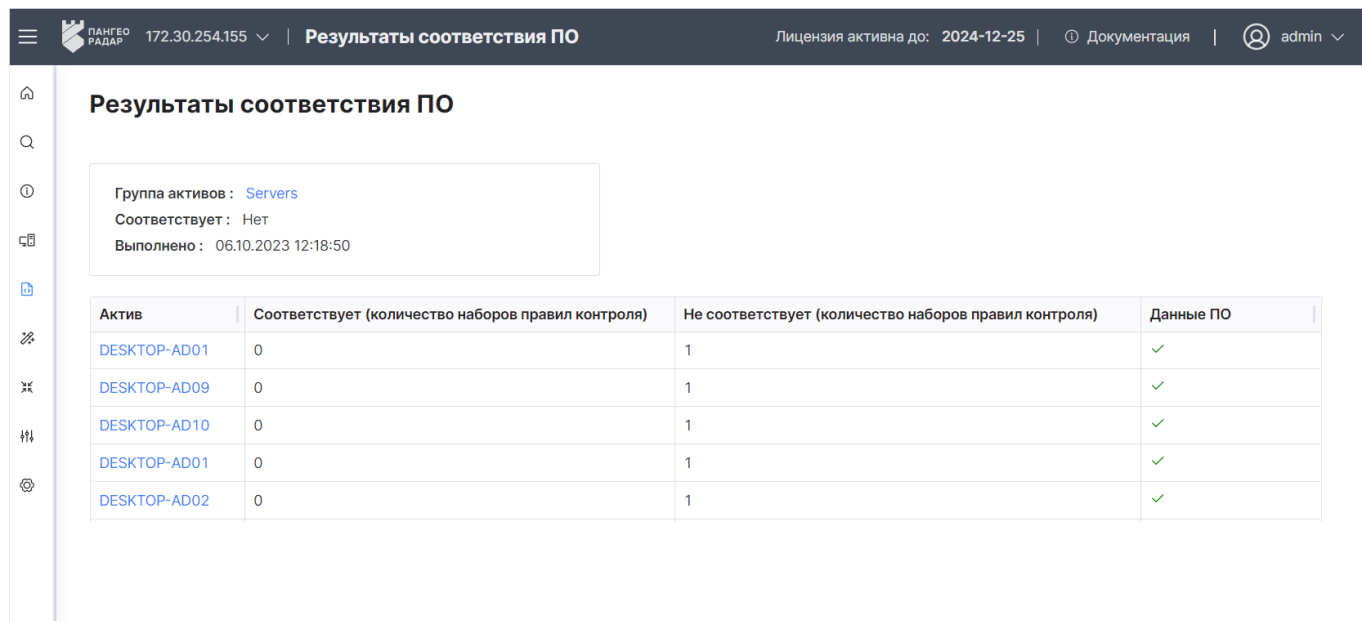
Запуск проверки соответствия ПО

Рис. 113 – 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. 114»).



Актив	Соответствует (количество наборов правил контроля)	Не соответствует (количество наборов правил контроля)	Данные ПО
DESKTOP-AD01	0	1	✓
DESKTOP-AD09	0	1	✓
DESKTOP-AD10	0	1	✓
DESKTOP-AD01	0	1	✓
DESKTOP-AD02	0	1	✓

Рис. 114 – 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.

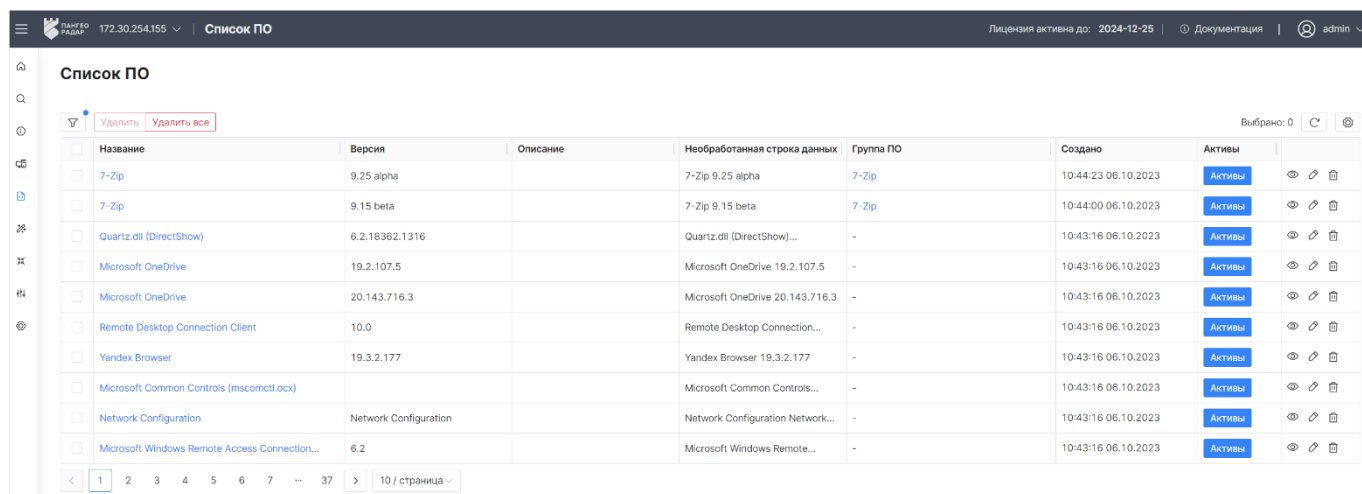
8.3 Список ПО

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. 115](#)»).



Название	Версия	Описание	Необработанные строки данных	Группа ПО	Создано	Активы
<input type="checkbox"/> 7-Zip	9.25 alpha		7-Zip 9.25 alpha	7-Zip	10:44:23 06.10.2023	Активны
<input type="checkbox"/> 7-Zip	9.15 beta		7-Zip 9.15 beta	7-Zip	10:44:00 06.10.2023	Активны
<input type="checkbox"/> Quartz.dll (DirectShow)	6.2.18362.1316		Quartz.dll (DirectShow)...	-	10:43:16 06.10.2023	Активны
<input type="checkbox"/> Microsoft OneDrive	19.2.107.5		Microsoft OneDrive 19.2.107.5	-	10:43:16 06.10.2023	Активны
<input type="checkbox"/> Microsoft OneDrive	20.143.716.3		Microsoft OneDrive 20.143.716.3	-	10:43:16 06.10.2023	Активны
<input type="checkbox"/> Remote Desktop Connection Client	10.0		Remote Desktop Connection...	-	10:43:16 06.10.2023	Активны
<input type="checkbox"/> Yandex Browser	19.3.2.177		Yandex Browser 19.3.2.177	-	10:43:16 06.10.2023	Активны
<input type="checkbox"/> Microsoft Common Controls (mscomctl.ocx)			Microsoft Common Controls...	-	10:43:16 06.10.2023	Активны
<input type="checkbox"/> Network Configuration	Network Configuration		Network Configuration Network...	-	10:43:16 06.10.2023	Активны
<input type="checkbox"/> Microsoft Windows Remote Access Connection...	6.2		Microsoft Windows Remote...	-	10:43:16 06.10.2023	Активны

Рис. 115 – 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. 116](#)»).

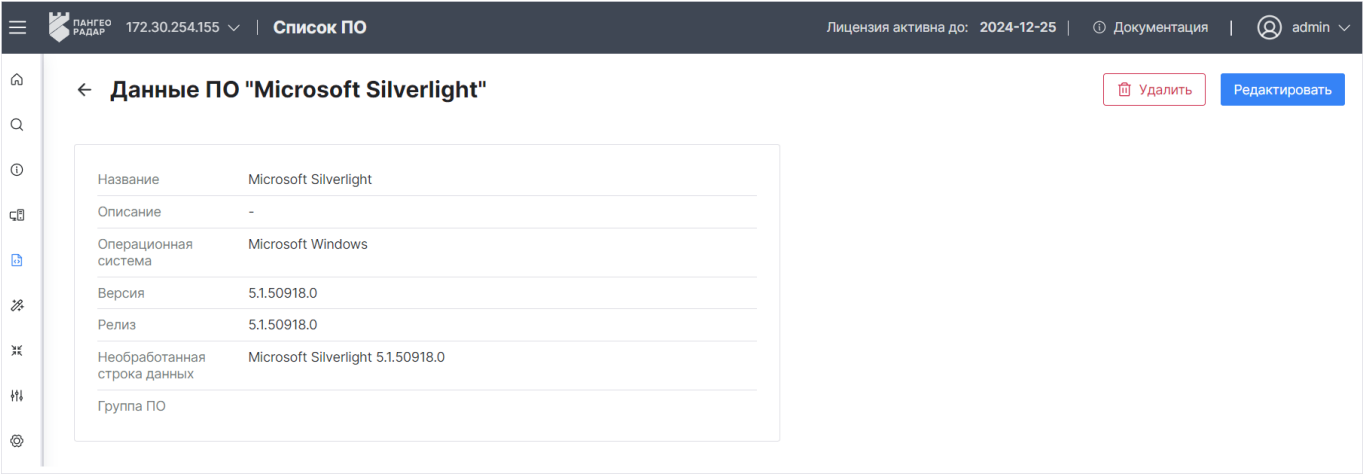


Рис. 116 – Форма "Данные ПО"

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. 117](#)»).

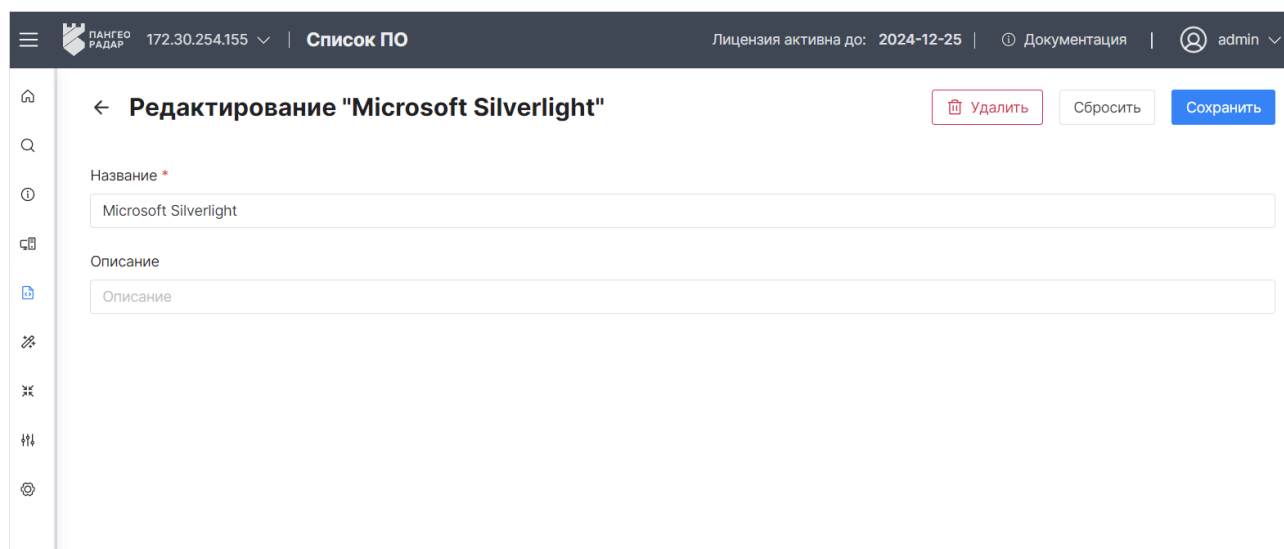


Рис. 117 – Форма «Редактирование списка ПО»


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. 118](#)»).

Список групп ПО			
<input type="checkbox"/>	Название	Добавить новые версии ПО	Описание
<input type="checkbox"/>	7-Zip	Нет	12:00:08 15.10.2024
<input type="checkbox"/>	string	Да	14:24:40 22.10.2024
<input type="checkbox"/>	string	Да	14:24:44 22.10.2024
<input type="checkbox"/>	string	Да	14:24:47 22.10.2024
<input type="checkbox"/>	string	Да	14:24:48 22.10.2024
<input type="checkbox"/>	test	Нет	12:00:08 15.10.2024




Рис. 118 – 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;

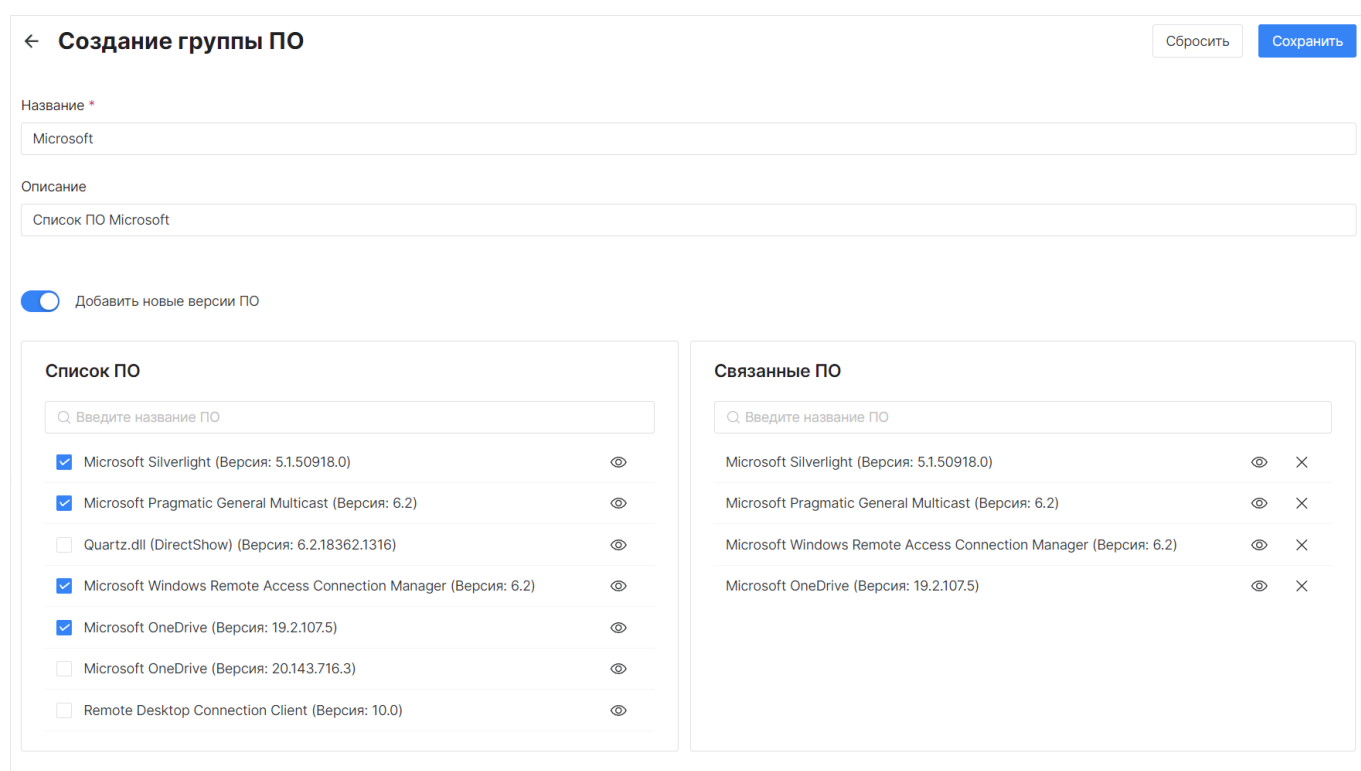
- **Создано** – дата и время создания группы.

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. 119»).



← **Создание группы ПО** Сбросить Сохранить








Название *
Microsoft

Описание
Список ПО Microsoft

☒ Добавить новые версии ПО

Список ПО

🔍 Введите название ПО

- ☒ Microsoft Silverlight (Версия: 5.1.50918.0) 
- ☒ Microsoft Pragmatic General Multicast (Версия: 6.2) 
- ☐ Quartz.dll (DirectShow) (Версия: 6.2.18362.1316) 
- ☒ Microsoft Windows Remote Access Connection Manager (Версия: 6.2) 
- ☒ Microsoft OneDrive (Версия: 19.2.107.5) 
- ☐ Microsoft OneDrive (Версия: 20.143.716.3) 
- ☐ Remote Desktop Connection Client (Версия: 10.0) 

Связанные ПО

🔍 Введите название ПО










- Microsoft Silverlight (Версия: 5.1.50918.0)  
- Microsoft Pragmatic General Multicast (Версия: 6.2)  
- Microsoft Windows Remote Access Connection Manager (Версия: 6.2)  
- Microsoft OneDrive (Версия: 19.2.107.5)  

Рис. 119 – 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. 120»).

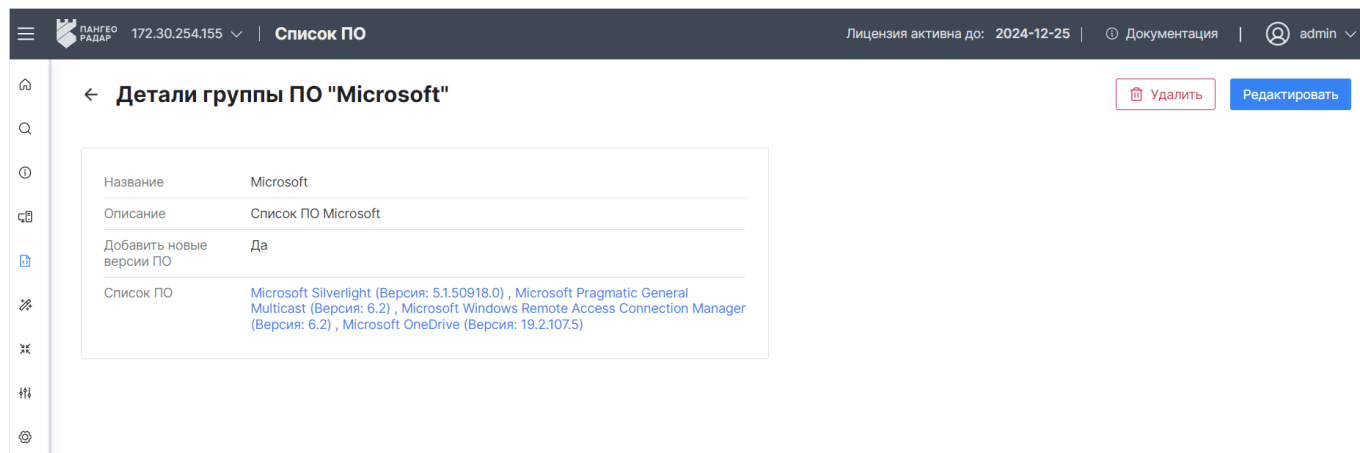



Рис. 120 – Форма "Детали группы ПО"

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.

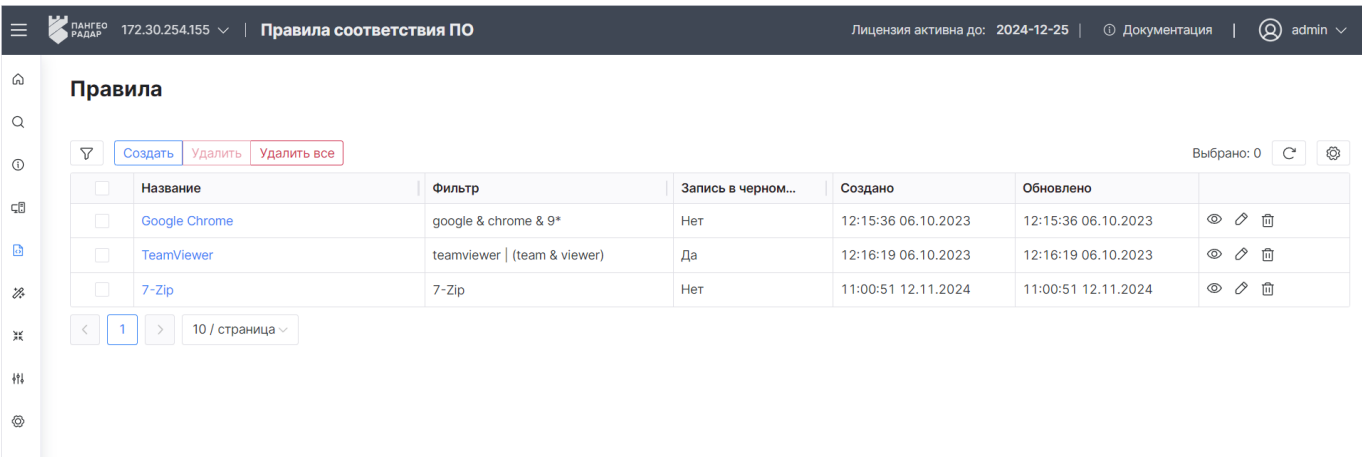
8.5 Правила соответствия ПО

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. 121](#)»).



Название	Фильтр	Запись в черном...	Создано	Обновлено
Google Chrome	google & chrome & 9*	Нет	12:15:36 06.10.2023	12:15:36 06.10.2023
TeamViewer	teamviewer (team & viewer)	Да	12:16:19 06.10.2023	12:16:19 06.10.2023
7-Zip	7-Zip	Нет	11:00:51 12.11.2024	11:00:51 12.11.2024


Рис. 121– 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. 122»).

← **Создание правила**

Очистить Сохранить

Название *

7-Zip

Фильтр

7-Zip

Показать справку

Поиск проводится по текстовым данным, включающим наименование вендора, название продукта и версию.

Проводится поиск одновременно по всем выражениям из запроса.

Выражения могут объединяться операторами "&" (и) и "|" (или).

Отрицание выражения производится символом "!". Выражение ".*" отбирает любые непробельные символы .

Выражения могут группироваться при помощи скобок.

Пример 1: Проверка, что установлена версия Mozilla firefox 21 или 22, но не версия 21.3. mozilla & firefox & ((21:* | 22:*) & !21.3)

Пример 2: Установлен Libreoffice или Microsoft Office. (Microsoft & Office) | Libreoffice

Пример 3: Поиск Antivirus, Antispyware и Antispam, но не Antigen. Anti:* & !Antigen


Пример 4: Поиск Photoshop или Gimp (adobe & photoshop) | (gnu & gimp)

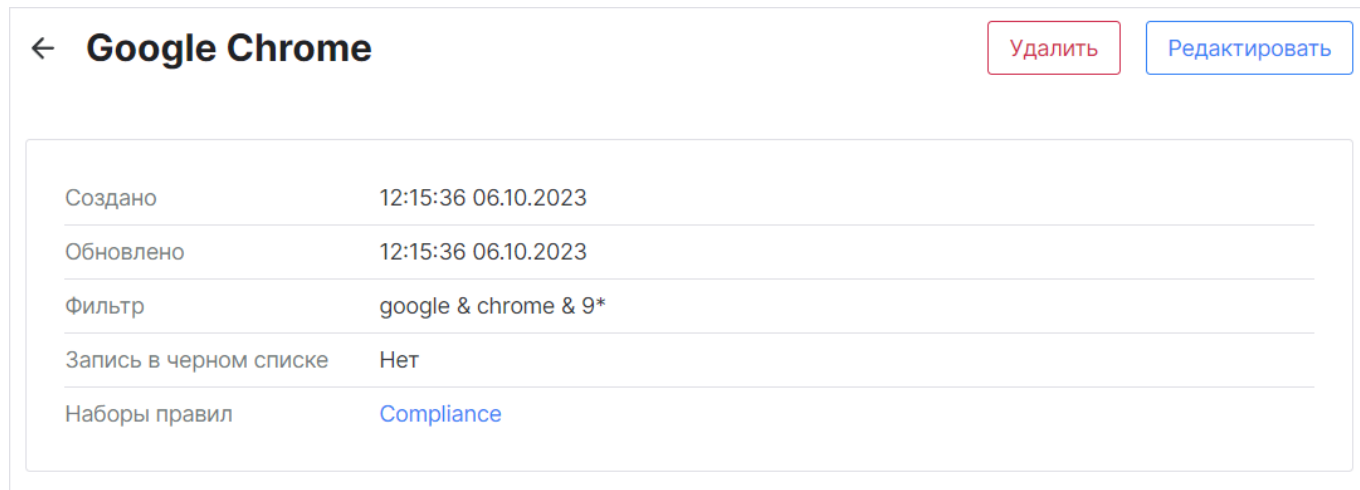
Запись в черном списке

Рис. 122 – 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. 123»).



Создано	12:15:36 06.10.2023
Обновлено	12:15:36 06.10.2023
Фильтр	google & chrome & 9*
Запись в черном списке	Нет
Наборы правил	Compliance

Рис. 123 – 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. 124](#)»).

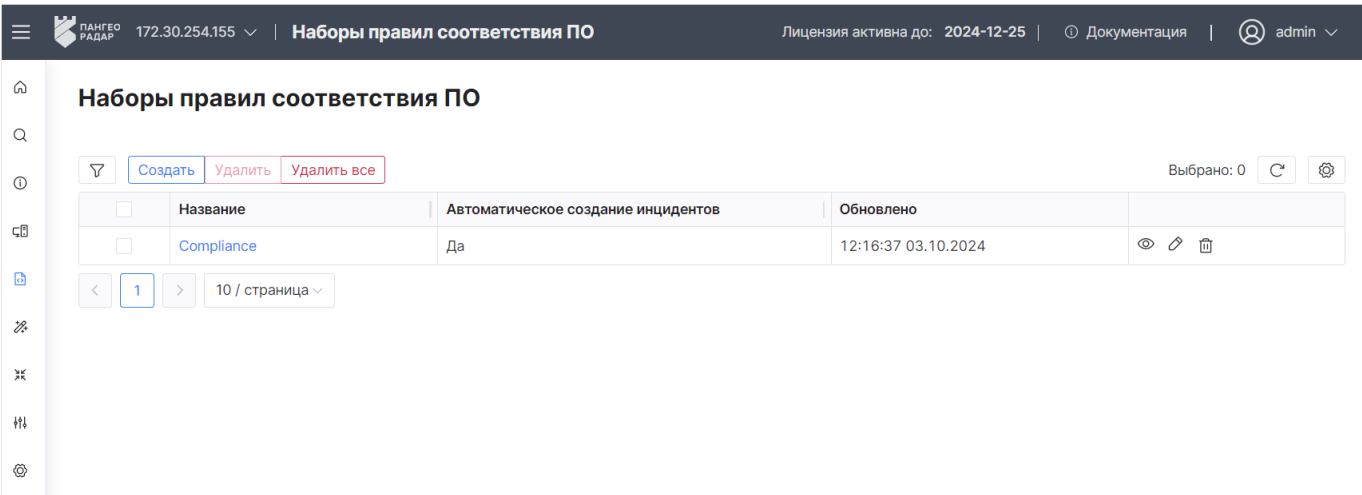





Рис. 124 – Раздел "Наборы правил соответствия ПО"

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. 125»).

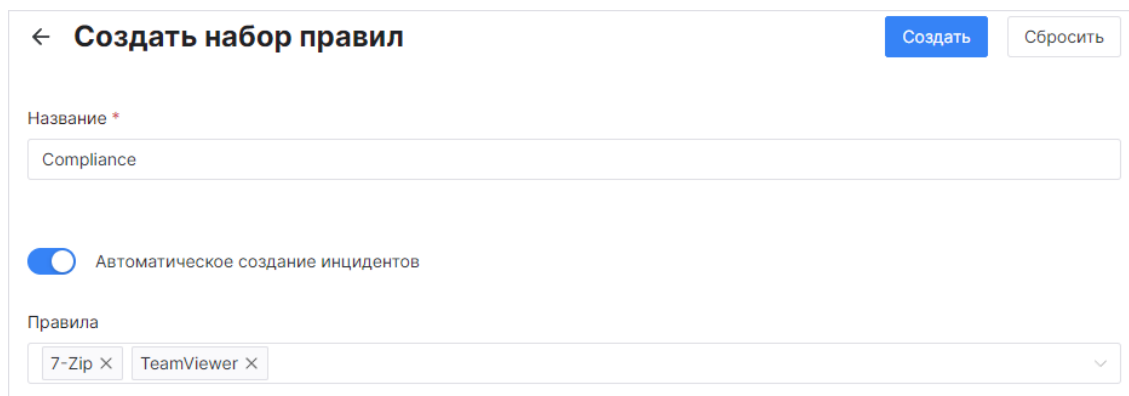



Рис. 125 – Форма "Создать набор правил"

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. 126»).

←

Compliance

Удалить

Редактировать

Детальная информация

Название

Compliance

Автоматическое создание инцидентов

Да

Правила

Название

Фильтр

Запись в черном...

Создано

Обновлено

Google Chrome

google & chrome & 9*

Нет

12:15:36 06.10.2023

12:15:36 06.10.2023

TeamViewer

teamviewer | (team & viewer)

Да

12:16:19 06.10.2023


12:16:19 06.10.2023

Рис. 126 – 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.

9.2 Правила корреляции

Для работы с правилами корреляции перейдите в раздел **Коррелятор → Правила корреляции** (см. «[Рис. 127](#)»).

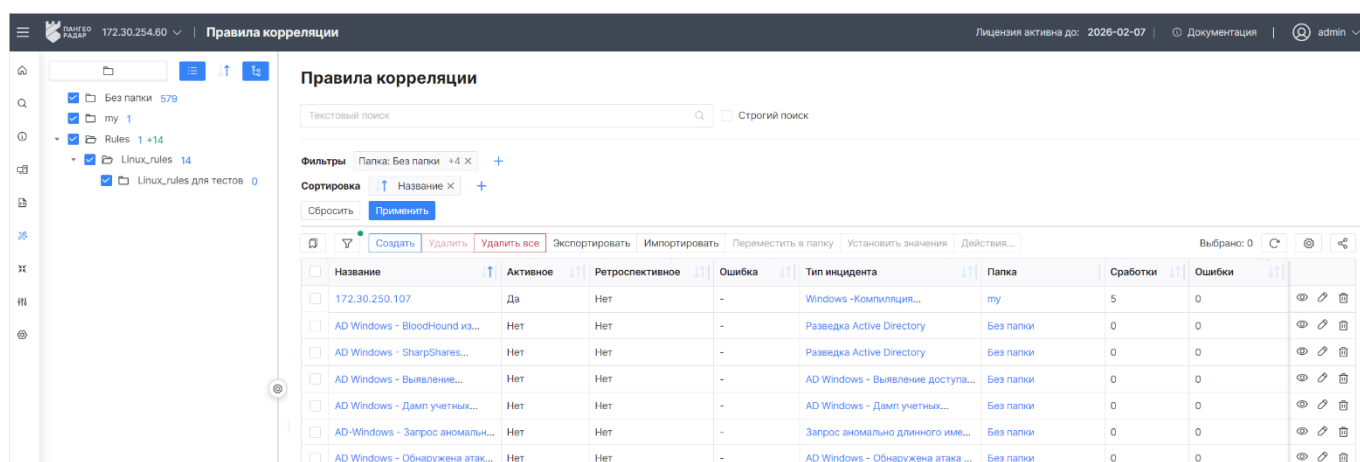



Рис. 127 – Раздел "Правила корреляции". Представление через универсальную таблицу

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. 128](#)»).

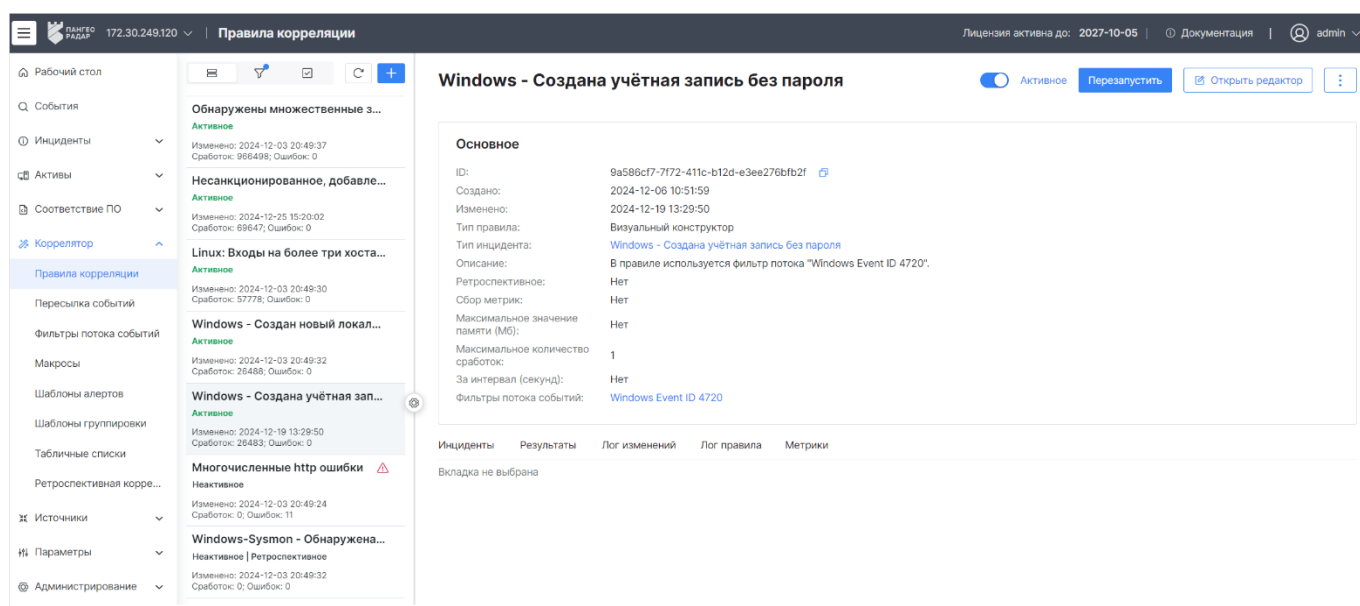


Рис. 128 – Раздел "Правила корреляции". Представление через боковую панель

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. 129»).

Инциденты

Результаты

Лог изменений

Лог правила

Метрики

▼

Создать

Удалить

Удалить все

↻

⚙

<input type="checkbox"/>	Срочность	Уровень риска	Название	Тип инцидента	Статус	Создано	Обновлено	Актив
<input type="checkbox"/>	0.09	2	Перебор паролей	Перебор паролей	Новый	13:52:20 28.08.2024	13:52:20 28.08.2024	172.30.249.21
<input type="checkbox"/>	0.07	0.5	Перебор паролей	Перебор паролей	В работе	13:13:54 25.07.2024	14:36:35 16.08.2024	localhost
<input type="checkbox"/>	0.07	0.5	Suspicious DNS request...	Suspicious DNS request...	Закрыт	17:01:50 11.07.2024	14:11:27 14.08.2024	localhost
<input type="checkbox"/>	0.07	0.5	Перебор хостов...	Перебор хостов...	Новый	14:01:57 16.07.2024	16:34:17 16.07.2024	localhost

<

1

>

10 / страница

Рис. 129 – Просмотр статистики работы правила. Вкладка "Инциденты"

Полный набор информации, отображаемы в таблице:

- Срочность – цифровое и цветное обозначение оценки срочности реагирования на инцидент;
- Уровень риска – цифровое и цветное 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 значения: 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. 130»).

Инциденты Результаты Лог изменений Лог правила Метрики					
<div><div></div><div>Удалить</div><div>Удалить все</div></div>		<div><div></div><div></div></div>			
<input type="checkbox"/>	Инцидент	Актив	Риск	Произошло	
<input type="checkbox"/>	-	-	5 ⓘ	12:35:59 28.08.2024	+ ⓘ 🗑
<input type="checkbox"/>	-	-	0.5 ⓘ	13:14:08 25.07.2024	+ ⓘ 🗑
<input type="checkbox"/>	-	-	0.5 ⓘ	13:13:58 25.07.2024	+ ⓘ 🗑
<input type="checkbox"/>	Перебор паролей	localhost	0.5 ⓘ	13:13:53 25.07.2024	ⓘ 🗑
<input type="checkbox"/>	Сбой активации лицензий	localhost	0.5 ⓘ	13:09:46 25.07.2024	ⓘ 🗑
<input type="checkbox"/>	Сбой активации лицензий	localhost	0.5 ⓘ	13:09:36 25.07.2024	ⓘ 🗑
<input type="checkbox"/>	Сбой активации лицензий	localhost	0.5 ⓘ	13:09:31 25.07.2024	ⓘ 🗑
<input type="checkbox"/>	Перебор хостов выполняется по запросам Kerberos TGS	localhost	0.5 ⓘ	16:34:16 16.07.2024	ⓘ 🗑
<input type="checkbox"/>	Перебор хостов выполняется по запросам Kerberos TGS	localhost	0.5 ⓘ	16:34:06 16.07.2024	ⓘ 🗑
<input type="checkbox"/>	Перебор хостов выполняется по запросам Kerberos TGS	localhost	0.5 ⓘ	16:34:01 16.07.2024	ⓘ 🗑
<div><div>< 1 2 3 4 5 6 7 ... 14 ></div><div>10 / страница ▾</div></div>					

Рис. 130 – 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. 131»).

Инциденты	Результаты	Лог изменений	Лог правила	Метрики
<div> <div> <div></div> <div></div> </div> <div> <div></div> <div></div> </div> </div>				
Действие	Дата создания	Системное	Кем изменен	Детали
Изменение	10:45:19 12.12.2024	Нет	admin	Показать детали
Изменение	18:12:42 11.12.2024	Нет	admin	Показать детали
Изменение	18:12:06 11.12.2024	Нет	admin	Показать детали
<div> <div> <div></div> <div>1</div> <div></div> </div> <div>10 / страница</div> </div>				

Рис. 131 – 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. 132»).

Инциденты

Результаты

Лог изменений

Лог правила

Метрики

Функция	Дата	Сообщение	Уровень сообщения
init	12:16:16 17.03.2025	failed to unmarshal action: json: cannot unmarshal string into Go...	<div><div></div>Ошибка</div>

<

1

>

10 / страница ▾

Рис. 132 – 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. 133»);

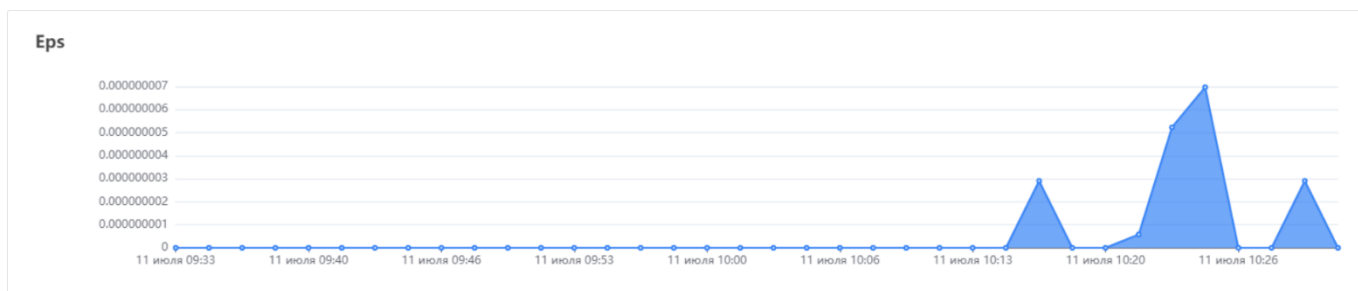


Рис. 133 – Метрика "EPS"

- задействованная память (см. «Рис. 134»):

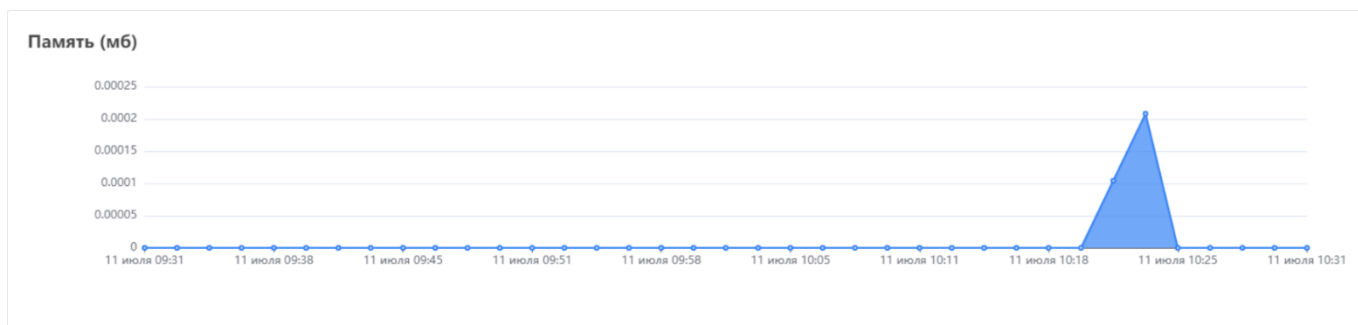


Рис. 134 – Метрика "Память"

- количество накопленных событий в группе (см. «Рис. 135»):

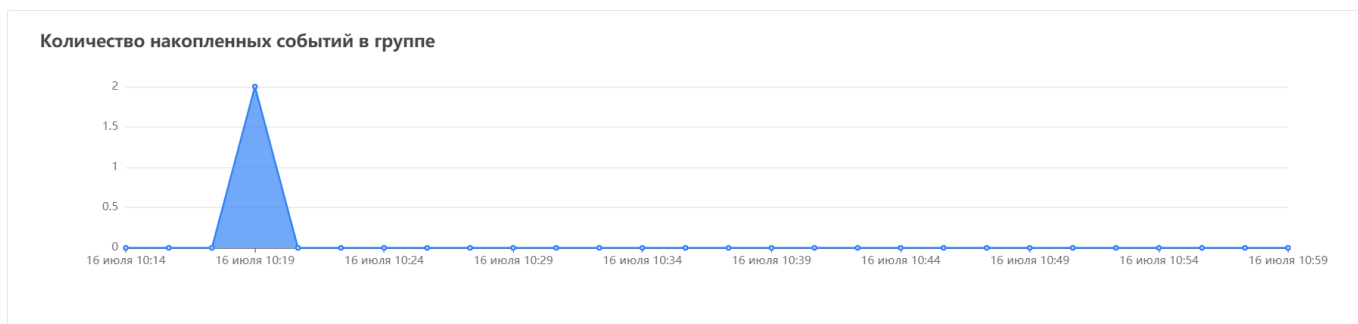


Рис. 135 – Метрика "Количество накопленных событий в группе"

- время выполнения функции `on_logline` (см. «Рис. 136»).

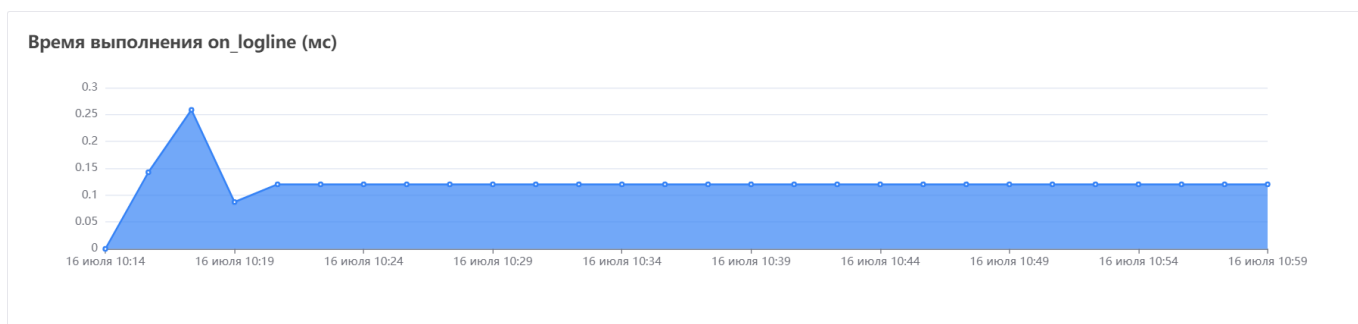


Рис. 136 – Метрика "Время выполнения on_logline"

- время выполнения функции `on_grouped` (см. «Рис. 137»).

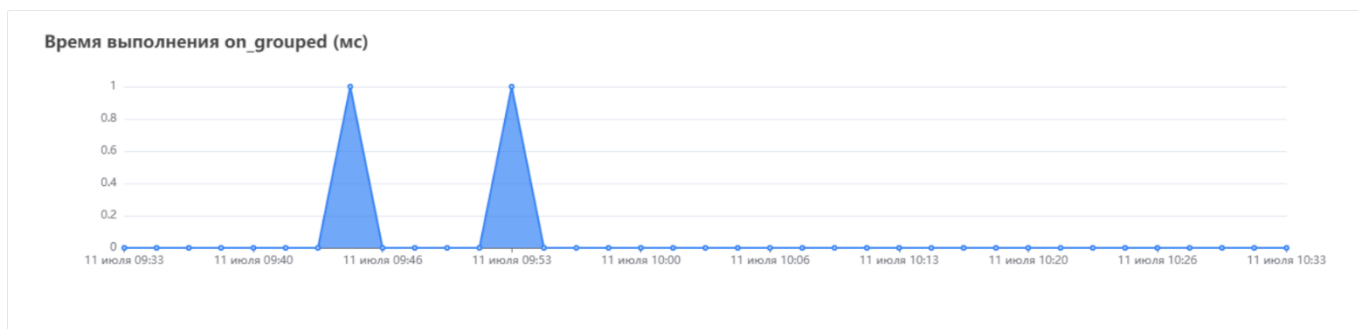


Рис. 137 – Метрика "Время выполнения on_grouped"

- количество ошибок, возникших во время "сработок" правила (см. «Рис. 138»).

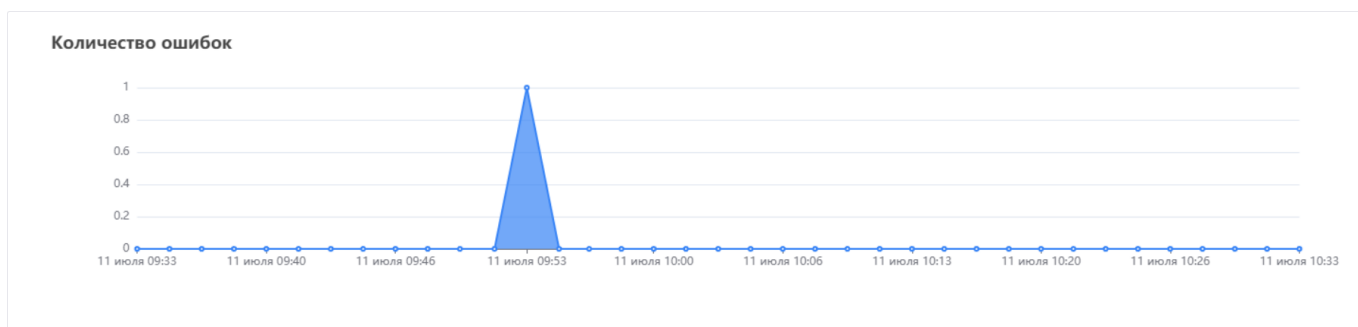


Рис. 138 – Метрика "Количество ошибок"

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. 139»).

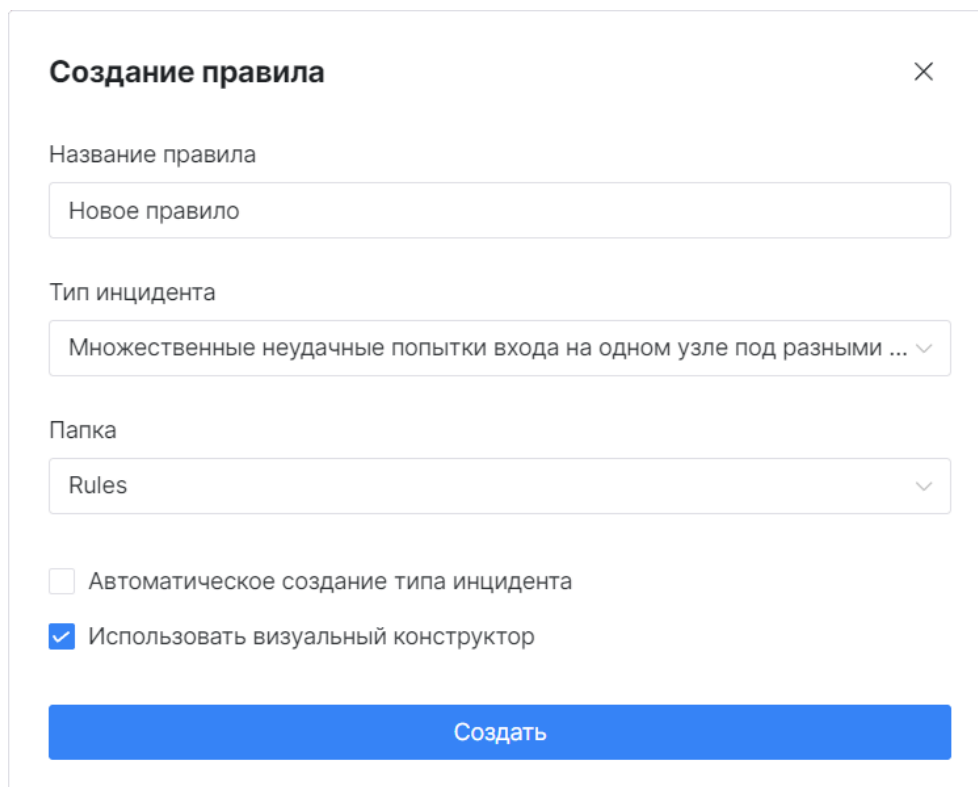


Рис. 139 – Окно "Добавить правило"

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 расписания работы правила;](#)
- [Шаг 3. Настройка фильтров потока;](#)
- [Шаг 4. Настройка алерта;](#)

- [Шаг 5. Настройка группера](#);
- [Шаг 6. Настройка условий](#);
- [Шаг 7. Настройка действий](#);
- [Шаг 8. 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. 140»).

The screenshot shows the configuration page for a rule named "Linux: Прослушка сетевого трафика". The interface includes a top navigation bar with the Pangeo Radar logo, user information, and a license expiration date. The main content area has a sidebar with navigation icons and a top bar with tabs for different configuration sections. The "Основное" tab is active, displaying fields for "Название" (Name), "Папка" (Folder), and "Тип инцидента" (Incident Type). Below these are several toggle switches for "Сбор метрик" (Collect metrics), "Ретроспективное" (Retrospective), "Использовать группировку" (Use grouping), "Создать результат при сработке правила" (Create result when rule triggers), and "Работа правила по расписанию" (Rule works by schedule). The "Описание" (Description) field contains a detailed note about the rule's purpose and the need for AuditD logging. At the bottom, there are input fields for "Максимальное количество сработок" (Maximum number of triggers) and "Максимальное значение памяти (МБ)" (Maximum memory value in MB).

Рис. 140 – 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;
- 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.

- выберите режим работы правила: постоянно или по расписанию, установив переключатель **Работа правила по расписанию** в соответствующее положение;
- 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 расписания работы правила

Если вы на первом шаге выбрали режим работы правила **По расписанию**, то необходимо выполнить настройку на вкладке "Расписание" (см. «Рис. 141»).

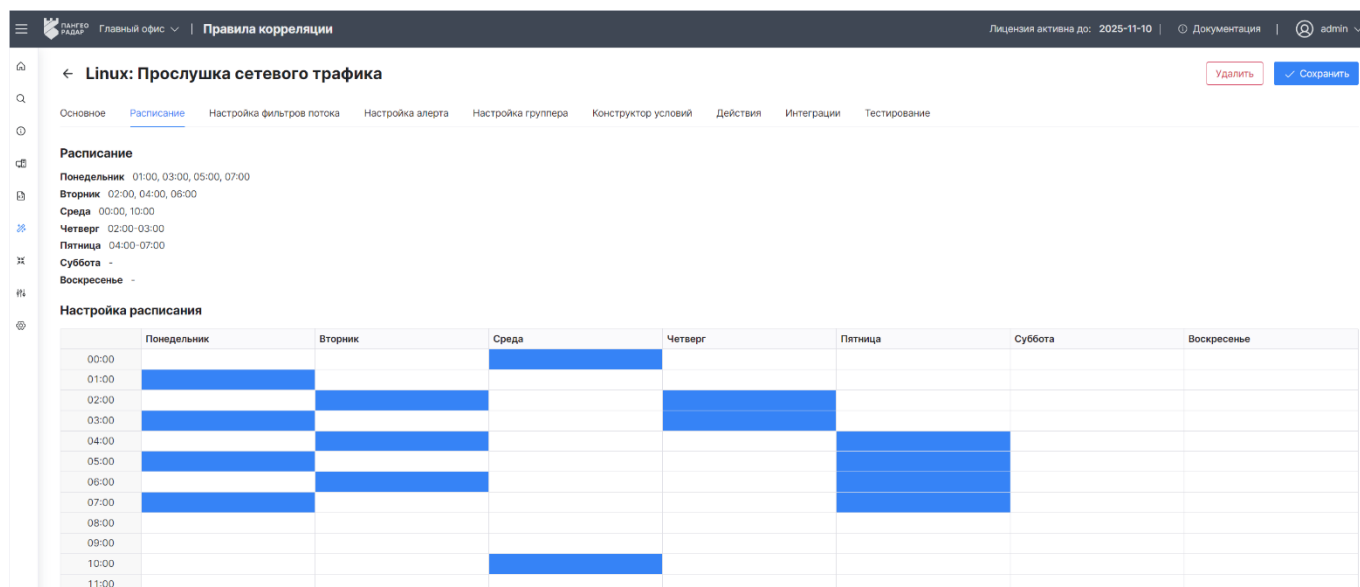


Рис. 141 – Настройка правила. Вкладка "Расписание"

В блоке **Настройка расписания** укажите период работы правила, нажав ЛКМ на соответствующие значения в таблице.

В блоке **Расписание** проверьте настроенное расписание работы правила.

9.2.2.1.3 Шаг 3. Настройка фильтров потока

Для работы правила в него необходимо добавить фильтр потока событий. Для этого перейдите на вкладку "Настройка фильтров потока" (см. «Рис. 142»).

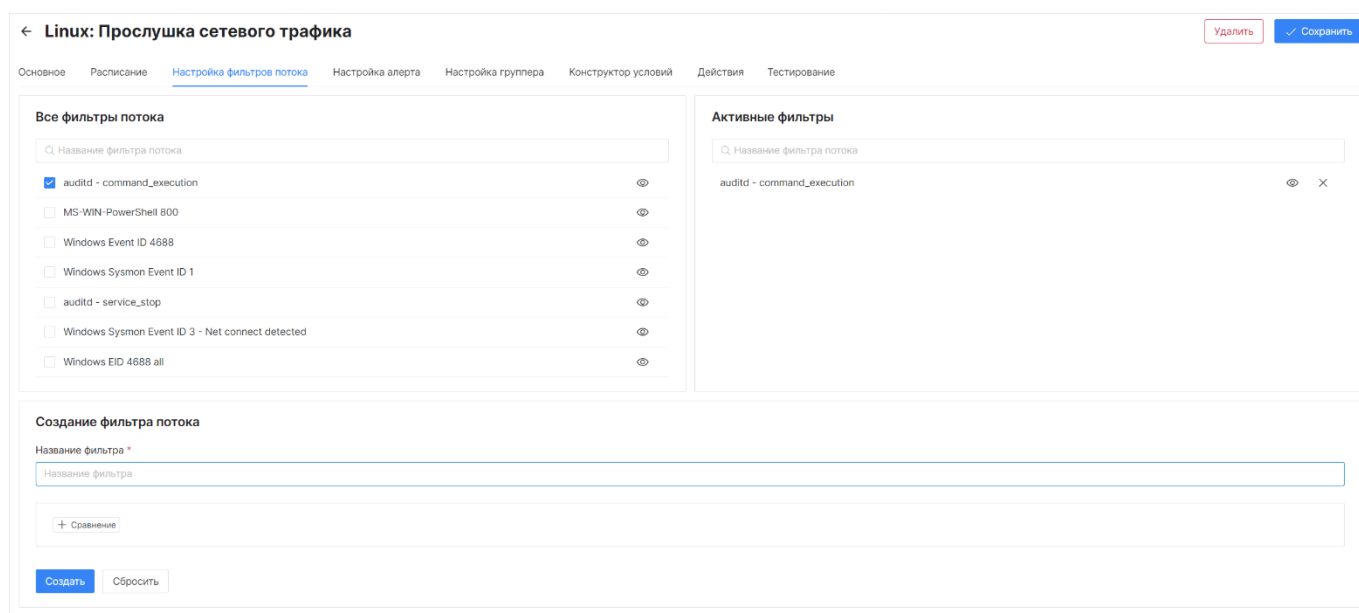




Рис. 142 – Настройка правила. Вкладка "Настройка фильтров потока"

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](#)».

9.2.2.1.4 Шаг 4. Настройка алерта

Если вы на первом шаге выбрали поведение: **Создавать результат при сработке правила**, то необходимо выполнить настройку на вкладке "Настройки алерта" (см. «[Рис. 143](#)»).

Linux: Прослушка сетевого трафика

Удалить
Сохранить

Основное
Расписание
Настройка фильтров потока
Настройка алерта
Настройка группера
Конструктор условий
Действия
Тестирование

Настройка алерта

Уровень риска

0
1
2
3
4
5
6
7
8
9
10

☒ Создать инцидент
☐ Назначить инцидент пользователю
☐ Логировать первое и последнее событие

Логировать указанное число событий

10
+
-

IP актива

observer.host.ip

FQDN актива

observer.host.fqdn

Hostname актива

observer.host.hostname

MAC актива

Техники Mitre

T1040

Группа инцидентов

Администраторский доступ

Шаблон

Обнаружена прослушка сетевого трафика.
Выполненная команда: {{ .First.initiator.command.executed }}

Рис. 143 – 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](#)».

9.2.2.1.5 Шаг 5. Настройка группера

Если вы на первом шаге выбрали вид правила **С группировкой событий**, то необходимо выполнить настройку на вкладке "Настройка группера" (см. «[Рис. 144](#)»).

The screenshot shows the 'Новое правило' (New Rule) configuration page. The 'Настройка группера' (Grouping Settings) tab is active. The configuration includes:

- Группировать по** (Group by): action, elastic_key
- Агрегировать по** (Aggregate by): Выбрать (Select)
- Размер окна группировки** (Window size): 4, Минуты (Minutes)
- Порог количества событий для срабатывания** (Threshold): 1
- Использовать цепочку** (Use chain): checked
- Агрегировать только уникальные события** (Aggregate only unique events): checked
- Время события** (Event time): @timestamp
- Формат времени** (Time format): RFC3339Nano | 2006-01-02T15:04:05.999999999+07:00 (Z07:00)

Below the main settings, there are two comparison rules:

- event.application равно значению в массиве event** (event.application equals value in array event). Количество событий: 1. Точное совпадение количества событий: checked. Отсутствует: unchecked.
- error равно значению в массиве event** (error equals value in array event). Количество событий: 1. Точное совпадение количества событий: unchecked. Отсутствует: checked.

Рис. 144 – 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. 145](#)»).

Рис. 145– 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. 146](#)»):

Рис. 146 – 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](#)».

9.2.2.1.6 Шаг 6. Настройка условий

Настройка условий "сработки" правила выполняется на вкладке "Конструктор условий" (см. «[Рис. 147](#)»).

Рис. 147 – 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 regex** (оператор "*проходит regex*") - 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;

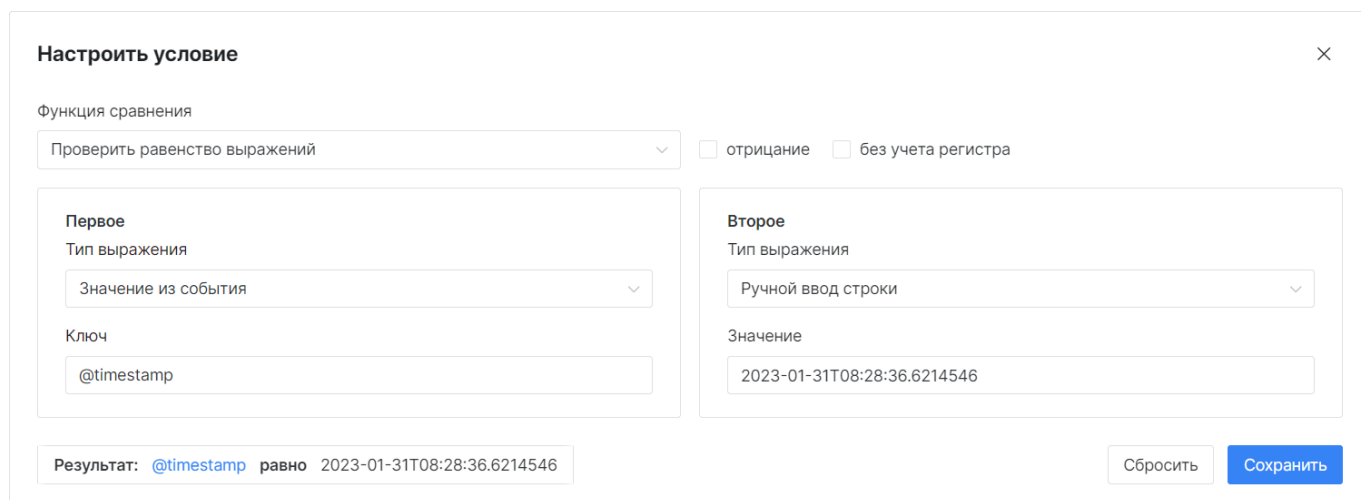
На вкладке доступны следующие элементы управления:

Кнопка	Действие
	добавление условия сравнения
	добавление группы условий
	добавление условия сравнения в группу
	изменение порядка условий сравнения
	удаление условия сравнения из правила
Нажатие ЛКМ на оператор И , ИЛИ	настройка поведения для выбранной группы условий

Кнопка	Действие
Нажатие ЛКМ на строку условия	редактирование выбранного условия

Для добавления условия выполните следующие действия:

1. Нажмите на кнопку . Откроется окно "Настроить условие" (см. «Рис. 148»).



Настроить условие

Функция сравнения

Проверить равенство выражений

☐ отрицание ☐ без учета регистра

Первое

Тип выражения

Значение из события

Ключ

@timestamp

Второе

Тип выражения

Ручной ввод строки

Значение


2023-01-31T08:28:36.6214546

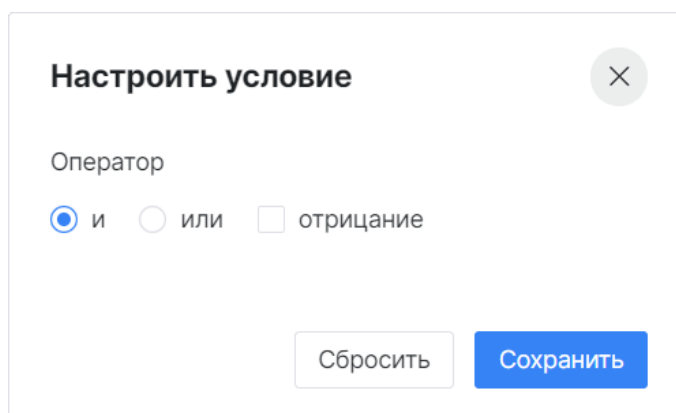
Результат: @timestamp равно 2023-01-31T08:28:36.6214546

Рис. 148 – 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 . Откроется окно "Настроить условие" (см. «Рис. 149»).



Настроить условие

Оператор

☒ и ☐ или ☐ отрицание

Рис. 149 – Добавление группы. Окно "Настроить условие"

2. Выберите оператор.

3. Если необходимо выполнить операцию "отрицание", то установите соответствующий флаг.

4. Нажмите кнопку **Сохранить**.

9.2.2.1.7 Шаг 7. 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 правило можно добавить неограниченное количество действий.

Настройка действий над табличными списками выполняется на вкладке "Действия" (см. «Рис. 150»).

← Новое правило

Удалить Сохранить

Основное Расписание Настройка фильтров потока Настройка алерта Настройка группера Конструктор условий Действия Тестирование

Установка значения в табличном списке ▾ 🗑️

Табличный список: host+username TTL: 0 - +

Составной ключ

host ☒ Значение ☐ Поле события

username ☒ Значение ☐ Поле события

Колонка: host Значение:

Удаление записи из табличного списка ^ ▾ 🗑️

Табличный список: host

Составной ключ

host ☐ Значение ☒ Поле события

Очистка табличного списка ^ 🗑️

Табличный список: IP

Добавить

Рис. 150 – 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.

9.2.2.1.8 Шаг 8. 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. 151»).

← Необычное время входа в систему

Основное Расписание Настройка фильтров потока Настройка алерта Настройка группера Конструктор условий Действия **Тестирование**

Временное окно: 1m Задержка отправки: 100 Задержка группера: 0

Запустить тест

Тестовый набор данных

Логлайн

```
{ "@timestamp": 1720603009001, "event": { "field": "test", "target": { "host": { "ip": "127.0.0.1", "fqdn": "", "hostname": "localhost" } } }
```

Добавить логлайн в тестовый набор

1. ("@timestamp":1720522980904,"event":{"field":"test","target":{"host":{"ip":"127.0.0.1","fqdn":"","hostname":"localhost"}}})

2. ("rs_collector_hostname":"v-stand-09","rs_relay_fqdn":"172.30.254.106","rs_relay_ip":"172.30.254.106","rs_collector_ts"...)

Код правила

Показать код

Ошибки

Ошибок нет

Лог



1. [info] agg total: 2 for hash key ...

Результаты сработки


Рис. 151 – 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. 152](#)»).

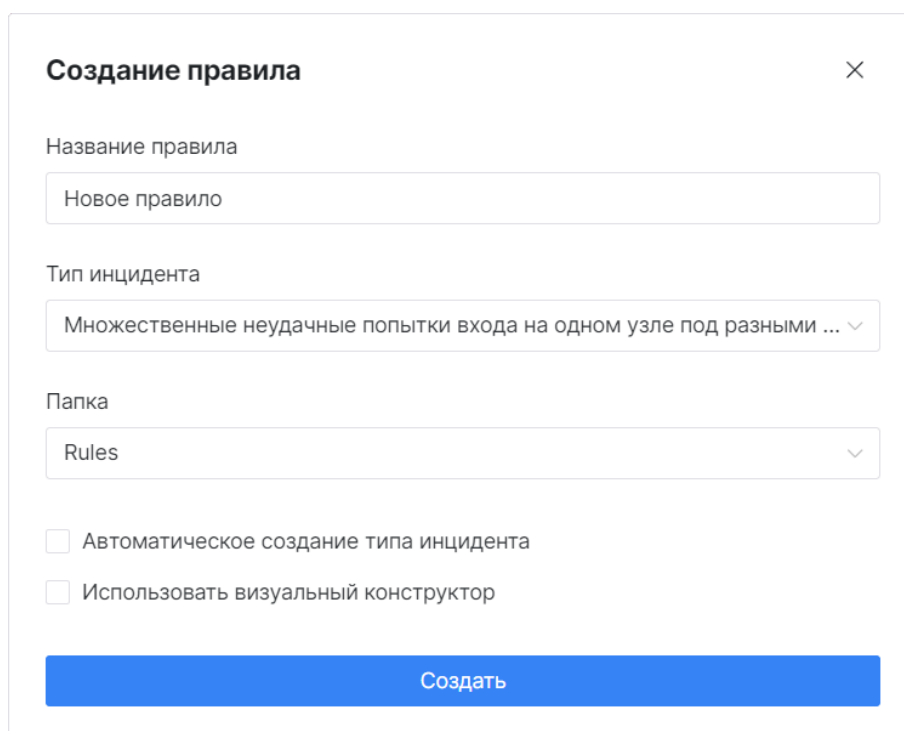


Рис. 152 – Окно "Добавить правило"

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;

- Примечание:** если опция включена, то убедитесь, что наименование правила корреляции не совпадает ни с одним наименованием типа инцидента.

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 расписания работы правила;](#)
- [Шаг 3. Настройка фильтров потока;](#)
- [Шаг 4. Настройка кода правила;](#)
- [Шаг 5. Настройка макросов;](#)
- [Шаг 6. 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. 153»).

ПАНЕЛЬ ЗАДАЧ

Главный офис ▾ | Правила корреляции

Лицензия активна до: 2025-11-10 | [Документация](#) | [admin](#) ▾

← Windows-Eventlog: Создание сессии C2 с помощью powercat, ncат или powerchellicmp

Удалить Сохранить

ОсновноеРасписаниеНастройка фильтров потокаКод правилаМакросыИнтеграцииТестирование

Основное

НазваниеПанка

Windows-Eventlog: Создание сессии C2 с помощью powercat, ncат или powerchellicmpБез папки

Тип инцидента

Windows: Использование протоколов неприкладного уровня, инициирование сессии C2

☐ Сбор метрик☐ Ретроспективное☒ Работа правила по расписанию

Описание

Данное правило срабатывает при обнаружении признаков установления командно-контрольного соединения (C2) с использованием утилит powercat, ncат, powerchellicmp.ps1 или аналогичных скриптов, которые используют нестандартные или слабо отслеживаемые каналы связи. Такие инструменты часто используются в рамках атак Red Team, малвари и post-exploitation утилит.
Для работы правила необходимо включить:
4688 — Создание нового процесса
4104 — Scriptblock logging

Ограничения

Максимальное количество сработокЗа интервал (секунд)

00

Максимальное значение памяти (Mб)

0

Рис. 153 – 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;
- выберите режим работы правила: постоянно или по расписанию, установив переключатель **Работа правила по расписанию** в соответствующее положение;
- 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 Шаг 2. Настройка расписания работы правила

Если вы на первом шаге выбрали режим работы правила **По расписанию**, то необходимо выполнить настройку на вкладке "Расписание" (см. «Рис. 154»).

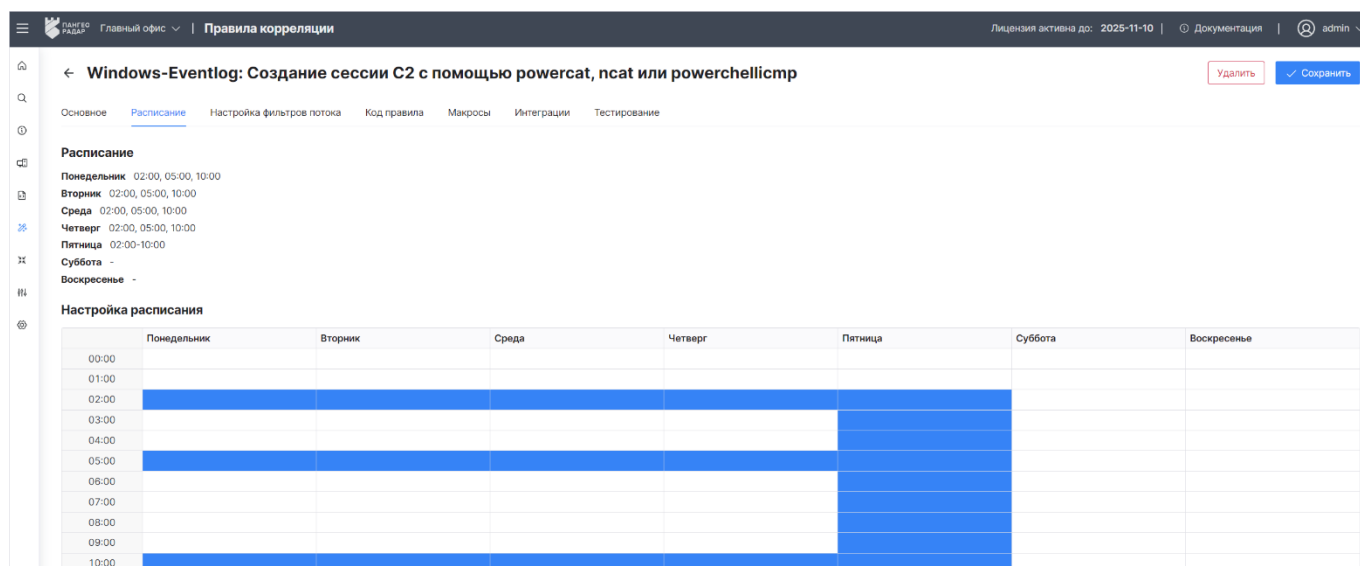


Рис. 154 – Настройка правила на скриптовом языке Lua. Вкладка "Расписание"

В блоке **Настройка расписания** укажите период работы правила, нажав ЛКМ на соответствующие значения в таблице.

В блоке **Расписание** проверьте настроенное расписание работы правила.

9.2.2.2.3 Шаг 3. Настройка фильтров потока

Для работы правила в него необходимо добавить фильтр потока событий. Для этого перейдите на вкладку "Настройка фильтров потока" (см. «[Рис. 155](#)»).

The screenshot shows the 'Множественные неудачные попытки входа' (Multiple failed login attempts) rule configuration. The 'Настройка фильтров потока' (Stream Filter Settings) tab is active. It features a top bar with 'Удалить' (Delete) and 'Сохранить' (Save) buttons. Below the tabs, there are three main sections: 1. 'Все фильтры потока' (All stream filters) with a search bar and a list of filters: 'Источник событий: windows' (checked), 'MS Windows Defender', and 'Пересылка нормализованных событий'. 2. 'Активные фильтры' (Active filters) showing 'Источник событий: windows' with an eye icon and a close 'X' icon. 3. 'Создание фильтра потока' (Create stream filter) with a text input for the filter name, a '+ Сравнение' (Compare) button, and 'Создать' (Create) and 'Сбросить' (Reset) buttons.

Рис. 155 – 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](#)».

9.2.2.2.4 Шаг 4. 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. 156](#)»).

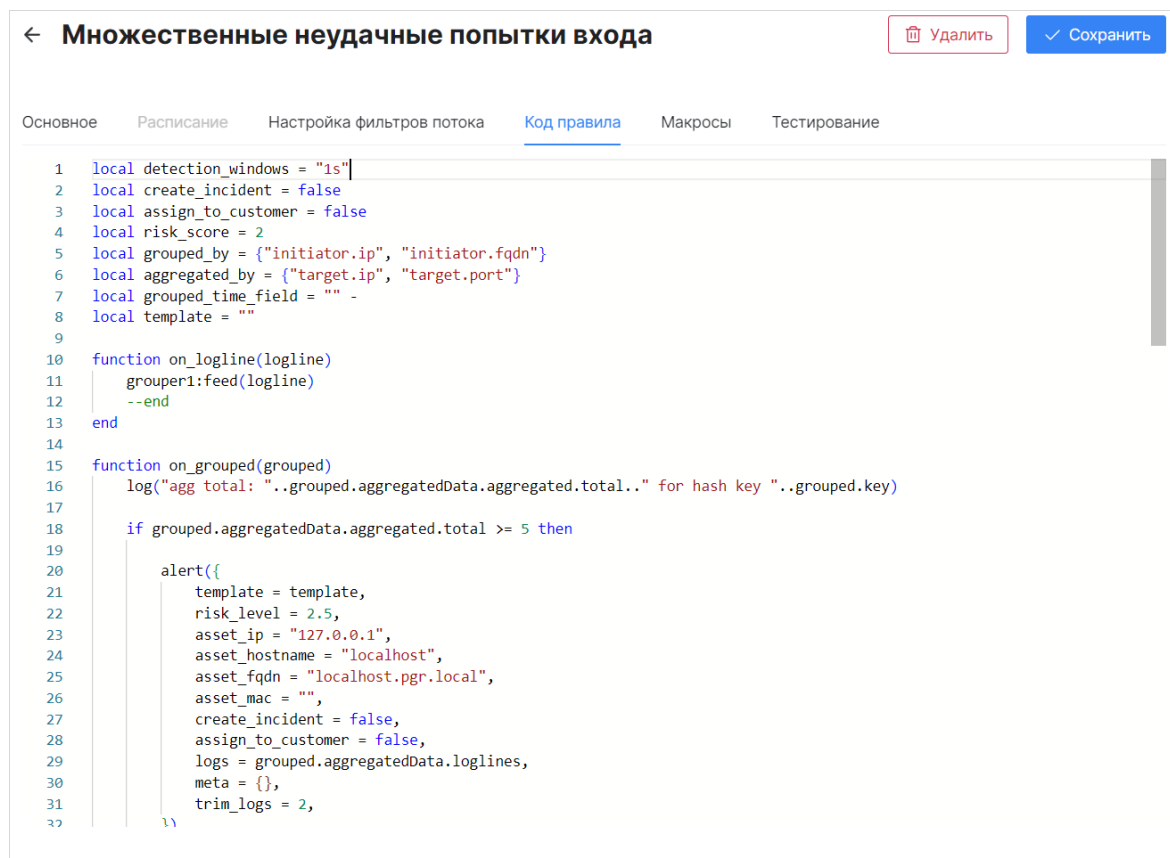


Рис. 156 – Настройка правила на скриптовом языке Lua. Вкладка "Код правила"

Для использования шаблона группировки начните вводить функцию `grouper.template.<наименование шаблона группировки>`. По мере ввода текста редактор отобразит список доступных шаблонов группировки.

Для использования шаблона алерта начните вводить функцию `alert.template.<наименование шаблона алерта>`. По мере ввода текста редактор отобразит список доступных шаблонов алертов.

Примечание: перед использованием шаблонов группировки и алертов в правиле, их необходимо создать в соответствующих разделах.

Пример использования шаблонов в редакторе Lua приведен на «Рис. 157».

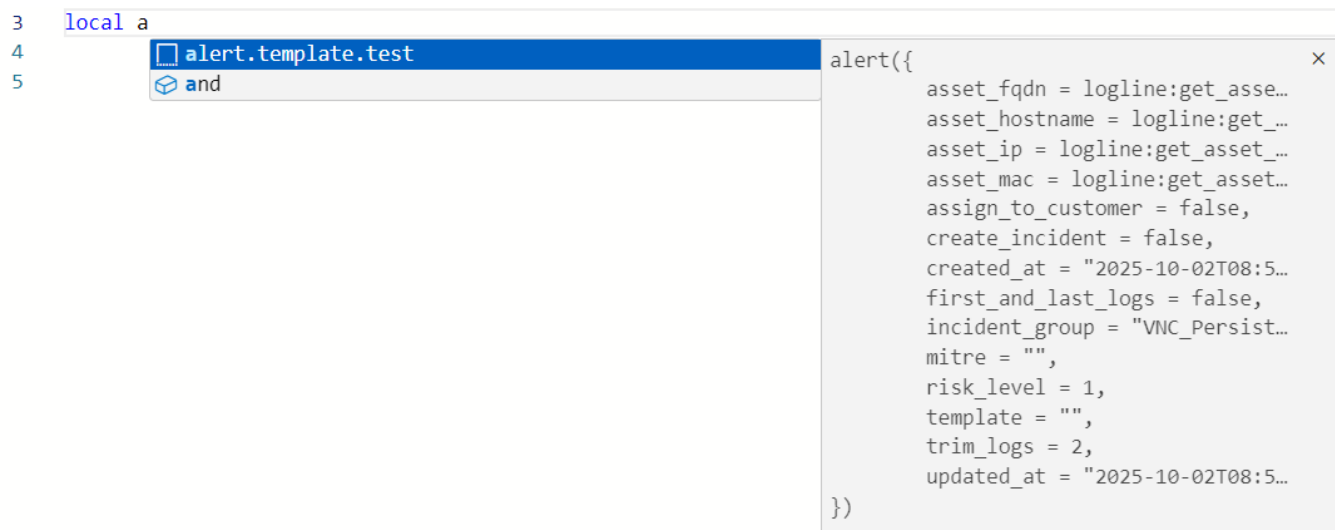


Рис. 157 – Пример использования шаблонов в редакторе Lua

9.2.2.2.5 Шаг 5. 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. 158»).

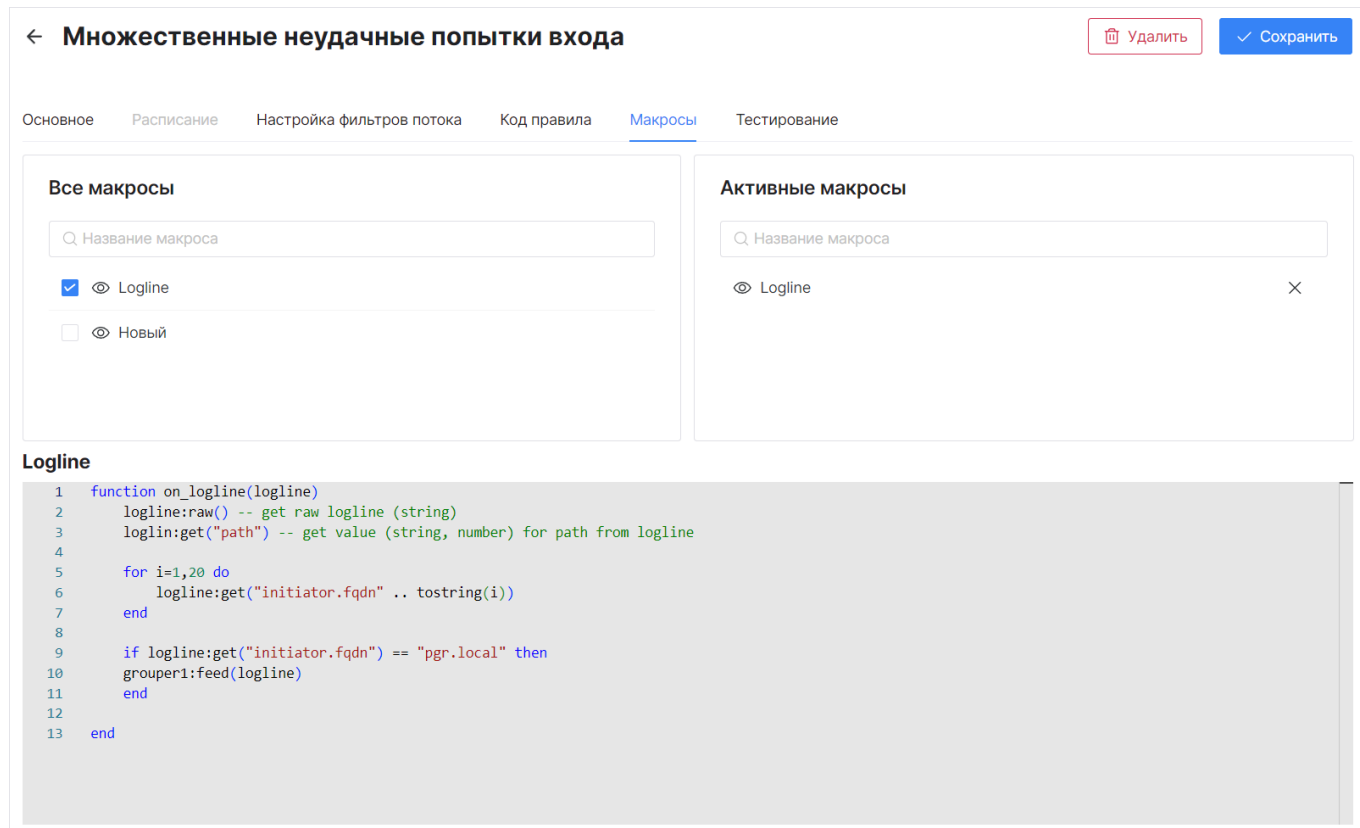




Рис. 158 – Настройка правила на скриптовом языке Lua. Вкладка "Макросы"

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](#)».



9.2.2.2.6 Шаг 6. 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. 159»).

Рис. 159 – 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 срабатки** 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  **Открыть редактор**.
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  **Активное** 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. 160»).

Окно с заголовком "Дублировать правило" и кнопкой закрытия (X). В центре находится текстовое поле с меткой "Название правила", содержащее текст "Необычное время входа в систему - Дубль". В нижнем правом углу расположены две кнопки: "Сбросить" (серая) и "Дублировать" (синяя).


Рис. 160 – 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 скриптовый 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  **Открыть редактор**.
2. В окне редактирования правила нажмите кнопку  **Удалить**.
3. Подтвердите удаление в открывшемся окне.
4. Правило будет удалено из платформы.

9.2.11 Массовые действия над правилами из боковой панели

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. 161](#)»).

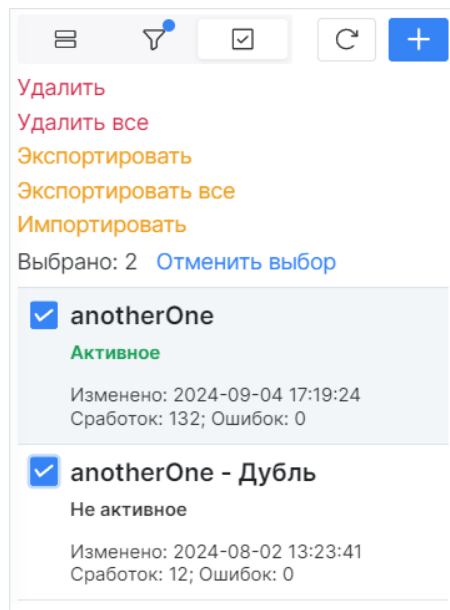


Рис. 161 – Массовые действия над правилами

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

9.2.12 Массовое изменение настроек правил корреляции

1. Перейдите в табличное представление раздела.
2. Выберите правила корреляции, установив соответствующие флаги.
3. Нажмите кнопку **Установить значения**. Откроется окно **Установить значения** (см. «Рис. 162»).

Установить значения ×

Максимальное количество сработок За интервал (секунд)

0 0

Максимальное значение памяти (Мб)

0

Сбросить Сохранить

Рис. 162 – Окно "Установить значения"

4. 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".

5. Нажмите кнопку **Сохранить**. Указанные параметры будут применены ко всем выбранным правилам корреляции.

9.2.13 Действия над результатами сработок правила

9.2.13.1 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.

9.2.13.2 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. 163»).

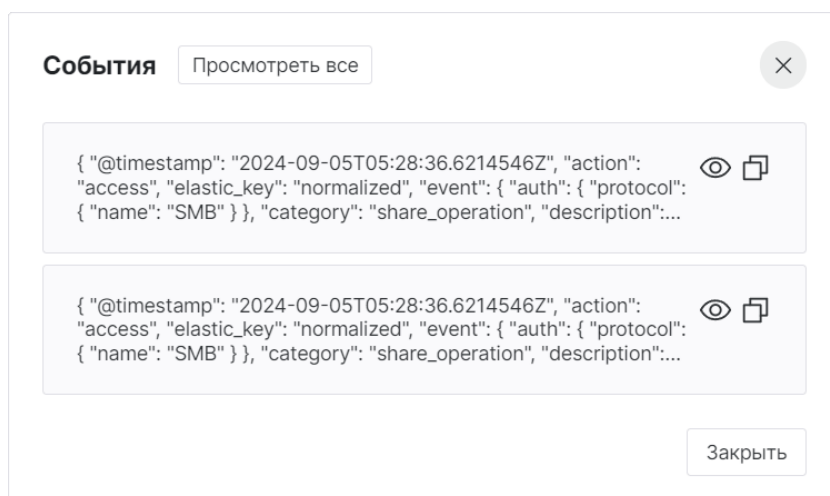



Рис. 163 – Просмотр события

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.

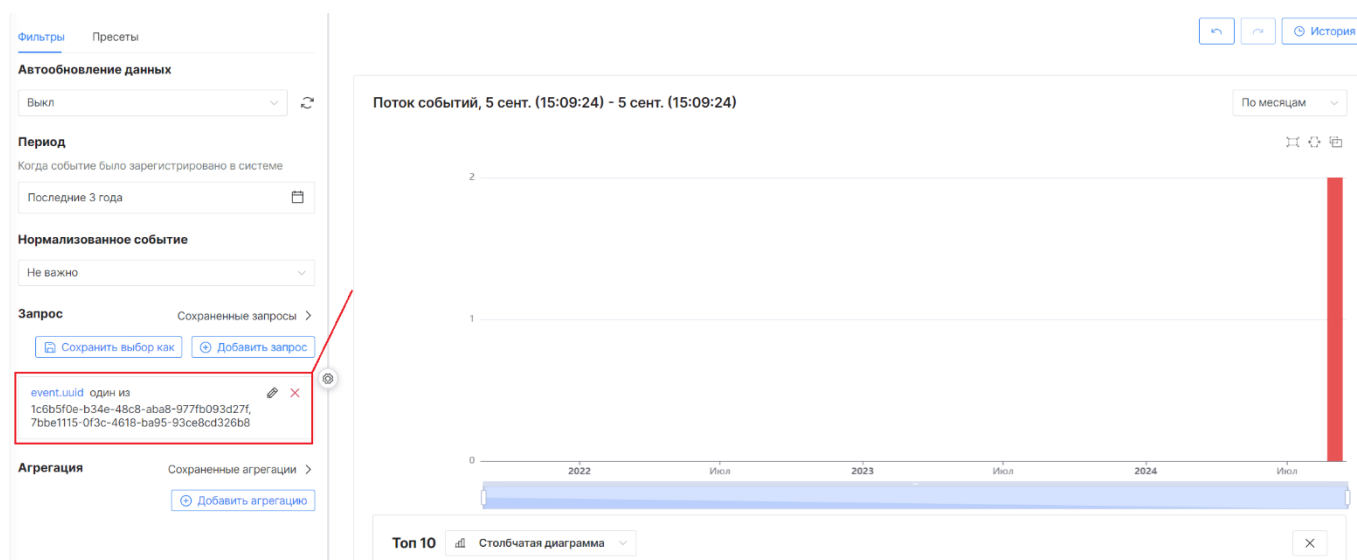


Рис. 164 – Просмотр потока событий по соответствующему запросу

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. 165»).

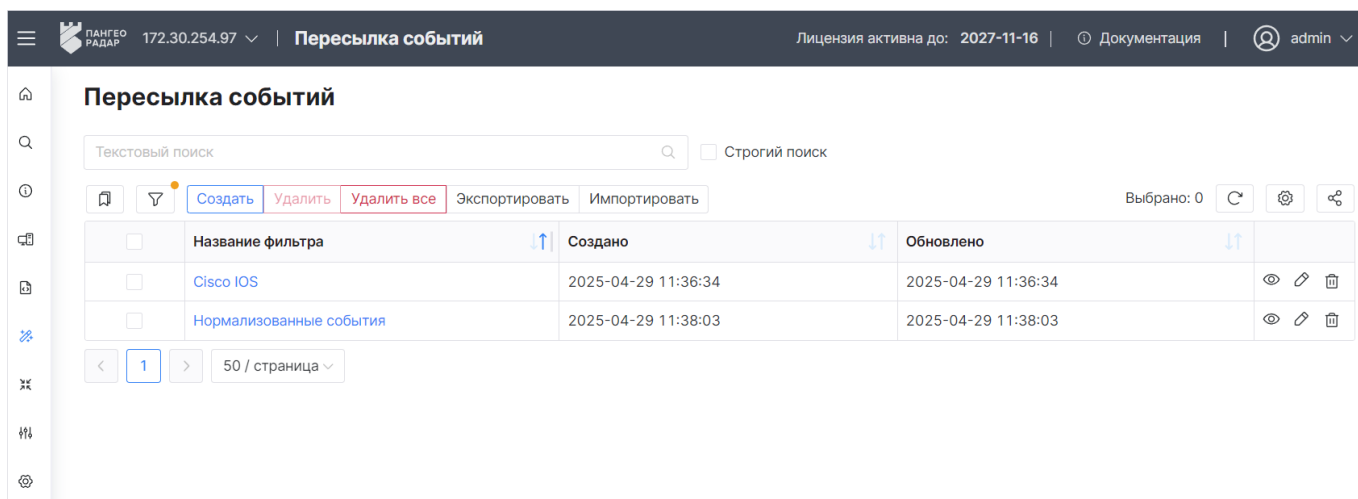


Рис. 165 – Раздел "Пересылка событий"

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 LogProxu** укажите IP-адрес узла, на который необходимо пересылать события (см. «Рис. 166»).

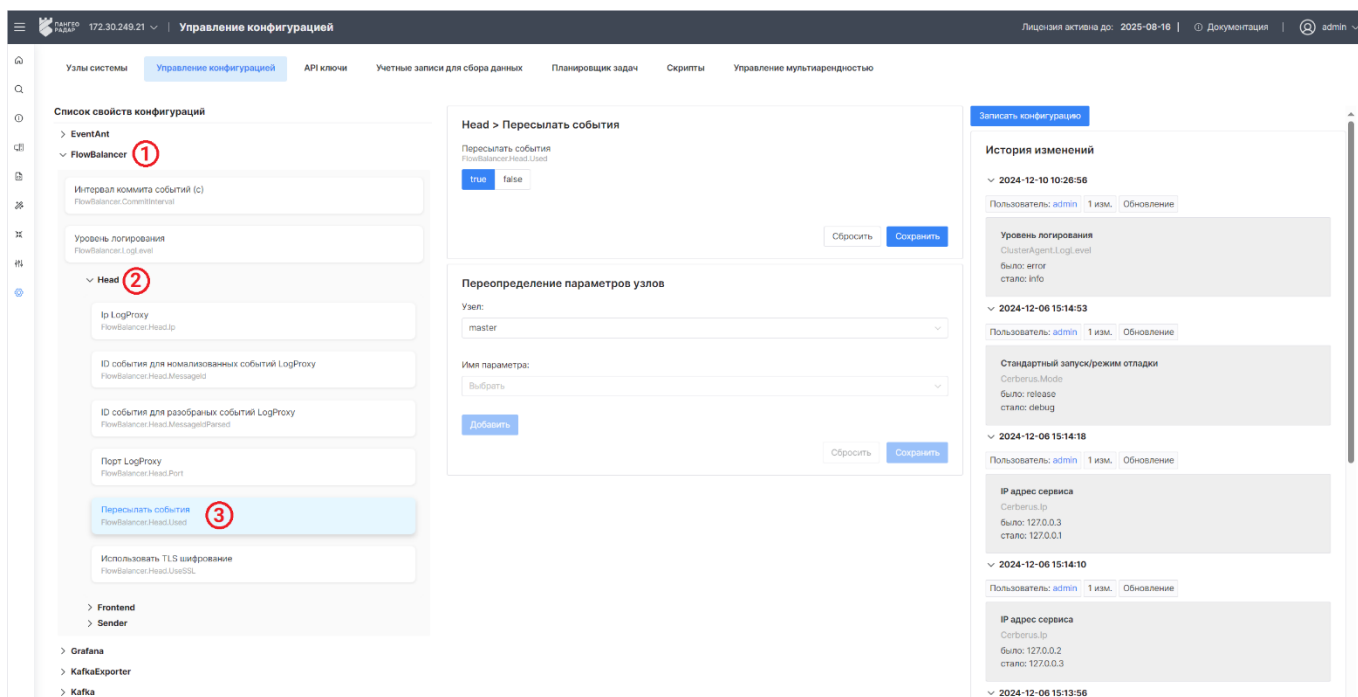


Рис. 166 – Управление конфигурацией сервиса FlowBalancer

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. 167»):
 - **Функция сравнения** -- "Проверить равенство выражений";
 - **Тип выражения** -- "Значение из события" и "Ручной ввод строки" соответственно;
 - **Ключ** -- "elastic_key";
 - **Значение** -- "normalized".

Настроить условие

×

Функция сравнения

Проверить равенство выражений

отрицание

Первое

Тип выражения

Значение из события

Ключ

elastic_key

Второе

Тип выражения

Ручной ввод строки

Значение

normalized

Результат: elastic_key равно normalized


Сбросить

Сохранить

Рис. 167 – Настройка фильтра для пересылки нормализованных событий

- Включите поток событий на основной узел.
- 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. 168»).

ПАНГЕО РАДАР

172.30.254.138

Пересылка событий

База знаний

admin

Cisco IOS

Изменено: 2024-09-05 16:07:37

Пересылка событий Windows

Изменено: 2024-09-05 16:04:56

Удалить

Дублировать

Редактировать

event.logsource равно Cisco IOS

event.subcategory равно значению в массиве из 2 элемента(ов)

Рис. 168 – 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. 169](#)»).

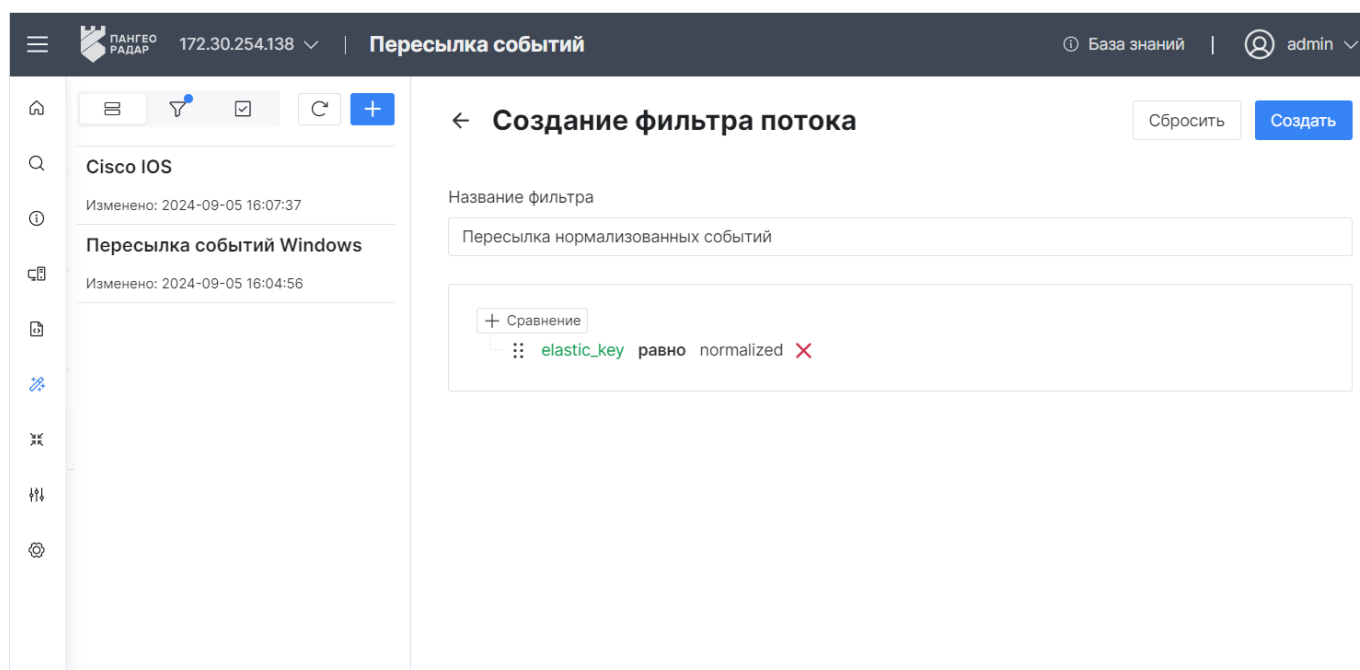


Рис. 169 – Форма "Создание фильтра для пересылки событий"

2. В поле **Название** укажите название фильтра и добавьте условие для сравнения нажав на кнопку + **Сравнение**. Откроется окно "Настроить условие" (см. «[Рис. 170](#)»).

Настроить условие ×

Функция сравнения
 Проверить равенство выражений ▼ ☐ отрицание

Первое

Тип выражения
 Значение из события ▼

Ключ
 elastic_key

Второе

Тип выражения
 Ручной ввод строки ▼

Значение
 normalized

Результат: elastic_key равно normalized Сбросить Сохранить

Рис. 170 – 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. 171](#)»).

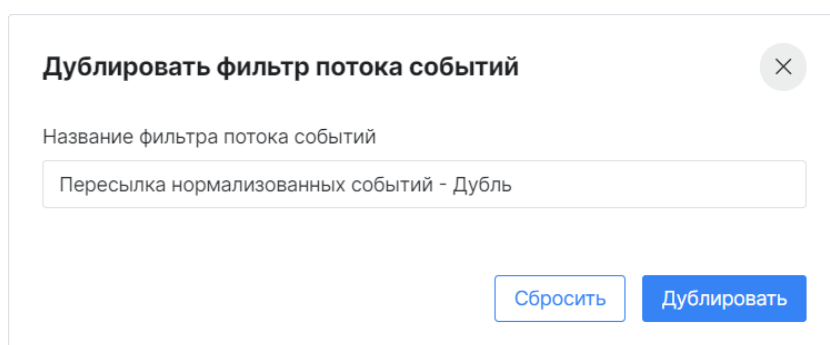


Рис. 171 - Окно "Дублировать фильтр потока событий"

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

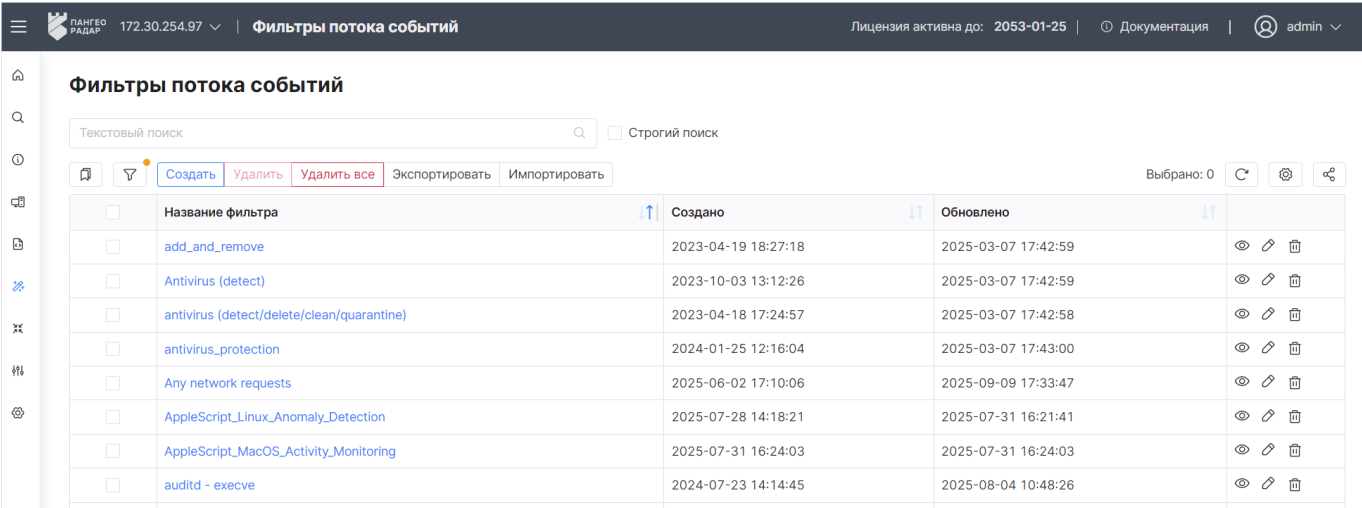
1. Начните процесс удаления фильтра через «[универсальные таблицы](#)» или инструмент «[боковая панель](#)».
2. Подтвердите удаление в открывшемся окне.
3. Фильтр будет удален из платформы.

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. 172»).




Фильтры потока событий			
Текстовый поиск <input type="text"/> <input type="checkbox"/> Строгий поиск			
Создать Удалить Удалить все Экспортировать Импортировать Выбрано: 0			
<input type="checkbox"/>	Название фильтра	Создано	Обновлено
<input type="checkbox"/>	add_and_remove	2023-04-19 18:27:18	2025-03-07 17:42:59
<input type="checkbox"/>	Antivirus (detect)	2023-10-03 13:12:26	2025-03-07 17:42:59
<input type="checkbox"/>	antivirus (detect/delete/clean/quarantine)	2023-04-18 17:24:57	2025-03-07 17:42:58
<input type="checkbox"/>	antivirus_protection	2024-01-25 12:16:04	2025-03-07 17:43:00
<input type="checkbox"/>	Any network requests	2025-06-02 17:10:06	2025-09-09 17:33:47
<input type="checkbox"/>	AppleScript_Linux_Anomaly_Detection	2025-07-28 14:18:21	2025-07-31 16:21:41
<input type="checkbox"/>	AppleScript_MacOS_Activity_Monitoring	2025-07-31 16:24:03	2025-07-31 16:24:03
<input type="checkbox"/>	auditd - execve	2024-07-23 14:14:45	2025-08-04 10:48:26

Рис. 172 – 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. 173»).

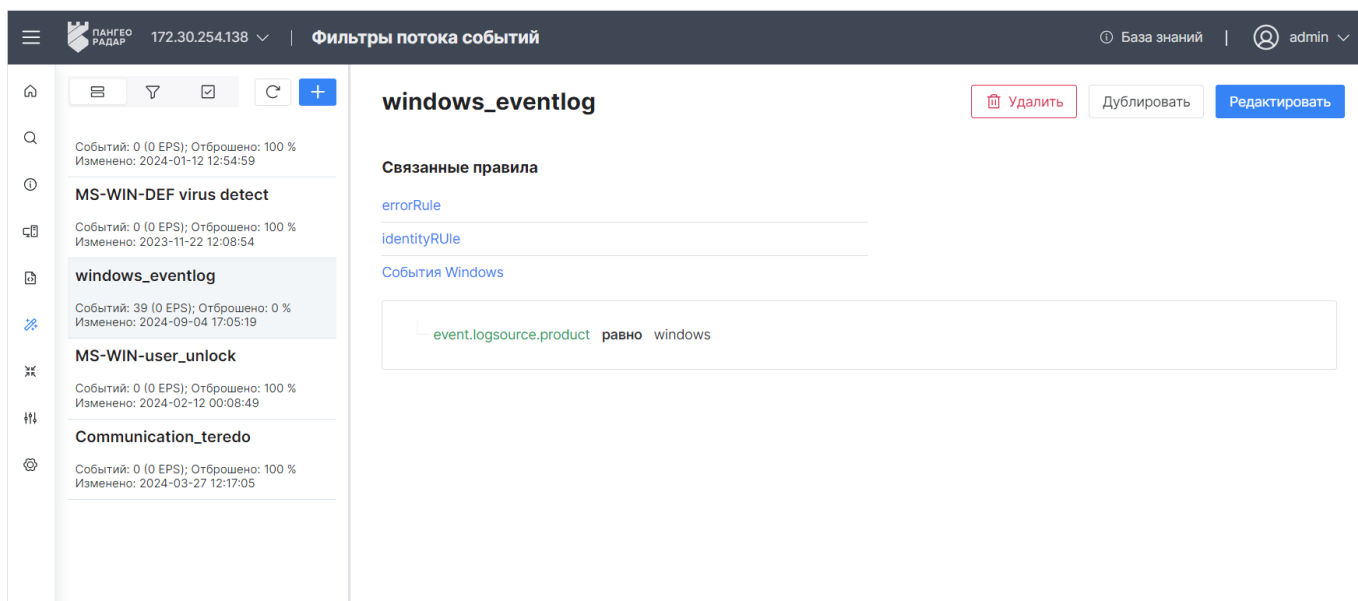


Рис. 173 – Форма просмотра фильтра потока событий

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. 174](#)»).

Рис. 174 – 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. 175»).

Рис. 175 – 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";

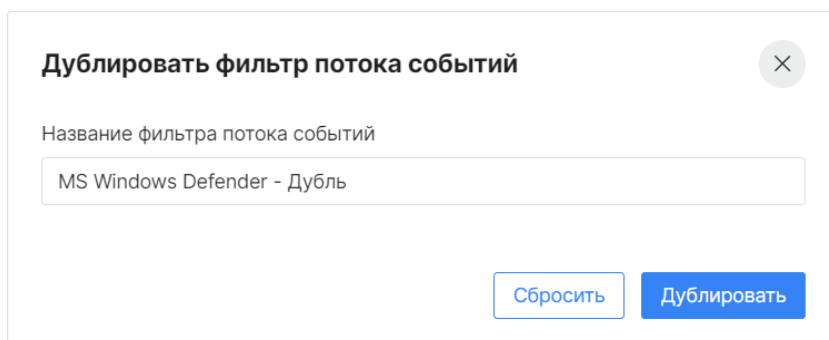
- в поле **Значение** укажите значение, по которому должно проверяться поле, указанное в поле **Ключ**. Если выбрана функция "Проверить наличие в массиве", то укажите массив значений.
 - В блоке **Результат** проверьте правильность заданного выражения.
 - Нажмите кнопку **Сохранить**.
4. Добавьте необходимое 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. 176](#)»).



Дублировать фильтр потока событий

Название фильтра потока событий

MS Windows Defender - Дубль

Сбросить Дублировать

Рис. 176 – 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. 177](#)»).

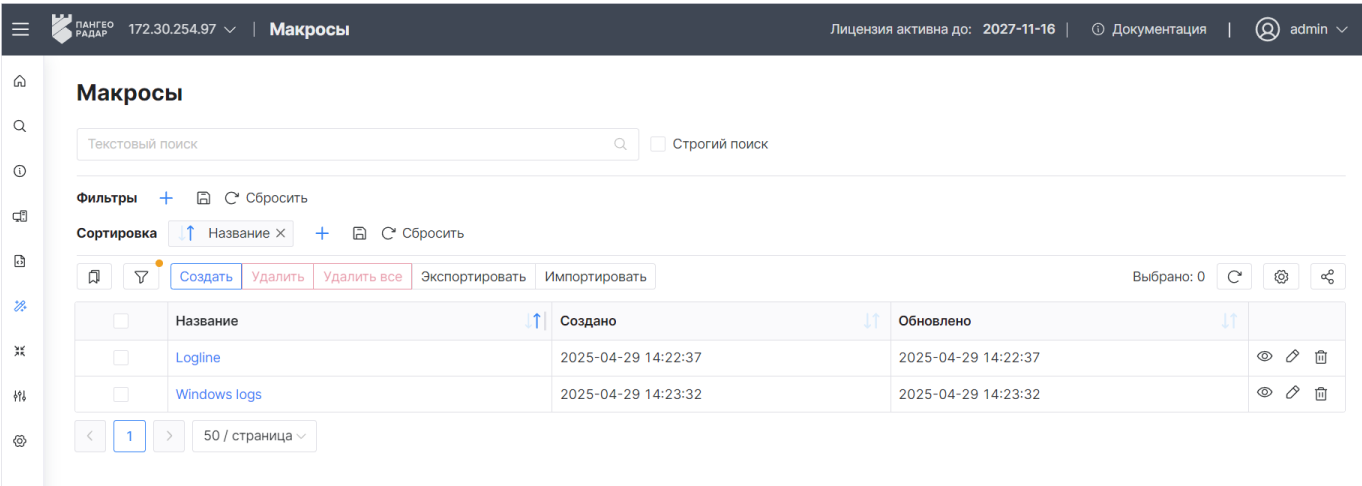


Рис. 177 – Раздел "Макросы"

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. 178»).



Рис. 178 – 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. 179»).



Рис. 179 – 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. 180](#)»).

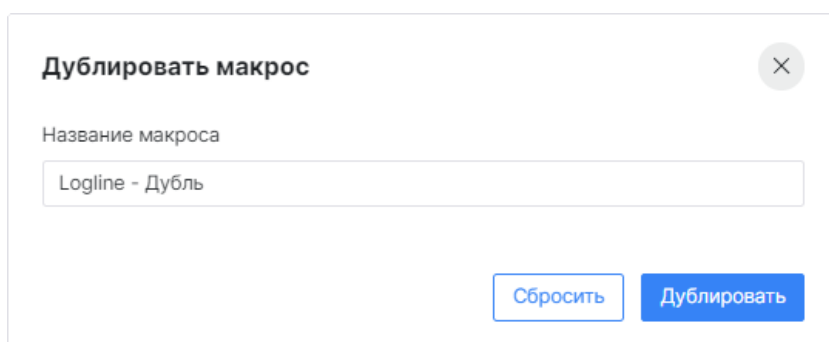


Рис. 180 – Окно "Дублировать макрос"

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.

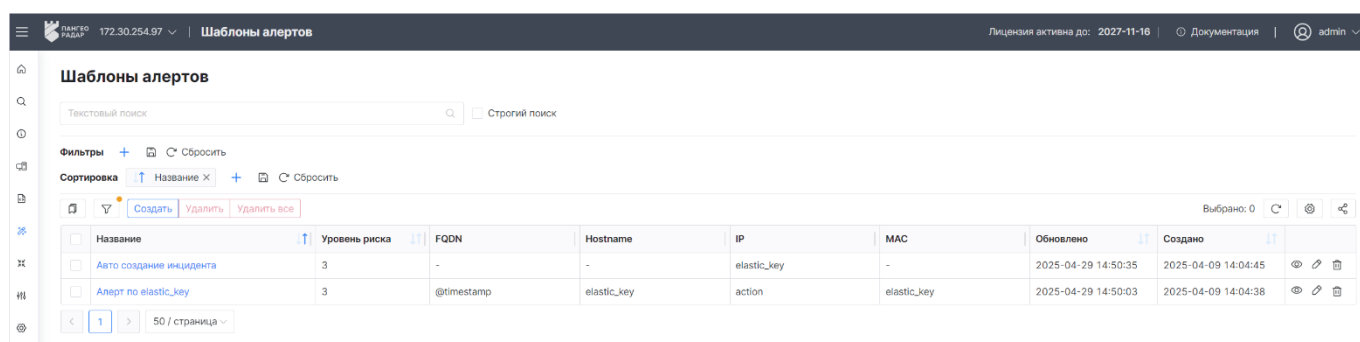
9.6 Шаблоны алертов

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. 181»).




Название	Уровень риска	FQDN	Hostname	IP	MAC	Обновлено	Создано
Авто создание инцидента	3	-	-	elastic_key	-	2025-04-29 14:50:35	2025-04-09 14:04:45
Алерт по elastic_key	3	@timestamp	elastic_key	action	elastic_key	2025-04-29 14:50:03	2025-04-09 14:04:38

Рис. 181 – 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. 182»).

ПАНЕЛЬ РАДАР 172.30.254.138 | Шаблоны алертов База знаний admin

Авто создание инцидента

Уровень риска: 0 1 2 3 4 5 6 7 8 9 10

☒ Создать инцидент
 ☐ Назначить инцидент пользователю
 ☐ Логировать первое и последнее событие
 Логировать указанное число событий

IP актива: elastic_key
 FQDN актива: action
 Hostname актива: event.application.risk
 MAC актива: @timestamp

Техники Mitre:
 Группа инцидентов:

Шаблон:

Рис. 182 –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. 183](#)»).

← Создать шаблон Создать

Название шаблона: Авто назначение

Уровень риска: 0 1 2 3 4 5 6 7 8 9 10

☐ Создать инцидент
 ☒ Назначить инцидент пользователю
 ☐ Логировать первое и последнее событие
 Логировать указанное число событий

IP актива: action
 FQDN актива: elastic_key
 Hostname актива: event.packet
 MAC актива: @timestamp

Техники Mitre: T1548, T1548.001
 Группа инцидентов:

Шаблон: Авто назначение

Рис. 183 – 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 чтобы инцидент был создан в статусе "Назначен";
- 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 **Группа инцидентов** выберите группу инцидентов, в которую автоматически будет помещен инцидент, созданный в результате "сработки" правила корреляции;
- 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. 184](#)»).

- **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. 186»).

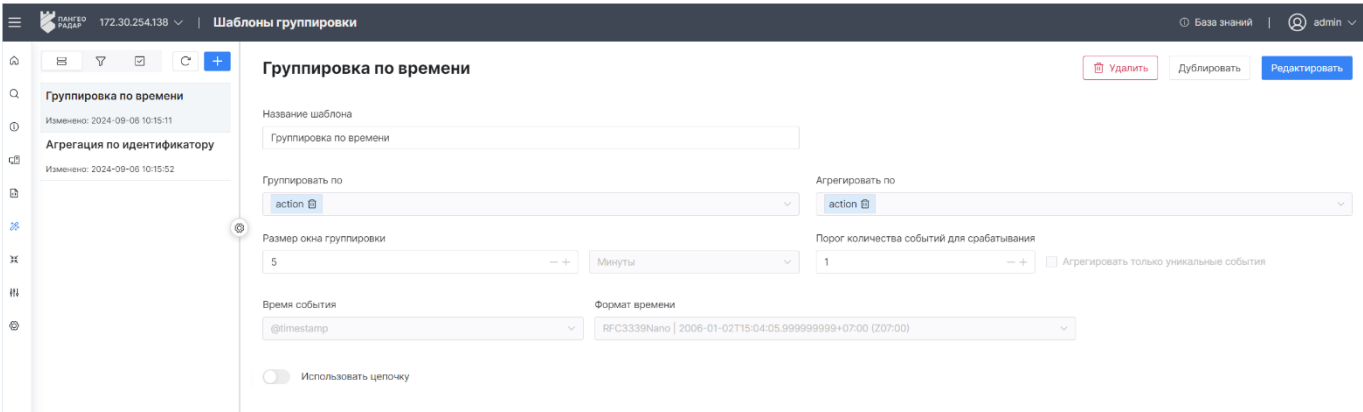


Рис. 186 – Форма просмотра шаблона группировки

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. 187»).

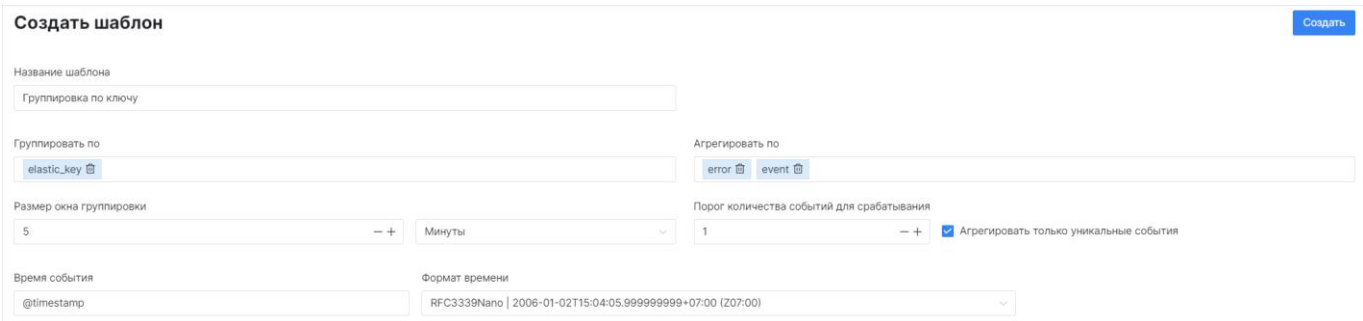


Рис. 187 – Форма "Создать шаблон"

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. 188](#)»).

Настроить условие

Функция сравнения
Проверить наличие в массиве

Строка
Тип выражения
Значение из события

Ключ
event.alert

Массив
Тип выражения
Массив строк

Значение
event
event.anomaly

Результат: event.alert равно значению в массиве из 2 элемента(ов)

Сбросить Сохранить

Рис. 188 – 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. 189»):

The screenshot shows a configuration interface for event chain conditions. At the top, there's a tab labeled '+ Сравнение'. Below it, a rule is defined: 'elastic_key равно значению в массиве' followed by a text input field containing '56723123476'. Below this rule, there's a section for 'Количество событий' (Number of events) with a numeric input set to '2' and increment/decrement buttons. To the right of the input are two options: a checked checkbox for 'Точное совпадение количества событий' (Exact match of the number of events) and a toggle switch for 'Отсутствует' (Absent), which is currently in the 'off' position. A red 'X' icon is visible in the top right corner of the configuration area.

Рис. 189 – 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. 190»).

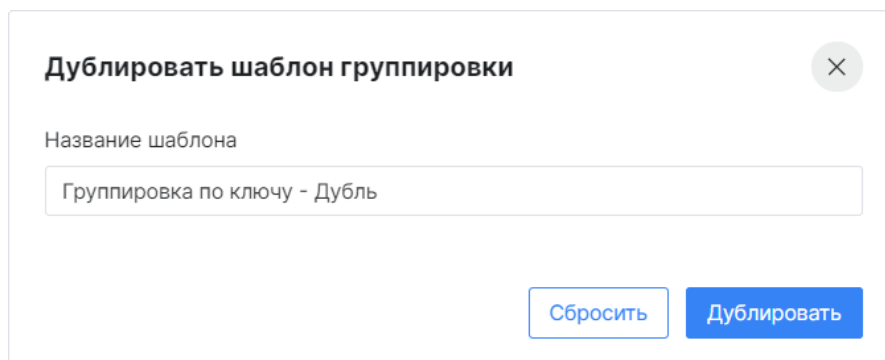


Рис. 190 – Окно "Дублировать шаблон группировки"

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** (см. «Рис. 191»).


Название	Описание	Записей	Создано
domain_controllers	# target.host.hostname #target.host.ip	2	2025-01-09 17:36:52
Domain controllers	Список контроллеров домена Пример: FQDN, IP, is_dc, RODC, Hostname	0	2023-10-09 12:50:58
administrators_group_names	Содержит имена административных групп	1	2025-06-25 15:51:58
Executable files: extensions, formats	-	27	2025-05-15 12:45:48
local-networks	-	3	2023-10-09 12:51:12
DNS-servers	Список DNS серверов	0	2023-10-09 12:51:53
customer domain controllers	# Пример: FQDN, IP, is_dc, RODC, Hostname	0	2023-09-28 14:43:22
IOCs	IOCs	0	2025-07-03 17:14:34

Рис. 191 – Раздел "Табличные списки"

В разделе отображается следующая информация:

- **Название** – наименование табличного списка;
- **Описание** – дополнительные сведения о табличном списке;
- **Записей** – количество записей в табличном списке;
- **Создано** – дата и время создания табличного списка.


9.8.2 Просмотр табличного списка

Для просмотра табличного списка нажмите кнопку  в нужной строке таблицы или нажмите по ссылке в колонке **Название**. Откроется представление через боковую панель и форма просмотра выбранного табличного списка (см. «Рис. 192»).

← Local IP addresses	Удалить	Дублировать	Редактировать
Текстовый поиск	Строгий поиск	Выбрано: 0	
Добавить запись	Удалить	Удалить все	Экспортировать все
Импортировать			
_id	Время жизни записи	ip	
127.0.0.1	-	127.0.0.1	
192.168.0.1	-	192.168.0.1	

Рис. 192 – Форма просмотра табличного списка

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`.

9.8.3 Создание табличного списка

1. Нажмите кнопку **Создать табличный список**. Откроется окно "Создание табличного списка" (см. «[Рис. 193](#)»).

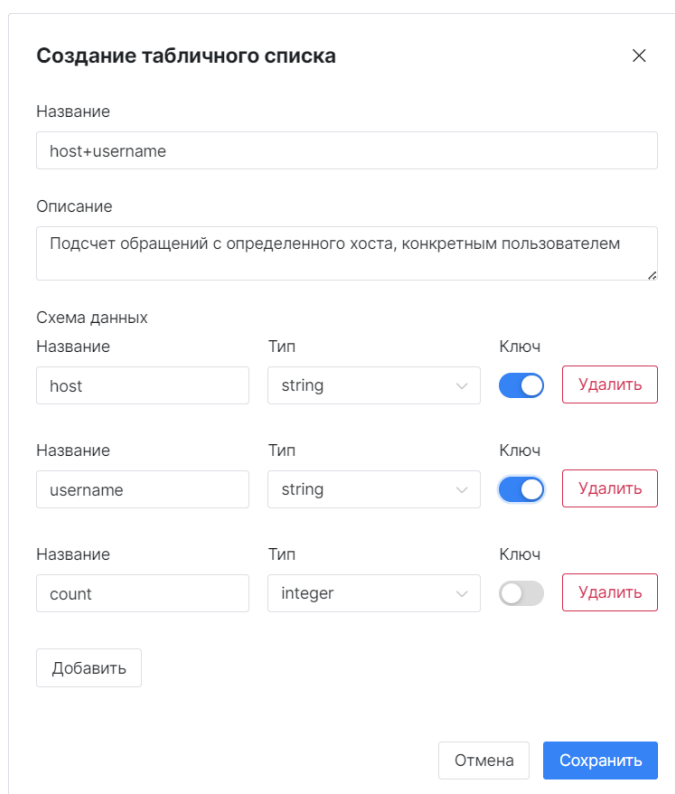


Рис. 193 – Окно "Создание табличного списка"

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;

Примечание: в качестве названия поля схемы данных нельзя использовать следующие значения: `_id`, `_ttl`, `rewrite`.

- в поле **Тип** из выпадающего списка выберите тип поля: `string`, `integer`, `bigint`, `double`, `ip-address`, `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**.

9.8.4 Работа с записями табличного списка

9.8.4.1 Добавление записи

1. Выберите табличный список и нажмите кнопку **Добавить запись**. Откроется окно "Создание записи" (см. «Рис. 194»).

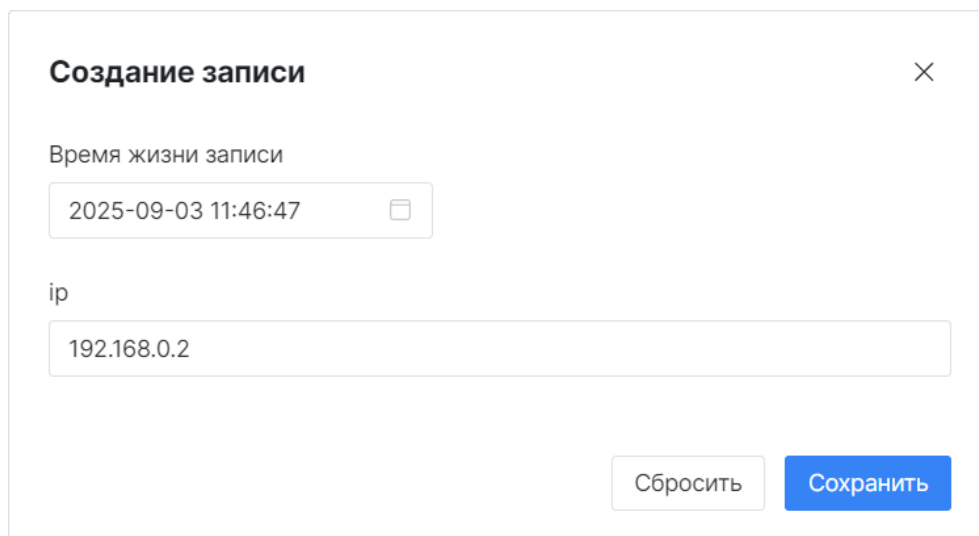




Рис. 194 – Окно "Создание записи"

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

9.8.4.2 Редактирование записи

1. Выберите из списка необходимый табличный список, найдите нужную запись и в соответствующей строке нажмите кнопку .
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

9.8.4.3 Дублирование записи

1. Выберите из списка необходимый табличный список, найдите нужную запись и в соответствующей строке нажмите кнопку .
2. При необходимости укажите в окне необходимую информацию.
3. Нажмите кнопку **Сохранить**.

9.8.4.4 Экспорт записей

Платформа позволяет экспортировать записи табличного списка в файлы следующих форматов:

- csv;
- xlsx;
- json.

Для экспорта записей выполните следующие действия:

1. Выберите из списка необходимый табличный список и нажмите кнопку **Экспортировать все**.
2. Из выпадающего списка выберите формат, в который необходимо экспортировать записи.
3. В открывшемся окне нажмите кнопку **Сохранить** и укажите путь для сохранения файла.

9.8.4.5 Импорт записей

1. Выберите из списка необходимый табличный список и нажмите кнопку **Импортировать**. Откроется окно "Импортировать" (см. «[Рис. 195](#)»).

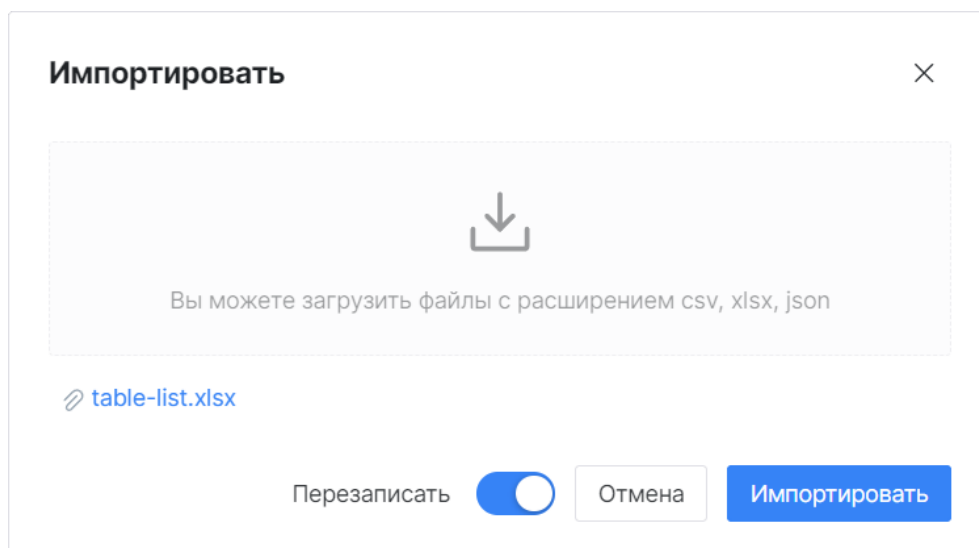



Рис. 195 – Импорт записей табличного списка

2. В открывшемся окне укажите путь к файлу с записями.
3. Если необходимо перезаписать данные в табличном списке, то включите соответствующий переключатель.
4. Нажмите кнопку **Импортировать**.

9.8.4.6 Удаление записи

1. Выберите из списка необходимый табличный список, найдите нужную запись и в соответствующей строке нажмите кнопку .
2. Подтвердите удаление в открывшемся окне.
3. Запись будет удалена из табличного списка.

9.8.4.7 Массовое удаление записей

Массовое удаление записей можно выполнить двумя способами.

Способ 1:

1. Выберите из списка необходимый табличный список и установите флаги напротив нужных записей.
2. Нажмите кнопку **Удалить**.
3. Подтвердите удаление в открывшемся окне.
4. Выбранные записи будут удалены из табличного списка.

Способ 2:

1. Выберите из списка необходимый табличный список и нажмите кнопку **Удалить все**.
2. Подтвердите удаление в открывшемся окне.
3. Все записи будут удалены из табличного списка.

9.8.5 Редактирование табличного списка

1. Начните процесс редактирования табличного списка через «[универсальные таблицы](#)» или инструмент «[боковая панель](#)».
2. Внесите необходимые изменения.
3. Нажмите кнопку **Сохранить**.

9.8.6 Дублирование табличного списка

1. Выберите из списка необходимый табличный список и нажмите кнопку **Дублировать**. Откроется окно "Дублирование табличного списка" (см. «[Рис. 196](#)»).

Дублирование табличного списка ✕

Название
host+username-дубль

Описание
Подсчет обращений с определенного хоста, конкретным пользователем

Схема данных

Название	Тип	Ключ	
host	string	<input checked="" type="checkbox"/>	Удалить
username	string	<input checked="" type="checkbox"/>	Удалить
count	integer	<input type="checkbox"/>	Удалить

Добавить

Отмена Сохранить

Рис. 196 – Окно "Дублирование табличного списка"

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

9.8.7 Импорт табличных списков

1. Начните процесс импорта табличных списков через [«универсальные таблицы»](#) или инструмент [«боковая панель»](#).
2. В открывшемся окне укажите путь к архиву с табличными списками.
3. Нажмите кнопку **Открыть**.

9.8.8 Экспорт табличных списков

1. Начните процесс экспорта табличных списков через [«универсальные таблицы»](#) или инструмент [«боковая панель»](#).
2. Будет сформирован архив с табличными списками в формате .zip.
3. Нажмите кнопку **Скачать** и укажите путь для сохранения архива.

9.8.9 Синхронизация табличных списков

Если **Платформа Радар** работает в режиме мультиарендности, то табличные списки при необходимости можно синхронизировать между подчиненными инстансами. Подробнее о процессе синхронизации см. раздел [«Синхронизация пользовательского контента»](#).

9.8.10 Удаление табличного списка

1. Начините процесс удаления табличного списка через «[универсальные таблицы](#)» или инструмент «[боковая панель](#)».
2. Подтвердите удаление в открывшемся окне.
3. Табличный список будет удален из платформы.

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. 197](#)»).

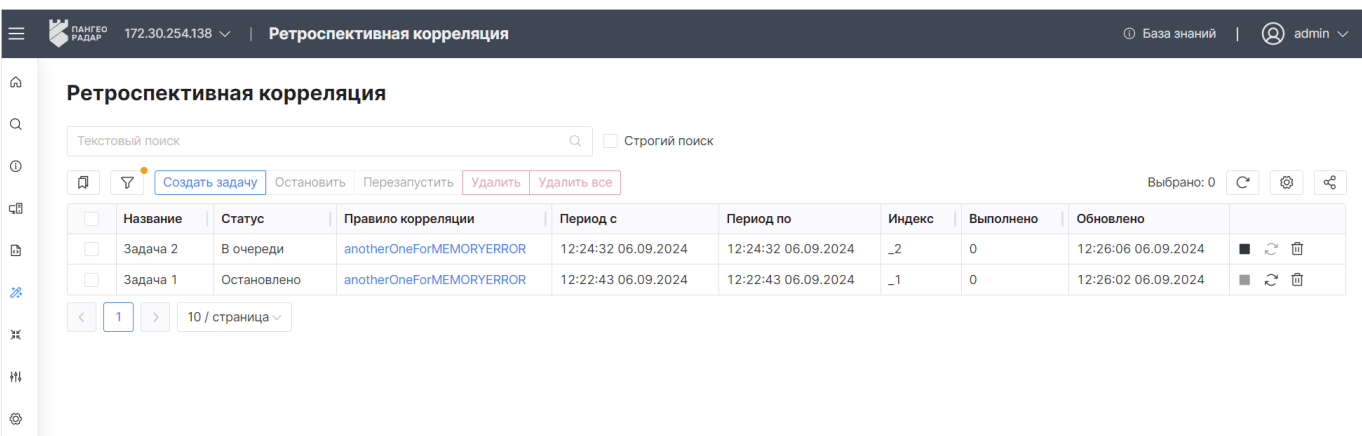


Рис. 197 – Раздел "Ретроспективная корреляция"

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. 198](#)»).

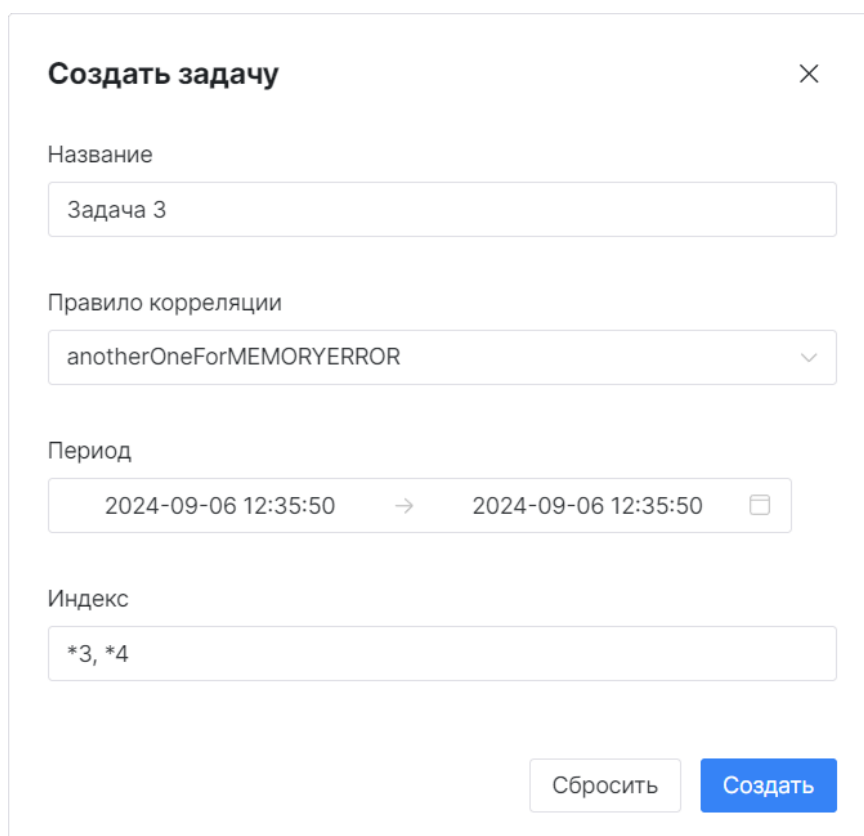




Рис. 198 – Окно "Создать задачу"

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 запущено.

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. 199](#)»).

The screenshot displays the 'Основные параметры' (Main Parameters) configuration page. The interface includes a top navigation bar with the 'Основные параметры' tab selected. The main content area is divided into several sections:

- Общие** (General): Includes fields for 'Название клиента' (Client Name), 'Риск принят: количество дней по умолчанию' (Risk accepted: default number of days) set to 90, 'Расположения' (Locations) with 'Москва' (Moscow) selected, 'Адрес системы' (System Address) set to 172.30.252.105, 'SSL сертификат' (SSL Certificate) and 'Ключ SSL сертификата' (SSL Certificate Key) upload buttons, and a 'Группа пользователей' (User Group) dropdown.
- Стратегия идентификации активов** (Asset Identification Strategy): Includes 'Стратегия идентификации активов' (Asset Identification Strategy) with radio buttons for IP (selected), MAC, and FQDN, and 'Совпадение PQDN' (PQDN Match) with a checkbox for 'Включает совпадение по имени хоста (PQDN)' (Includes match by host name (PQDN)).
- Настройки аудита действий** (Action Audit Settings): Includes 'Перечень логируемых действий' (List of actions to be logged) with a dropdown menu showing 'Удаление X', 'Просмотр записи X', 'Изменение X', 'Создание X', 'Импорт X', and 'Экспорт X', and 'Время жизни аудита (секунды)' (Audit lifetime (seconds)) set to 2592000.
- Переоткрытие инцидентов** (Incident Reopening): Includes 'Создавать новый инцидент для повторных происшествий, если инцидент закрыт' (Create a new incident for recurring incidents if the incident is closed) with radio buttons for 'Создавать новый инцидент' (Create a new incident) and 'Перекрывать инцидент' (Reopen incident), and 'Минимальный уровень риска для повторного открытия инцидентов' (Minimum risk level for reopening incidents) with radio buttons for 'Высокий' (High), 'Средний' (Medium), 'Низкий' (Low), and 'Отсутствует' (None).
- Создание инцидентов из результатов сканирования** (Incident Creation from Scan Results): Includes 'Автоматически создавать инциденты при импорте результатов сканирования' (Automatically create incidents when importing scan results) checkbox and 'Минимальный уровень важности для открытия инцидента' (Minimum importance level for opening an incident) slider set to 1.

Рис. 199 – Раздел "Основные параметры"

Раздел содержит следующие блоки:

- **Общее** – настройка значений по умолчанию для следующих параметров платформы:
 - Название клиента;
 - Количество дней, по истечении которых будет принят риск инцидента;
 - Расположения (используются в сведениях об активах);
 - Адрес системы, SSL-сертификат, Ключи SSL сертификата - настройка параметров подключения и входа в веб-интерфейс платформы. Например, данные параметры могут быть настроены для работы платформы DNS-инфраструктуре;
 - Группа пользователей, которая будет назначаться по умолчанию для инцидентов, связанных с активами без назначенного "ответственного пользователя".
- **Создание инцидентов из результатов сканирования** – настройка автоматического создания инцидентов;
- **Стратегия идентификации активов** – настройка сравнения отдельных атрибутов актива 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;
- **Настройка аудита действий** – настройка перечня действий пользователей, которые будут журналироваться в платформе. Просмотр журнала действий пользователей выполняется в разделе **Администрирование** → **Пользователи и роли** → вкладка «Аудит действий»);
- **Переоткрытие инцидентов** – настройка поведения платформы при возникновении повторных происшествий.

После внесения любых изменений, для того чтобы они вступили в силу, необходимо нажать кнопку **Сохранить**.

Общее

Пример блока приведен на [Рис. 200](#).

Общее

Название клиента

Название клиента

Риск принят: количество дней по умолчанию

90 — +

Принятие риска инцидента установит это значение в качестве срока по умолчанию (параметр "Принять до"). Чтобы оставить значение даты "Принять до" пустым, укажите значение 0.

Расположения

Москва Ростов +

Адрес системы *

172.30.252.105

SSL сертификат

Выбрать файл

Ключ SSL сертификата

Выбрать файл

Группа пользователей по умолчанию для инцидентов, связанных с активами, без определенного "ответственного пользователя"

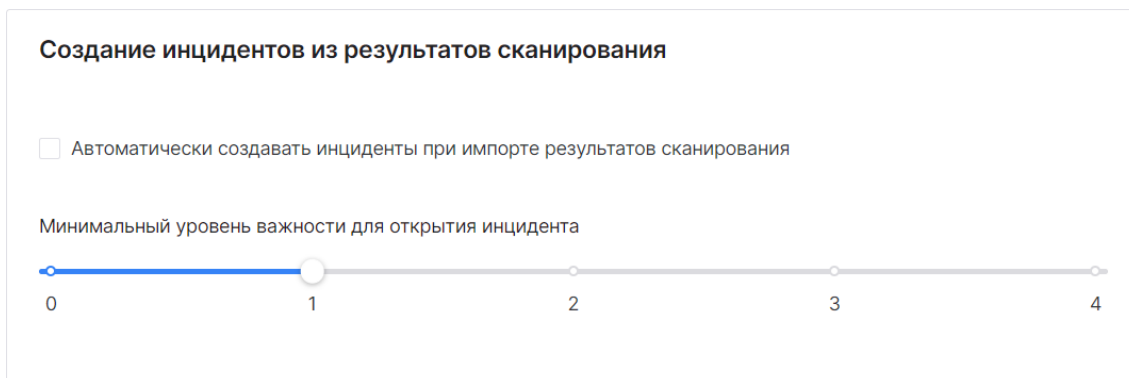
Рис. 200 – Раздел "Основные параметры". Блок "Общее"

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 **Расположения** укажите геоданные организации;
- в поле **Адрес системы** при необходимости измените IP/FQDN адрес платформы, который был указан при установке;
- в полях **SSL сертификат** и **Ключ SSL сертификата** загрузите предварительно сгенерированный сертификат и соответствующий ключ;
- 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".

Создание инцидентов из результатов сканирования

Пример блока приведен на [Рис. 201](#).



Создание инцидентов из результатов сканирования

☐ Автоматически создавать инциденты при импорте результатов сканирования

Минимальный уровень важности для открытия инцидента

0 1 2 3 4

Рис. 201 – Раздел "Основные параметры". Блок "Создание инцидентов из результатов сканирования"

Выполните следующие действия:

- при необходимости включите автоматическое создание инцидентов при импорте результатов сканирования, установив соответствующий флаг;
- установите минимальный уровень важности для открытия инцидента. Важность – это числовой показатель важности угрозы. Данный показатель будет учитываться в процессе создания инцидента и будет влиять на показатель "срочность инцидента".

Стратегия идентификации активов

Пример блока приведен на «[Рис. 202](#)».

Стратегия идентификации активов

Стратегия идентификации активов

☒ IP ☐ MAC ☐ FQDN

Совпадение PQDN

☐ Включает совпадение по имени хоста (PQDN), где выбрана стратегия идентификации FQDN.

Внимание! Если имя хоста определено в нескольких доменах, совпадение по PQDN не проверяется, т.к. мы не знаем какой домен правильный

Рис. 202 – Раздел "Основные параметры". Блок "Стратегия идентификации активов"

Выполните следующие действия:

- в поле **Стратегия идентификации активов** выберите одну из стратегий (IP, FQDN, MAC), которая будет применена при идентификации активов;
- 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.

Настройки аудита действий

Пример блока приведен на [Рис. 203](#).

Настройки аудита действий

Перечень логируемых действий

Удаление × Просмотр записи × Изменение × Создание × Импорт × Экспорт ×

Время жизни аудита (секунды)

2592000

При указании 0 данные хранятся бессрочно

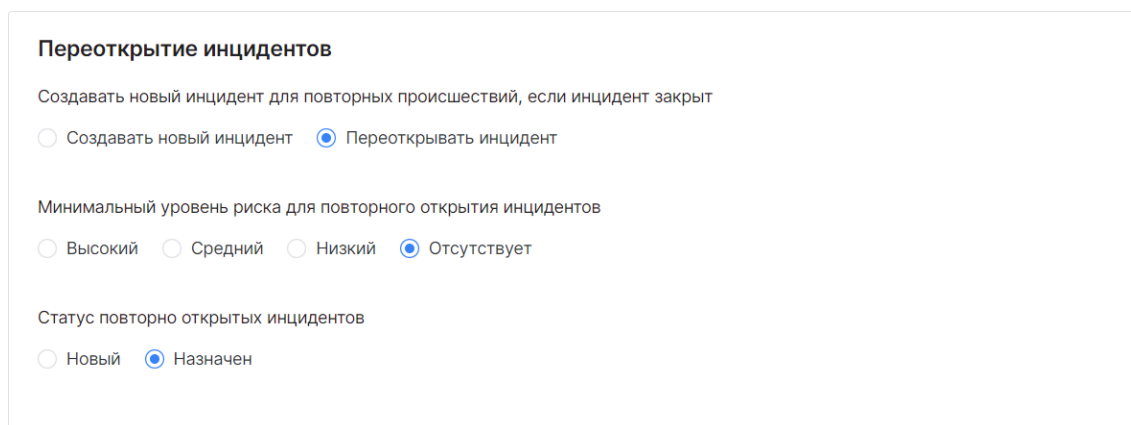
Рис. 203 – Раздел "Основные параметры". Блок "Настройки аудита действий"

Выполните следующие действия:

- в поле **Перечень логируемых действий** из выпадающего списка выберите действия пользователей, которые необходимо отслеживать. Для отслеживания доступны следующие действия пользователей над сущностями:
 - **Создание;**
 - **Просмотр;**
 - **Изменение;**
 - **Импорт;**
 - **Экспорт;**
 - **Удаление.**
- в поле **Время жизни аудита (секунды)** укажите время жизни записи о действии пользователя в платформе. При значении "0" записи будут храниться бессрочно.

Переоткрытие инцидентов

Пример блока приведен на «Рис. 204».



Переоткрытие инцидентов

Создавать новый инцидент для повторных происшествий, если инцидент закрыт

☐ Создавать новый инцидент ☒ Переоткрывать инцидент

Минимальный уровень риска для повторного открытия инцидентов

☐ Высокий ☐ Средний ☐ Низкий ☒ Отсутствует

Статус повторно открытых инцидентов

☐ Новый ☒ Назначен

Рис. 204 – Раздел "Основные параметры". Блок "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. 205»).

Скриншот интерфейса раздела "Оповещения по задержкам".

Верхняя панель: Логотип "РАДAR", IP-адрес 172.30.254.155, заголовок "Оповещения по задержкам", лицензия активна до 2024-12-25, ссылки на документацию и профиль администратора (admin).

Основное меню: Основное, **Оповещения по задержкам**, Черный список ID плагинов. Кнопка "Сохранить".

Четыре карточки настроек по уровням риска:

- Высокий**: Нормально 3, Небольшая задержка 5, Задержка 10. Создан 2020-12-09 23:13:30, Обновлено 2020-12-09 23:13:30.
- Средний**: Нормально 5, Небольшая задержка 28, Задержка 56. Создан 2020-12-09 23:13:30, Обновлено 2024-11-08 13:01:12.
- Низкий**: Нормально 28, Небольшая задержка 84, Задержка 168. Создан 2020-12-09 23:13:30, Обновлено 2020-12-09 23:13:30.
- Отсутствует**: Нормально 84, Небольшая задержка 0, Задержка 0. Создан 2020-12-09 23:13:30, Обновлено 2024-11-08 13:01:21.

Настройка оповещений:

- ☐ Отправлять оповещение при каждом изменении времени обработки
- ☒ Отправлять оповещение единожды после достижения последнего показателя времени удержания
 - Через 1 день
- ☒ Для инцидентов с риском "Высокий", после достижения последнего показателя времени удержания, отправлять оповещение регулярно
 - Через 5 дней
- ☐ Для инцидентов с риском "Средний", после достижения последнего показателя времени удержания, отправлять оповещение регулярно
 - Через 5 дней
- ☒ Для инцидентов с риском "Низкий", после достижения последнего показателя времени удержания, отправлять оповещение регулярно
 - Через 5 дней
- ☐ Для инцидентов с риском "Отсутствует", после достижения последнего показателя времени удержания, отправлять оповещение регулярно
 - Через 5 дней
- ☐ Отправлять группу сообщений раз в неделю
 - Каждый Понедельник

Тексты оповещений:

Общий текст, отправляемый в каждом оповещении: [Поле для ввода]

Текст сообщения об изменении времени удержания инцидента от "Задержки" до "Недопустимого": [Поле для ввода]

Текст сообщения об изменении времени удержания инцидента от "Небольшой задержки" до "Задержки": [Поле для ввода]

Текст сообщения об изменении времени удержания инцидента от "Нормального" до "Небольшой задержки": [Поле для ввода]

Рис. 205 – 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

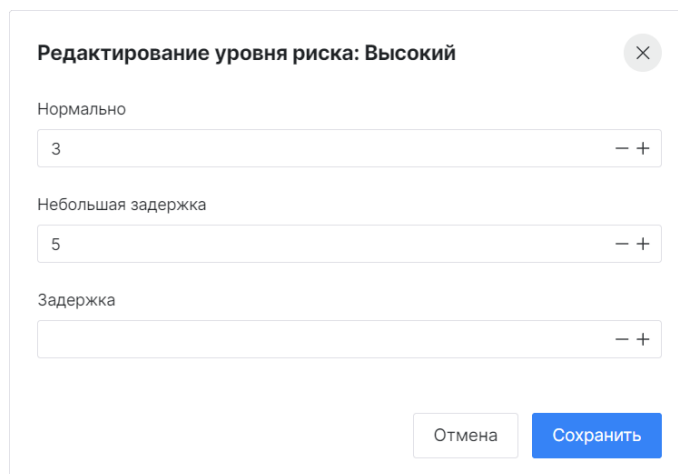
Для каждого уровня риска (высокий, средний, низкий, отсутствует) можно настроить 3 контрольных отсечки по времени разбора инцидента:

- **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. 206»).



Редактирование уровня риска: Высокий

Нормально

3

Небольшая задержка

5

Задержка

Отмена Сохранить

Рис. 206 – Окно "Редактирование уровня риска"

- В полях **Нормально**, **Небольшая задержка**, **Задержка** укажите необходимое количество дней.
- 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. 207»).

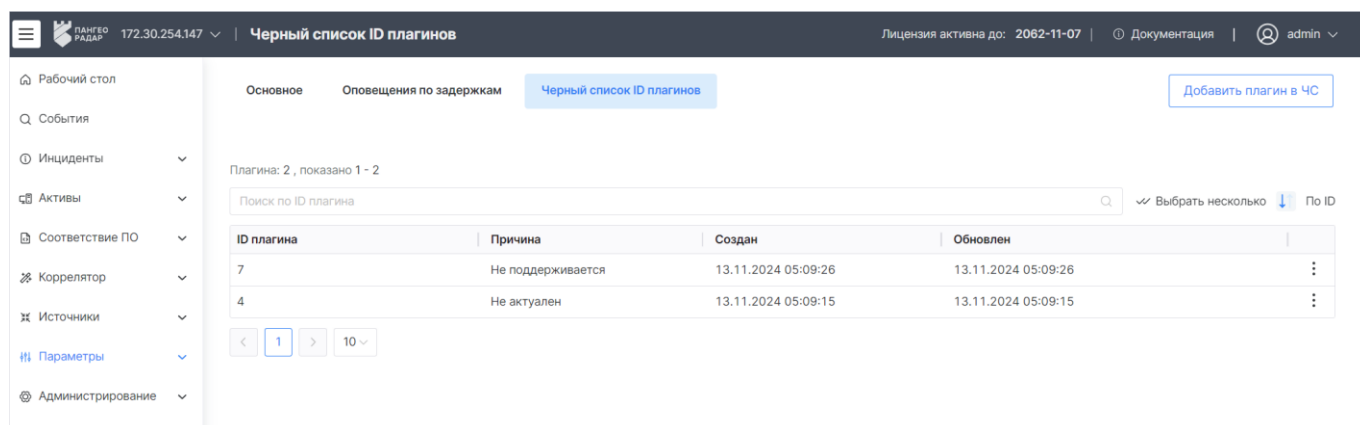


Рис. 207 – Раздел "Черный список ID плагинов"

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. 208»).

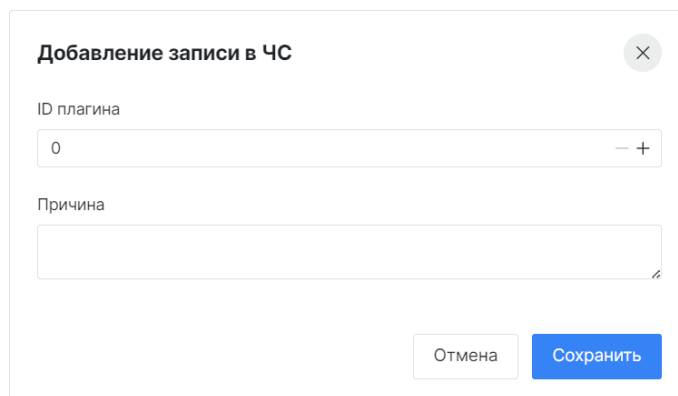


Рис. 208 – Добавление плагина в ЧС"

2. Укажите в окне следующую информацию:

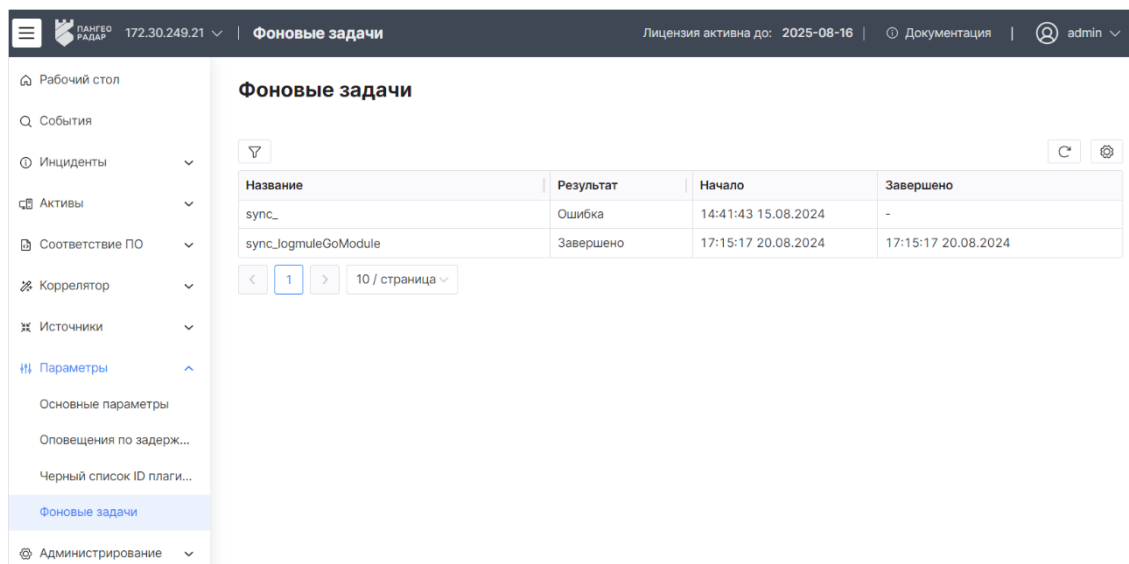
- в поле **ID** укажите идентификатор плагина;
- в поле **Причина** укажите причину добавления плагина в черный список.

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. 209»).



Название	Результат	Начало	Завершено
sync_	Ошибка	14:41:43 15.08.2024	-
sync_logmuleGoModule	Завершено	17:15:17 20.08.2024	17:15:17 20.08.2024

Рис. 209 – 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 экземпляров интеграции.

Экземпляры интеграции могут находиться в следующих состояниях:

- **Активно** – по экземпляру интеграции выполняется взаимодействие со сторонней системой;
- **Неактивно** – по экземпляру интеграции не выполняется взаимодействие со сторонней системой.

Примечание: Процессы работы с различными типами интеграций рассмотрены в соответствующих разделах.

Все действия над экземплярами интеграций выполняются в разделе **Параметры → Интеграции** (см. «[Рис. 210](#)»).

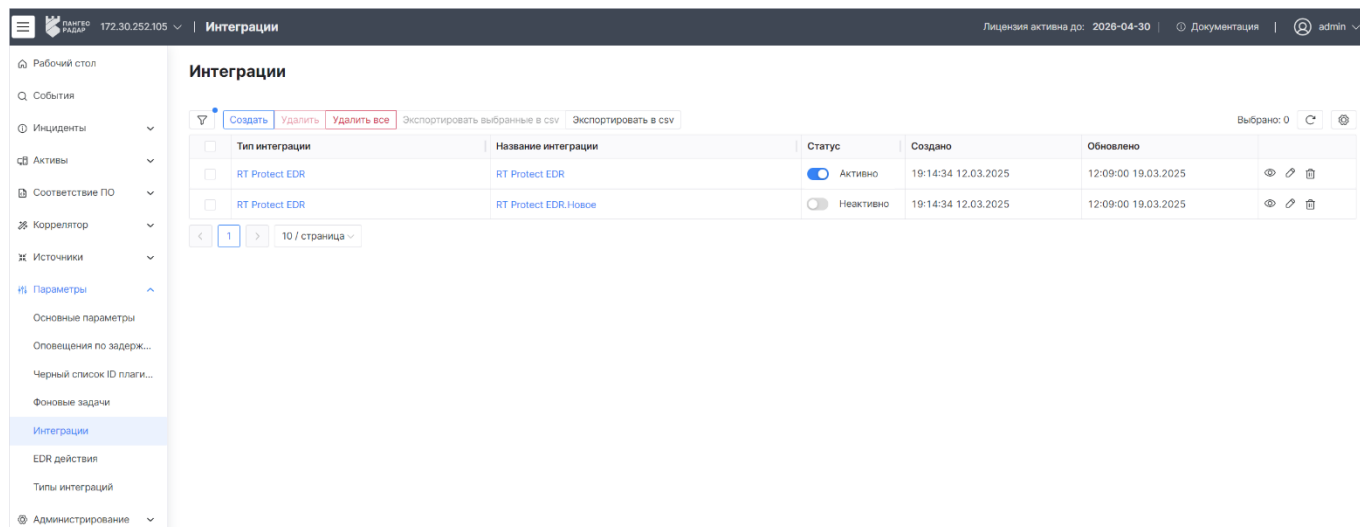


Рис. 210 – Раздел "Интеграции"

В разделе отображается следующая информация:

- **Тип интеграции** – наименование типа интеграции, к которой относится интеграция;
- **Название интеграции** – наименование экземпляра 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. 211](#)»).

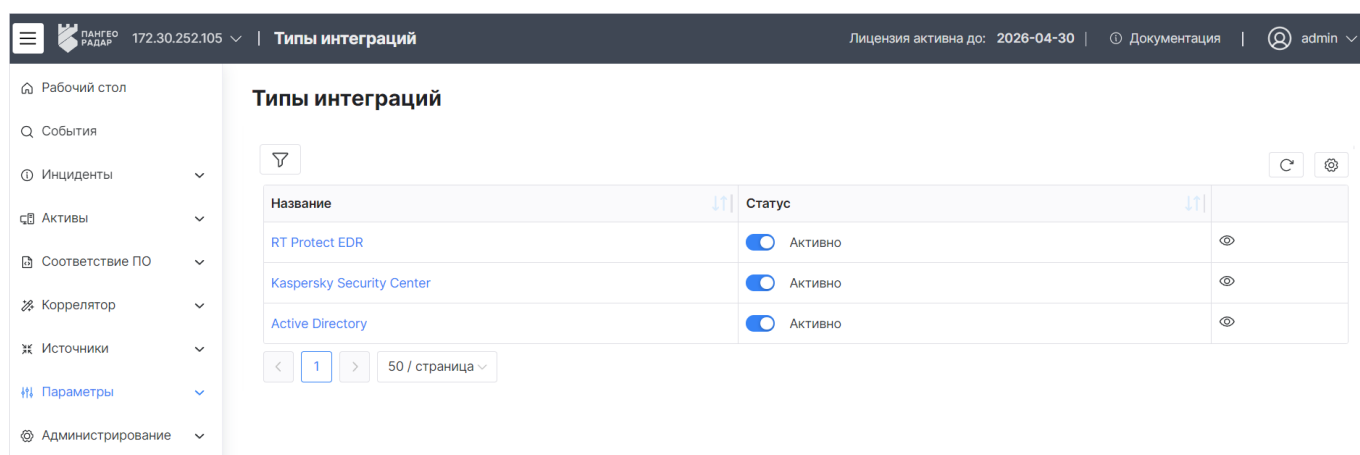


Рис. 211 – Раздел "Типы интеграций"

В разделе отображается наименование сторонних систем, с которыми в платформе можно настроить интеграцию.


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;
- «[Active Directory](#)» – служба каталогов от Microsoft, предназначенная для централизованного хранения информации о пользователях, компьютерах, сетевых устройствах и ресурсах компании.

Тип интеграции может находиться 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 содержанием папок описано в разделе (см. раздел **Интерфейс** → «[Папки контента](#)»).

Для работы с папками перейдите в раздел **Параметры** → **Папки контента** (см. «[Рис. 212](#)»).

ПАНГЕО РАДАР

172.30.254.60

Папки контента

Лицензия активна до: 2026-02-07 | Документация | admin

Папки контента

Создать

Удалить

Экспортировать выбранные в csv

Экспортировать в csv

Переместить в папку

Выбрано: 0

<input type="checkbox"/>	Название	Правила	Создано	Обновлено	Родительская папка	Кем создано	
<input type="checkbox"/>	my	1	2001-01-01 02:30:17	2001-01-01 02:30:17	-	admin	
<input type="checkbox"/>	Без папки	594	2025-04-22 15:00:15	2025-04-22 15:00:15	-	admin	
<input type="checkbox"/>	Rules	94	2001-01-01 02:30:17	2001-01-01 02:30:17	-	admin	
<input type="checkbox"/>	Linux_rules	90	2001-01-01 02:30:17	2001-01-01 02:30:17	Rules	admin	
<input type="checkbox"/>	Linux_rules для тестов	4	2001-01-01 02:30:17	2001-01-01 02:30:17	Linux_rules	admin	
<input type="checkbox"/>	Windows_rules	0	2001-01-01 02:30:17	2001-01-01 02:30:17	Rules	admin	

Рис. 212 – 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 сущностей](#)».

Управление шаблонами выполняется в разделе **Параметры** → **Шаблоны** (см. «[Рис. 213](#)»).

ПАНГЕО РАДАР

172.30.254.97

Шаблоны

Лицензия активна до: 2027-11-16 | Документация | admin

Шаблоны

Удалить

Удалить все

Экспортировать

Экспортировать все

Экспортировать выбранные в csv

Экспортировать в csv

Импортировать

Выбрано: 0

<input type="checkbox"/>	Название	Сущность	Тип шаблона	Создано	Обновлено	
<input type="checkbox"/>	kafka_test_preset	Профиль сбора	Редактирование	2025-04-11 11:03:39	2025-04-11 11:03:39	
<input type="checkbox"/>	eventlog_test	Профиль сбора	Редактирование	2025-04-11 11:31:49	2025-04-11 11:31:49	
<input type="checkbox"/>	udp_input_preset	Профиль сбора	Редактирование	2025-04-11 11:47:20	2025-04-11 11:47:20	
<input type="checkbox"/>	tcp_input_preset_1	Профиль сбора	Редактирование	2025-04-11 14:48:06	2025-04-11 14:48:06	
<input type="checkbox"/>	mseven6_52	Профиль сбора	Редактирование	2025-04-14 12:23:25	2025-04-14 12:23:25	
<input type="checkbox"/>	local_eventlog	Профиль сбора	Редактирование	2025-04-14 12:41:10	2025-04-14 12:41:10	
<input type="checkbox"/>	tcp_input_2520 Cisco-ASA	Профиль сбора	Редактирование	2025-04-14 13:50:18	2025-04-14 13:50:18	
<input type="checkbox"/>	smb_52	Профиль сбора	Редактирование	2025-04-14 15:44:22	2025-04-14 15:44:22	

Рис. 213 – 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. 214](#)».

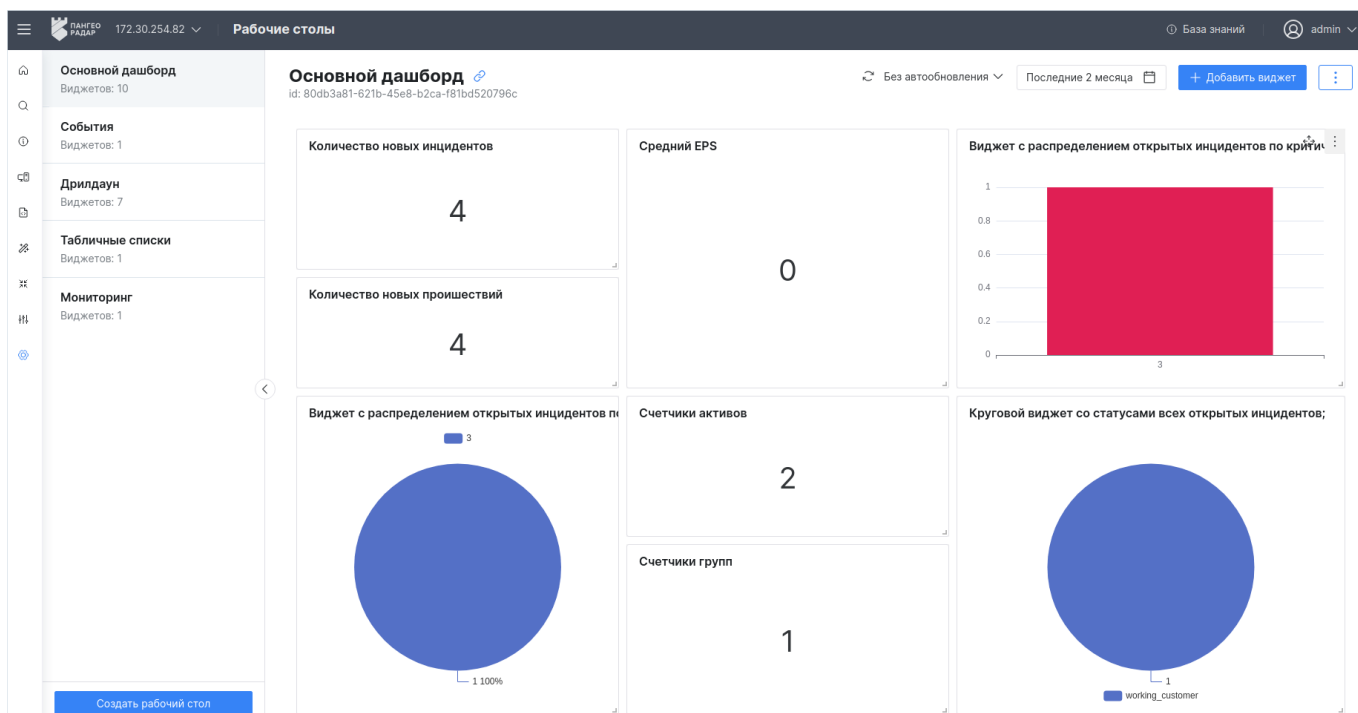


Рис. 214 – Интерфейс раздела "Рабочие столы"

Раздел состоит из следующих блоков:





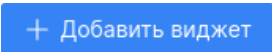

- **Список рабочих столов**, в котором отображается информация о доступных рабочих столах:
 - название рабочего стола;
 - количество виджетов, добавленных на рабочий стол.
- **Рабочая область**, в которой отображается информация о выбранном рабочем столе:
 - название рабочего стола;
 - идентификатор рабочего стола;
 - информация о виджетах, добавленных на рабочий стол: заголовок, описание и содержимое виджета (см. «Рис. 215»);
 - режим автообновления рабочего стола;
 - период времени, за который формируется информация для рабочего стола.

Пример отображения информации о виджете приведен на «Рис. 215».






Рис. 215 – Пример виджета

На странице доступны следующие элементы управления рабочим столом:


Кнопка	Действие
	создание нового рабочего стола
	копирование ссылки на рабочий стол
	обновление отображаемой информации
	выбор временного диапазона для формирования данных
	создание виджета в конструкторе
	доступ к следующим действиям над рабочим столом: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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. 216»).

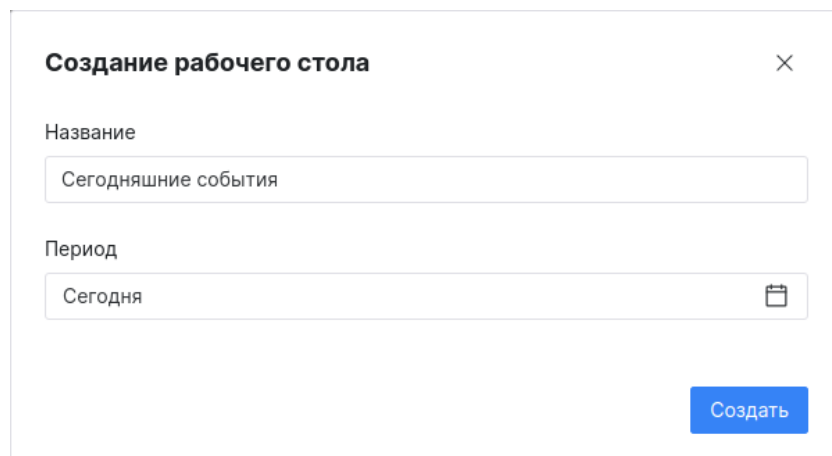


Рис. 216 – Окно "Создание рабочего стола"

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. 217»](#)).

Сегодняшние события [🔗](#) Назад

id: 21c17a2d-21e1-4da6-b74f-f0abbabaa9b5

Название

Сегодняшние события

Период

Сегодня 📅

Пользователи

Выбрать ▼

Группы пользователей

Выбрать ▼

Сбросить Сохранить

Рис. 217 – 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:

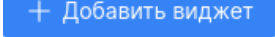
1. Нажмите кнопку . Откроется окно выбора временного диапазона.
2. Выберите период. Доступные значения:
 - за все время;
 - текущие: минута, час, день, месяц, год;
 - последние: минуты, часы, месяца, года;
 - период можно указать вручную в соответствующих полях. Поддерживается формат дат из «[Grafana. 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. 218](#)»).

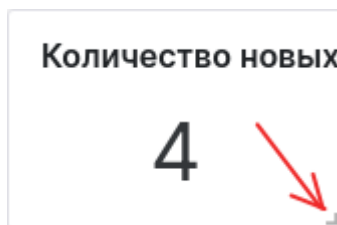



Рис. 218 – Кнопка изменения размера виджета


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. 219»).

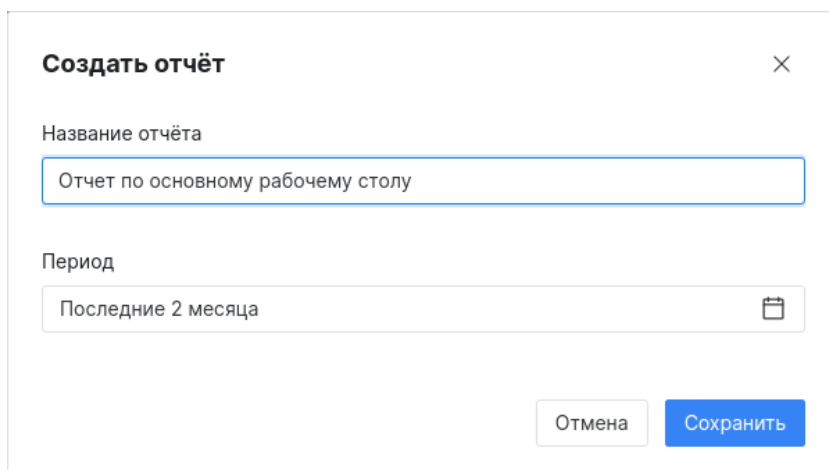


Рис. 219 – Окно "Создать отчет"

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. 220»).

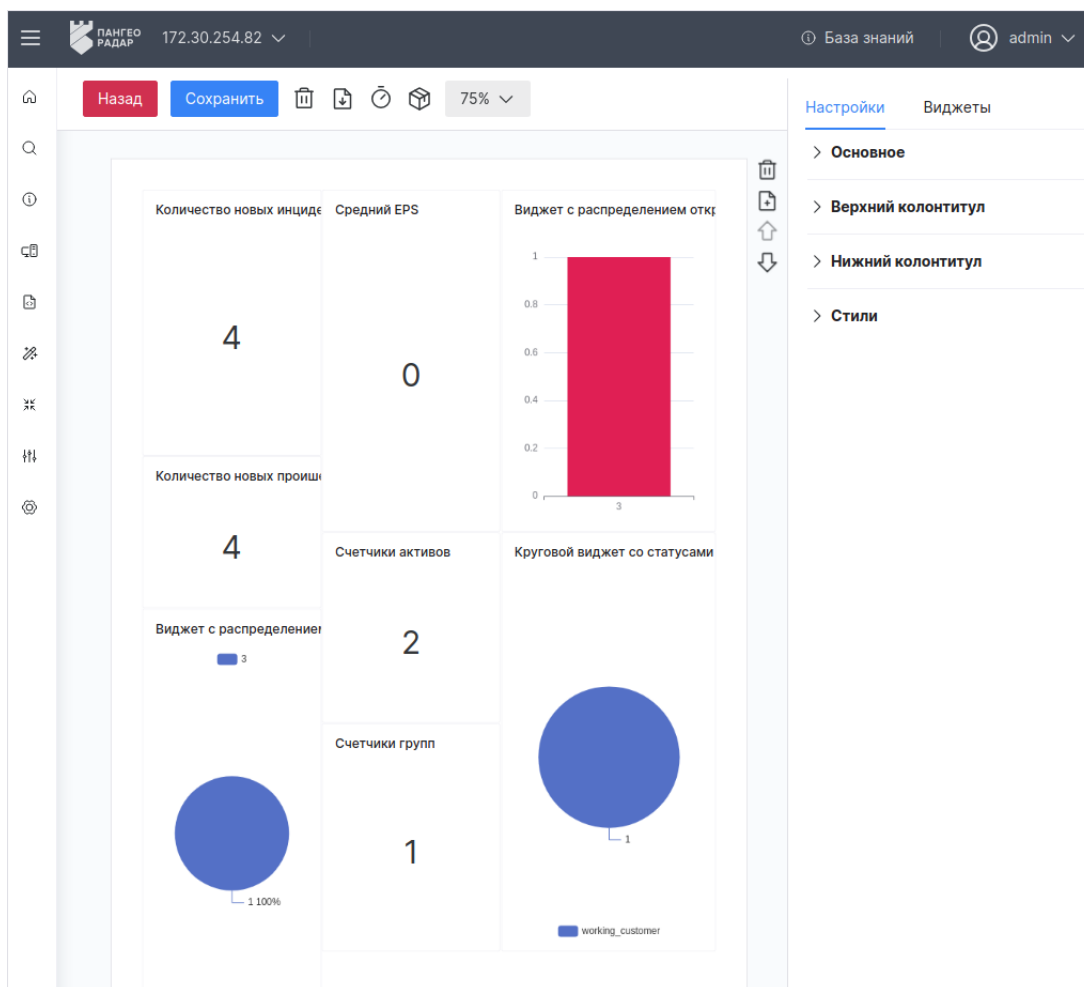



Рис. 220 – Страница с отчетом

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. 221](#)».

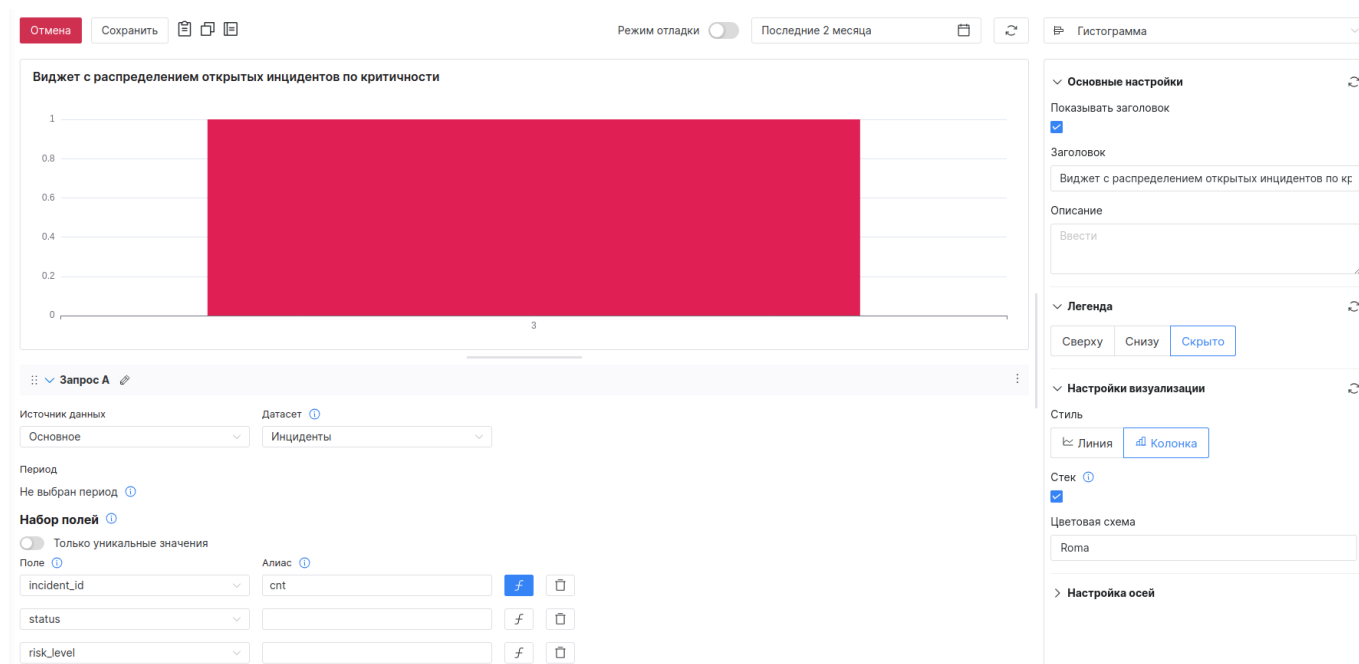


Рис. 221 – Страница "Конструктор виджетов"

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. 222](#)»).

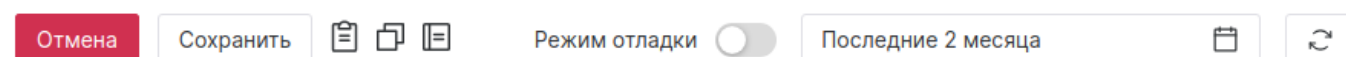

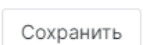






Рис. 222 – Конструктор виджетов. Блок "Панель действий"

На панели действий доступны следующие элементы управления:

Кнопка	Действие
	отмена изменений и возврат на предыдущую страницу
	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. 223](#)»).



Рис. 223 – Конструктор виджетов. Блок "Режим визуализации"

В режиме отладки можно посмотреть корректность работы написанных запросов (см. «[Рис. 224](#)»).

Запрос A Запрос B

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

Рис. 224 – Конструктор виджетов. Блок "Режим отладки"

Конструктор запросов

Блок располагается под режимом визуализации/отладки (см. «Рис. 225»).

> Запрос A

> Запрос B

Источник данных

Метрики системы

Датасет

Общие метрики

Период

Последний час

Набор полей

Поле

go_goroutines

Алиас

test

Дата

+ Добавить

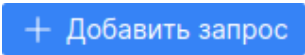



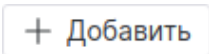



Условия фильтрации

+ Добавить

+ Добавить запрос

Рис. 225 – Конструктор виджетов. Блок "Конструктор запросов"

В конструкторе запросов доступны следующие элементы управления запросами:

Кнопка	Действие
	добавление запроса
	изменение расположения запроса
	изменение наименования запроса
	доступ к следующим действиям над запросом: <ul style="list-style-type: none"> - скопировать настройки; - вставить настройки; - дублировать; - удалить.
	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. 226](#)»).

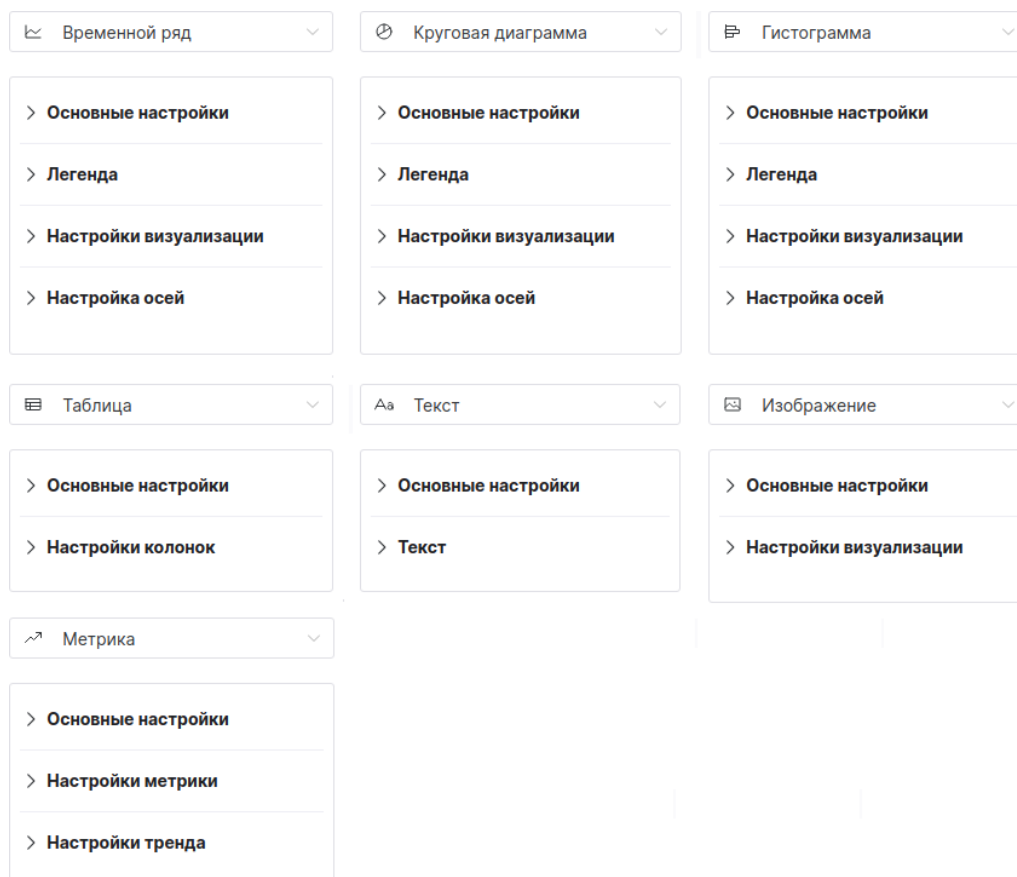


Рис. 226 – Конструктор виджетов. Блок "Настройка внешнего вида виджета"

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 .

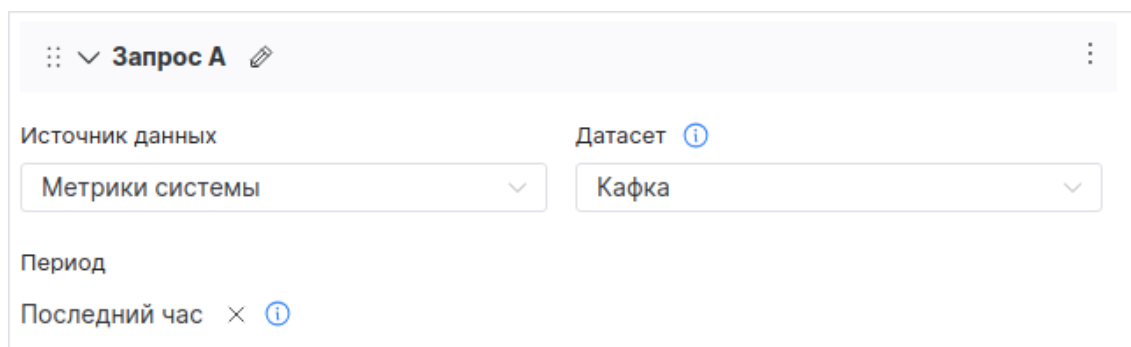
При необходимости вы можете изменить наименование запроса нажав кнопку .

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. 227](#)»).



The screenshot shows a web interface for building queries. At the top, there's a header bar with a menu icon, a dropdown labeled 'Запрос А', and an edit icon. Below this, there are two main sections: 'Источник данных' (Data Source) and 'Датасет' (Dataset). Under 'Источник данных', there is a dropdown menu currently showing 'Метрики системы'. Under 'Датасет', there is a dropdown menu currently showing 'Кафка'. Below these, there is a 'Период' (Period) section with a label 'Последний час' and a close icon 'x', followed by an information icon 'i'.

Рис. 227 – Конструктор запросов. Выбор источника данных, датасета и периода

Соответствие источников данных и датасетов приведено в таблице:

Источник данных	Датасет
Основное	Инциденты
События	<ul style="list-style-type: none">– Все;– Нормализованные;– Обработанные;– Ошибки.
Метрики системы	<ul style="list-style-type: none">– 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. 227](#)») 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

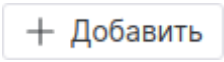
На данном шаге вы добавляете в запрос конкретные поля из выбранного датасета. Для каждого поля при необходимости можно задать **Алиас** и **Агрегацию**.

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 .
3. Появятся параметры для настройки поля (см. «[Рис. 228](#)»).

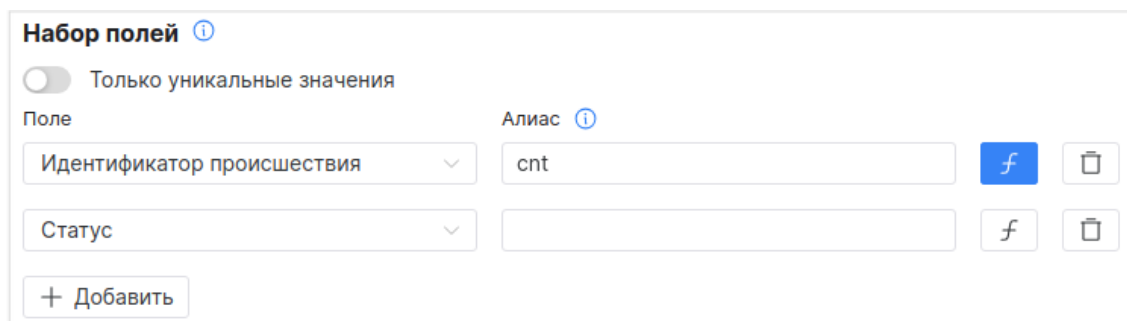


Рис. 228 – Конструктор запросов. Набор полей

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. 229](#)»).

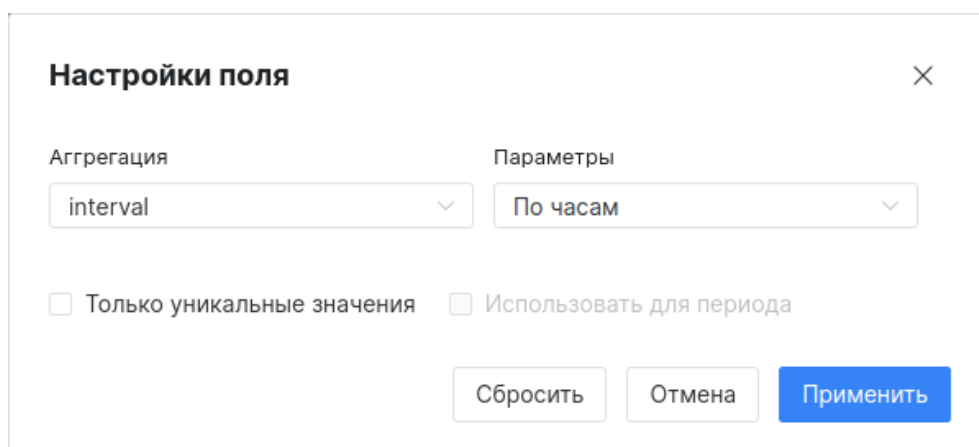
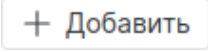


Рис. 229 – Окно "Настройки поля"

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 . Появятся параметры для настройки условия фильтрации (см. «Рис. 230»).

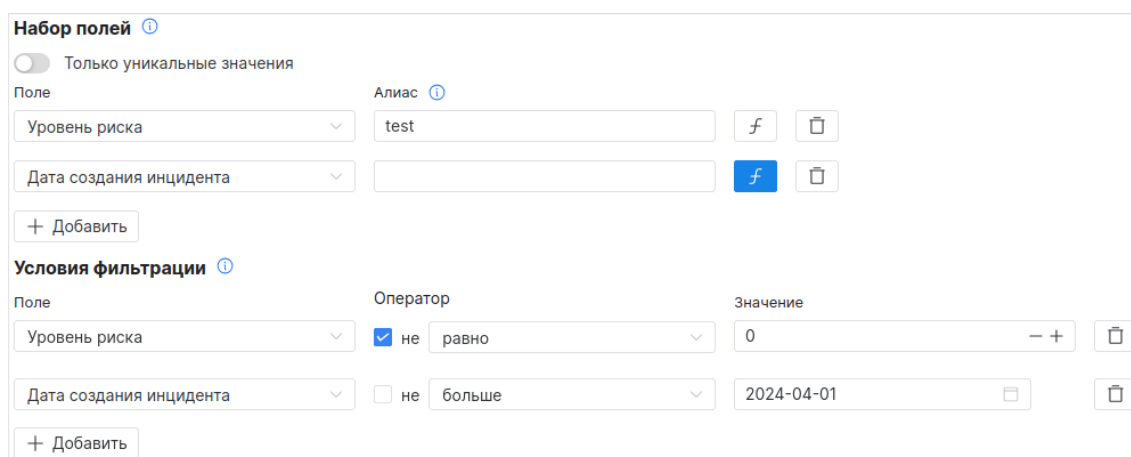


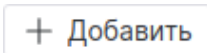
Рис. 230 – Конструктор запросов. Условия фильтрации

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  и выберите поле, по которому вы хотите выполнить группировку (см. «Рис. 231»).

The screenshot shows a web interface for configuring widgets. It includes sections for 'Поле' (Field) with a dropdown menu and an 'Алиас' (Alias) input field. Below this are 'Условия фильтрации' (Filtering conditions) and 'Группировка' (Grouping) sections, each with a '+ Добавить' (Add) button. The 'Сортировка' (Sorting) section also has a '+ Добавить' button. At the bottom, there are input fields for 'Лимит' (Limit) and 'Оффсет' (Offset), each with a '- +' control.

Рис. 231 – 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. 231»).
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. 232](#)»).

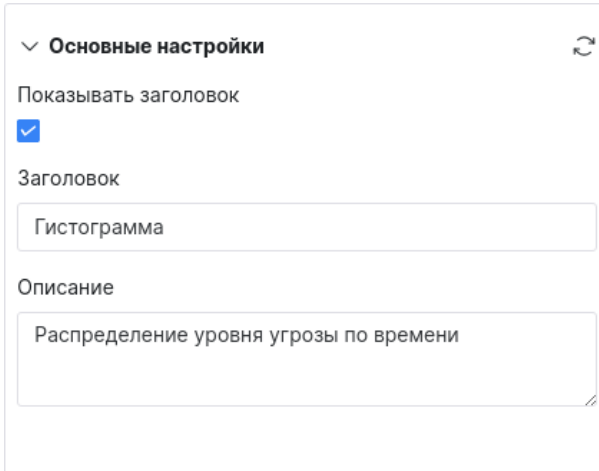


Рис. 232 – Основные настройки виджетов

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. 233](#)»

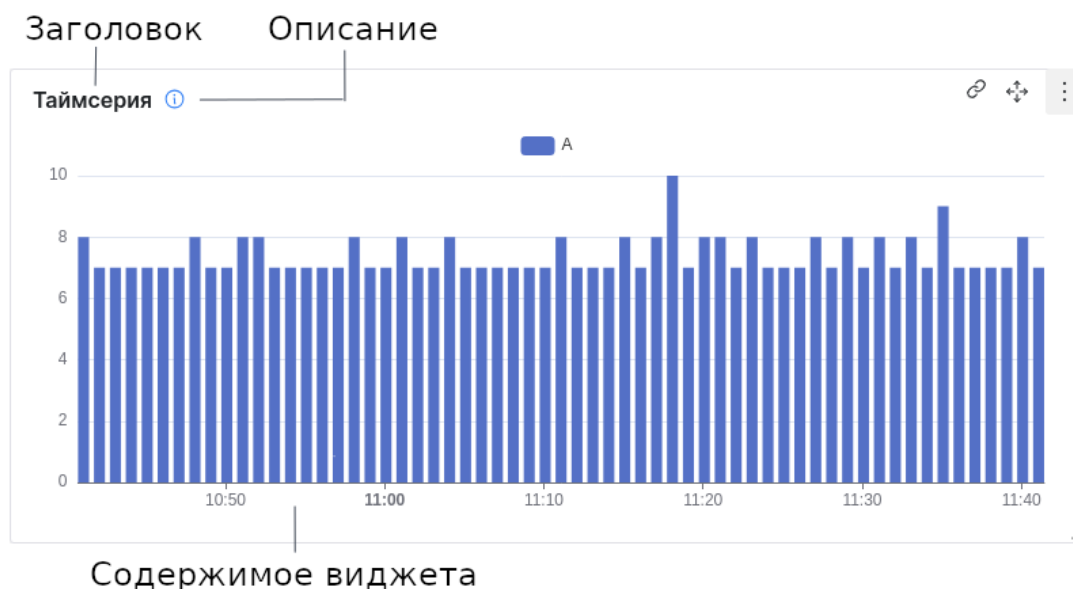


Рис. 233 – Отображение основных настроек на виджете

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. 234».

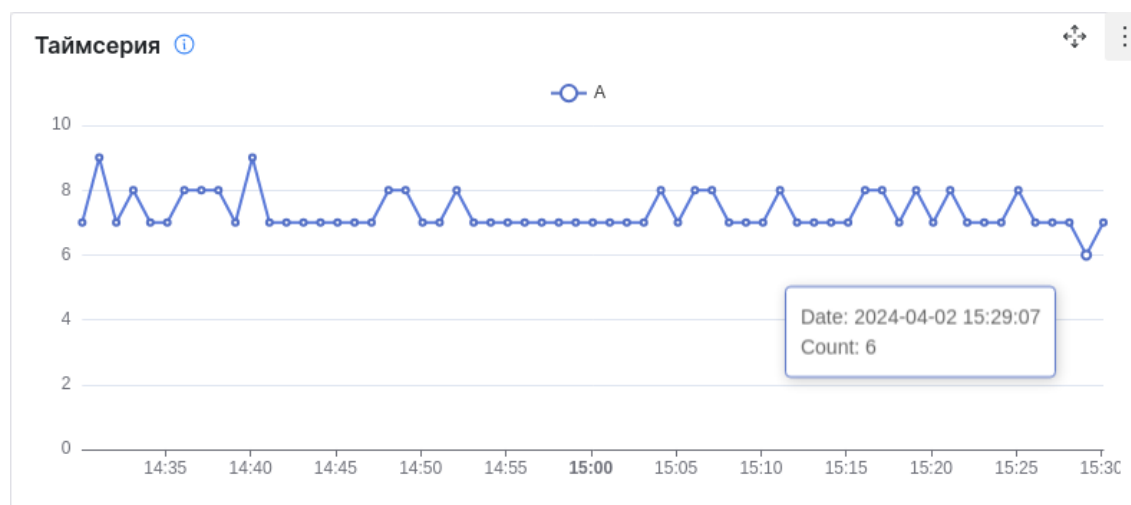


Рис. 234 – Виджет "Временной ряд"

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. 235».

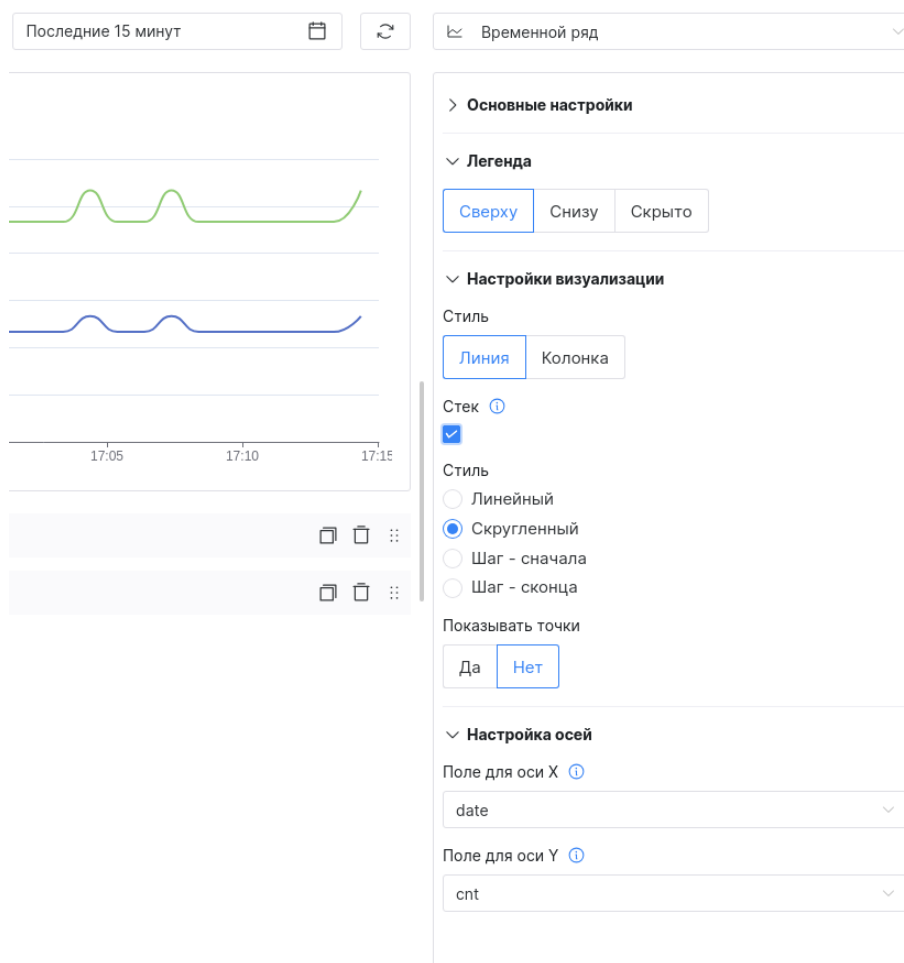


Рис. 235 – Виджет "Временной ряд". Настройки

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. 236».

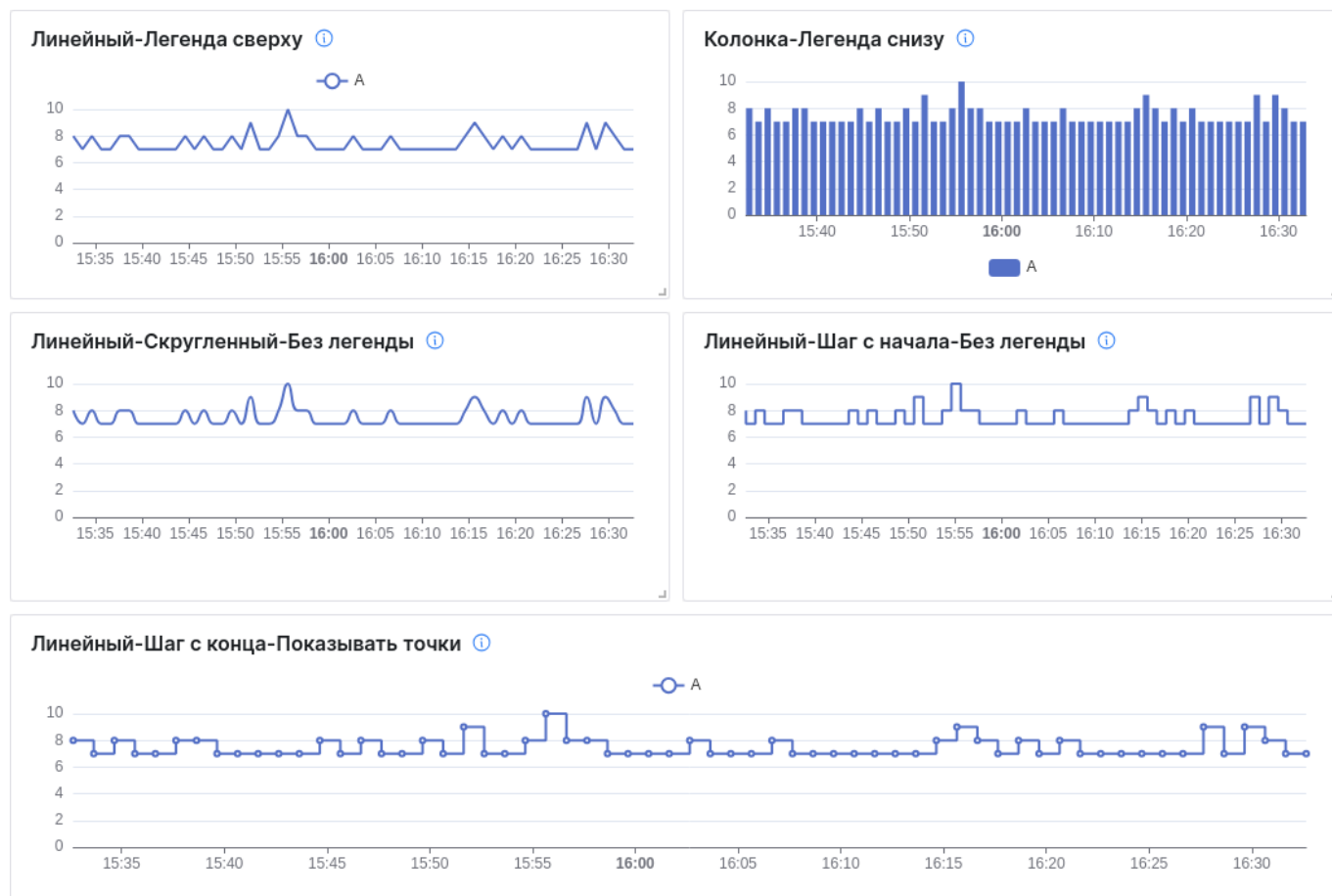


Рис. 236 – Примеры визуализации настроек виджета "Временной ряд"

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. 237».



Рис. 237 – 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. 238](#)».

- 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. 240](#)».

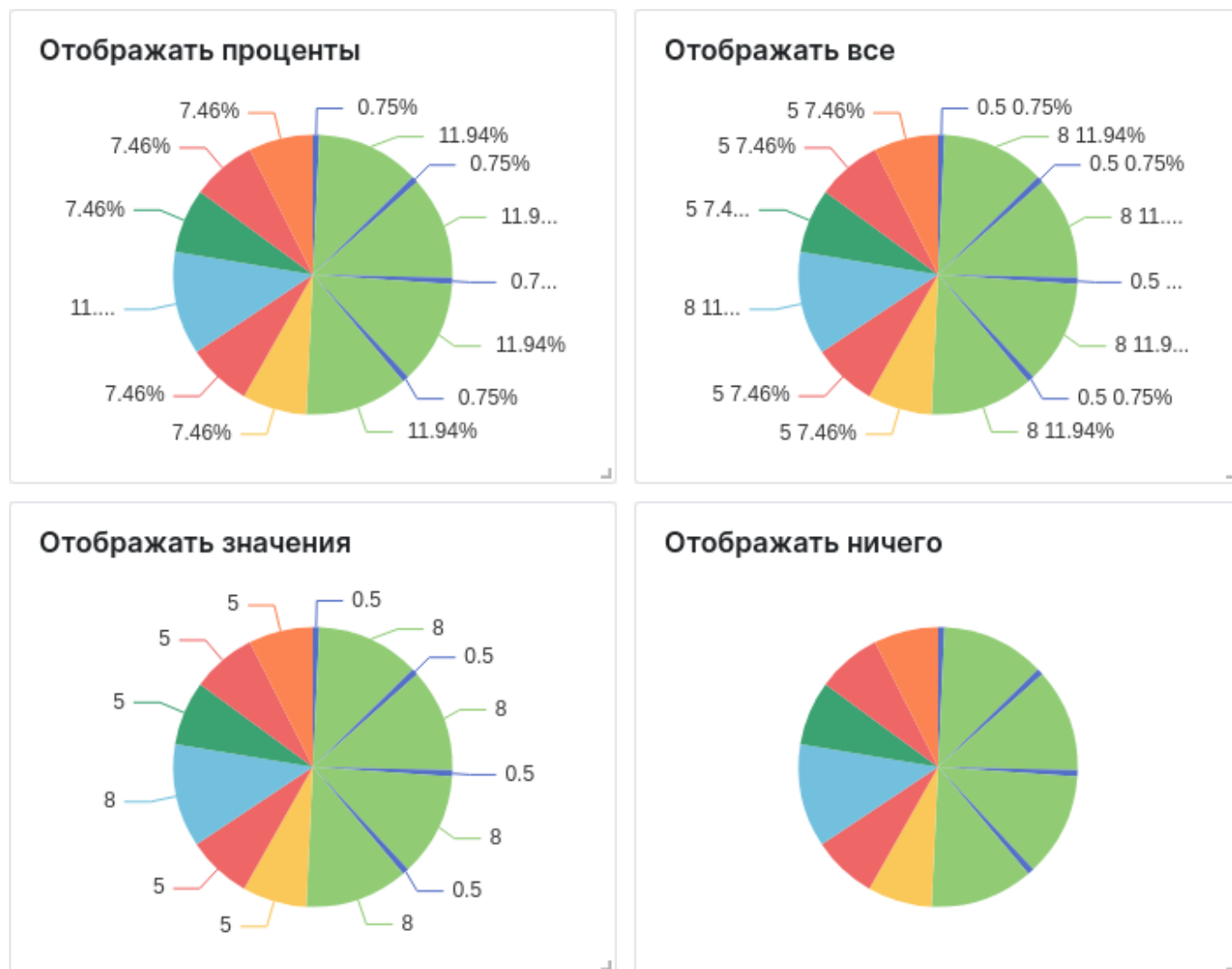


Рис. 240 – Примеры визуализации настроек виджета "Круговая диаграмма"

12.3.4 Таблица

Виджет отображает выбранные показатели в табличном варианте. Пример визуализации приведен на «Рис. 241».

таблица с топ-5 активов (или групп активов) по открытым инцидентам

Наименование актива	Количество
DESKTOP-AD02	2
DESKTOP-AD03	1
DESKTOP-AD04	2
DESKTOP-AD05	1
DESKTOP-AD09	1

Рис. 241 – Виджет "Таблица"

Пример блока "Настройки" приведен на «Рис. 242».

Таблица

> Основные настройки

▼ Настройки колонок

⋮

key date

label Дата

☐ Сгруппировать значения

⋮

key go_goroutines

label Количество потоков

☒ Сгруппировать значения

+ Добавить


Стратегия обработки некорректных значений

☒ Использовать значения по-умолчанию

☐ Игнорировать

Рис. 242 – 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. 243](#)».

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. 243 – 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. 244](#)».

Ежедневная проверка ⓘ

Памятка при работе с рабочим столом:

1. Сначала проверь поток событий.

2. Затем выяви угрозы.

3. Составь топ -5 угроз по критичности

4. Создай и распечатай отчет.

5. Свяжись по телефону с руководителем по номеру 0511.

6. Доложи об угрозах.

Рис. 244 – Виджет "Текст"

Пример настроек приведен на «[Рис. 245](#)».

Aa Текст
▼

▼ **Основные настройки**

Показывать заголовок
☒

Заголовок

Ежедневная проверка

Описание

Виджет для описания ежедневных проверок

▼ **Текст**

Контент

Памятка при работе с рабочим столом:

 1. Сначала проверь поток событий.
 2. Затем выяви угрозы.
 3. Составь топ -5 угроз по критичности
 4. Создай и распечатай отчет.
 5. Свяжись по телефону с руководителем по номеру 0511.
 6. Доложи об угрозах.

Рис. 245 – 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. 246».

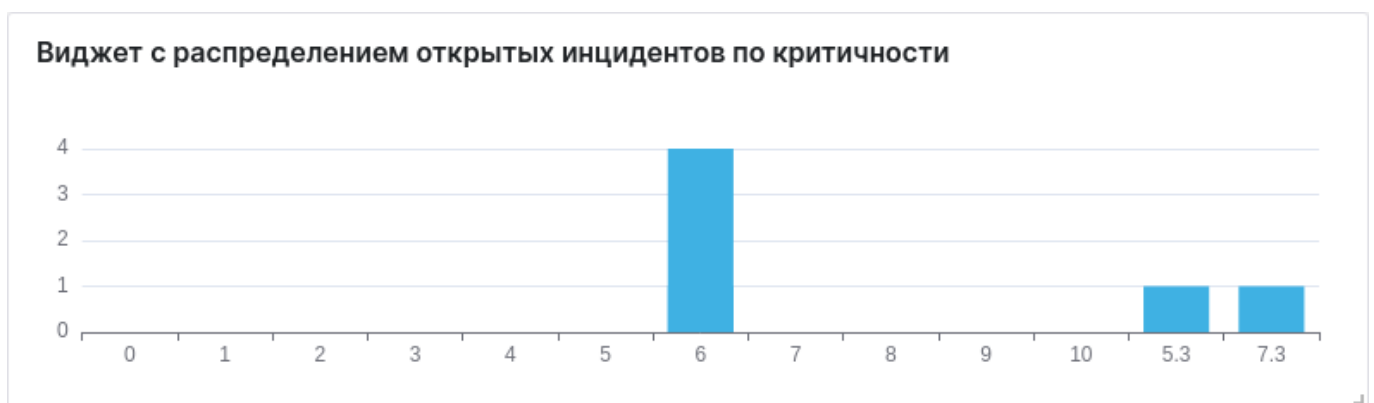


Рис. 246 – Виджет "Гистограмма"

Настройка внешнего вида виджета включает в себя следующие шаги:

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

Помимо основных шагов при необходимости можно настроить следующие параметры:

- Основные настройки;

- Легенда;
- Переопределение значений.

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.

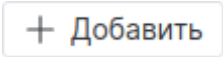
Пример настройки осей приведен на [Рис. 247](#).

Рис. 247 – Виджет "Гистограмма". Настройка осей

Для настройки осей выполните следующие действия:

1. Выберите стратегию обработки некорректных значений:
 - использовать значения по умолчанию;
 - игнорировать.
2. Из выпадающего списка выберите поле для оси X.

3. 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 ;
- укажите диапазон в соответствующем поле;
- если вы хотите использовать значения, не входящие в диапазон, то установите соответствующий флаг.

4. Из выпадающего списка выберите поле для оси Y.

5. В поле **Разделить значения по полю** при необходимости укажите поле, по которому будут группироваться значения. В этом случае в столбце гистограммы будет суммироваться кол-во всех записей, имеющих значение для выбранного поля.

Примечание: 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**.

Если вы настроили разделение значений по полю, то станет доступен параметр **Накопление** для столбца гистограммы.

Параметр **Накопление** может принимать следующие значения:

- Без накопления:



- С накоплением:



- Нормированная:



6. Проверьте отображение осей на виджете.

Пример отображения с накоплением и без накопления приведен на [Рис. 248](#).



Рис. 248 – Примеры визуализации виджета с накоплением и без накопления

12.3.6.2 Шаг 2. Настройка визуализации

Пример настройки визуализации приведен на [Рис. 249](#).

Гистограмма

> Основные настройки

> Легенда

▼ Настройки визуализации

Стиль

Линия Колонка

Цветовая схема

Roma

> Настройка осей

> Переопределение значений

Рис. 249 – Виджет "Гистограмма". Настройка визуализации

Настройка позволяет выбрать следующие параметры:

- стиль диаграммы: линия или колонка;
- 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. 250](#)».

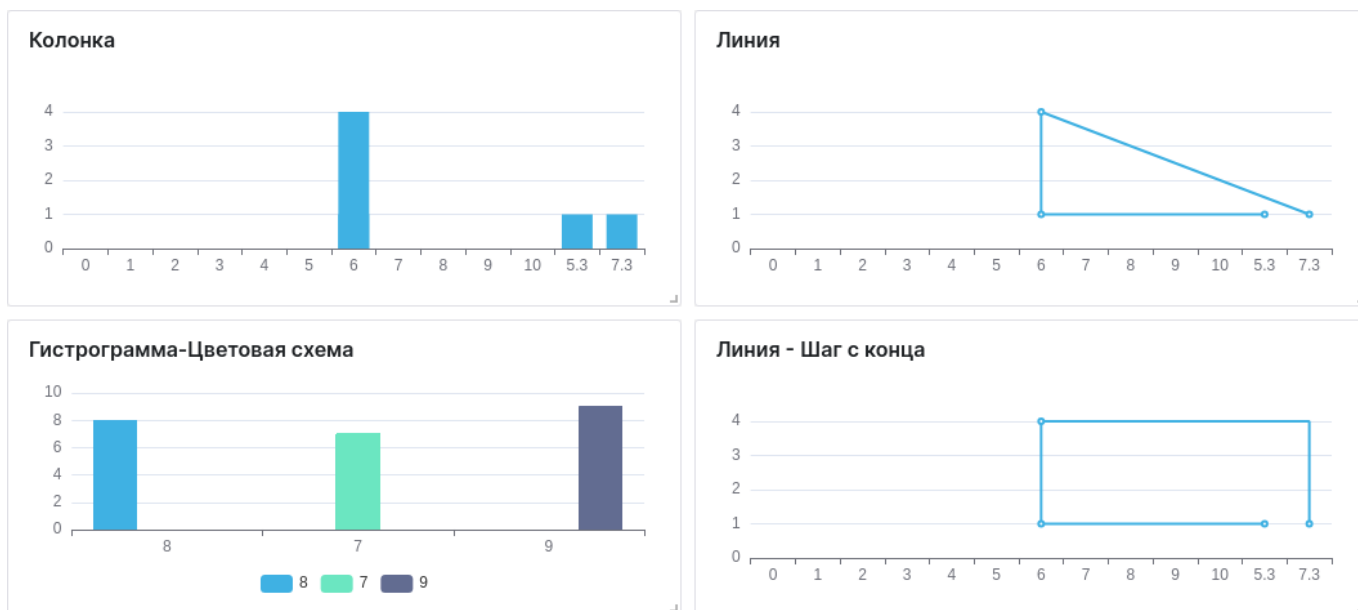


Рис. 250 – Примеры визуализации настроек виджета "Гистограмма".

Для настройки визуализации выполните следующие действия:

1. Выберите стиль: линия или колонка.
2. Если выбран стиль линия, то выберите ее тип: линейный, скругленный, шаг с начала, шаг с конца.
3. Выберите цветовую схему.

12.3.7 Метрика

Виджет отображает тренд изменения выбранного показателя за период времени. Пример внешнего вида приведен на «Рис. 251».

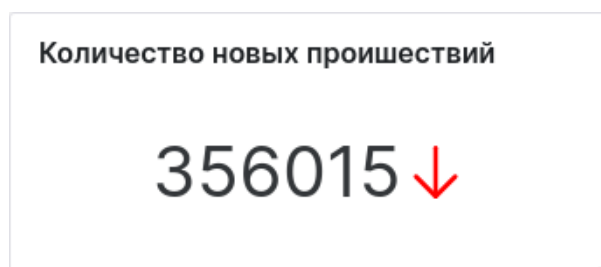


Рис. 251 – Виджет "Метрика"

Пример настроек приведен на «Рис. 252».

↻ Метрика ▾

> Основные настройки

▾ Настройки метрики ↻

Использовать значение из поля

go_goroutines ▾

Серия с данными

A ▾

▾ Настройки тренда ↻

Включить отображение тренда

☒

Инвертировать тренд

☐

Поле со значениями

go_goroutines ▾

Серия с данными

A ▾

Серия для прогнозирования

B ▾

Рис. 252 – 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. 253](#)».

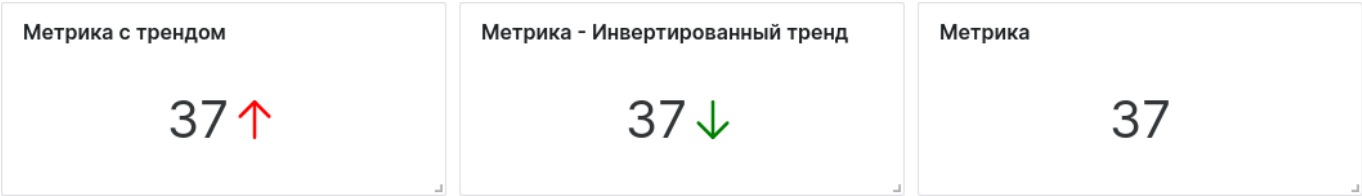


Рис. 253 – Примеры визуализации настроек виджета "Метрика"

12.3.8 Изображение

Виджет отображает изображение, загруженное пользователем.

Пример внешнего вида представлен на «[Рис. 254](#)».

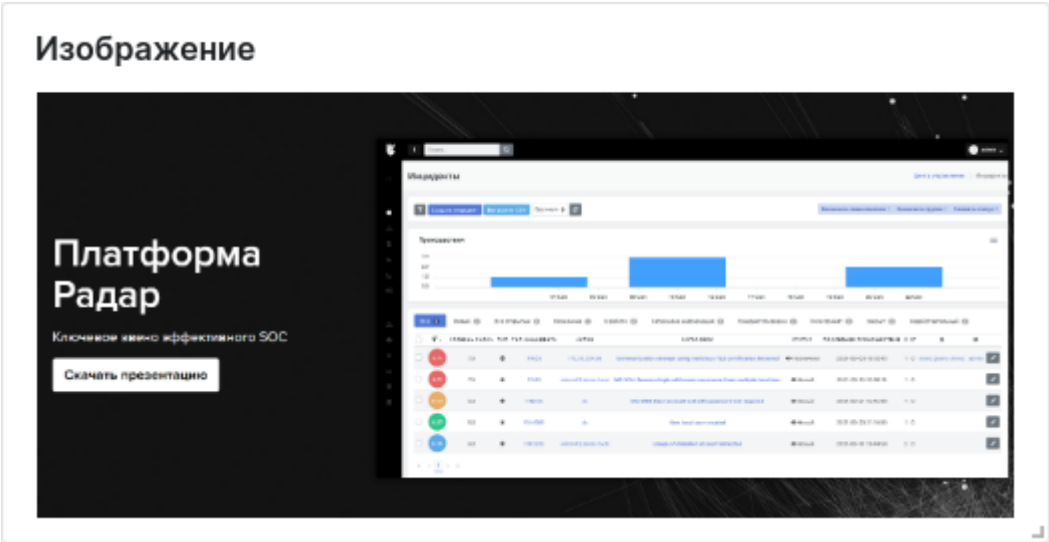


Рис. 254 – Виджет "Изображение"

Пример настроек приведен на «[Рис. 255](#)».

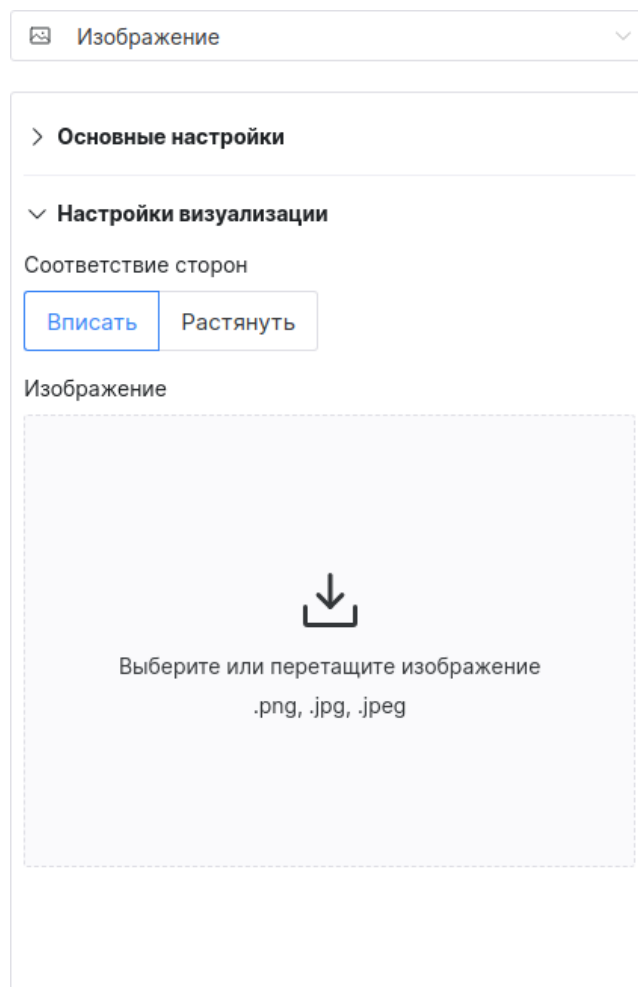


Рис. 255 – Виджет "Изображение". Настройки




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. 256](#)») выберите предустановку и нажмите кнопку .

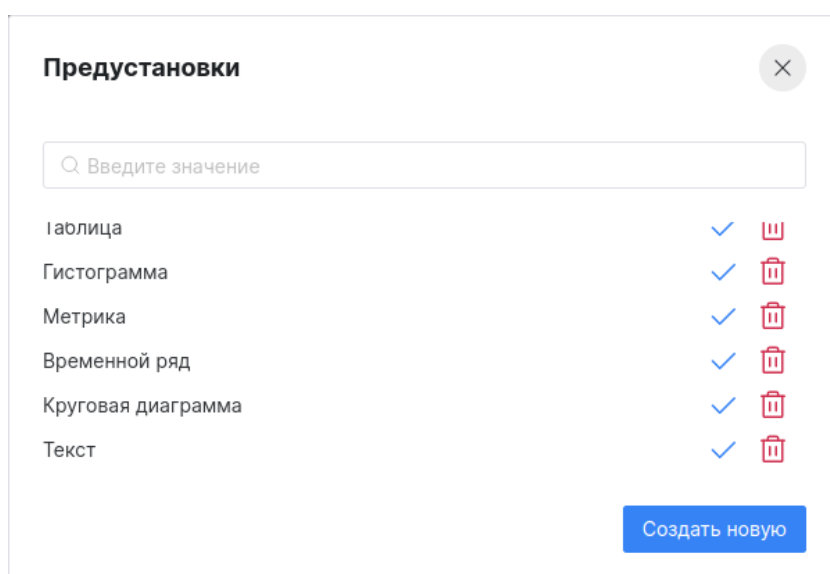



Рис. 256 – Окно "Предустановки"

Для создания предустановки выполните следующие действия:

1. Настройте запросы и визуализацию виджета.
2. Нажмите кнопку  и в открывшемся окне "Предустановки" (см. «[Рис. 256](#)») 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. 257](#)»).

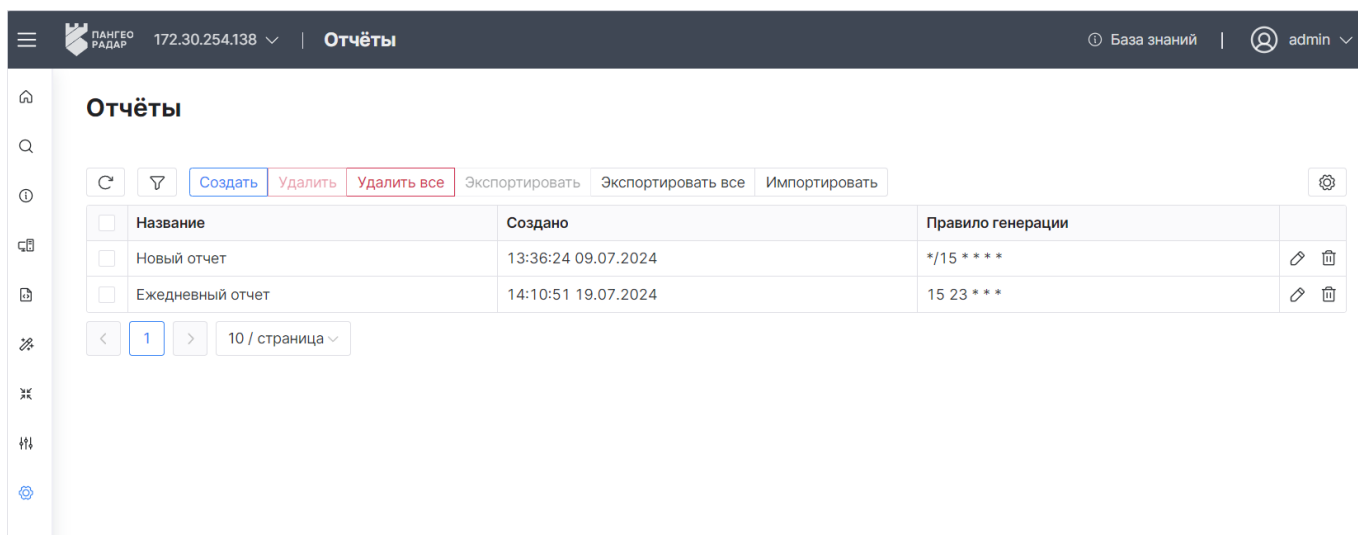


Рис. 257 – Раздел "Отчеты"

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. 258»).

Рис. 258 – 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. 259»).

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. 261](#)»).

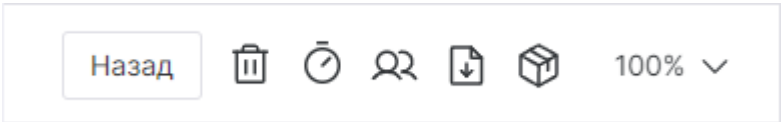


Рис. 261 – Страница "Конструктор отчета". Блок "Панель действий"

На панели действий доступны следующие элементы управления:

Кнопка	Действие
	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. 262](#)».

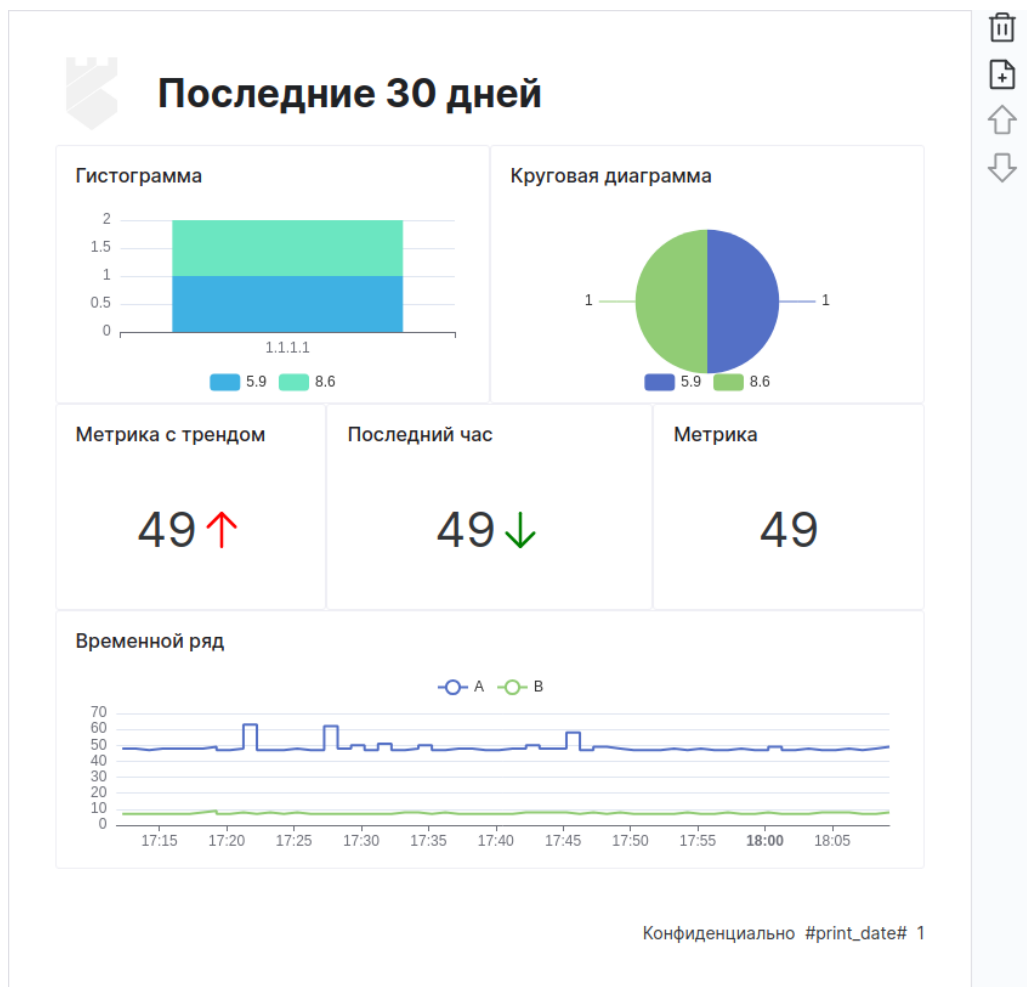


Рис. 262 – Страница "Конструктор отчета". Блок "Рабочая область"

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: <ul style="list-style-type: none"> – 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.

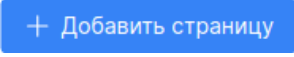

Настройка отчета состоит из следующих процессов:

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. 263](#)»).

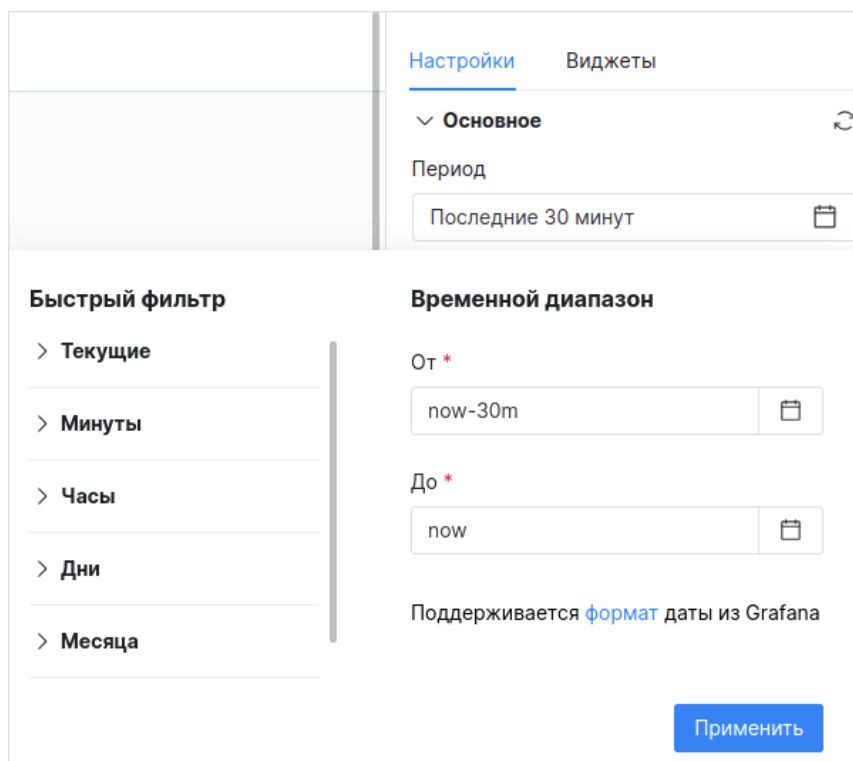



Рис. 263 – Выбор периода формирования данных виджетов

Для настройки периода выполните следующие действия:

1. В поле **Период** нажмите кнопку . Откроется окно выбора временного диапазона (см. «[Рис. 263](#)»).
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. 264](#)»).

Настройки Виджеты

▼ Основное

Период

Последние 30 минут

Маска для генерации названия ⓘ

##NAME##, ##DAY##, ##MONTH##, ##YEAR##

Рис. 264 – 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. 265»).

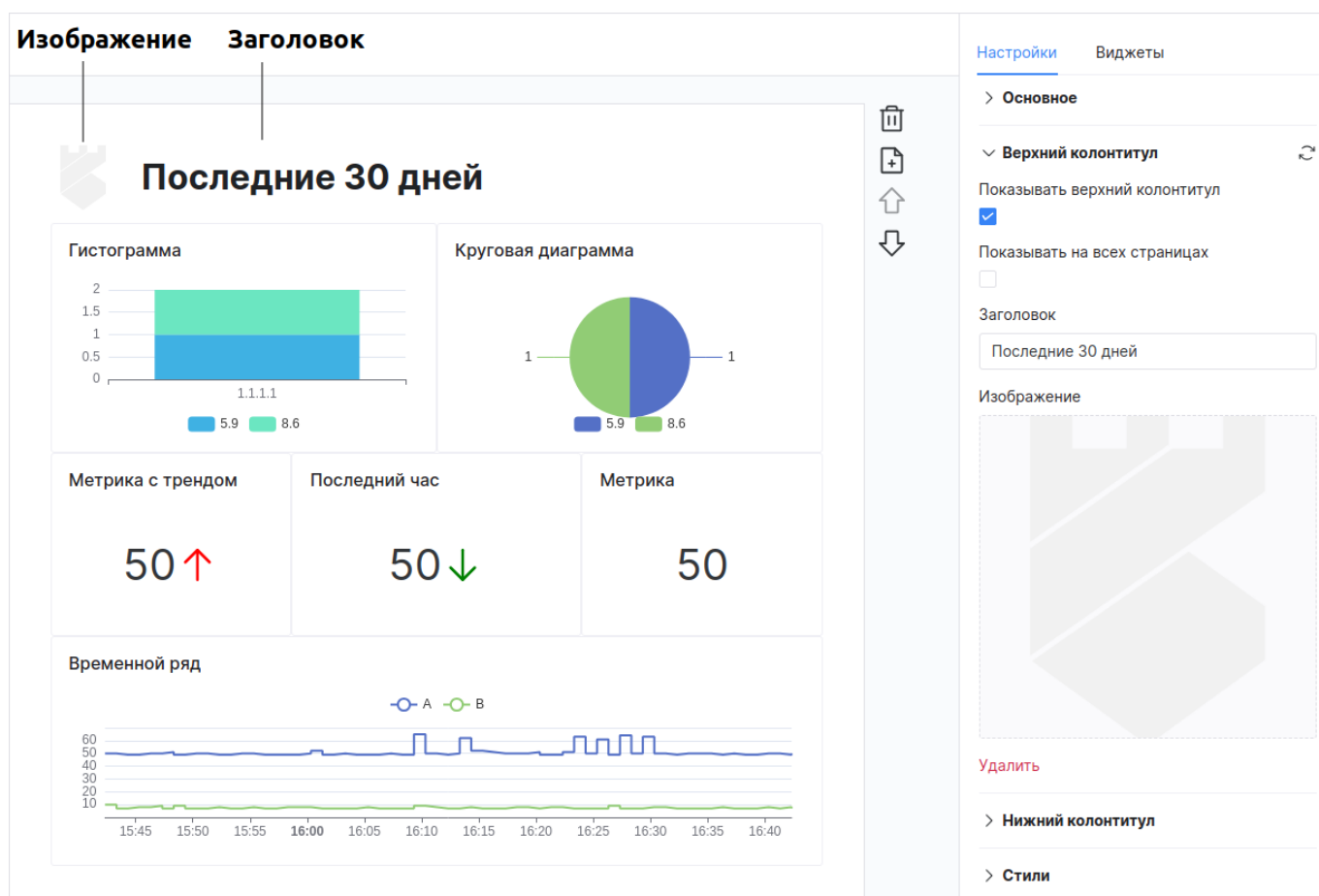


Рис. 265 – Настройка верхнего колонтитула

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** → **Ниžний колонтитул** (см. «Рис. 266»).

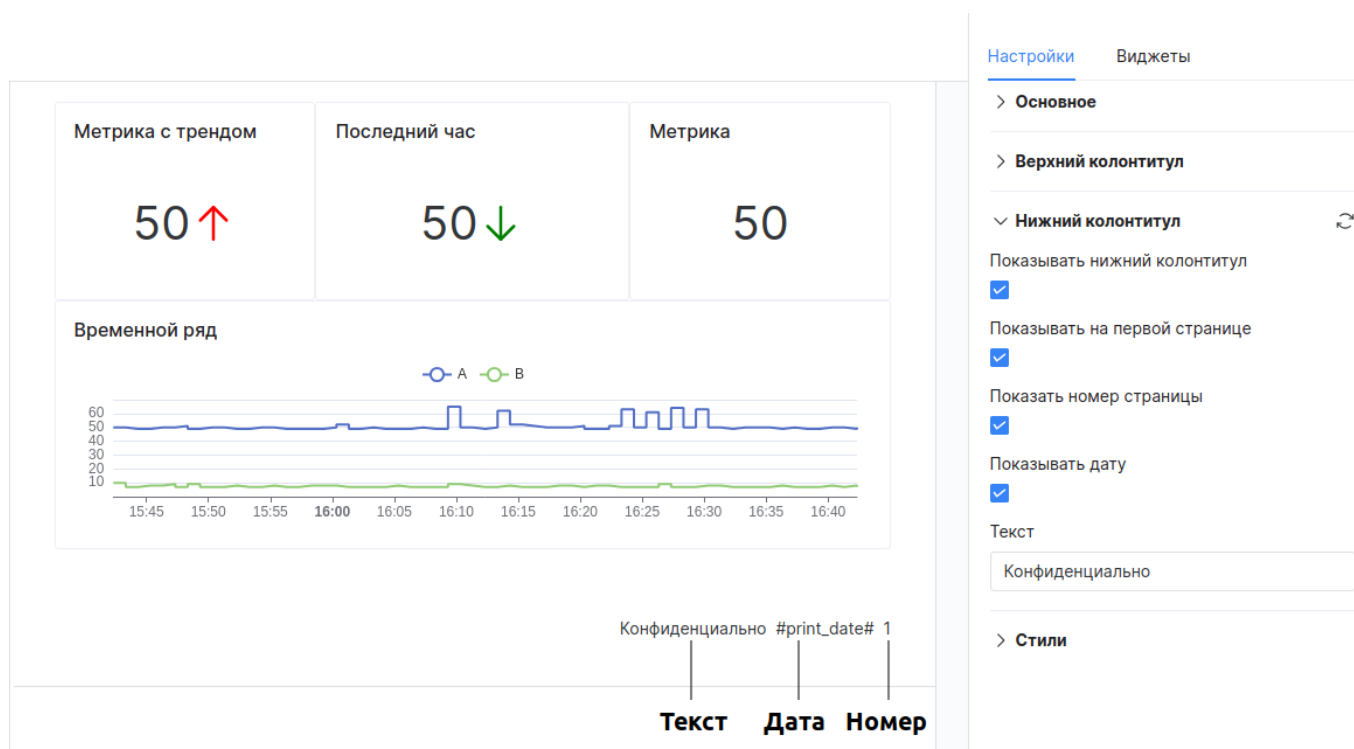


Рис. 266 – Настройка нижнего колонтитула

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 включает 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. 267»).

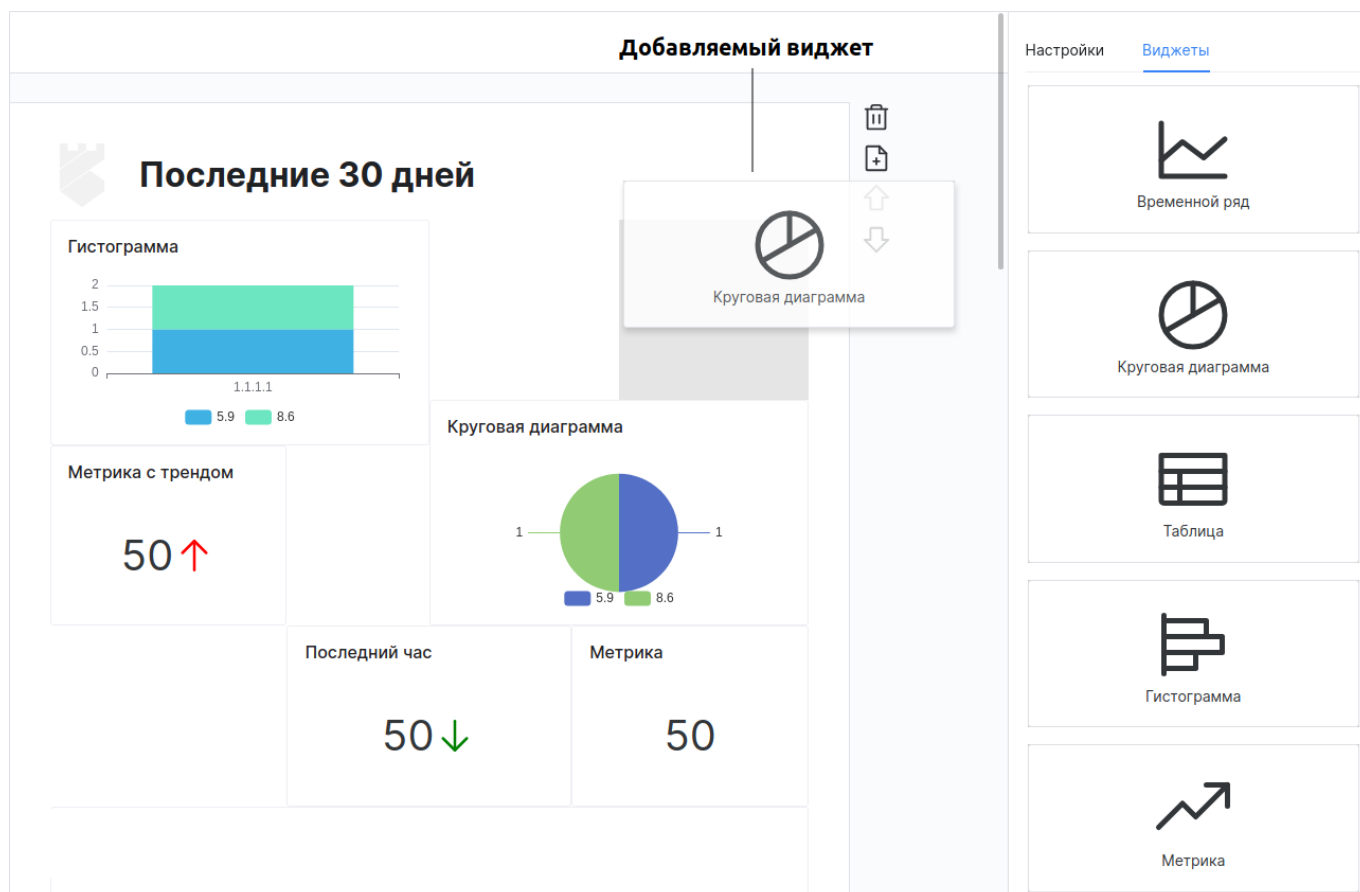



Рис. 267 – Страница "Конструктор отчета". Вкладка "Виджеты"

Для добавления виджета на страницу отчета выполните следующие действия:

1. Наведите курсор мыши на нужный виджет и нажмите 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. 268»).

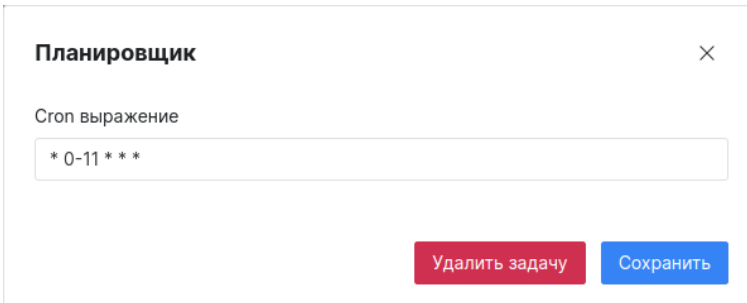




Рис. 268 – Окно "Планировщик"

2. Укажите в окне **Срок 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. 269»).

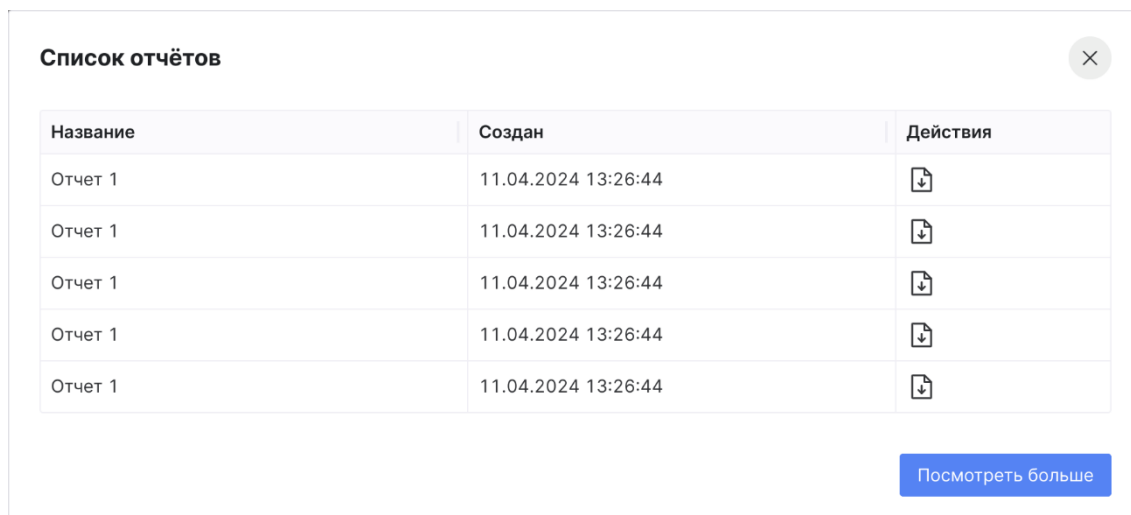


Рис. 269 – Окно "Список отчетов"

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. 270](#)»).

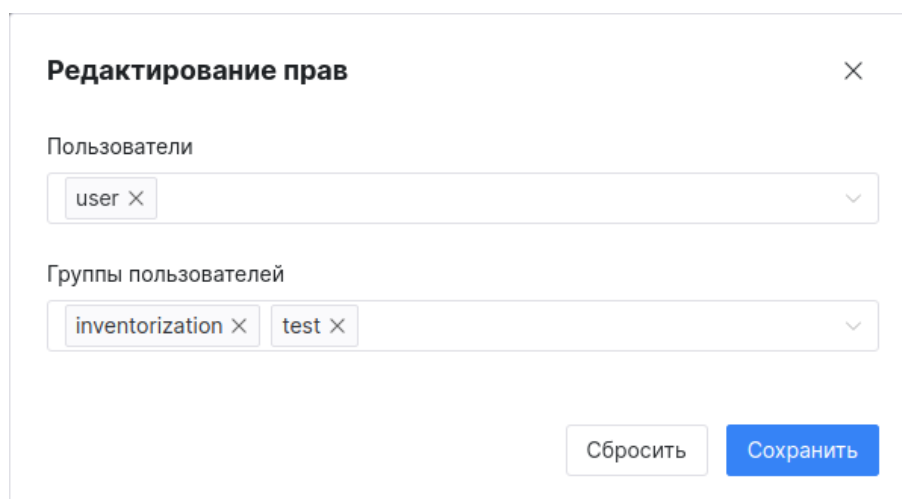


Рис. 270 – Окно "Редактирование прав"

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. 271](#)»).

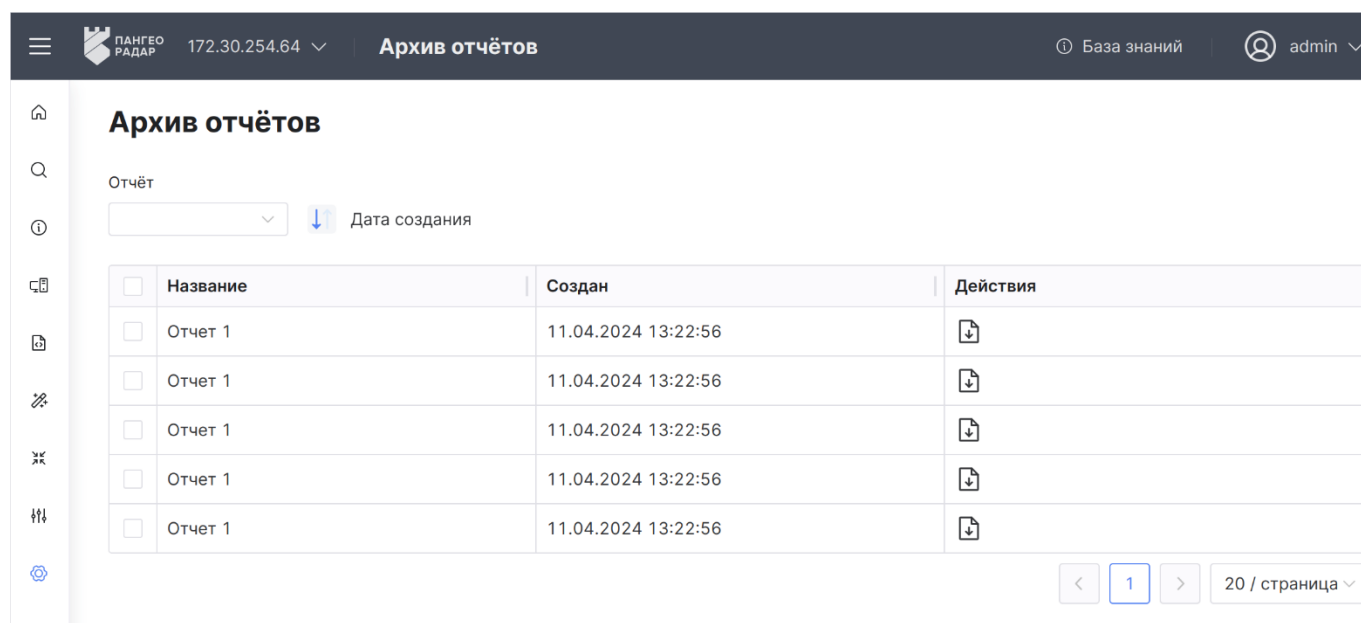


Рис. 271 – Раздел "Архив отчетов"


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. 272](#)»).

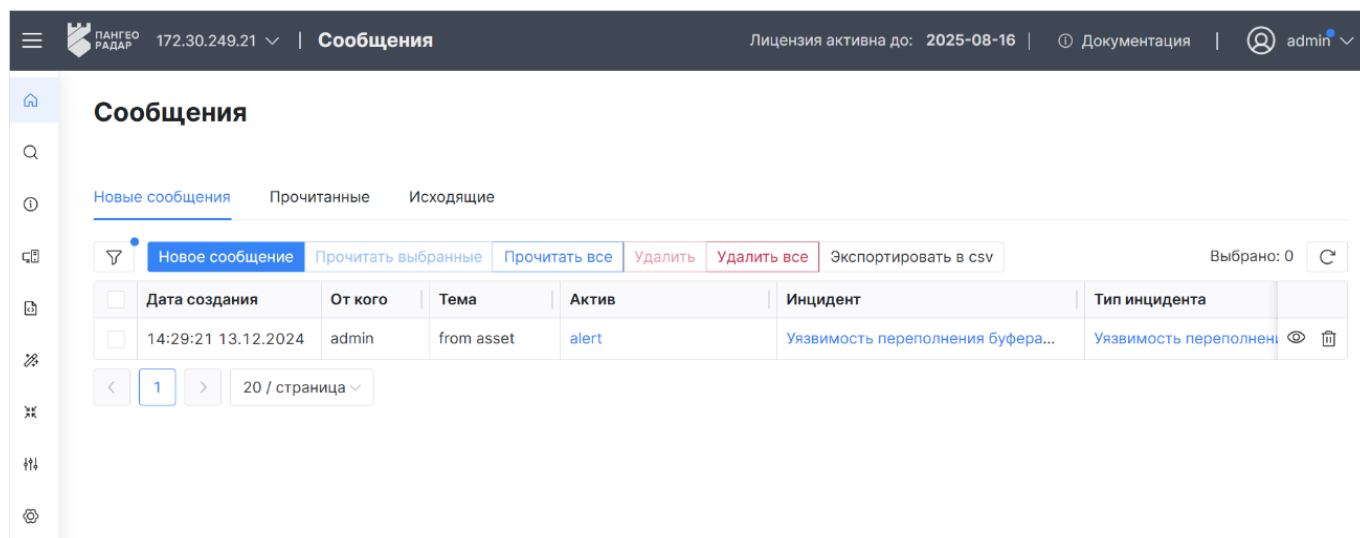


Рис. 272 – Раздел "Сообщения"

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. 273](#)»)

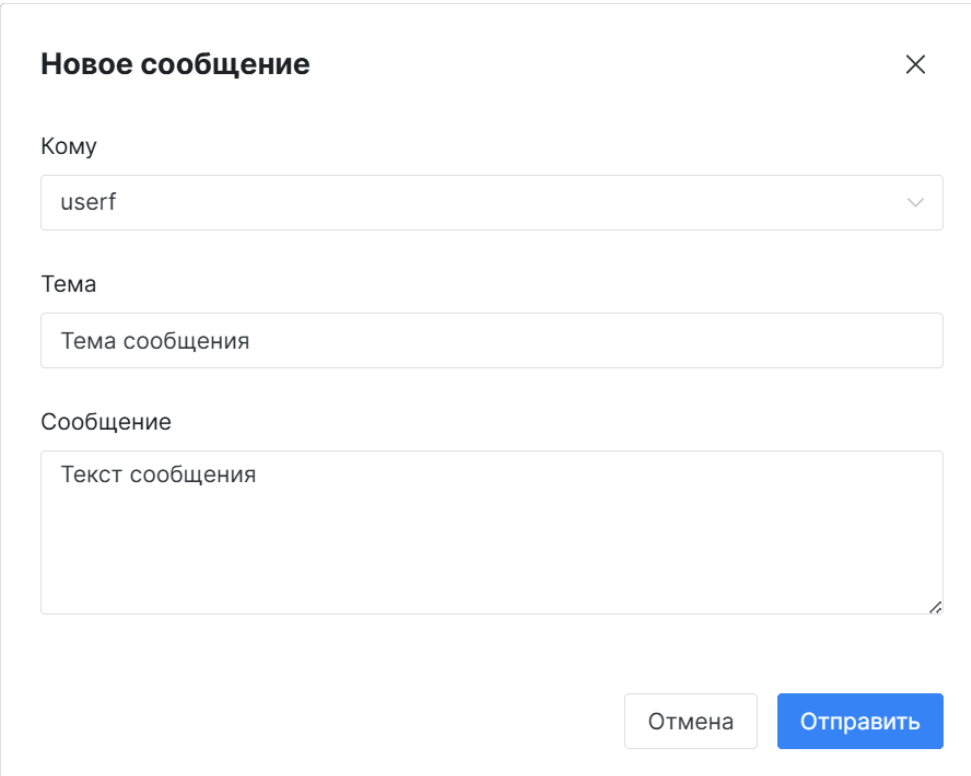


Рис. 273 – Окно "Новое сообщение"

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. 274](#)»).

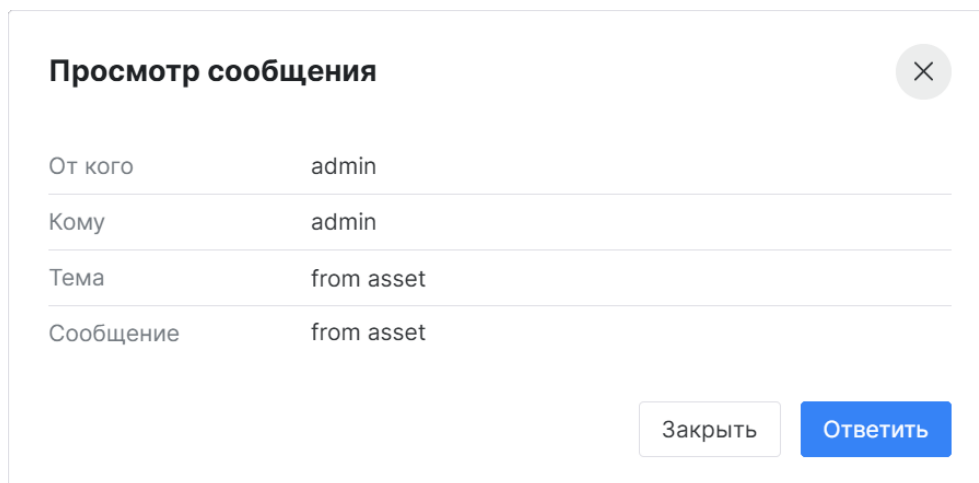


Рис. 274 – Окно "Просмотр сообщения"

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. 274») и нажмите кнопку **Ответить**. Откроется окно "Новое сообщение" (см. «Рис. 273»).
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. 275](#)»).

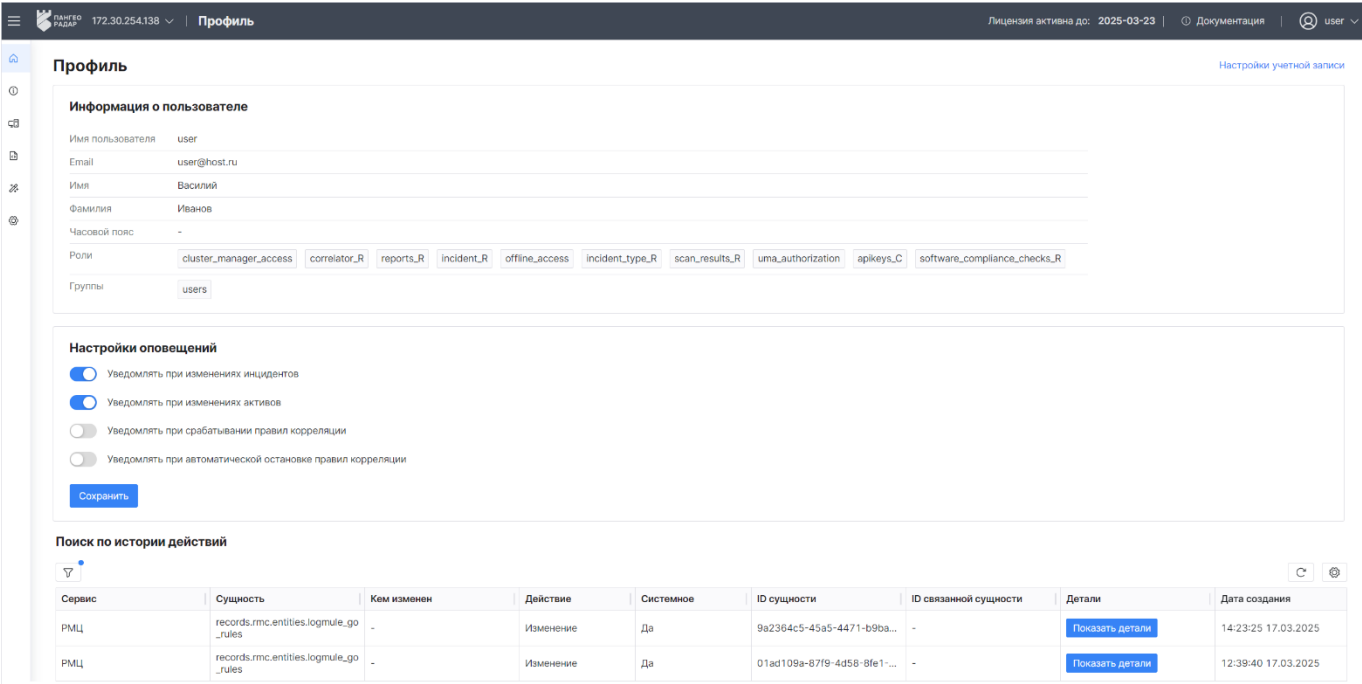


Рис. 275 – Раздел "Профиль"

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. 276»).

Рис. 276 – 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. 277»).

Рис. 277 – 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. 278»).


Аутентификатор

* Обязательные поля

1. Установите [FreeOTP](https://freeotp.github.io/) или Google Authenticator. Оба приложения доступны на [Google Play](https://play.google.com/) и в Apple App Store.

- FreeOTP
- Google Authenticator

2. Откройте приложение и просканируйте баркод, либо введите ключ.



[Unable to scan?](#)

3. Введите одноразовый код, выданный приложением, и нажмите сохранить для завершения установки.

Provide a Device Name to help you manage your OTP devices.

Одноразовый код *

Device Name

Отмена

Сохранить

Рис. 278 – 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. 279»).

Сессии				
IP	Начата	Последний доступ	Истекает	Клиенты
172.30.253.1	Mar 18, 2025, 3:41:16 PM	Mar 18, 2025, 4:57:54 PM	Mar 19, 2025, 1:41:16 AM	radar-ui account
172.30.253.1	Mar 18, 2025, 4:20:45 PM	Mar 18, 2025, 4:55:46 PM	Mar 19, 2025, 2:20:45 AM	radar-ui
<button>Выйти из всех сессий</button>				

Рис. 279 – 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. 280»).

Лог учетной записи				
Дата	Событие	IP	Клиент	Детали
Mar 18, 2025, 4:23:37 PM	logout	172.30.254.1		
Mar 18, 2025, 4:20:45 PM	login	172.30.253.1	radar-ui	auth_method = openid-connect , username = admin
Mar 18, 2025, 4:05:46 PM	login	172.30.254.1	radar-ui	auth_method = openid-connect , username = admin
Mar 18, 2025, 4:05:45 PM	login	172.30.254.1	radar-ui	auth_method = openid-connect , username = admin
Mar 18, 2025, 4:05:36 PM	login	172.30.254.1	account	auth_method = openid-connect , username = admin
Mar 18, 2025, 3:41:16 PM	login	172.30.253.1	radar-ui	auth_method = openid-connect , username = admin
Mar 18, 2025, 10:42:03 AM	logout	172.30.253.1		
Mar 18, 2025, 10:41:29 AM	login	172.30.253.1	radar-ui	auth_method = openid-connect , username = admin
Mar 18, 2025, 10:39:52 AM	logout	172.30.253.1		
Mar 18, 2025, 10:39:28 AM	login	172.30.253.1	radar-ui	auth_method = openid-connect , username = admin

Рис. 280 – 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. 281».

Поиск по истории действий

Фильтры +

Сортировка ↑

Дата создания X

Сбросить

Применить

Сервис	Сущность	Кем изменен	Действие	Системное	ID сущности	ID связанной сущности	Детали	Дата создания
Cruddy	records.cruddy.entities.user	user	records.cruddy.actions.edit	Нет	afef0a74-82ed-4e95-87cb-...	-	<div>Показать детали</div>	11:57:16 18.03.2025
РМЦ	records.rmc.entities.logmule_go_rules	-	Изменение	Да	9a2364c5-45a5-4471-b9ba-...	-	<div>Показать детали</div>	14:23:25 17.03.2025
РМЦ	records.rmc.entities.logmule_go_rules	-	Изменение	Да	01ad109a-87f9-4d58-8fe1-...	-	<div>Показать детали</div>	12:39:40 17.03.2025
РМЦ	Фильтр потока	-	Изменение	Да	f97192dd-a270-41e1-90cb-...	-	<div>Показать детали</div>	12:39:40 17.03.2025
РМЦ	Ключ табличного списка	-	Изменение	Да	229da3c0-2f9c-4fb6-b8b9-...	-	<div>Показать детали</div>	12:39:40 17.03.2025
РМЦ	records.rmc.entities.logmule_go_rules	-	Создание	Да	01ad109a-87f9-4d58-8fe1-...	-	<div>Показать детали</div>	12:21:35 17.03.2025
РМЦ	Фильтр потока	-	Изменение	Да	f97192dd-a270-41e1-90cb-...	-	<div>Показать детали</div>	12:21:35 17.03.2025
РМЦ	Ключ табличного списка	-	Изменение	Да	229da3c0-2f9c-4fb6-b8b9-...	-	<div>Показать детали</div>	12:21:35 17.03.2025
РМЦ	records.rmc.entities.logmule_go_rules	-	Изменение	Да	d873fe67-4d86-43db-86e2-...	-	<div>Показать детали</div>	12:16:16 17.03.2025
РМЦ	records.rmc.entities.logmule_go_rules	-	Создание	Да	d873fe67-4d86-43db-86e2-...	-	<div>Показать детали</div>	12:16:01 17.03.2025

< 1 2 3 4 5 6 7 ... 162 >

10 / страница >>

Рис. 281 – 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. 282»).

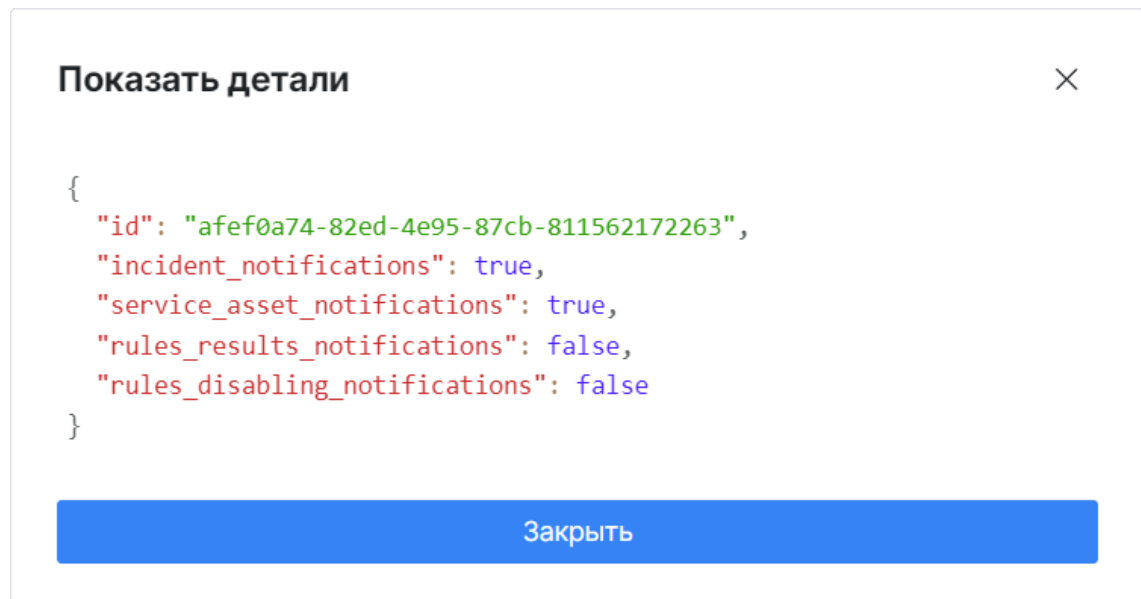


Рис. 282 – Окно "Показать детали"

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. 283»](#));

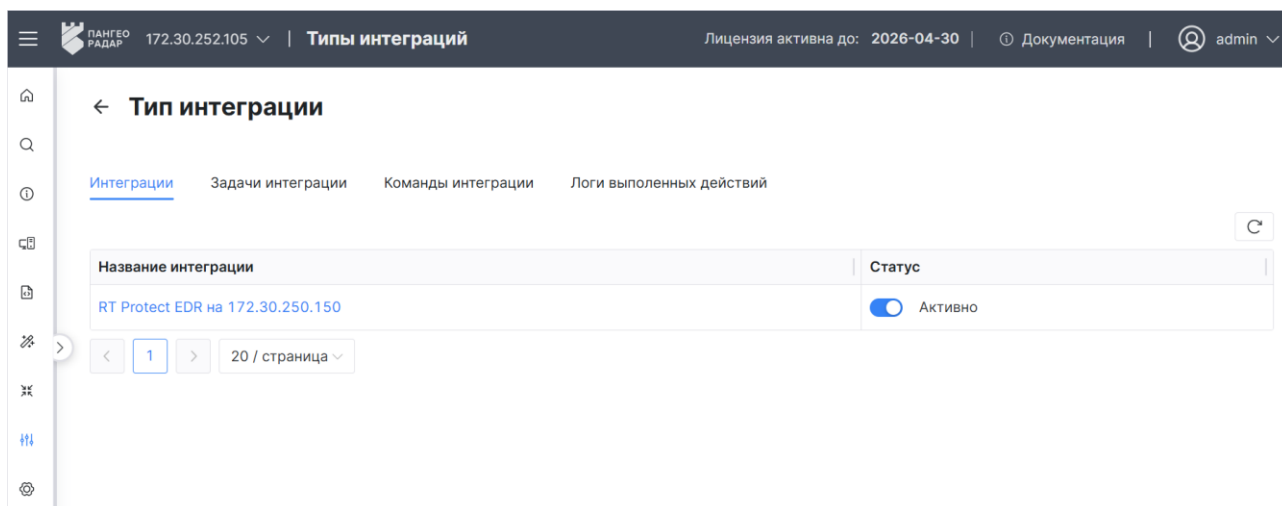


Рис. 283 – Просмотр типа интеграции RT Protect EDR. Вкладка "Интеграции"

- **Задачи интеграции.** Пример вкладки приведен на «Рис. 284».

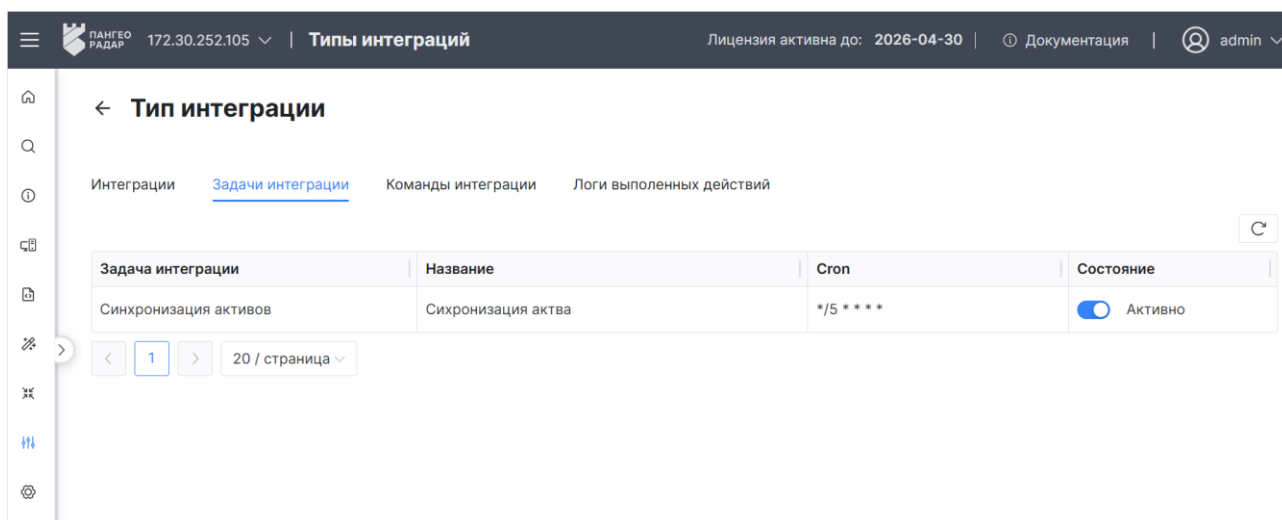


Рис. 284 – Просмотр типа интеграции RT Protect EDR. Вкладка "Задачи интеграции"

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. 285».

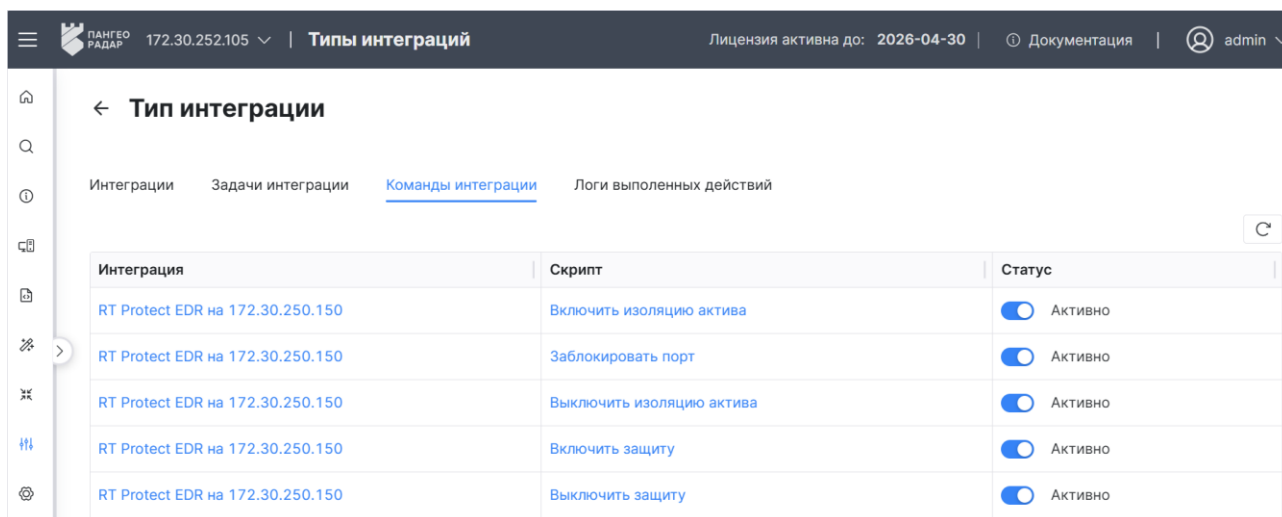


Рис. 285 – Просмотр типа интеграции RT Protect EDR. Вкладка "Команды интеграции"

На вкладке отображается информация об активных действиях, созданных в рамках интеграций:

- **Интеграция** – наименование интеграции, для которой выполняется команда;
- **Скрипт** – наименование команды;
- **Статус** – состояние команды: Активно, Неактивно.
- **Логи выполненных действий.** Пример вкладки приведен на «Рис. 286».

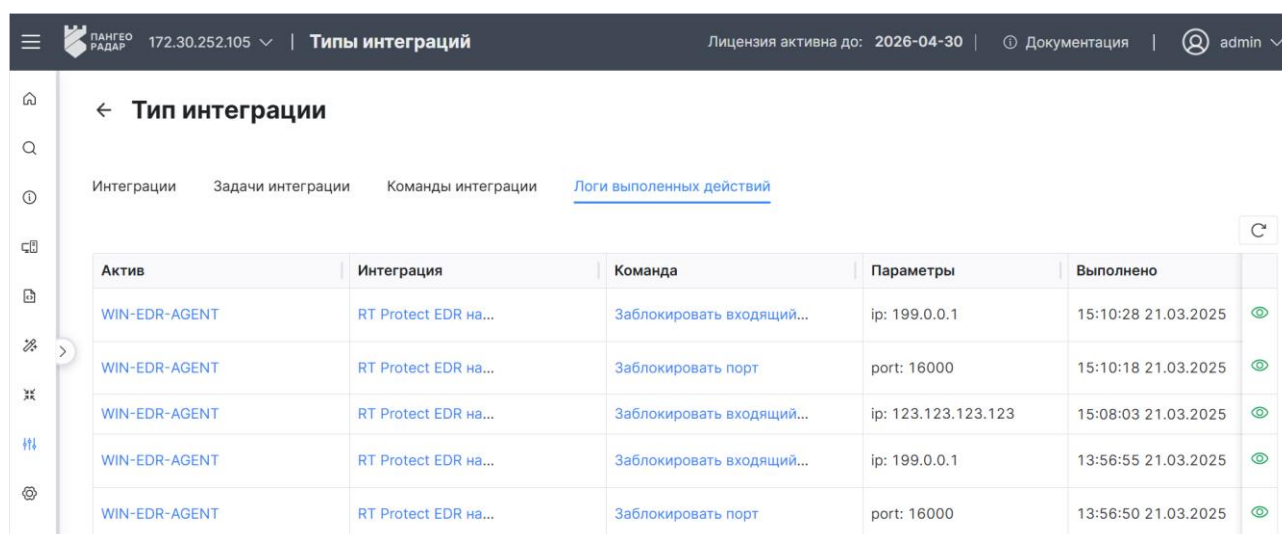



Рис. 286 – Просмотр типа интеграции RT Protect EDR. Вкладка "Логи выполненных действий"

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. 287»).

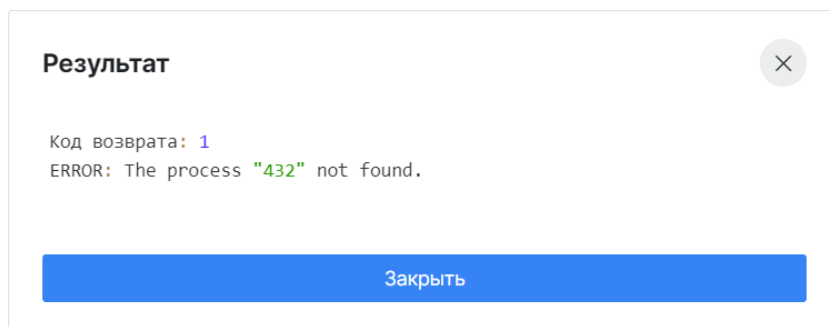


Рис. 287 – Окно "Результат"

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. 288](#)»).

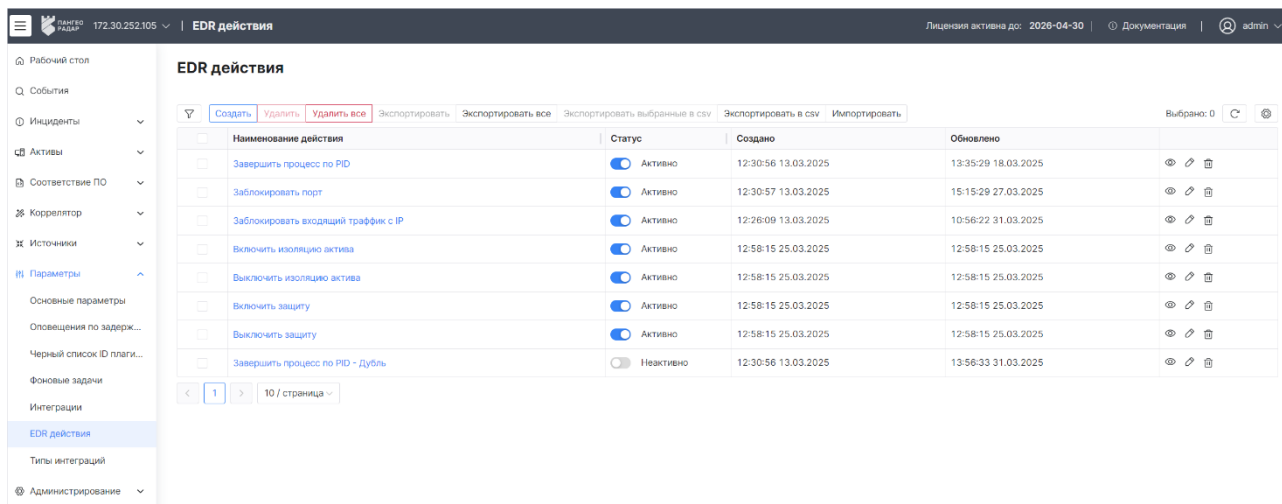


Рис. 288 – Раздел "EDR действия"

16.1.2.1 Создание EDR действия

1. Нажмите кнопку **Создать**. Откроется форма **Создание действия EDR** (см. «Рис. 289»).


Рис. 289 – 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

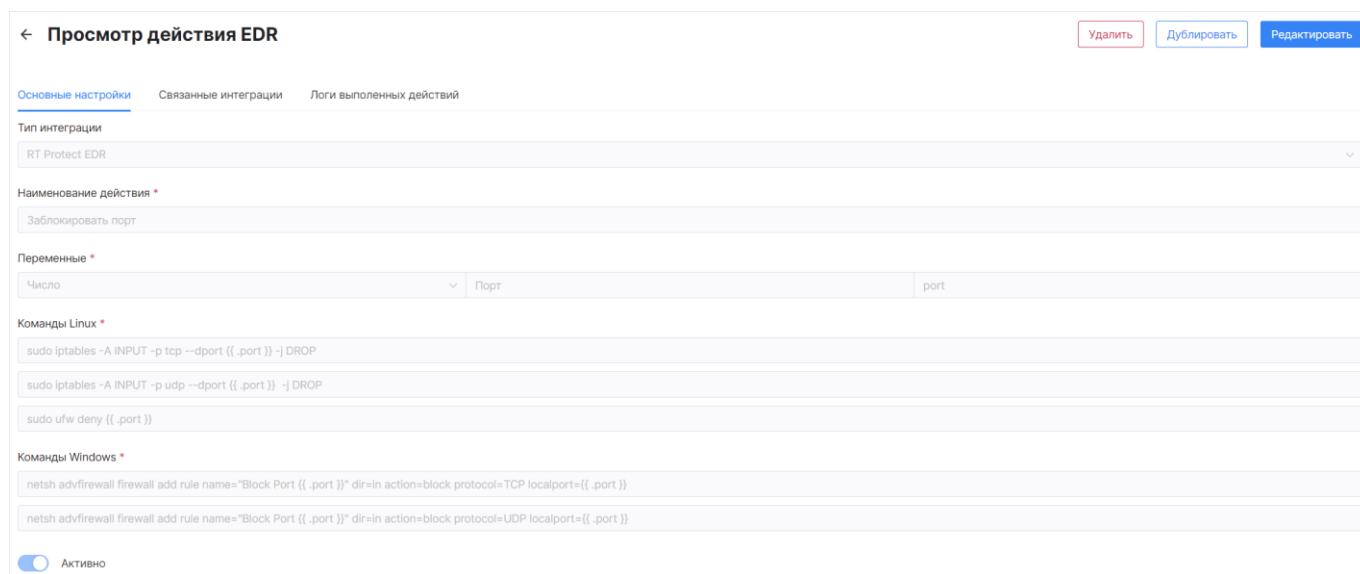
Для просмотра информации об EDR действии нажмите кнопку  в строке нужного действия. Откроется форма "Просмотр действия EDR".

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. 290](#)».



← Просмотр действия EDR

Удалить Дублировать Редактировать

Основные настройки Связанные интеграции Логи выполненных действий

Тип интеграции
RT Protect EDR

Наименование действия *
Заблокировать порт

Переменные *
Число Port port

Команды Linux *
sudo iptables -A INPUT -p tcp --dport {{ .port }} -j DROP
sudo iptables -A INPUT -p udp --dport {{ .port }} -j DROP
sudo ufw deny {{ .port }}

Команды Windows *
netsh advfirewall firewall add rule name="Block Port {{ .port }}" dir=in action=block protocol=TCP localport={{ .port }}
netsh advfirewall firewall add rule name="Block Port {{ .port }}" dir=in action=block protocol=UDP localport={{ .port }}

☒ Активно

Рис. 290 – 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. 291](#)».

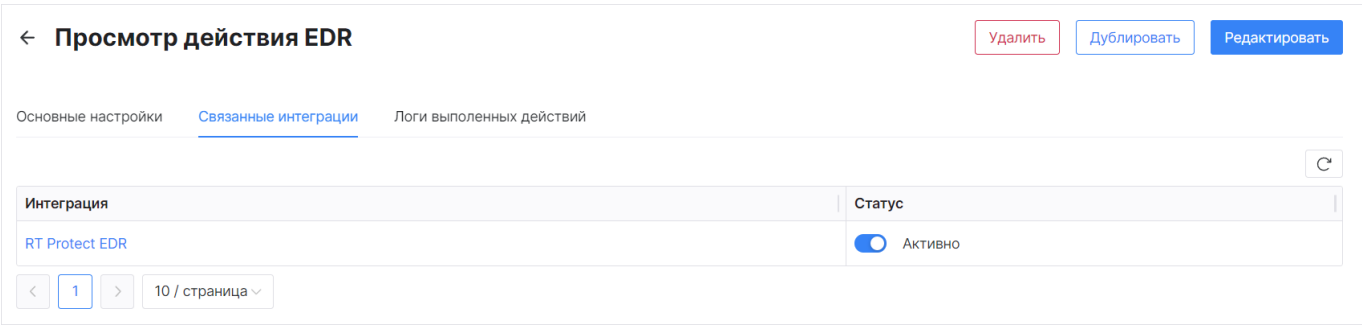


Рис. 291 – Форма "Просмотр действия EDR". Вкладка "Связанные интеграции"

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. 292».

← Просмотр действия EDR

Удалить Дублировать Редактировать

Основные настройки Связанные интеграции Логи выполненных действий


Актив	Параметры	Выполнено	Кем выполнен	Интеграция	Команда	Дата старта	Код возврата	
WIN-EDR-AGENT	port: 16000	15:10:18 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	Заблокировать порт	15:10:00 21.03.2025	0	🟢
WIN-EDR-AGENT	port: 16000	13:56:50 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	Заблокировать порт	13:56:39 21.03.2025	0	🟢
WIN-EDR-AGENT	port: 16000	12:30:31 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	Заблокировать порт	12:30:18 21.03.2025	0	🟢
WIN-EDR-AGENT	port: 16000	12:17:49 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	Заблокировать порт	12:17:38 21.03.2025	0	🟢
WIN-EDR-AGENT	port: 16000	10:35:54 20.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	Заблокировать порт	10:35:36 20.03.2025	0	🟢
WIN-EDR-AGENT	port: 23123123	12:32:01 19.03.2025	admin	RT Protect EDR на 172.30.250.150	Заблокировать порт	12:31:56 19.03.2025	1	🔴
WIN-EDR-AGENT	port: 23123123	12:29:57 19.03.2025		RT Protect EDR на 172.30.250.150	Заблокировать порт	12:29:52 19.03.2025	1	🔴
WIN-EDR-AGENT	port: 3212312312312	17:13:13 17.03.2025	admin	RT Protect EDR на 172.30.250.150	Заблокировать порт	17:13:04 17.03.2025	1	🔴
WIN-EDR-AGENT	port: 3123123123	13:44:16 17.03.2025	admin	RT Protect EDR на 172.30.250.150	Заблокировать порт	13:44:11 17.03.2025	1	🔴
WIN-EDR-AGENT	port: 13123123123213	13:32:59 17.03.2025	admin	RT Protect EDR на 172.30.250.150	Заблокировать порт	13:32:56 17.03.2025	1	🔴

1 2 10 / страница

Рис. 292 – 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. 293](#)»).

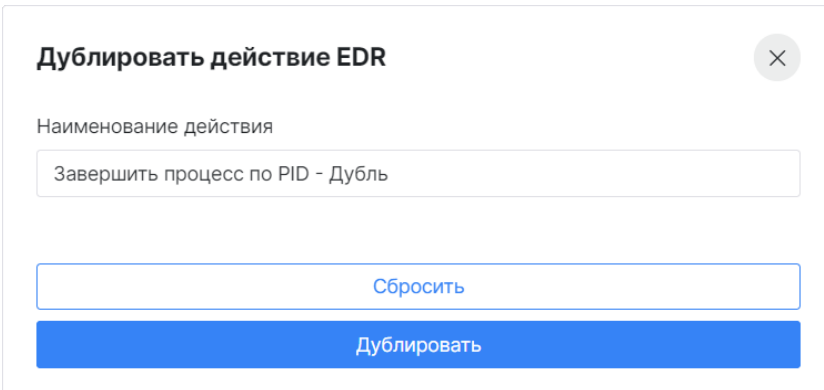


Рис. 293 – Окно "Дублировать действие EDR"

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 удаления 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. 294](#)»).

← **Создание интеграции**

Сбросить Проверить Сохранить

Название интеграции *

RT Protect EDR с управляющим сервером на <IP-адрес сервера>

☒ Статус

Тип интеграции *

RT Protect EDR

Адрес API сервера *

172.30.250.150

Токен аутентификации

Логин *

admin

Пароль *

admin

Порт *

443

Использовать задание синхронизации

☒

Использовать активные действия интеграции

☒

Сбросить Проверить Сохранить

Рис. 294 – 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. 295»).

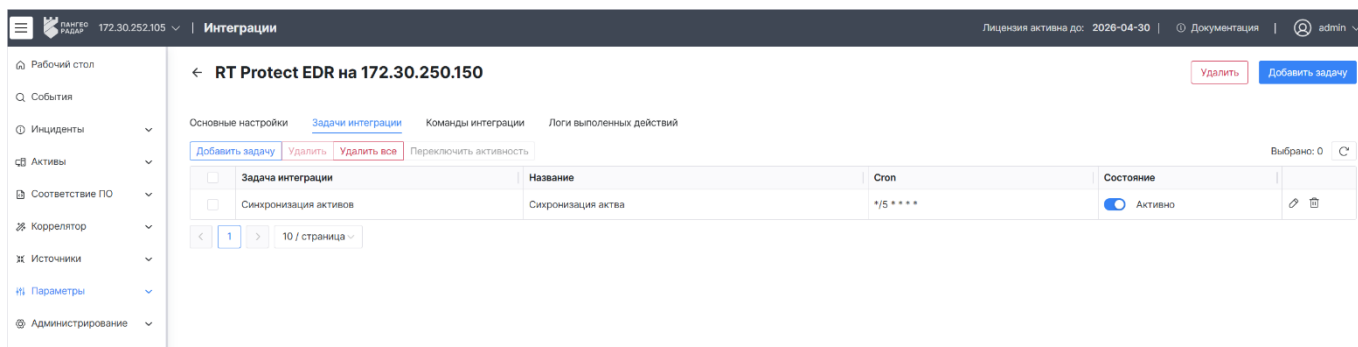


Рис. 295 – Настройка интеграции. Задачи интеграции

3. Нажмите кнопку **Добавить задачу**. Откроется окно "Добавить задачу" (см. «Рис. 296»).

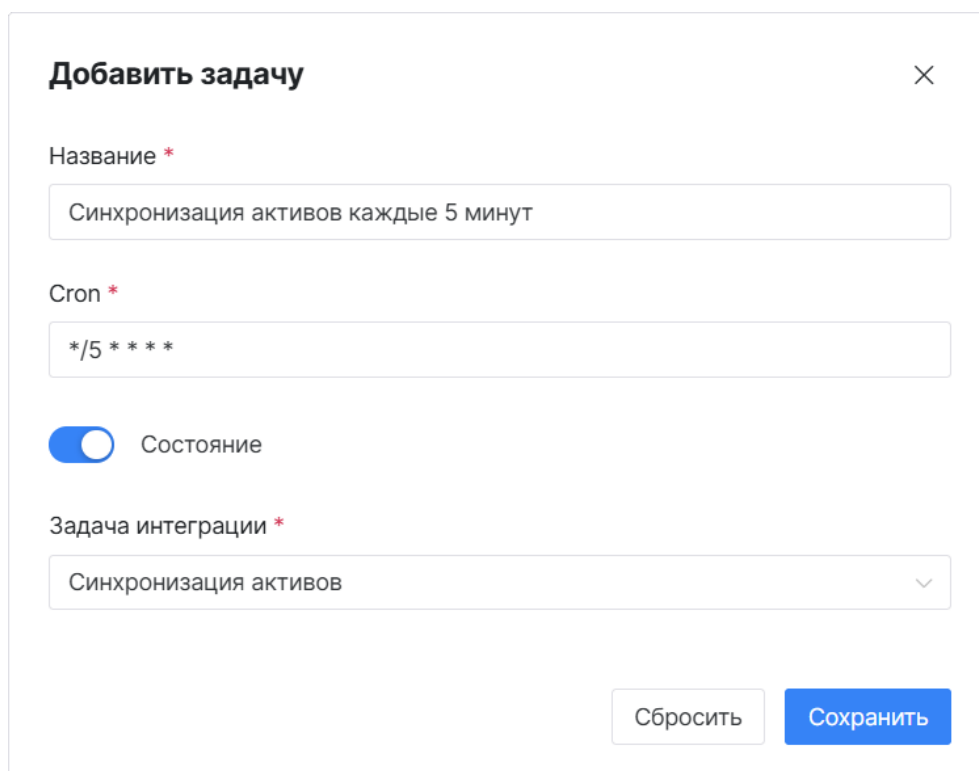


Рис. 296 – Окно "Добавить задачу"


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. 297](#)»).

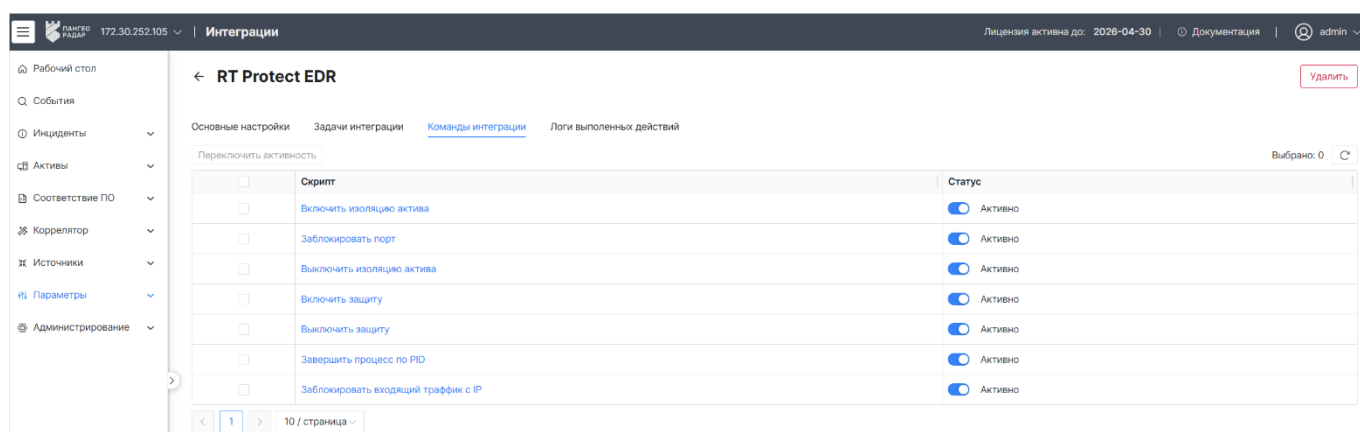


Рис. 297 – Настройка интеграции. Команды интеграции

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.
- «Работа с активами»:
 - выполнение активных действий по связанным интеграциям;
 - просмотр журнала выполненных действий на активе.

- «Работа с инцидентами» – просмотр журнала выполненных действий по инциденту;
- «Просмотр журнала выполнения действий по интеграции».

16.1.4.1 Работа с правилами корреляции

16.1.4.1.1 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. 298»).

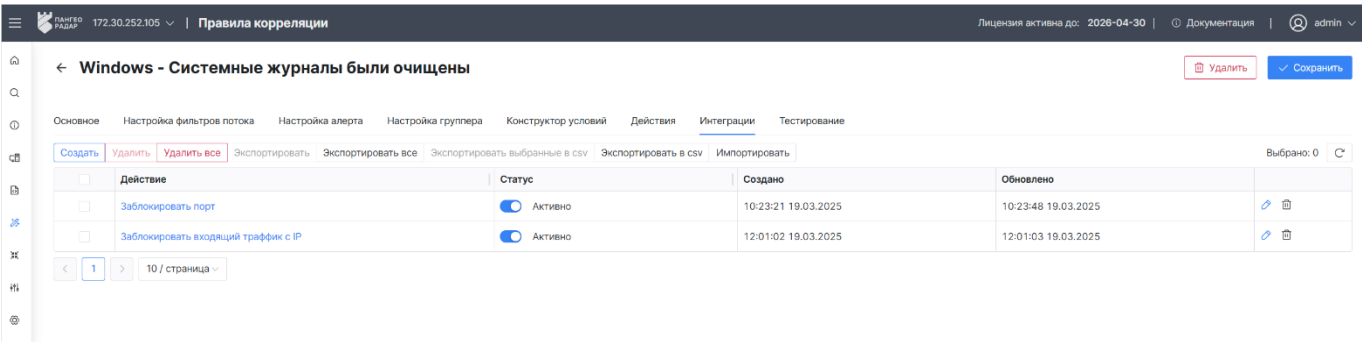


Рис. 298 – Конструктор правила корреляции. Вкладка "Интеграции"

3. Нажмите кнопку **Создать**. Откроется окно "Действия интеграции" (см. «Рис. 299» - «Рис. 300»).

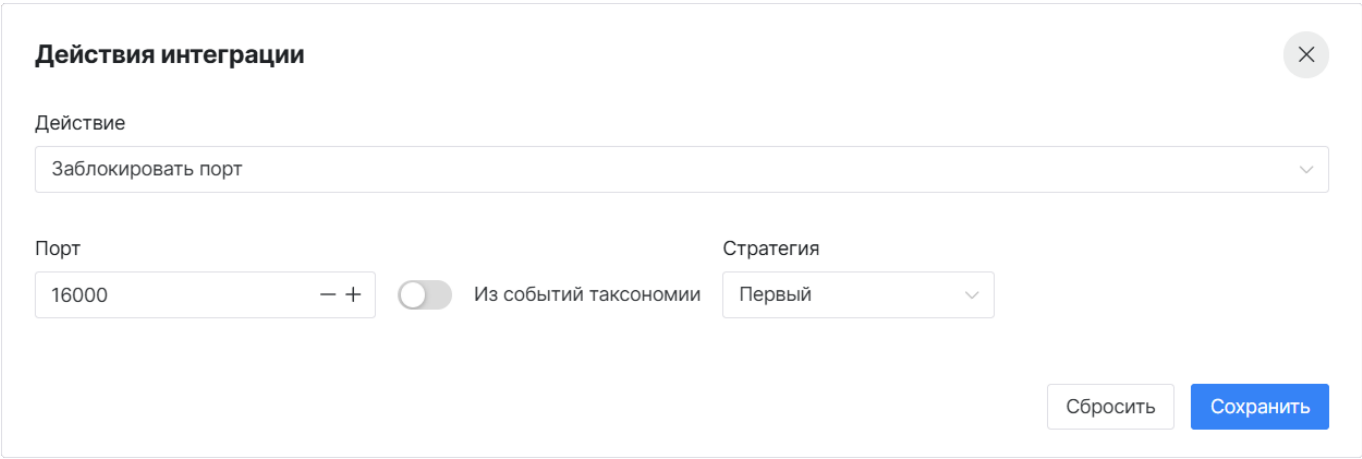


Рис. 299 – Настройка действия интеграции с дополнительными параметрами

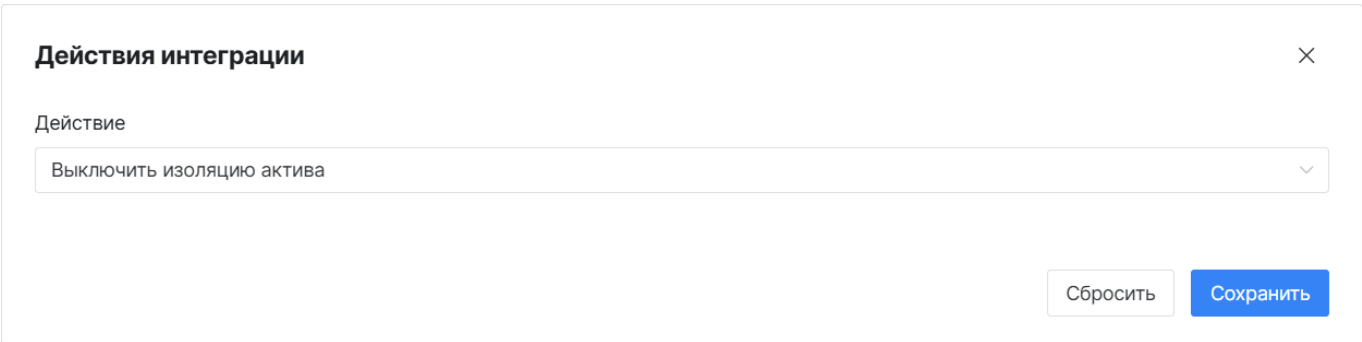


Рис. 300 – Настройка действия интеграции без дополнительных параметров

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 трафик 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.

16.1.4.1.2 Просмотр действий интеграции

Для просмотра добавленных в правило действий интеграции откройте его на просмотр и перейдите на вкладку "Интеграции" (см. «Рис. 301»).

← Windows - Системные журналы были очищены

Активное

Перезапустить

Открыть редактор

Основное

ID: a3491b6f-46a1-43e4-ab22-9ec9c9a5530f

Создано: 2025-03-18 14:15:00

Изменено: 2025-03-19 12:02:08

Тип правила: Визуальный конструктор

Тип инцидента: Windows - Системные журналы были очищены

Описание: Правило детектирует очистку журналов Windows.

Ретроспективное: Нет

Сбор метрик: Нет

Максимальное значение памяти (МБ): Нет

Максимальное количество срабатываний: Нет

За интервал (секунд): Нет

Фильтры потока событий: Windows_event_logs_cleared

Инциденты

Результаты

Интеграции

Лог изменений

Лог правила

Метрики

Создать

Удалить

Удалить все

Экспортировать

Экспортировать все

Экспортировать выбранные в csv

Экспортировать в csv

Импортировать

Выбрано: 0

	Действие	Статус	Создано	Обновлено	
<input type="checkbox"/>	Заблокировать порт	Активно	10:23:21 19.03.2025	10:23:48 19.03.2025	✎ 🗑
<input type="checkbox"/>	Заблокировать входящий трафик с IP	Активно	12:01:02 19.03.2025	12:01:03 19.03.2025	✎ 🗑

1

10 / страница

Рис. 301 – 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.

16.1.4.2 Работа с активами

16.1.4.2.1 Просмотр связей с интеграциями и журнала выполненных действий

Откройте актив на просмотр (см. «Рис. 302»).

← WIN-EDR-AGENT

РедактироватьДобавить в группуНаписать ответственному⋮

Основное

IP	172.30.250.161
FQDN	-
MAC	-
OC	Microsoft Windows Server 2022 Standard Evaluation - 64 bit
Группа актива	group
Тип актива	Host
Расположение	https://172.30.250.150/api/agent/1/
Ответственный	-
Группа ответственных	-
Дата последнего сканирования	Не произведено
Активен	Да
В локальной сети	Нет
Сетевая видимость	Штатный доступ в Интернет через Proxy

Сетевые интерфейсы

Название	IP	MAC
Ethernet0	172.30.250.161	

Программное обеспечение

Агент RT Protect EDR, версия - 2.0.178.2678

Microsoft Edge, версия - 134.0.3124.51

Microsoft Edge, версия - 134.0.3124.66

Показать больше

Аппаратное обеспечение

memory , Capacity: 16 GB, PartNumber: , SerialNumber: , Manufacturer: , ConfiguredClockSpeed:

processor , name: Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz, manufacturer: , caption: , numberOfCores: 8, addressWidth:

Описание

https://172.30.250.150/api/agent/1/

Инциденты

Срочность

0.94

Название

Windows - Системные журналы были очищены

Статус

Новый

Создано

15:09:59 21.03.2025

<

1

>

10 / страница

Связи с интеграциями

Интеграция	Тип интеграции	URI	Действие
RT Protect EDR на 172.30.250.150	RT Protect EDR	https://172.30.250.150/api/agent/1/	Выполнить действие

Логи выполненных действий

Команда

Параметры

Выполнено

Кем выполнен

Интеграция

Заблокировать входящий трафик с IP	ip: 199.0.0.1	15:10:28 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150
Заблокировать порт	port: 16000	15:10:18 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150
Заблокировать входящий трафик с IP	ip: 123.123.123.123	15:08:03 21.03.2025	admin	RT Protect EDR на 172.30.250.150

<

1

2

3

4

>


10 / страница

Рис. 302 – 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.

16.1.4.2.2 Выполнение активных действий на активе

1. Откройте актив на просмотр (см. «Рис. 302»).
2. В блоке **Связи с интеграциями** нажмите кнопку **Выполнить действие**. Откроется окно "Выполнить действие" (см. «Рис. 303»).

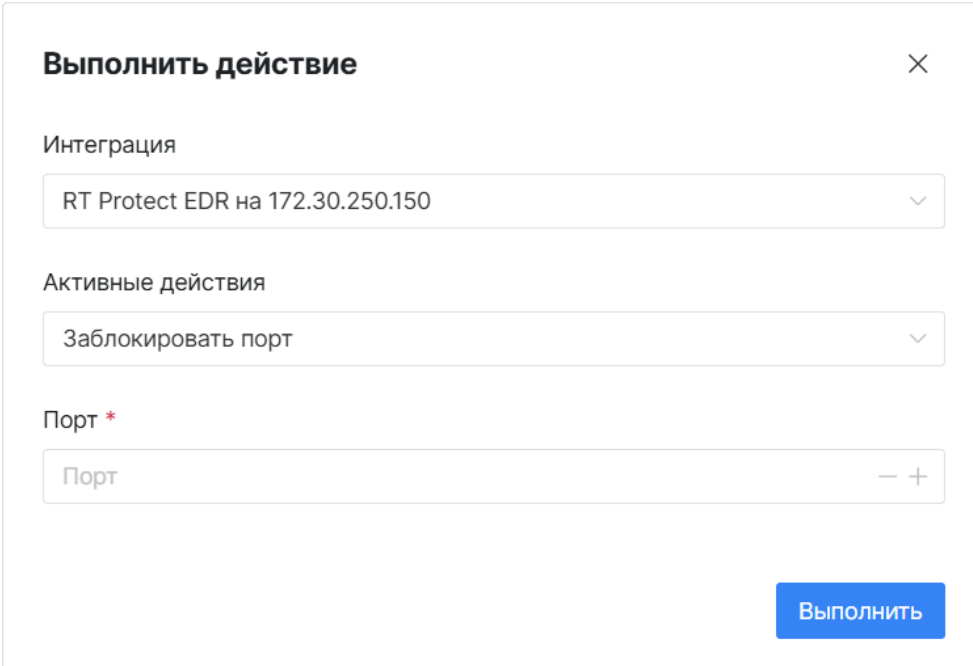


Рис. 303 – Окно "Выполнить действие"

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**.

16.1.4.3 Работа с инцидентами

Откройте инцидент на просмотр (см. «Рис. 304»).

← ID: 16

Статус: Новый Переназначить Редактировать Написать ответственным

Windows - Системные журналы были очищены

1

Содержимое журнала событий Windows было удалено вручную. Это событие может указывать на попытку злоумышленника скрыть следы незаконной деятельности путем удаления журналов. С помощью групповой политики можно ограничить выполнение отдельных действий и возможности доступа путем назначения прав и разрешений. При этом право/разрешение позволяет учетной записи пользователя выполнять определенные действия на компьютере, такие как резервное копирование файлов и папок или выключение компьютера. Удаление файлов журнала представляет высокий риск, поэтому такие события следует тщательно расследовать.

9

Источник: Коррелятор

Кол-во повторных открытий: 0

Кол-во происшествий: 1

Правило корреляции: Windows - Системные журналы были очищены

Дата создания

21.03.2025 15:09:59

Тип инцидента

Windows - Системные журналы были очищены

Показать описание

Последнее происшествие

21.03.2025 15:09:58

Показать больше

Результат анализа

На хосте 172.30.250.161 были очищены журналы security, пользователем Administrator, the journal "security" was cleared

Рекомендации по устранению инцидента:

Происшествия

Показать в событиях

Выбрано: 0

<input type="checkbox"/>	FQDN	IP	Отправлено в НКЦКИ	Начало активности	Конец активности	
<input type="checkbox"/>	win-edr-agent.edr-agent.local	172.30.250.161	Нет	15:09:58 21.03.2025	15:09:58 21.03.2025	

1

10 / страница

Логи выполненных действий

Команда	Параметры	Актив	Дата старта	Выполнено	Интеграция	Код возврата	Кем выполнен	
Заблокировать входящий трафик с IP	ip: 199.0.0.1	WIN-EDR-AGENT	15:10:18 21.03.2025	15:10:28 21.03.2025	RT Protect EDR на 172.30.250.150	0	Windows - Системные журналы были очищены	
Заблокировать порт	port: 16000	WIN-EDR-AGENT	15:10:00 21.03.2025	15:10:18 21.03.2025	RT Protect EDR на 172.30.250.150	0	Windows - Системные журналы были очищены	

1

10 / страница

Рис. 304 – Просмотр инцидента

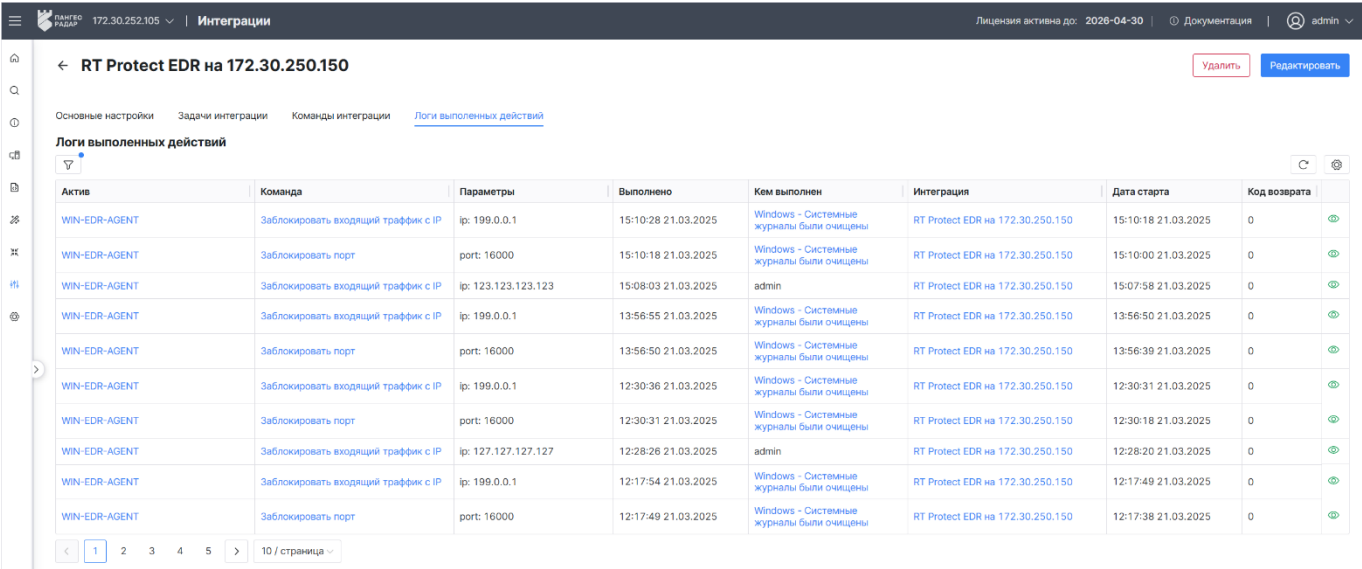
При интеграции с системой **RT Protect EDR** при анализе инцидента в блоке **Логи выполненных действий** доступен просмотр следующей дополнительной информации:

- **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.

16.1.4.4 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. 305»).




Актив	Команда	Параметры	Выполнено	Кем выполнено	Интеграция	Дата старта	Код возврата	
WIN-EDR-AGENT	Заблокировать входящий трафик с IP	ip: 199.0.0.1	15:10:28 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	15:10:18 21.03.2025	0	👁
WIN-EDR-AGENT	Заблокировать порт	port: 16000	15:10:18 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	15:10:00 21.03.2025	0	👁
WIN-EDR-AGENT	Заблокировать входящий трафик с IP	ip: 123.123.123.123	15:08:03 21.03.2025	admin	RT Protect EDR на 172.30.250.150	15:07:58 21.03.2025	0	👁
WIN-EDR-AGENT	Заблокировать входящий трафик с IP	ip: 199.0.0.1	13:56:55 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	13:56:50 21.03.2025	0	👁
WIN-EDR-AGENT	Заблокировать порт	port: 16000	13:56:50 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	13:56:39 21.03.2025	0	👁
WIN-EDR-AGENT	Заблокировать входящий трафик с IP	ip: 199.0.0.1	12:30:36 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	12:30:31 21.03.2025	0	👁
WIN-EDR-AGENT	Заблокировать порт	port: 16000	12:30:31 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	12:30:18 21.03.2025	0	👁
WIN-EDR-AGENT	Заблокировать входящий трафик с IP	ip: 127.127.127.127	12:28:26 21.03.2025	admin	RT Protect EDR на 172.30.250.150	12:28:20 21.03.2025	0	👁
WIN-EDR-AGENT	Заблокировать входящий трафик с IP	ip: 199.0.0.1	12:17:54 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	12:17:49 21.03.2025	0	👁
WIN-EDR-AGENT	Заблокировать порт	port: 16000	12:17:49 21.03.2025	Windows - Системные журналы были очищены	RT Protect EDR на 172.30.250.150	12:17:38 21.03.2025	0	👁

Рис. 305 – 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. 306](#)»).

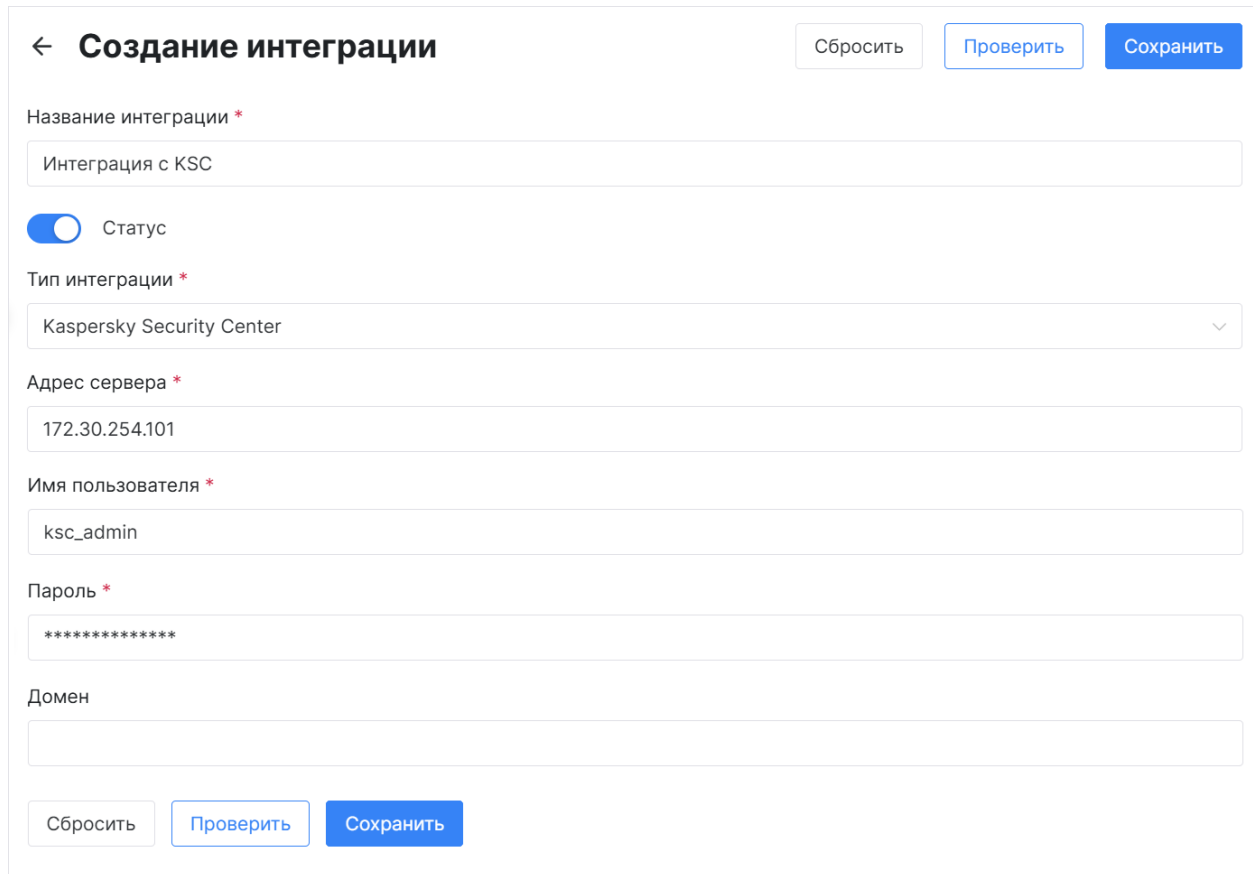



Рис. 306 – Создание интеграции с KSC

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. 307](#)»).

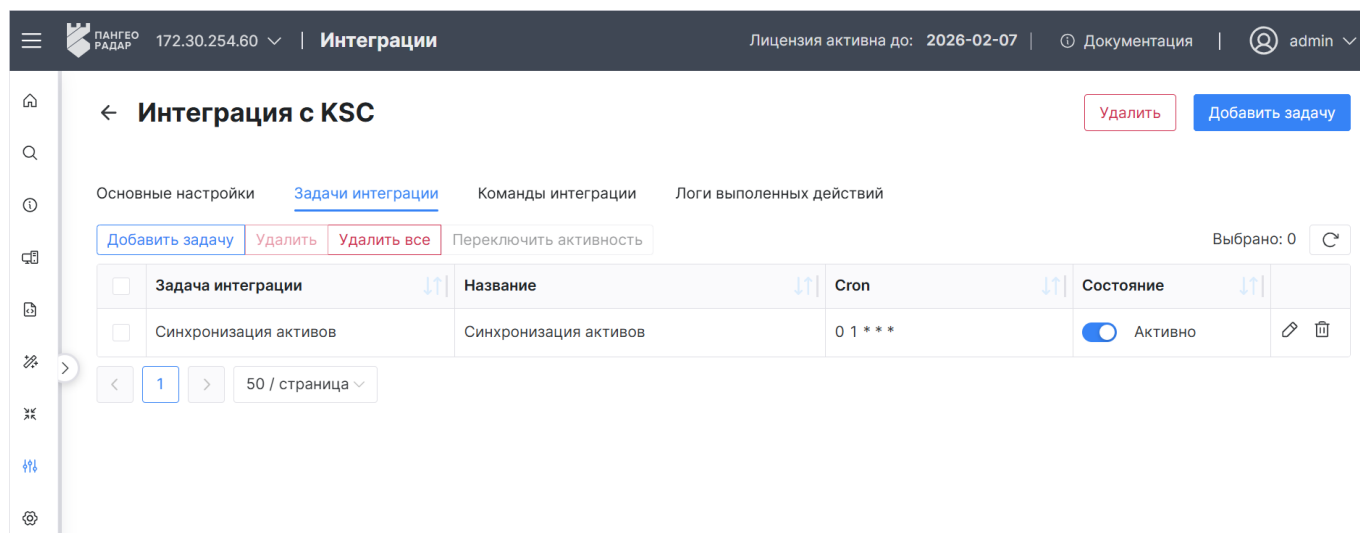


Рис. 307 – Настройка интеграции. Вкладка "Задачи интеграции"

3. Нажмите кнопку **Добавить задачу**. Откроется окно "Добавить задачу" (см. «[Рис. 308](#)»).

Добавить задачу ✕

Название *
Синхронизация активов

Cron *
0 1 * * *

☒ Состояние

Задача интеграции *
Синхронизация активов

Сбросить Сохранить

Рис. 308 – 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 сведения 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".

16.3 Active Directory

16.3.1 Характеристики системы

Наименование системы – Active Directory (далее AD).

Назначение системы – служба каталогов от Microsoft, предназначенная для централизованного хранения информации о пользователях, компьютерах, сетевых устройствах и ресурсах компании.

Разработчик системы – Microsoft.

Сайт – [Общие сведения о доменных службах Active Directory | Microsoft Learn](#).

Возможности, предоставляемые интеграцией:

- получение информации о компьютерах и сетевых устройствах от AD;
- импорт полученной информации в активы.

16.3.2 Настройка интеграции

Перед выполнением настройки интеграции активируйте тип интеграции **Active Directory**. Подробнее см. раздел «[Типы интеграций](#)».

Процесс настройки интеграции с **AD** включает в себя следующие шаги:

- «[Шаг 1. Создание экземпляра интеграции с AD](#)».
- «[Шаг 2. Создание задачи по синхронизации активов](#)».
- «[Шаг 3. Активация экземпляра интеграции с AD](#)».

16.3.2.1 Шаг 1. Создание экземпляра интеграции с AD

1. Перейдите в раздел **Параметры** → **Интеграции**.
2. Нажмите кнопку **Создать**. Откроется окно "Создание интеграции" (см. «[Рис. 309](#)»).

←

Создание интеграции

Сбросить

Проверить

Создать

Название интеграции *

Интеграция с AD

☒ Статус

Тип интеграции *

Active Directory

Адрес AD контроллера *

172.30.254.52

− +

Порт *

389

− +

Использовать защищенное соединение *

☒

Домен *

dom.local

Логин для подключения *

Administrator

Пароль для подключения *

.....

Пользовательский фильтр ⓘ

(objectClass=*)

Список DN для сканирования *

DC=dom,DC=local

− +

Поиск в глубину * ⓘ

☒

Импортировать узлы не старше * ⓘ

0

− +

Сбросить

Проверить

Создать


Рис. 309 – Создание интеграции с KSC

3. Укажите в окне следующую информацию:

- **Название интеграции** – укажите наименование интеграции;
- **Тип интеграции** – из выпадающего списка выберите значение "Active Directory". Поля формы автоматически изменятся для настройки выбранного типа интеграции;
- **Адрес AD контроллера** – укажите IP-адрес сервера, на котором установлена роль Active Directory Domain Services (AD DS) и который отвечает за управление безопасностью и информацией о пользователях, компьютерах, группах и других сущностях в пределах домена AD;

- **Порт** – укажите порт для подключения к серверу;
 - **Использовать защищенное соединение** – включите переключатель если необходимо использовать протокол LDAPS, иначе будет использоваться протокол LDAP;
 - **Домен** – укажите домен, в котором располагается AD контроллер;
 - **Логин для подключения** – укажите логин пользователя для подключения к серверу AD контроллера;
 - **Пароль для подключения** – укажите пароль пользователя;
 - **Пользовательский фильтр** – укажите LDAP фильтр для уточнения параметров выборки сущностей из дерева домена;
 - **Список DN для сканирования** – укажите список **Distinguished Name (DN)** для сканирования. DN представляет собой уникальный идентификатор записи (entry) в иерархической структуре каталога и описывает путь к объекту в дереве, где каждый уровень — это отдельный компонент;
 - **Поиск в глубину** – включите переключатель если необходимо выполнять поиск в поддереве, иначе поиск будет выполняться на одном уровне иерархии;
 - **Срок устаревания активов (дни)** – укажите количество дней, по истечении которых будут игнорироваться объекты, последнее изменение параметра lastLogon которых, было позже указанного количества дней. Если указано значение 0, то политика устаревания не применяется.
4. Нажмите кнопку **Проверить**. Будет выполнена проверка подключения к серверу AD контроллера. После успешной проверки соединения с сервером станет доступно сохранение экземпляра интеграции.
 5. Нажмите кнопку **Сохранить**.

16.3.2.2 Шаг 2. Создание задачи по синхронизации активов

1. Откройте интеграцию на редактирование (кнопка .
2. Перейдите на вкладку "Задачи интеграции" (см. «Рис. 310»).

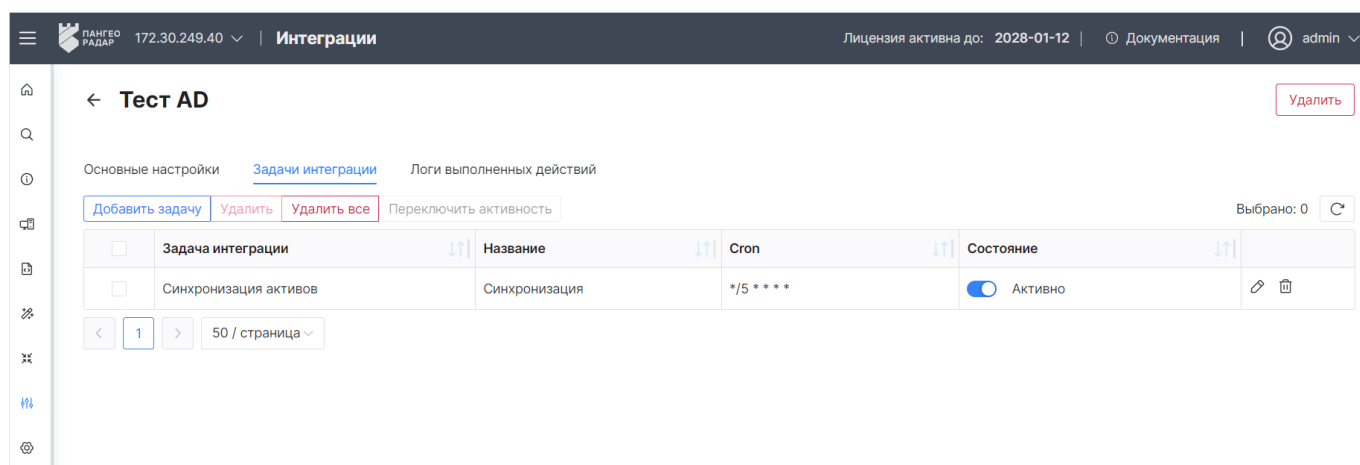
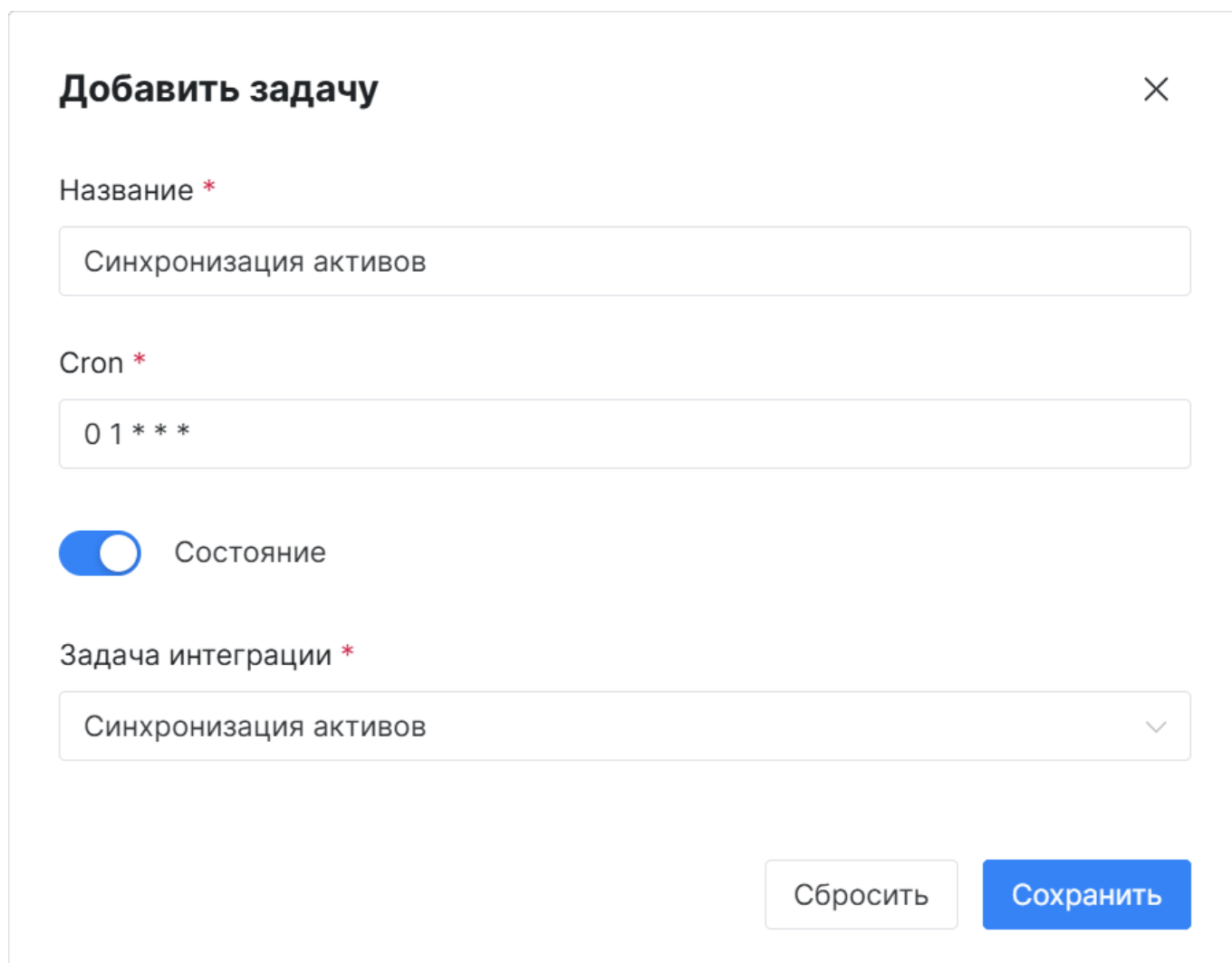


Рис. 310 – Настройка интеграции. Вкладка "Задачи интеграции"

3. Нажмите кнопку **Добавить задачу**. Откроется окно "Добавить задачу" (см. «Рис. 311»).



Добавить задачу ✕

Название *

Синхронизация активов

Cron *

0 1 * * *

☒ Состояние

Задача интеграции *

Синхронизация активов

Сбросить Сохранить

Рис. 311 – 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**.

16.3.2.3 Шаг 3. Активация экземпляра интеграции с AD


Чтобы по экземпляру интеграции выполнялось взаимодействие с системой **AD**, ее необходимо активировать.

Для активации интеграции перейдите в раздел **Параметры** → **Интеграции** и в колонке **Статус** установите переключатель в положение "Включен".

16.3.3 Работа с интеграцией

В ходе работы интеграции будет выполняться сканирование активов в соответствии с параметрами периодической задачи и настройками экземпляра интеграции:

1. Запускается периодическая задача.
2. **Платформа Радар** запрашивает у AD информацию о компьютерах и сетевых устройствах. Запрос выполняется в соответствии с пользовательским фильтром по всем указанным DN для сканирования.
3. Информация об узлах импортируется в активы платформы. Импортируются только те узлы, которые попали под политику устаревания.
4. На форме просмотра актива в таблице **Связи с интеграциями** появляется дополнительная информация:
 - наименование экземпляра интеграции, в рамках которой получены сведения об активе;
 - номер SID сущности из AD, на основании которого создан актив;
 - дата и время последней синхронизации активов с AD;
 - признак устаревания сведений об активе, отображается в случае, если при очередной синхронизации, актив не был найден в AD.

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".