kaspersky

Kaspersky Unified Monitoring and Analysis Platform

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 2.0.0.306

kaspersky

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 13.07.2022

Обозначение документа: 643.46856491.00116-03 90 01

https://www.kaspersky.ru
https://support.kaspersky.ru

О "Лаборатории Касперского" https://www.kaspersky.ru/about/company

kaspersky

Содержание

Об этом документе 13
Источники информации о программе 14
Источники для самостоятельного поиска информации 14
Обсуждение программ "Лаборатории Касперского" на Форуме 15
О программе 16
Что нового 17
Комплект поставки сертифицированной версии 18
Архитектура программы 19
Ядро 20
Коллектор 20
Коррелятор 23
Хранилище 24
Кластеры, шарды и реплики 24
Основные сущности 24
О тенантах 25
О событиях 25
Об алертах 27
Об инцидентах 28
Об активах 28
О ресурсах 28
О сервисах 28
Об агентах 29
Об уровне важности 29
Требования 31
Аппаратные и программные требования 31
Установка и удаление KUMA 34
Указания по эксплуатации и требования к среде 34
Требования к установке программы 35
Установка для демонстрации 36
Подготовка файла инвентаря для демонстрационной установки 37
Демонстрационная установка программы 38
Расширение демонстрационной установки 38
Установка KUMA в производственной среде 39
Настройка сетевого доступа 41
Подготовка контрольной машины 42
Подготовка целевой машины 43
Подготовка файла инвентаря 44
Установка программы 45
Создание сервисов 46

Изменение корневого сертификата ... 46
Удаление KUMA ... 47
Обновление предыдущих версий KUMA ... 47
Вход в веб-интерфейс программы ... 48
Лицензирование программы ... 49
О Лицензионном соглашении ... 49
О лицензии ... 49
О Лицензионном сертификате ... 50
О лицензионном ключе ... 50
О файле ключа ... 51
Добавление лицензионного ключа в веб-интерфейс программы ... 51
Просмотр информации о добавленном лицензионном ключе в веб-интерфейсе программы ... 52
Удаление лицензионного ключа в веб-интерфейсе программы ... 53
Процедура приемки ... 54
Проверка целостности файлов KUMA ... 54
Безопасное состояние ... 55
Проверка правильной установки и работоспособности программы ... 55
Разделение доступа к функциям программы по пользовательским ролям ... 57
Роли пользователей ... 57
Управление пользователями ... 69
Создание пользователя ... 69
Редактирование пользователя ... 70
Редактирование своей учетной записи ... 71
Интеграция с другими решениями ... 73
Интеграция с Kaspersky Security Center ... 73
Настройка параметров интеграции с Kaspersky Security Center ... 74
Добавление тенанта в список тенантов для интеграции с Kaspersky Security Center ... 75
Создание подключения к Kaspersky Security Center ... 75
Изменение подключения к Kaspersky Security Center ... 76
Удаление подключения к Kaspersky Security Center ... 77
Работа с задачами Kaspersky Security Center ... 77
Импорт событий из базы Kaspersky Security Center ... 79
Интеграция с Kaspersky Endpoint Detection and Response ... 80
Интеграция с Kaspersky CyberTrace ... 81
Интеграция поиска по индикаторам CyberTrace ... 81
Интеграция интерфейса CyberTrace ... 84
Интеграция с Kaspersky Threat Intelligence Portal ... 87
Инициализация интеграции ... 87
Запрос данных от Kaspersky Threat Intelligence Portal ... 88
Просмотр данных от Kaspersky Threat Intelligence Portal ... 89

Обновление данных от Kaspersky Threat Intelligence Portal 89
Интеграция с R-Vision Incident Response Platform 90
Настройка интеграции в KUMA....90
Настройка интеграции в R-Vision IRP 92
Работа с алертами с помощью R-Vision IRP 100
Интеграция с Active Directory 102
Подключение по протоколу LDAP 102
Авторизация с помощью доменных учетных записей 110
Интеграция с НКЦКИ 114
Доступные категории и типы инцидентов 116
Сферы деятельности компании 116
Интеграция с Security Vision Incident Response Platform 117
Настройка интеграции в KUMA....119
Настройка интеграции в Security Vision IRP 119
Интеграция с Kaspersky Industrial CyberSecurity for Networks 124
Настройка интеграции в KICS for Networks 125
Настройка интеграции в KUMA....125
Включение и выключение интеграции с KICS for Networks 126
Изменение частоты обновления данных....126
Особенности импорта информации об активах из KICS for Networks 126
Изменение статуса актива KICS for Networks 127
Ресурсы KUMA 128
Операции с ресурсами 129
Создание, переименование, перемещение и удаление папок ресурсов 130
Создание, дублирование, перемещение, редактирование и удаление ресурсов....131
Экспорт и импорт ресурсов....132
Правила корреляции 134
Правила корреляции типа standard....135
Правила корреляции типа simple 139
Правила корреляции типа operational....142
Переменные в коррелляторах....144
Нормализаторы....158
Параметры нормализатора 159
Условие передачи данных в дополнительный нормализатор....164
Предустановленные нормализаторы 165
Преобразования....168
Коннекторы 169
Просмотр параметров коннектора 170
Добавление коннектора 170
Параметры коннекторов....171

Правила агрегации 194
Правила обогащения 194
Обогащение, тип константа 195
Обогащение, тип cybertrace 195
Обогащение, тип словарь 196
Обогащение, тип dns 196
Обогащение, тип событие (для ресурса обогащения) 196
Обогащение, тип событие (для нормализатора) 197
Обогащение, тип шаблон 197
Обогащение, тип часовой пояс 197
Обогащение, тип геоданные 198
Точки назначения 199
Тип nats 200
Тип tcp 201
Тип http 203
Тип diode 204
Тип kafka 206
Тип file 208
Тип storage 209
Тип correlator 210
Фильтры 212
Операнды фильтров 214
Операторы фильтров 215
Поиск по данным поля события Extra 215
Создание фильтра в ресурсах 216
Правила реагирования 217
Правила реагирования для Kaspersky Security Center 217
Правила реагирования для пользовательского скрипта 218
Правила реагирования для KICS for Networks 219
Шаблоны уведомлений 220
Активные листы 224
Словари 225
Прокси-серверы 226
Секреты 226
Сервисы KUMA 229
Инструменты сервисов 231
Получение идентификатора сервиса 231
Перезапуск сервиса 231
Удаление сервиса 232
Окно Разделы 232

Окно активных листов коррелятора ... 233
Поиск связанных событий ... 234
Наборы ресурсов для сервисов ... 235
Создание коллектора ... 235
Запуск мастера установки коллектора ... 236
Установка коллектора в сетевой инфраструктуре KUMA ... 250
Проверка правильности установки коллектора ... 251
Создание коррелятора ... 252
Запуск мастера установки коррелятора ... 253
Установка коррелятора в сетевой инфраструктуре KUMA ... 262
Проверка правильности установки коррелятора ... 263
Создание агента ... 263
Создание набора ресурсов для агента ... 264
Создание сервиса агента в веб-интерфейсе KUMA ... 266
Установка агента в сетевой инфраструктуре KUMA ... 266
Автоматически созданные агенты ... 269
Обновление агентов ... 269
Создание хранилища ... 270
Создание набора ресурсов для хранилища ... 270
Создание сервиса хранилища в веб-интерфейсе KUMA ... 271
Установка хранилища в сетевой инфраструктуре KUMA ... 272
Аналитика ... 273
Панель мониторинга ... 273
Создание макета панели мониторинга ... 274
Выбор макета панели мониторинга ... 275
Выбор макета панели мониторинга в качестве макета по умолчанию ... 275
Редактирование макета панели мониторинга ... 276
Удаление макета панели мониторинга ... 276
Преднастроенные виджеты ... 276
Включение и отключение режима ТВ ... 278
Отчеты ... 278
Шаблон отчета ... 279
Сформированные отчеты ... 283
Состояние источников ... 285
Список источников событий ... 286
Политики мониторинга ... 287
Виджеты ... 288
Стандартные виджеты ... 291
Настраиваемая аналитика по событиям ... 293
Настраиваемая аналитика по активным листам ... 297

Добавление виджета ... 300
Редактирование виджетов ... 300
Работа с тенантами ... 301
Выбор тенанта ... 302
Правила принадлежности к тенантам ... 302
Кросс-тенанты - сценарий 2 ... 303
Кросс-тенанты - сценарий 3 ... 304
Кросс-тенанты - сценарий 4 ... 305
Кросс-тенанты - сценарий 5 ... 306
Работа с инцидентами ... 307
О таблице инцидентов ... 307
Параметры отображения для таблицы инцидентов ... 309
Сохранение и выбор конфигураций фильтра инцидентов ... 309
Удаление конфигураций фильтра инцидентов ... 310
Просмотр информации об инциденте ... 310
Создание инцидента ... 312
Привязка активов к инцидентам ... 313
Привязка алертов к инцидентам ... 313
Привязка пользователей к инцидентам ... 314
Обработка инцидентов ... 314
Изменение инцидентов ... 315
Автоматическая привязка алертов к инцидентам ... 315
Категории и типы инцидентов ... 316
Экспорт инцидентов в НКЦКИ ... 317
Работа в режиме иерархии ... 320
Первое включение режима иерархии ... 321
Создание сертификата узла ... 321
Соединение узлов в иерархическую структуру ... 322
Подключение к родительскому узлу ... 323
Подключение дочернего узла ... 323
Отключение от узла ... 324
Изменение узла ... 324
Ошибки при подключении узлов ... 325
Просмотр своей ветви иерархии и доступных узлов ... 327
Изменение профиля узла ... 327
Просмотр инцидентов от узлов-потомков ... 328
Включение и выключение режима иерархии ... 329
Работа с алертами ... 330
Фильтрация алертов ... 330
Настройка таблицы алертов ... 331

Сохранение и выбор конфигураций фильтра алертов ... 332
Удаление конфигураций фильтра алертов ... 332
Просмотр информации об алерте ... 333
Обработка алертов ... 335
Детализированный анализ ... 336
Срок хранения алертов ... 337
Правила сегментации алертов ... 338
Уведомления об алертах ... 339
Работа с событиями ... 341
Фильтрация и поиск событий ... 341
Формирование SQL-запроса с помощью конструктора ... 343
Создание SQL-запроса вручную ... 345
Ограничение сложности запросов в режиме детализированного анализа ... 348
Фильтрация событий по периоду ... 349
Сохранение и выбор конфигураций фильтра событий ... 350
Удаление конфигураций фильтра событий ... 350
Поддерживаемые функции ClickHouse ... 351
Изменение параметров фильтра в окне статистики ... 352
Изменение фильтра в области деталей события ... 352
Изменение фильтра в таблице событий ... 352
Просмотр информации о событии ... 353
Экспорт событий ... 353
Выбор хранилища ... 354
Получение статистики по событиям в таблице ... 355
Настройка таблицы событий ... 355
Обновление таблицы событий ... 356
Открытие окна корреляционного события ... 357
Ретроспективная проверка ... 359
Работа с геоданными ... 361
Формат геоданных ... 361
Конвертация геоданных из MaxMind и IP2Location ... 362
Импорт и экспорт геоданных ... 363
Сопоставление геоданных по умолчанию ... 365
Передача в KUMA событий из изолированных сегментов сети ... 366
Конфигурационный файл diode-агента ... 368
Описание полей секретов ... 373
Установка Linux-агента в изолированном сегменте сети ... 374
Установка Windows-агента в изолированном сегменте сети ... 374
Управление активами ... 376
Категории активов ... 376

Добавление категории активов 377
Настройка таблицы активов 378
Поиск активов 379
Просмотр информации об активе 379
Добавление активов 381
Добавление информации об активах в веб-интерфейсе KUMA 383
Импорт информации об активах из Kaspersky Security Center 384
Импорт информации об активах из MaxPatrol 385
Импорт информации об активах из KICS for Networks 390
Назначение активу категории 390
Активная категория активов 391
Операнды и операторы фильтра категоризации 392
Изменение параметров активов 392
Раздел Информация об оборудовании 393
Удаление активов 394
Обновление программ сторонних производителей и закрытие уязвимостей на активах Kaspersky Security Center 394
Перемещение активов в выбранную группу администрирования 396
Аудит активов 397
Настройка аудита активов 398
Хранение и поиск событий аудита активов 399
Включение и выключение аудита активов 399
Управление KUMA 401
Просмотр метрик KUMA 401
Работа с задачами KUMA 405
Просмотр таблицы задач 405
Настройка отображения таблицы задач 406
Просмотр результата выполнения задачи 406
Повторный запуск задачи 407
Подключение к SMTP-серверу 407
Онлайн-справка KUMA 408
Журналы KUMA 408
Резервное копирование KUMA 409
Сбои в работе KUMA после восстановления из резервной копии 410
Уведомления KUMA 410
Обращение в службу технической поддержки 412
REST API 413
Создание токена 414
Настройка прав доступа к API 414
Авторизация API-запросов 415
Стандартная ошибка 415

Операции ... 416
Просмотр списка активных листов на коррелляторе ... 417
Импорт записей в активный лист ... 419
Поиск алертов ... 422
Закрытие алертов ... 428
Поиск активов ... 429
Импорт активов ... 433
Удаление активов ... 437
Поиск событий ... 439
Просмотр информации о кластере ... 442
Поиск ресурсов ... 444
Загрузка файла с ресурсами ... 446
Просмотр содержимого файла с ресурсами ... 447
Импорт ресурсов ... 448
Экспорт ресурсов ... 450
Скачивание файла с ресурсами ... 451
Поиск сервисов ... 452
Поиск тенантов ... 455
Просмотр информации о предъявителе токена ... 457
Обновление словаря в сервисах ... 458
Получение словаря ... 461
Команды для запуска и установки компонентов вручную ... 462
Устранение уязвимостей и установка критических обновлений в программе ... 463
Действия после сбоя или неустранимой ошибки в работе программы ... 464
Способы получения технической поддержки ... 465
Техническая поддержка через Kaspersky CompanyAccount ... 465
АО "Лаборатория Касперского" ... 467
Информация о стороннем коде ... 469
Уведомления о товарных знаках ... 470
Приложения ... 471
Модель данных нормализованного события ... 471
Модель данных алерта ... 488
Модель данных актива ... 491
Модель данных учетной записи ... 499
Поля событий аудита ... 502
Поля событий с общей информацией ... 503
Пользователь успешно вошел в систему или не смог войти ... 504
Логин пользователя успешно изменен ... 505
Роль пользователя успешно изменена ... 506
Другие данные пользователя успешно изменены ... 507

Пользователь успешно вышел из системы 508
Пароль пользователя успешно изменен 509
Пользователь успешно создан 510
Токен доступа пользователя успешно изменен 511
Сервис успешно создан 512
Сервис успешно удален 513
Сервис успешно перезагружен 514
Сервис успешно перезапущен 515
Сервис успешно запущен 516
Сервис успешно сопряжен 517
Статус сервиса изменен 517
Индекс хранилища удален пользователем 518
Раздел хранилища автоматически удален в связи с истечением срока действия 518
Активный лист успешно очищен или операция завершилась с ошибкой 519
Элемент активного листа успешно удален или операция завершилась с ошибкой 520
Активный лист успешно импортирован или операция завершилась с ошибкой 521
Активный лист успешно экспортирован 522
Ресурс успешно добавлен 523
Ресурс успешно удален 524
Ресурс успешно обновлен 525
Актив успешно создан 526
Актив успешно удален 527
Категория актива успешно добавлена 528
Категория актива успешно удалена 528
Параметры успешно обновлены 529
Соответствие терминов 530
Приложение. Значения параметров программы в сертифицированной конфигурации 531
Параметры подключения к SMTP-серверу 531
Чекбокс Выключено 531

kaspersky

Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного обеспечения "Kaspersky Unified Monitoring and Analysis Platform" (далее также "KUMA", "программа").

Подготовительные процедуры изложены в разделах "Установка и удаление KUMA (на стр. 34)" и "Процедура приемки (на стр. 54)" и содержат процедуры безопасной установки и первоначальной настройки программы, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования (на стр. 31)" приведены минимально необходимые системные требования для безопасной установки программы.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование программы, а также инструкции и указания по безопасному использованию программы.

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование KUMA, а также поддержка организаций, использующих KUMA.

kaspersky

Источники информации о программе

Указанные источники информации о программе (в частности, электронная справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

В этом разделе

Источники для самостоятельного поиска информации 14

Обсуждение программ "Лаборатории Касперского" на Форуме 15

Источники для самостоятельного поиска информации

Вы можете использовать следующие источники для самостоятельного поиска информации о KUMA:

- страница KUMA на веб-сайте "Лаборатории Касперского";
- страница KUMA на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, обратитесь в Службу технической поддержки "Лаборатории Касперского".

Для использования источников информации на веб-сайтах требуется подключение к интернету.

Страница KUMA на веб-сайте "Лаборатории Касперского"

На странице KUMA (https://www.kaspersky.ru/enterprise-security/unified-monitoring-and-analysis-platform) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница KUMA содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Страница KUMA в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице KUMA в Базе знаний (https://support.kaspersky.ru/business) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к KUMA, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка

Программа содержит файлы полной и контекстной справки.

В полной справке вы можете найти информацию о настройке и использовании KUMA.

В контекстной справке вы можете найти информацию об окнах KUMA: описание параметров KUMA и ссылки на описания задач, в которых используются эти параметры.

Справка может быть включена в состав программы либо располагаться онлайн на веб-ресурсе "Лаборатории Касперского". Если справка расположена онлайн, то при ее вызове будет открыто окно браузера. Для отображения онлайн-справки требуется соединение с интернетом.

Обсуждение программ "Лаборатории Касперского" на Форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме (https://forum.kaspersky.com/forum/%D1%80%D1%83%D1%81%D1%81%D0%BA%D0%BE%D1%8F%D0%B7%D1%8B%D1%87%D0%BD%D1%8B%D0%B9-%D1%84%D0%BE%D1%80%D1%83%D0%BC-162/).

На Форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

kaspersky

О программе

Kaspersky Unified Monitoring and Analysis Platform (далее KUMA или "программа") – это комплексное программное решение, сочетающее в себе следующие функциональные возможности:

- получение, обработка и хранение событий информационной безопасности;
- анализ и корреляция поступающих данных;
- поиск по полученным событиям;
- создание уведомлений о выявлении признаков угроз информационной безопасности.

Программа построена на микросервисной архитектуре. Это означает, что вы можете создавать и настраивать только необходимые микросервисы (далее также "сервисы"), что позволяет использовать KUMA и как систему управления журналами, и как полноценную SIEM-систему. Кроме того, благодаря гибкой маршрутизации потоков данных вы можете использовать сторонние сервисы для дополнительной обработки событий.

Основными угрозами, для противостояния которым используется KUMA, являются:

- угрозы, связанные с пропуском событий ИБ (в отношении информационной системы, в которой функционирует ОО);
- угрозы, связанные с невозможностью выявления связанных событий ИБ (в отношении информационной системы, в которой функционирует ОО);
- угрозы, связанные с несвоевременным реагированием на инциденты ИБ (в отношении информационной системы, в которой функционирует ОО);
- угрозы, связанные с нарушением целостности информации, передаваемой от источников событий ИБ (в отношении информационной системы, в которой функционирует ОО).

В программе реализованы следующие функции безопасности:

- идентификация и аутентификация пользователей;
- управление средствами аутентификации;
- управление учетными записями пользователей;
- управление доступом к функциональным возможностям по управлению (администрированию) ОО (параметры настройки) на основе ролевого метода управления доступом;
- идентификация компонентов ИС;
- обеспечение доверенного канала между компонентами ОО;
- регистрация событий ИБ, связанных с администрированием, контролем защищенности и функционирования SIEM-системы;
- мониторинг (просмотр, анализ) результатов регистрации событий ИБ;
- сбор данных SIEM-системой;
- анализ данных SIEM-системой;
- реагирование при выявлении инцидентов ИБ в ИС;
- поддержка правил выявления инцидентов ИБ;
- передача информации о выявленных инцидентах ИБ.

kaspersky

В этом разделе

Что нового.....17

Комплект поставки сертифицированной версии.....18

Что нового

- Реализована глубокая интеграция с Kaspersky Endpoint Detection and Response Expert (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response" на стр. 80) (KEDR Expert). Интеграция доступна только с лицензией Symphony XDR.
- Добавлена интеграция с Kaspersky Industrial CyberSecurity for Networks (на стр. 124) в сценариях инвентаризации активов и реагирования.
- Расширена интеграция с Kaspersky Security Center (на стр. 73).
- Расширены возможности SQL-поиска (см. раздел "Поддерживаемые функции ClickHouse" на стр. 351) по событиям в хранилище.
- Расширены возможности компонентов сбора событий (коллекторов):
  - Добавлено обогащение информацией о регионе по IP-адресу (см. раздел "Работа с геоданными" на стр. 361) (GeoIP).
  - Добавлена возможность обогащения из словарей (таблиц) (см. раздел "Словари" на стр. 225), наполняемых вручную в веб-интерфейсе или по API.
  - Добавлена возможность корректировать время с учетом часового пояса (см. раздел "Правила обогащения" на стр. 194) источника событий.
- Добавлены вычисляемые переменные (см. раздел "Переменные в корреляторах" на стр. 144) для покрытия сложных сценариев детектирования угроз при корреляции событий.
- Добавлена возможность сбора событий из изолированного сегмента с дата-диодом (см. раздел "Передача в KUMA событий из изолированных сегментов сети" на стр. 366) при отсутствии возможности передачи сетевых UDP-пакетов.
- Добавлена возможность настройки пользовательских шаблонов (см. раздел "Шаблоны уведомлений" на стр. 220) и правил уведомления (см. раздел "Уведомления об алертах" на стр. 339) об алертах.
- Расширены инструменты аналитики (см. раздел "Аналитика" на стр. 273), добавлены новые виджеты (см. раздел "Настраиваемая аналитика по активным листам" на стр. 297).
- Добавлена функция аудита активов (см. раздел "Аудит активов" на стр. 397).
- Добавлена (см. раздел "Предустановленные нормализаторы" на стр. 165) поддержка телеметрии о трафике sFlow для поддержки оборудования Juniper. Аналогично Netflow данные события можно собирать без ограничений при использовании лицензии с активным модулем Netflow.

Комплект поставки сертифицированной версии

В комплект поставки входят следующие файлы:

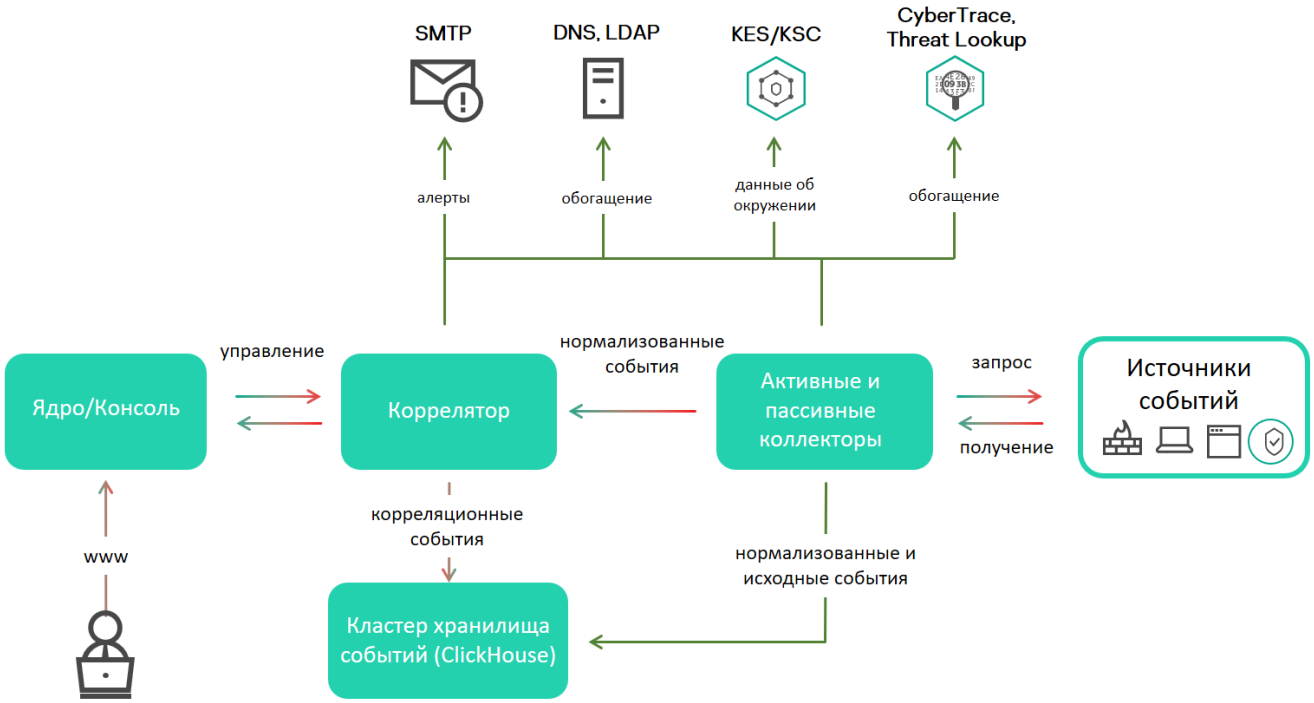
- kuma-ansible-installer-<номер сборки>.tar.gz для установки компонентов KUMA;
- файлы с информацией о версии (примечания к выпуску) на русском и английском языках.

Архитектура программы

Стандартная установка программы включает следующие компоненты:

- Один или несколько *коллекторов* (см. раздел "*Коллектор*" на стр. 20), которые получают сообщения из источников событий и осуществляют их парсинг, нормализацию и, если требуется, фильтрацию и/или агрегацию.
- *Коррелятор* (на стр. 23), который анализирует полученные из коллекторов нормализованные события, выполняет необходимые действия с активными листами и создает алерты в соответствии с правилами корреляции.
- *Ядро* (на стр. 20), включающее графический интерфейс для мониторинга и управления настройками компонентов системы.
- *Хранилище* (на стр. 24), в котором содержатся нормализованные события и зарегистрированные алерты.

События передаются между компонентами по надежным транспортным протоколам (при желании с шифрованием). Вы можете настроить балансировку нагрузки для ее распределения между экземплярами сервисов, а также включить автоматическое переключение на резервный компонент в случае недоступности основного. Если недоступны все компоненты, события сохраняются в буфере жесткого диска и передаются позже. Размер буферного диска для временного хранения событий можно менять.



kaspersky

В этом разделе

Ядро 20
Коллектор 20
Коррелятор 23
Хранилище 24
Основные сущности 24

Ядро

Ядро – это центральный компонент KUMA, на основе которого строятся все прочие сервисы (см. раздел "О сервисах" на стр. 28) и компоненты (см. раздел "О ресурсах" на стр. 28). Предоставляемый Ядром графический пользовательский интерфейс веб-интерфейса предназначен как для повседневного использования операторами и аналитиками, так и для настройки системы в целом.

Ядро позволяет выполнять следующие задачи:

- создавать и настраивать сервисы (или компоненты) программы, а также интегрировать в систему необходимое программное обеспечение;
- централизованно управлять сервисами и учетными записями пользователей программы;
- визуально представлять статистические данные о работе программы;
- расследовать угрозы безопасности на основе полученных событий.

Коллектор

Коллектор – это компонент программы (см. раздел "О сервисах" на стр. 28), который получает сообщения из источников событий (см. раздел "О событиях" на стр. 25), обрабатывает их и передает в хранилище (на стр. 24), коррелятор (на стр. 23) и/или сторонние сервисы для выявления алертов (см. раздел "Об алертах" на стр. 27).

Для каждого коллектора нужно настроить один коннектор (см. раздел "Коннекторы" на стр. 169) и один нормализатор (см. раздел "Нормализаторы" на стр. 158). Вы также можете настроить любое количество дополнительных нормализаторов, фильтров (см. раздел "Фильтры" на стр. 212), правил обогащения (см. раздел "Правила обогащения" на стр. 194) и правил агрегации (см. раздел "Правила агрегации" на стр. 194). Для того чтобы коллектор мог отправлять нормализованные события в другие сервисы, необходимо добавить точки назначения. Как правило, используются две точки назначения: хранилище и коррелятор.

Алгоритм работы коллектора состоит из следующих этапов:

a. **Получение сообщений из источников событий**

   Для получения сообщений требуется настроить активный или пассивный коннектор (см. раздел "Коннекторы" на стр. 169). Пассивный коннектор только ожидает события от указанного источника, а активный – инициирует подключение к источнику событий, например к системе управления базами данных.

Коннекторы различаются по типу. Выбор типа коннектора зависит от транспортного протокола для передачи сообщений. Например, для источника событий, передающего сообщения по протоколу TCP, необходимо установить коннектор типа TCP.

В программе доступны следующие типы коннекторов:

- internal;
- tcp;
- udp;
- netflow;
- sflow;
- nats;
- kafka;
- http;
- sql;
- file;
- diode;
- ftp;
- nfs;
- wmi;
- wec;
- snmp.

b. Парсинг и нормализация событий

События, полученные коннектором, обрабатываются с помощью парсера и правил нормализации (см. раздел "Нормализаторы" на стр. 158), заданных пользователем. Выбор нормализатора зависит от формата сообщений, получаемых из источника события. Например, для источника, отправляющего события в формате CEF, необходимо выбрать нормализатор типа CEF.

В программе доступны следующие нормализаторы:

- JSON.
- CEF.
- Regexp.
- Syslog (как для RFC3164 и RFC5424).
- CSV.
- Ключ-значение.
- XML.
- NetFlow v5.
- NetFlow v9.
- IPFIX (v10).

c. Фильтрация нормализованных событий

Вы можете настроить фильтры (на стр. 212), которые позволяют отбирать для дальнейшей обработки только события, удовлетворяющие заданным условиям. События, не удовлетворяющие условиям фильтрации, на этом этапе отсеиваются и далее не обрабатываются.

d. Обогащение и преобразование нормализованных событий

Правила обогащения (на стр. 194) позволяют дополнить содержащуюся в событии информацию данными из внутренних и внешних источников. В программе представлены следующие источники обогащения:

- константы;
- cybertrace;
- словари;
- dns;
- события;
- ldap;
- шаблоны;
- данные о часовых поясах;
- геоданные.

Правила преобразования позволяют преобразовать содержимое события в соответствии с заданными условиями. В программе представлены следующие методы преобразования:

- lower – перевод всех символов в нижний регистр;
- upper – перевод всех символов в верхний регистр;
- regexp – извлечение подстроки с использованием регулярных выражений RE2;
- substring – выбор текстовых строк по заданным номерам позиции;
- replace – замена текста введенной строкой;
- trim – удаление заданных символов;
- append – добавление символов в конец значения поля;
- prepend – добавление символов в начало значения поля.

e. Агрегация нормализованных событий

Вы можете настроить правила агрегации (на стр. 194), чтобы уменьшить количество схожих сообщений, передаваемых в хранилище и/или коррелятор. Например, можно агрегировать в одно событие все сообщения о сетевых подключениях, выполненных по одному и тому же протоколу (транспортного и прикладного уровней) между двумя IP-адресами и полученных в течение заданного интервала времени. Если настроены правила агрегации, несколько сообщений могут обрабатываться и сохраняться как одно событие. Это помогает снизить нагрузку на сервисы, которые отвечают за дальнейшую обработку событий, экономит место для хранения и экономит частоту обработки событий (EPS).

f. Передача нормализованных событий

По завершении всех этапов обработки событие отправляется в настроенные точки назначения (на стр. 199).

kaspersky

Коррелятор

Коррелятор – это компонент программы, который анализирует нормализованные события (см. раздел "О событиях" на стр. 25). В процессе корреляции может использоваться информация из активных листов (см. раздел "Активные листы" на стр. 224) и/или словарей (см. раздел "Словари" на стр. 225).

Полученные в ходе анализа данные применяются для выполнения следующих задач:

- выявление алертов (см. раздел "Об алертах" на стр. 27);
- уведомление (см. раздел "Правила реагирования" на стр. 217) о выявленных алертах;
- управление содержимым активных листов;
- отправка корреляционных событий в настроенные точки назначения (на стр. 199).

Корреляция событий выполняется в реальном времени. Принцип работы коррелятора основан на сигнатурном анализе событий. Это значит, что каждое событие обрабатывается в соответствии с правилами корреляции (см. раздел "Правила корреляции" на стр. 134), заданными пользователем. При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, программа создает корреляционное событие и отправляет его в Хранилище (на стр. 24). Корреляционное событие можно также отправлять на повторный анализ в коррелятор, позволяя таким образом настраивать правила корреляции на срабатывание от предыдущих результатов анализа. Результаты одного корреляционного правила могут использоваться другими корреляционными правилами.

Вы можете распределять правила корреляции и используемые ими активные листы между корреляторами, разделяя таким образом нагрузку между сервисами. В этом случае коллекторы будут отправлять нормализованные события во все доступные корреляторы.

Алгоритм работы Коррелятора состоит из следующих этапов:

a. **Получение события**

   Коррелятор получает нормализованное событие (см. раздел "О событиях" на стр. 25) из коллектора или другого сервиса.

b. **Применение правил корреляции**

   Правила корреляции (на стр. 134) можно настроить на срабатывание на основе одного события или последовательности событий. Если по правилам корреляции не был выявлен алерт (см. раздел "Об алертах" на стр. 27), обработка события завершается.

c. **Реагирование на алерт**

   Вы можете задать действия, которые программа будет выполнять при выявлении алерта. В программе доступны следующие действия:

   - обогащение события;
   - операции с активными листами;
   - отправка уведомлений;
   - сохранение корреляционного события.

d. **Отправка корреляционного события**

   При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, программа создает корреляционное событие и отправляет его в хранилище. На этом обработка события коррелятором завершается.

kaspersky

Хранилище

Хранилище KUMA используется для хранения нормализованных событий (см. раздел "О событиях" на стр. 25) таким образом, чтобы к ним обеспечивался быстрый и бесперебойный доступ из KUMA с целью извлечения аналитических данных. Скорость и бесперебойность доступа обеспечивается за счет использования технологии ClickHouse. Таким образом *хранилище* – это кластер ClickHouse, связанный с сервисом (см. раздел "Сервисы KUMA" на стр. 229) хранилища KUMA.

Компоненты хранилища: кластеры, шарды, реплики, киперы (см. раздел "Кластеры, шарды и реплики" на стр. 24)

При выборе конфигурации кластера ClickHouse учитывайте требования вашей организации к хранению событий. Дополнительные сведения см. в документации ClickHouse https://clickhouse.tech/docs/ru.

В хранилищах можно создавать *пространства*. Пространства позволяют организовать в кластере структуру данных и, например, хранить события определенного типа вместе.

Кластеры, шарды и реплики

Кластер (cluster) – логическая группа машин, обладающих всеми накопленными нормализованными событиями KUMA. Подразумевает наличие одного или нескольких логических *шардов*.

Шард (shard) – логическая группа машин, обладающих некоторой **частью** всех накопленных в кластере нормализованных событий. Подразумевает наличие одной или нескольких *реплик*. Увеличение количества шардов позволяет:

- Накапливать больше событий за счет увеличения общего количества серверов и дискового пространства.
- Поглощать больший **поток** событий за счет распределения нагрузки, связанной со вставкой новых событий.
- Уменьшить время поиска событий за счет распределения поисковых зон между несколькими машинами.

Реплика (replica) – машина, являющаяся членом логического шарда и обладающая одной копией данных этого шарда. Если реплик несколько – копий тоже несколько (данные реплицируются). Увеличение количества реплик позволяет:

- Улучшить отказоустойчивость.
- Распределить общую нагрузку, связанную с поиском данных, между несколькими машинами (однако для этой цели лучше увеличить количество шардов).

Кипер (keeper) – опциональная роль реплики, подразумевающая ее участие в **координации** репликации данных на уровне **всего** кластера. На весь кластер требуется хотя бы одна реплика с этой ролью. Рекомендуемое количество таких реплик – 3. Число реплик, участвующих в координации репликации, должно быть **нечетным**.

Основные сущности

В этом разделе описаны основные сущности, с которыми работает KUMA.

kaspersky

В этом разделе

О тенантах 25
О событиях 25
Об алертах 27
Об инцидентах 28
Об активах 28
О ресурсах 28
О сервисах 28
Об агентах 29
Об уровне важности 29

О тенантах

В KUMA действует режим мультитенантности, при котором один экземпляр программы KUMA, установленный в инфраструктуре основной организации (далее "главный тенант"), позволяет ее изолированным филиалам (далее "тенантам") получать и обрабатывать свои события.

Управление системой происходит централизовано через общий веб-интерфейс, при этом тенанты работают независимо друг от друга и имеют доступ только к своим ресурсам (см. раздел "Ресурсы KUMA" на стр. 128), сервисам (см. раздел "Сервисы KUMA" на стр. 229) и настройкам. События тенантов хранятся (см. раздел "Хранилище" на стр. 24) раздельно.

Пользователи могут иметь доступ сразу к нескольким тенантам. При этом можно выбирать (см. раздел "Выбор тенанта" на стр. 302), данные каких тенантов будут отображаться в разделах веб-интерфейса KUMA.

По умолчанию в KUMA созданы два тенанта:

- Главный (или Main) – в нем содержатся ресурсы и сервисы, относящиеся к главному тенанту. Эти ресурсы доступны только главному администратору (см. раздел "Роли пользователей" на стр. 57).
- Общий – в этот тенант главный администратор может поместить ресурсы, категории активов и политики мониторинга, которые смогут задействовать пользователи всех тенантов.

О событиях

События – это случаи активности сетевых устройств и служб, связанных с безопасностью, которые можно обнаружить и записать. Например, события включают попытки входа в систему, взаимодействия с базой данных и рассылку информации с датчиков. Каждое отдельное событие может показаться бессмысленным, но если рассматривать их вместе, они формируют более широкую картину сетевой активности, помогающую идентифицировать угрозы безопасности. Это основная функциональность KUMA.

KUMA получает события из журналов и реструктурирует их, приводя данные из разнородных источников к единому формату (этот процесс называется нормализацией). После этого события фильтруются, агрегируются и отправляются в сервис коррелятора для анализа и в сервис хранилища для хранения. Когда KUMA распознает заданное событие или последовательность событий, создаются *корреляционные*

события, которые также анализируются и сохраняются. Если событие или последовательность событий указывают на возможную угрозу безопасности, KUMA создает алерт: это оповещение об угрозе, к которому привязываются все относящиеся к нему данные и которое требует внимания специалиста по безопасности.

На протяжении своего жизненного цикла события претерпевают изменения и могут называться по-разному. Так выглядит жизненный цикла типичного события:

Первые шаги выполняются в коллекторе (см. раздел "Коллектор" на стр. 20).

1. "Сырое" событие. Исходное сообщение, полученное KUMA от источника событий с помощью коннектора (см. раздел "Коннекторы" на стр. 169), называется *"сырым" событием*. Это необработанное сообщение, и KUMA пока не может использовать его. Чтобы с таким событием можно было работать, его требуется нормализовать (см. раздел "Нормализаторы" на стр. 158), то есть привести к модели данных KUMA. Это происходит на следующем этапе.
2. Нормализованное событие. Нормализатор – это набор парсеров, которые преобразуют данные "сырого" события так, чтобы они соответствовали модели данных KUMA (см. раздел "Модель данных нормализованного события" на стр. 471). После этой трансформации исходное сообщение становится *нормализованным событием* и может быть проанализировано в KUMA. С этого момента KUMA работает только с нормализованными событиями. Необработанные, "сырые" события больше не используются, но их можно сохранить как часть нормализованных событий внутри поля `Raw`.

   В программе представлены следующие нормализаторы:

   - JSON
   - CEF
   - Regexp
   - Syslog (как для RFC3164 и RFC5424)
   - CSV/TSV
   - Ключ-значение
   - XML
   - Netflow v5, v9, IPFIX (v10), sFlow v5
   - SQL

   По завершении этого этапа нормализованные события можно использовать для анализа.
3. Точка назначения (см. раздел "Точки назначения" на стр. 199). После обработки события коллектором, оно готово к пересылке в другие сервисы KUMA: в коррелятор (на стр. 23) и/или хранилище (на стр. 24) KUMA.

Следующие этапы жизненного цикла события проходят в корреляторе (см. раздел "Коррелятор" на стр. 23).

Типы событий:

1. Базовое событие. Событие, которое было нормализовано.
2. Агрегированное событие. Чтобы не тратить время и ресурсы на обработку большого количества однотипных сообщений, похожие события можно объединять в одно событие. Такие события ведут себя и обрабатываются так же, как и базовые события, но в дополнение ко всем параметрам родительских событий (событий, которые были объединены) агрегированные события имеют счетчик, показывающий количество родительских событий, которые они представляют. Агрегированные события также хранят время, когда были получены первое и последнее родительские события.

3. Корреляционные события. При обнаружении последовательности событий, удовлетворяющих условиям правила корреляции, программа создает *корреляционное событие*. Эти события можно фильтровать, обогащать и агрегировать. Их также можно отправить на хранение или в коррелятор на анализ.
4. Событие аудита. События аудита создаются при выполнении в KUMA определенных действий (см. раздел "Поля событий аудита" на стр. 502), связанных с безопасностью, и используются для обеспечения целостности системы. Они хранятся не менее 365 дней.
5. Событие мониторинга. Такие события используются для отслеживания изменений в количестве данных, поступающих в KUMA.

Об алертах

В KUMA *алерты* создаются при получении последовательности событий (см. раздел "О событиях" на стр. 25), запускающей правило корреляции (см. раздел "Правила корреляции" на стр. 134). Аналитики KUMA создают правила корреляции для проверки входящих событий на предмет возможных угроз безопасности, поэтому при срабатывании правила корреляции появляется предупреждение о возможной вредоносной активности. Сотрудники службы безопасности, ответственные за защиту данных, должны изучить эти алерты и при необходимости отреагировать на них.

KUMA автоматически присваивает уровень важности (см. раздел "Об уровне важности" на стр. 29) каждому алерту. Этот параметр показывает, насколько важны или многочисленны процессы, запустившие правило корреляции. В первую очередь следует обрабатывать алерты с более высоким уровнем важности. Значение уровня важности автоматически обновляется при получении новых событий корреляции, но сотрудник службы безопасности также может задать его вручную. В этом случае уровень важности алерта больше не обновляется автоматически.

К алертам привязаны относящиеся к ним события, благодаря чему происходит обогащение алертов данными из событий. В KUMA также можно детально анализировать алерты (см. раздел "Детализированный анализ" на стр. 336).

На основании алертов можно создать инциденты (см. раздел "Об инцидентах" на стр. 28).

Ниже представлен жизненный цикл алерта:

1. KUMA создает алерт при срабатывании правила корреляции. Алерт обновляется, если правило корреляции срабатывает снова. Алерту присваивается статус **Новый**.
2. Сотрудник службы безопасности назначает оператора для расследования алерта. Статус алерта меняется на **Назначен**.
3. Оператор выполняет одно из следующих действий:
   - Закрывает алерт как ложно положительный (статус алерта меняется на **Закрыт**).
   - Реагирует на угрозу и закрывает алерт (статус алерта меняется на **Закрыт**).

   После этого алерт больше не обновляется новыми событиями, и, если правило корреляции срабатывает снова, создается новый алерт.

Работа с алертами в KUMA описана в этом разделе (см. раздел "Работа с алертами" на стр. 330).

kaspersky

Об инцидентах

Если характер поступающих в KUMA данных, создаваемых корреляционных событий (см. раздел "О событиях" на стр. 25) и алертов (см. раздел "Об алертах" на стр. 27) указывает на возможную атаку или уязвимость, признаки такого происшествия можно объединить в *инцидент*. Это позволяет специалистам службы безопасности анализировать проявления угрозы комплексно и облегчает реагирование.

Инцидентам (см. раздел "Работа с инцидентами" на стр. 307) можно присваивать категории, типы и уровни важности, а также назначать их сотрудникам, ответственным за защиту данных, для обработки.

Инциденты можно экспортировать в НКЦКИ (см. раздел "Экспорт инцидентов в НКЦКИ" на стр. 317).

Об активах

Активы – это сетевые устройства, зарегистрированные в KUMA. Активы генерируют сетевой трафик при отправке и получении данных. Программа KUMA может быть настроена для отслеживания этой активности и создания базовых событий (см. раздел "О событиях" на стр. 25) с четким указанием того, откуда исходит трафик и куда он направляется. В событии могут быть записаны исходные и целевые IP-адреса, а также DNS-имена. Если вы регистрируете актив с определенными параметрами (например, конкретным IP-адресом), формируется связь между этим активом и всеми событиями, в которых указаны эти параметры (в нашем случае IP-адрес).

Активы можно разделить на логические группы. Это позволяет создать прозрачную структуру вашей сети, а также дает дополнительные возможности при работе с правилами корреляции (см. раздел "Правила корреляции" на стр. 134). Когда обрабатывается событие, к которому привязан актив, категория этого актива также принимается во внимание. Например, если вы присвоите высокий уровень важности (см. раздел "Об уровне важности" на стр. 29) определенной категории активов, то связанные с этими активами базовые события породят корреляционные события с более высоким уровнем важности. Это, в свою очередь, приведет к появлению алертов (см. раздел "Об алертах" на стр. 27) с более высоким уровнем важности и, следовательно, более быстрой реакцией на такой алерт.

Рекомендуется регистрировать сетевые активы в KUMA, поскольку их использование позволяет формулировать четкие и универсальные правила корреляции для более эффективного анализа событий.

Работа с активами в KUMA описана в этом разделе (см. раздел "Управление активами" на стр. 376).

О ресурсах

Ресурсы – это компоненты KUMA, которые содержат параметры для реализации различных функций: например, установления связи с заданным веб-адресом или преобразования данных по определенным правилам. Из этих компонентов, как из частей конструктора, собираются наборы ресурсов для сервисов (на стр. 235), на основе которых в свою очередь создаются сервисы (см. раздел "Сервисы KUMA" на стр. 229) KUMA.

О сервисах

Сервисы – это основные компоненты KUMA (см. раздел "Архитектура программы" на стр. 19), с помощью которых осуществляется работа с событиями: получение, обработка, анализ и хранение. Каждый сервис состоит из двух частей, работающих вместе:

- Одна часть сервиса создается внутри веб-интерфейса KUMA на основе набора ресурсов для сервисов (см. раздел "Наборы ресурсов для сервисов" на стр. 235).
- Вторая часть сервиса устанавливается в сетевой инфраструктуре, где развернута система KUMA, в качестве одного из ее компонентов. Серверная часть сервиса может состоять из нескольких экземпляров: например, сервисы одного и того же агента или хранилища могут быть установлены сразу на нескольких машинах.

Между собой части сервисов соединены с помощью идентификатора сервисов (см. раздел "Получение идентификатора сервиса" на стр. 231).

Об агентах

Агенты KUMA – это сервисы (см. раздел "Сервисы KUMA" на стр. 229), которые используются для пересылки необработанных событий (см. раздел "О событиях" на стр. 25) с серверов и рабочих станций в коллекторы (см. раздел "Коллектор" на стр. 20) KUMA.

Типы агентов:

- wmi – используются для получения данных с удаленных машин Windows с помощью Windows Management Instrumentation. Устанавливается на устройства Windows.
- wec – используются для получения журналов Windows с локальной машины помощью Windows Event Collector. Устанавливается на устройства Windows.
- tcp – используются для получения данных по протоколу TCP. Устанавливается на устройства Linux и Windows.
- udp – используются для получения данных по протоколу UDP. Устанавливается на устройства Linux и Windows.
- nats – используются для коммуникации через NATS. Устанавливается на устройства Linux и Windows.
- kafka – используются для коммуникации с помощью kafka. Устанавливается на устройства Linux и Windows.
- http – используются для связи по протоколу HTTP. Устанавливается на устройства Linux и Windows.
- file – используются для получения данных из файла. Устанавливается на устройства Linux и Windows.
- ftp – используются для получения данных по протоколу File Transfer Protocol. Устанавливается на устройства Linux и Windows.
- nfs – используются для получения данных по протоколу Network File System. Устанавливается на устройства Linux и Windows.
- snmp – используются для получения данных с помощью Simple Network Management Protocol. Устанавливается на устройства Linux и Windows.
- diode – используются вместе с диодами данных для получения событий из изолированных сегментов сети. Устанавливается на устройства Linux.

Об уровне важности

Параметр *Уровень важности* отражает, насколько чувствительны для безопасности происшествия, обнаруженные коррелятором (см. раздел "Коррелятор" на стр. 23) KUMA. Он показывает порядок, в котором

следует обрабатывать алерты (см. раздел "Об алертах" на стр. 27), а также указывает, требуется ли участие старших специалистов по безопасности.

Коррелятор автоматически назначает уровень важности корреляционным событиям (см. раздел "О событиях" на стр. 25) и алертам, руководствуясь настройками правил корреляции (см. раздел "Правила корреляции" на стр. 134). Уровень важности алерта также зависит от активов (см. раздел "Об активах" на стр. 28), связанных с обработанными событиями, так как правила корреляции принимают во внимание уровень важности категории этих активов. Если к алерту или корреляционному событию не привязаны активы с уровнем важности или не привязаны активы вообще, уровень важности такого алерта или корреляционного события приравнивается к уровню важности породившего их правила корреляции. Уровень важности алерта или корреляционного события всегда больше или равен уровню важности породившего их правила корреляции.

Уровень важности алерта можно изменить вручную. Измененный вручную уровень важности перестает автоматически обновляться правилами корреляции.

Возможные значения уровня важности:

- Низкий
- Средний
- Высокий
- Критический

kaspersky

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы программы, а также указания по эксплуатации и требования к среде.

В этом разделе

Аппаратные и программные требования 31

Совместимость с другими программами 33

Аппаратные и программные требования

Рекомендуемые требования к оборудованию

На перечисленном ниже оборудовании могут обрабатываться до 40 000 событий в секунду. Этот показатель зависит от типа анализируемых событий и от эффективности парсера. Следует также учитывать, что большее количество ядер будет эффективнее, чем их меньшее количество, но с более высокой частотой процессора.

- Серверы для установки коллекторов:
  - Процессор: Intel® или AMD™ от 4 ядер (8 потоков) с поддержкой набора инструкций SSE 4.2 или 8 vCPU (виртуальных процессоров).
  - ОЗУ: 16 ГБ.

    Каждому коллектору, на котором используется обогащения событий геоданными (см. раздел "Работа с геоданными" на стр. 361), требуется дополнительный объем оперативной памяти, равный размеру базы геоданных.
  - Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt.
- Серверы для установки коррелляторов:
  - Процессор: Intel или AMD от 4 ядер (8 потоков) с поддержкой набора инструкций SSE 4.2 или 8 vCPU (виртуальных процессоров).
  - ОЗУ: 16 ГБ.
  - Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt.
- Серверы для установки Ядра:
  - Процессор: Intel или AMD от 4 ядер (8 потоков) с поддержкой набора инструкций SSE 4.2 или 4 vCPU (виртуальных процессоров).
  - ОЗУ: 16 ГБ.

    При импорте геоданных серверу требуется дополнительный объем оперативной памяти, равный размеру базы геоданных.
  - Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt.

- Серверы для установки хранилищ:
  - Процессор: Intel или AMD от 12 ядер (24 потока) с поддержкой набора инструкций SSE 4.2 или 24 vCPU (виртуальных процессоров).

    Требуется поддержка команд SSE4.2.
  - ОЗУ: 48 ГБ.
  - Диск: 500 ГБ доступного места на диске, смонтированного в разделе /opt.

  Для подключения системы хранения данных (далее также СХД) к серверам хранилища требуется использовать высокоскоростные протоколы (например, Fiber Chanell или iSCSI 10G). Мы не рекомендуем подключать СХД с использованием протоколов прикладного уровня (например, NFS, SMB).

  Использование твердотельных накопителей позволяет улучшить индексирование кластерных узлов и повысить эффективность поиска.

  Смонтированные локально жесткие диски или твердотельные накопители эффективнее внешних дисковых массивов (JBOD). Рекомендуется использовать RAID 0 для скорости, а RAID 10 для избыточности.

  Для повышения надежности не рекомендуется развертывать все кластерные узлы на одном JBOD-массиве или одном физическом сервере (если используются виртуальные серверы).

  Для повышения эффективности рекомендуется держать все серверы в одном центре данных.
- Машины для установки агентов Windows:
  - Процессор: одноядерный, 1.4 ГГц или выше.
  - ОЗУ: 512 МБ.
  - Диск: 1 ГБ.
  - ОС:
    - Microsoft® Windows® 2012.
    - Microsoft Windows Server® 2012 R2.
    - Microsoft Windows Server 2016.
    - Microsoft Windows Server 2019.
    - Microsoft Windows 10 (20H2, 21H1).
- Машины для установки агентов Linux®:
  - Процессор: одноядерный, 1.4 ГГц или выше.
  - ОЗУ: 512 МБ.
  - Диск: 1 ГБ.
  - ОС:
    - Ubuntu 20.04 LTS, 21.04.
    - Oracle® Linux версии 8.6 или выше.
    - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7.1).

kaspersky

Требования к программному обеспечению

Для развертывания компонентов Коллектор, Коррелятор, Ядро и Хранилище поддерживается использование операционных систем Oracle linux 8.6 или выше и Astra Linux Special Edition (исполнение РУСБ.10015-01).

Требования к сети

Пропускная способность сетевого интерфейса должна быть не менее 100 Мбит/с.

Чтобы программа KUMA обрабатывала более 20 000 событий в секунду, необходимо обеспечить скорость передачи данных между узлами ClickHouse не менее 1 Гбит/с. Рекомендуемая скорость передачи данных между узлами – 10 Гбит/с.

Дополнительные требования

Компьютеры, используемые для веб-интерфейса KUMA:

- Процессор: Intel® Core™ i3 8-го поколения.
- ОЗУ: 8 ГБ.
- Установленный браузер Google™ Chrome™ 102 или более поздней версии либо Mozilla™ Firefox™ 103 или более поздней версии.

kaspersky

Установка и удаление KUMA

В этом разделе описана установка KUMA. KUMA можно установить на одном сервере для ознакомления с возможностями программы (см. раздел "Установка для демонстрации" на стр. 36). KUMA также можно установить в производственной среде.

В этом разделе

Указания по эксплуатации и требования к среде 34

Требования к установке программы 35

Установка для демонстрации 36

Установка KUMA в производственной среде 39

Удаление KUMA 47

Обновление предыдущих версий KUMA 47

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.
8. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.
9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).

11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).
15. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
16. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

Требования к установке программы

Требования при установке на операционной системе Oracle Linux

- Образ диска для установки доступен на официальном сайте Oracle https://yum.oracle.com/ISOS/OracleLinux/OL8/u5/x86_64/OracleLinux-R8-U5-x86_64-dvd.iso.
- Убедиться, что в операционной системе установлен Python версии 3.6 или выше.
- Убедиться, что в операционной системе НЕ включен модуль SELinux. Работа KUMA и установщика KUMA совместно с включенным SELinux не поддерживается.
- Убедиться, что в операционной системе установлена система управления пакетами pip3.
- Убедиться, что в операционной системе установлены следующие пакеты:
  - netaddr
  - firewalld

  Эти пакеты можно установить с помощью команды `pip3 install netaddr firewalld`.

Требования при установке на операционной системе Astra Linux Special Edition

- Убедиться, что в операционной системе установлен Python версии 3.6 или выше.
- Убедиться, что в операционной системе установлена система управления пакетами pip3.
- Убедиться, что в операционной системе установлены следующие пакеты:
  - python3-apt
  - curl
  - libcurl4

  Эти пакеты можно установить с помощью команды `apt install python3-apt curl libcurl4`.
- Убедиться, что в операционной системе установлены следующие зависимые пакеты:
  - netaddr

- python3-cffi-backend

Эти пакеты можно установить с помощью следующих команд:

- `apt install python3-cffi-backend`
- `pip3 install netaddr`

> Если вы собираетесь из KUMA обращаться к базам данных Oracle DB (см. раздел "Тип sql" на стр. 179), необходимо установить пакет libaio1.

- Пользователю, под которым вы собираетесь устанавливать программу, требуется присвоить необходимый уровень прав с помощью команды `sudo pdpl-user -i 63 <имя пользователя>`.

Общие требования к установке

- Имя сервера, на котором запускается установщик, должно отличаться от `localhost` или `localhost.<домен>`.
- Перед развертыванием программы требуется убедиться, что серверы, предназначенные для установки ее компонентов, соответствуют аппаратным и программным требованиям (см. раздел "Аппаратные и программные требования" на стр. 31).
- Адресация компонентов KUMA осуществляется по полному доменному имени (FQDN) хоста. Перед установкой программы убедитесь, что команда `hostnamectl status` возвращает правильное имя FQDN хоста в поле `Static hostname`.
- Для синхронизации времени на всех серверах с сервисами KUMA рекомендуется использовать протокол Network Time Protocol (NTP).

Установка для демонстрации

Для демонстрации вы можете развернуть компоненты KUMA на одном сервере. Перед установкой программы ознакомьтесь с требованиями к установке KUMA (см. раздел "Требования к установке программы" на стр. 35), а также аппаратными и системными требованиями (см. раздел "Аппаратные и программные требования" на стр. 31).

Установка KUMA происходит в несколько этапов:

a. **Подготовка контрольной машины (на стр. 42)**

   Контрольная машина используется в процессе установки программы: на ней распаковывается и запускаются файлы установщика.

b. **Подготовка целевой машины (на стр. 43)**

   На целевые машины устанавливаются компоненты программы. Контрольную машину можно использовать в качестве целевой.

c. **Подготовка файла инвентаря для демонстрационной установки (на стр. 37)**

   Создайте файл инвентаря с описанием сетевой структуры компонентов программы, с помощью которого установщик сможет развернуть KUMA.

d. **Установка программы для демонстрации (см. раздел "Демонстрационная установка программы" на стр. 38)**

Установите программу и получите URL и учетные данные для входа в веб-интерфейс.

При необходимости установленную на демонстрации программу можно разнести на разные серверы (см. раздел "Расширение демонстрационной установки" на стр. 38) для полноценной работы.

В этом разделе

Подготовка файла инвентаря для демонстрационной установки 37

Демонстрационная установка программы 38

Расширение демонстрационной установки 38

Подготовка файла инвентаря для демонстрационной установки

Установка, обновление и удаление компонентов KUMA производится из папки с распакованным установщиком с помощью инструмента Ansible® и созданного пользователем *файла инвентаря* с перечнем хостов компонентов KUMA и других параметров. В случае демонстрационной установке хост для всех компонентов будет указан один и тот же. Файл инвентаря имеет формат YAML.

► *Чтобы создать файл инвентаря для демонстрационной установки:*

1. Перейдите в директорию установщика KUMA, выполнив следующую команду:

   ```
   cd kuma-ansible-installer
   ```

2. Создайте файл инвентаря, скопировав шаблон single.inventory.yml.template:

   ```
   cp single.inventory.yml.template single.inventory.yml
   ```

3. Отредактируйте параметры файла инвентаря:

   - Если вы хотите, чтобы при установке были созданы демонстрационные сервисы, присвойте параметру deploy_example_services значение true.

     ```
     deploy_example_services: true
     ```

     Демонстрационные сервисы можно создать только при первичной установке KUMA – при обновлении системы с помощью того же файла инвентаря демонстрационные сервисы созданы не будут.

   - Если вы устанавливаете KUMA в производственной среде и имеете отдельную контрольную машину, присвойте параметру ansible_connection значение ssh:

     ```
     ansible_connection: ssh
     ```

4. Замените в файле инвентаря все строки `kuma.example.com` на хост целевой машины (см. раздел "Подготовка целевой машины" на стр. 43), на которую следует установить компоненты KUMA.

Файл инвентаря создан. С его помощью можно установить KUMA для демонстрации.

Рекомендуется не удалять файл инвентаря после установки KUMA:

- Если этот файл изменить (например, дополнить данными о новом сервере для коллектора), его можно использовать повторно для обновления системы новым компонентом.
- Этот же файл инвентаря можно использовать для удаления KUMA.

kaspersky

Демонстрационная установка программы

Установка KUMA производится помощью инструмента Ansible и YML-файла инвентаря (см. раздел "Подготовка файла инвентаря" на стр. 44). Установка производится с контрольной машины (см. раздел "Подготовка контрольной машины" на стр. 42), при этом все компоненты KUMA устанавливаются на целевых машинах (см. раздел "Подготовка целевой машины" на стр. 43).

► *Чтобы установить KUMA для демонстрации:*

1. На контрольной машине войдите в папку с распакованным установщиком.
2. Подложите в папку <папка установщика>/roles/kuma/files/ файл с лицензионным ключом.

   Файл ключа (см. раздел "О файле ключа" на стр. 51) должен иметь название license.key.
3. Запустите установщик, выполнив следующую команду:

   ```
   sudo ./install.sh single.inventory.yml
   ```
4. Примите условия Лицензионного соглашения.

   Если вы не примите условия Лицензионного соглашения, программа не будет установлена.

   Компоненты KUMA установлены на целевой машине. На экране будет отображен URL веб-интерфейса KUMA (см. раздел "Вход в веб-интерфейс программы" на стр. 48) и указано имя пользователя и пароль, которые необходимо использовать для доступа к веб-интерфейса.

   По умолчанию адрес веб-интерфейса KUMA – `https://kuma.example.com:7220`.
   Учетные данные, используемые для входа по умолчанию (после первого входа требуется изменить пароль учетной записи admin (см. раздел "Управление пользователями" на стр. 69)):
   - логин – `admin`
   - пароль – `mustB3Ch@ng3d!`

   Рекомендуется сохранить файл инвентаря, использованный для установки программы. С его помощью можно дополнить систему компонентами или удалить KUMA.

Демонстрационную установку можно расширить (см. раздел "Расширение демонстрационной установки" на стр. 38) до полноценной.

Расширение демонстрационной установки

Расширение демонстрационной установки производится путем установки программы по шаблону distributed.inventory.yml (см. раздел "Подготовка файла инвентаря" на стр. 44) поверх установленной KUMA.

Расширение демонстрационной установки производится в несколько этапов:

a. **Установка программы (см. раздел "Установка KUMA в производственной среде" на стр. 39)**

   На этапе подготовке файла инвентаря укажите хост демонстрационного сервера поместите в группе `core`.

b. **Удаление демонстрационных сервисов**

В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** скопируйте идентификаторы (см. раздел "Получение идентификатора сервиса" на стр. 231) существующих сервисов и удалите (см. раздел "Удаление сервиса" на стр. 232) их.

Затем удалите сервисы с машины, где они были установлены, с помощью команды `sudo /opt/kaspersky/kuma/kuma <collector/correlator/storage> --id <идентификатор сервиса> --uninstall`. Повторите команду удаления для каждого сервиса.

c. **Пересоздание сервисов на нужных машинах (см. раздел "Создание сервисов" на стр. 46)**

Установка KUMA в производственной среде

Перед установкой программы ознакомьтесь с требованиями к установке KUMA (см. раздел "Требования к установке программы" на стр. 35), а также аппаратными и системными требованиями (см. раздел "Аппаратные и программные требования" на стр. 31). Установка KUMA происходит в несколько этапов:

a. **Настройка сетевого доступа (на стр. 41)**

   Убедитесь, что все необходимые порты открыты для взаимодействия между компонентами KUMA с учетом структуры безопасности на вашем предприятии.

b. **Подготовка контрольной машины (на стр. 42)**

   Контрольная машина используется в процессе установки программы: на ней распаковывается и запускаются файлы установщика.

c. **Подготовка целевых машин (см. раздел "Подготовка целевой машины" на стр. 43)**

   На целевые машины устанавливаются компоненты программы.

d. **Подготовка файла инвентаря (на стр. 44)**

   Создайте файл инвентаря с описанием сетевой структуры компонентов программы, с помощью которого установщик сможет развернуть KUMA.

e. **Установка программы (на стр. 45)**

   Установите программу и получите URL и учетные данные для входа в веб-интерфейс.

f. **Создание сервисов (на стр. 46)**

   Создайте сервисы в веб-интерфейсе KUMA и установите их на предназначенных для них целевых машинах.

В этом разделе

Настройка сетевого доступа 41
Подготовка контрольной машины 42
Подготовка целевой машины 43
Подготовка файла инвентаря 44
Установка программы 45
Создание сервисов 46
Изменение корневого сертификата 46

kaspersky

kaspersky

Настройка сетевого доступа

Для правильной работы программы нужно убедиться, что компоненты KUMA могут взаимодействовать с другими компонентами и программами по сети через протоколы и порты, указанные во время установки компонентов KUMA. В таблице ниже показаны значения сетевых портов по умолчанию.

Таблица 1. Сетевые порты, используемые для взаимодействия компонентов KUMA друг с другом

Протокол	Порт	Направление	Назначение подключения
HTTPS	7222	От клиента KUMA к серверу с компонентом Ядро KUMA.	Реверс-прокси к системе CyberTrace.
HTTPS	8123	От сервиса хранилища к узлу кластера ClickHouse.	Запись и получение нормализованных событий в кластере ClickHouse.
HTTPS	9009	Между репликами кластера ClickHouse.	Внутренняя коммуникация между репликами кластера ClickHouse для передачи данных кластера.
TCP	2181	От узлов кластера ClickHouse к сервису координации репликации ClickHouse keeper.	Получение и запись репликами серверов ClickHouse метаинформации о реплицировании.
TCP	2182	От сервисов координации репликации ClickHouse keeper друг к другу.	Внутренняя коммуникация между сервисами координации репликации, используемая для достижения кворума.
TCP	7210	От всех компонентов KUMA на сервер Ядра KUMA	Получение конфигурации KUMA от сервера Ядра KUMA
TCP	7215	От коллектора KUMA к коррелятору KUMA	Отправка данных коллектором в коррелятор KUMA
TCP	7220	От клиента KUMA к серверу с компонентом Ядро KUMA	Доступ пользователей к веб-интерфейса KUMA
TCP	7221 и другие порты, используемые для установки сервисов в качестве значения параметра --api.port <порт>	От Ядра KUMA к сервисам KUMA	Администрирование сервисов из веб-интерфейса KUMA
TCP	7223	К серверу Ядра KUMA.	Порт, используемый по умолчанию для API-запросов.
TCP	8001	От Victoria Metrics к серверу ClickHouse.	Получение метрик работы сервера ClickHouse.
TCP	9000	От клиента ClickHouse к узлу кластера ClickHouse.	Запись и получение данных в кластере ClickHouse.

kaspersky

Подготовка контрольной машины

Контрольная машина используется в процессе установки программы: на ней распаковывается и запускаются файлы установщика.

► *Чтобы подготовить контрольную машину для установки KUMA:*

1. Установите на контрольную машину операционную систему (см. раздел "Аппаратные и программные требования" на стр. 31) и установите на нее необходимые пакеты (см. раздел "Требования к установке программы" на стр. 35).
2. Настройте сетевой интерфейс (см. раздел "Настройка сетевого доступа" на стр. 41).

   Для удобства можно воспользоваться утилитой с графическим интерфейсом nmtui.
3. Настройте синхронизацию системного времени с NTP-сервером:
   a. Если машина не имеет прямого доступа в интернет, отредактируйте файл /etc/chrony.conf, заменив значение `2.pool.ntp.org` на имя или IP-адрес внутреннего NTP-сервера вашей организации.
   b. Запустите сервис синхронизации системного времени, выполнив следующую команду:

      ```
      sudo systemctl enable --now chronyd
      ```
   c. Выждите несколько секунд и выполните следующую команду:

      ```
      sudo timedatectl | grep 'System clock synchronized'
      ```

      Если системное время синхронизировано верно, вывод будет содержать строку System clock synchronized: yes.
4. Сгенерируйте SSH-ключ для аутентификации на SSH-серверах целевых машин, выполнив следующую команду:

   ```
   sudo ssh-keygen -f /root/.ssh/id_rsa -N "" -C kuma-ansible-installer
   ```
5. Убедитесь, что контрольная машина имеет сетевой доступ (см. раздел "Настройка сетевого доступа" на стр. 41) ко всем целевым машинам по имени хоста (см. раздел "Подготовка целевой машины" на стр. 43) и скопируйте SSH-ключ на каждую из них, выполнив следующую команду:

   ```
   sudo ssh-copy-id -i /root/.ssh/id_rsa root@<имя хоста контрольной машины>
   ```
6. Скопируйте архив с установщиком KUMA на контрольную машину и распакуйте его с помощью следующей команды (потребуется около 2 ГБ дискового пространства):

   ```
   sudo tar -xpf kuma-ansible-installer-<version>.tar.gz
   ```

Контрольная машина готова для установки KUMA.

kaspersky

Подготовка целевой машины

На целевые машины устанавливаются компоненты программы.

► *Чтобы подготовить целевую машину для установки компонентов KUMA:*

1. Установите на контрольную машину операционную систему (см. раздел "Аппаратные и программные требования" на стр. 31) и установите на нее необходимые пакеты (см. раздел "Требования к установке программы" на стр. 35).
2. Настройте сетевой интерфейс (см. раздел "Настройка сетевого доступа" на стр. 41).

   Для удобства можно воспользоваться утилитой с графическим интерфейсом nmtui.
3. Настройте синхронизацию системного времени с NTP-сервером:

   a. Если машина не имеет прямого доступа в интернет, отредактируйте файл /etc/chrony.conf, заменив значение `2.pool.ntp.org` на имя или IP-адрес внутреннего NTP-сервера вашей организации.

   b. Запустите сервис синхронизации системного времени, выполнив следующую команду:

   ```
   sudo systemctl enable --now chronyd
   ```

   c. Выждите несколько секунд и выполните следующую команду:

   ```
   sudo timedatectl | grep 'System clock synchronized'
   ```

   Если системное время синхронизировано верно, вывод будет содержать строку System clock synchronized: yes.
4. Установите имя хоста. Настоятельно рекомендуется использовать FQDN. Например: kuma-1.mydomain.com.

   Не следует изменять имя хоста KUMA после установки: это приведет к невозможности проверки подлинности сертификатов и нарушит сетевое взаимодействие между компонентами программы.
5. Зарегистрируйте целевую машину в DNS-зоне вашей организации для преобразования имен хостов в IP-адреса.

   Если в вашей организации не используется DNS-сервер, вы можете использовать для преобразования имен файл /etc/hosts. Содержимое файлов можно автоматически создать для каждой целевой машины при установке KUMA.
6. Выполните следующую команду и запишите результат:

   ```
   hostname -f
   ```

   Данное имя хоста потребуется указать при установке KUMA. Целевая машина должна быть доступна по этому имени для контрольной машины (см. раздел "Подготовка контрольной машины" на стр. 42).

Целевая машина готова для установки компонентов KUMA.

Контрольную машину можно использовать в качестве целевой. Для этого подготовьте контрольную машину, а затем выполните на ней шаги 4–6 из инструкции по подготовке целевой машины.

kaspersky

Подготовка файла инвентаря

Установка, обновление и удаление компонентов KUMA производится из папки с распакованным установщиком с помощью инструмента Ansible и созданного пользователем *файла инвентаря* с перечнем хостов компонентов KUMA и других параметров. Файл инвентаря имеет формат YAML.

► *Чтобы создать файл инвентаря:*

1. Перейдите в директорию установщика KUMA, выполнив следующую команду:

   ```
   cd kuma-ansible-installer
   ```

2. Создайте файл инвентаря, скопировав шаблон distributed.inventory.yml.template:

   ```
   cp distributed.inventory.yml.template distributed.inventory.yml
   ```

3. Отредактируйте параметры файла инвентаря:

   - Если вы хотите, чтобы при установке были созданы демонстрационные сервисы, присвойте параметру deploy_example_services значение true.

     ```
     deploy_example_services: true
     ```

     Демонстрационные сервисы можно создать только при первичной установке KUMA – при обновлении системы с помощью того же файла инвентаря демонстрационные сервисы созданы не будут.

   - Если машины не зарегистрированы в DNS-зоне вашей организации, присвойте параметру generate_etc_hosts значение true, а также для каждой машины в инвентаре замените значения параметра `ip (0.0.0.0)` на актуальные IP-адреса.

     ```
     generate_etc_hosts: true
     ```

     При использование этого параметра установщик автоматически дополнит файлы /etc/hosts на машинах, куда устанавливаются компоненты KUMA, IP-адресами машин из файла инвентаря.

   - Если вы устанавливаете KUMA в производственной среде и имеете отдельную контрольную машину, присвойте параметру ansible_connection значение ssh:

     ```
     ansible_connection: ssh
     ```

4. Укажите в файле инвентаря хост целевых машин (см. раздел "Подготовка целевой машины" на стр. 43), на которых следует установить компоненты KUMA. Если машины не зарегистрированы в DNS-зоне вашей организации, замените значения параметра `ip (0.0.0.0)` на актуальные IP-адреса.

   Хосты указываются в следующих разделах файла инвентаря:

   - `core` – раздел для указания хоста и IP-адреса целевой машины, на которой будет установлено Ядро KUMA. В этом разделе можно указать только один хост.
   - `collector` – раздел для указания хоста и IP-адреса целевой машины, на которой будет установлен коллектор. В этом разделе можно указать один или более хостов.
   - `correlator` – раздел для указания хоста и IP-адреса целевой машины, на которой будет установлен коррелятор. В этом разделе можно указать один или более хостов.
   - `storage` – раздел для указания хостов и IP-адресов целевых машин, на которых будут установлены компоненты хранилища. В этом разделе можно указать один или более хостов.

     Компоненты хранилища: кластеры, шарды, реплики, киперы (см. раздел "Кластеры, шарды и реплики" на стр. 24)

Каждая машина в разделе `storage` может иметь следующие комбинации параметров:

- `shard` + `replica` + `keeper`
- `shard` + `replica`
- `keeper`

Если указаны параметры `shard` и `replica`, машина является частью кластера и принимает участие в накоплении и поиске нормализованных событий KUMA. Если дополнительно указан параметр `keeper`, машина также принимает участие в координации репликации данных на уровне всего кластера.

Если указан только параметр `keeper`, машина **не** будет накапливать нормализованные события, но будет участвовать в координации репликации данных на уровне всего кластера. Значения параметра keeper должны быть уникальными.

Если в рамках одного шарда определено несколько реплик, значение параметра replica должно быть уникальным **в рамках этого шарда**.

Файл инвентаря создан. С его помощью можно установить KUMA.

Рекомендуется не удалять файл инвентаря после установки KUMA:

- Если этот файл изменить (например, дополнить данными о новом сервере для коллектора), его можно использовать повторно для обновления системы новым компонентом.
- Этот же файл инвентаря можно использовать для удаления KUMA.

Установка программы

Установка KUMA производится помощью инструмента Ansible и YML-файла инвентаря (см. раздел "Подготовка файла инвентаря" на стр. 44). Установка производится с контрольной машины (см. раздел "Подготовка контрольной машины" на стр. 42), при этом все компоненты KUMA устанавливаются на целевых машинах (см. раздел "Подготовка целевой машины" на стр. 43).

► *Чтобы установить KUMA:*

1. На контрольной машине войдите в папку с распакованным установщиком (см. раздел "Подготовка контрольной машины" на стр. 42).
2. Подложите в папку <папка установщика>/roles/kuma/files/ файл с лицензионным ключом.

   Файл ключа (см. раздел "О файле ключа" на стр. 51) должен иметь название license.key.
3. Запустите установщик, выполнив следующую команду:

   ```
   sudo ./install.sh distributed.inventory.yml
   ```
4. Примите условия Лицензионного соглашения.

   Если вы не примите условия Лицензионного соглашения, программа не будет установлена.

Компоненты KUMA установлены на целевых машинах. На экране будет отображен URL веб-интерфейса KUMA (см. раздел "Вход в веб-интерфейс программы" на стр. 48) и указано имя пользователя и пароль, которые необходимо использовать для доступа к веб-интерфейса.

По умолчанию адрес веб-интерфейса KUMA – `https://kuma.example.com:7220`.
Учетные данные, используемые для входа по умолчанию (после первого входа требуется изменить пароль учетной записи admin (см. раздел "Управление пользователями" на стр. 69)):
- логин – `admin`
- пароль – `mustB3Ch@ng3d!`
Рекомендуется сохранить файл инвентаря, использованный для установки программы. С его помощью можно дополнить систему компонентами или удалить KUMA.

Создание сервисов

Сервисы KUMA (на стр. 229) следует устанавливать только после завершения развертывания KUMA (см. раздел "Установка программы" на стр. 45). Сервисы можно устанавливать в любом порядке.

При развертывании нескольких сервисов KUMA на одном хосте в процессе установки требуется указать уникальные порты для каждого сервиса с помощью параметров `--api.port <порт>`.

Ниже перечислены разделы, в которых описано создание сервисов:

- Создание хранилища (на стр. 270)
- Создание коррелятора (на стр. 252)
- Создание коллектора (на стр. 235)
- Создание агентов KUMA (см. раздел "Создание агента" на стр. 263)

Изменение корневого сертификата

После установки Ядра KUMA создается уникальный самоподписанный корневой сертификат с соответствующим ключом. Этот сертификат используется для подписи всех других сертификатов, используемых для внутренней связи между компонентами KUMA, а также для запросов REST API. Корневой сертификат хранится на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

Вы можете использовать сертификат и ключ своей компании вместо самоподписанного корневого сертификата и ключа KUMA.

Перед изменением сертификата KUMA обязательно сделайте резервную копию предыдущего сертификата и ключа с именами backup_external.cert и backup_external.key.

► *Чтобы изменить корневой сертификат KUMA:*

1. Переименуйте файлы сертификата и ключа вашей компании в external.cert и external.key.

   Ключи должны быть в PEM-формате.
2. Поместите external.cert и external.key в папку /opt/kaspersky/kuma/core/certificates/.

3. Перезапустите службу kuma-core, выполнив команду `sudo systemctl restart kuma-core`.
4. Перезапустите браузер, с помощью которого вы работаете в веб-интерфейсе KUMA.

Сертификат и ключ вашей компании используются для внутренней связи между компонентами KUMA и для запросов REST API.

Удаление KUMA

При удалении KUMA используется инструмент Ansible и созданный пользователем файл инвентаря (см. раздел "Подготовка файла инвентаря" на стр. 44).

► *Чтобы удалить KUMA:*

1. На контрольной машине войдите в директорию установщика:

   ```
   cd kuma-ansible-installer
   ```

2. Выполните следующую команду:

   ```
   sudo ./uninstall.sh <файл инвентаря>
   ```

KUMA и все данные программы удалены с серверов.

Базы данных, которые использовались KUMA (например, база данных хранилища ClickHouse), и содержащуюся в них информацию следует удалить отдельно.

Обновление предыдущих версий KUMA

KUMA версии 2.x можно установить поверх версий 1.5.x и выше. Для этого следуйте инструкции по установке программы в производственной среде (см. раздел "Установка KUMA в производственной среде" на стр. 39) и на этапе подготовке файла инвентаря (см. раздел "Подготовка файла инвентаря" на стр. 44) перечислите в нем хосты уже развернутой системы KUMA.

После обновления KUMA необходимо очистить кеш браузера.

kaspersky

Вход в веб-интерфейс программы

► *Чтобы войти в веб-интерфейс программы:*

1. В браузере введите следующий адрес:

   `https://<IP-адрес или FQDN сервера Ядра KUMA>:7220`

   Откроется страница авторизации веб-интерфейса с запросом на ввод имени и пароля для входа.
2. В поле **Логин** введите логин учетной записи.
3. В поле **Пароль** введите пароль указанной учетной записи.
4. Нажмите на кнопку **Логин**.

Откроется главное окно веб-интерфейса программы.

В режиме мультитенантности (см. раздел "О тенантах" на стр. 25) при первом входе в веб-интерфейс программы пользователю отображаются данные только для тех тенантов, которые были выбраны (см. раздел "Выбор тенанта" на стр. 302) для него при создании его учетной записи.

► *Чтобы выйти из веб-интерфейса программы,*

откройте веб-интерфейс KUMA, в левом нижнем углу окна нажмите на имя учетной записи пользователя и в открывшемся меню учетной записи нажмите на кнопку **Выход**.

kaspersky

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием программы.

В этом разделе

О Лицензионном соглашении 49
О лицензии 49
О Лицензионном сертификате 50
О лицензионном ключе 50
О файле ключа 51
Добавление лицензионного ключа в веб-интерфейс программы 51
Просмотр информации о добавленном лицензионном ключе в веб-интерфейсе программы 52
Удаление лицензионного ключа в веб-интерфейсе программы 53

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки KUMA.
- Прочитав документ LICENSE. Этот документ включен в комплект поставки программы и находится внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

  После развертывания программы документ доступен директории /opt/kaspersky/kuma/LICENSE.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Лицензия предоставляется при приобретении программы. По истечении срока действия лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно создание новых ресурсов). Чтобы продолжить использование KUMA в режиме полной функциональности, вам нужно продлить срок действия лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

О Лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, количество обрабатываемых событий в секунду);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в программу, применив *файл ключа*. Лицензионный ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы программы требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и резервным.

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного лицензионного ключа.

Резервный лицензионный ключ – лицензионный ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

О файле ключа

Файл ключа – это файл с названием license.key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения KUMA.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии.
- Получить файл ключа на веб-сайте "Лаборатории Касперского" (https://keyfile.kaspersky.com/ru/) на основе имеющегося кода активации.

Добавление лицензионного ключа в веб-интерфейс программы

В веб-интерфейсе KUMA можно добавить лицензионный ключ программы.

Только пользователи с ролью администратора могут добавлять лицензионные ключи.

► *Чтобы добавить лицензионный ключ в веб-интерфейс KUMA:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Лицензия**.

   Откроется окно с условиями лицензии KUMA.
2. Выберите ключ, который хотите добавить:

- Если необходимо добавить активный ключ, нажмите кнопку **Добавить активный лицензионный ключ**.

  Эта кнопка не отображается, если в программу уже был добавлен лицензионный ключ. Если вы хотите добавить активный лицензионный ключ вместо уже добавленного ключа, текущий лицензионный ключ необходимо удалить (см. раздел "Удаление лицензионного ключа в веб-интерфейсе программы" на стр. 53).

- Если вы хотите добавить резервный ключ, нажмите кнопку **Добавить резервный лицензионный ключ**.

  Эта кнопка неактивна, пока не будет добавлен активный ключ. Если вы хотите добавить резервный лицензионный ключ вместо уже добавленного ключа, текущий резервный лицензионный ключ необходимо удалить (см. раздел "Удаление лицензионного ключа в веб-интерфейсе программы" на стр. 53).

Откроется окно выбора файла лицензионного ключа.

3. Выберите файл лицензии, указав путь к папке и имя лицензионного ключа (файла с расширением KEY).

Лицензионный ключ из выбранного файла загружен в программу. Информация о лицензионном ключе отображается в разделе **Параметры** → **Лицензия**.

Просмотр информации о добавленном лицензионном ключе в веб-интерфейсе программы

В веб-интерфейсе KUMA можно просмотреть информацию о добавленном лицензионном ключе. Информация о лицензионном ключе отображается в разделе **Параметры** → **Лицензия**.

Только пользователи с ролью администратора могут просматривать информацию о лицензии.

В окне закладки **Лицензия** отображается следующая информация о добавленных лицензионных ключах:

- **Истекает** – дата истечения срока действия лицензионного ключа.
- **Осталось дней** – количество дней до истечения срока действия лицензии.
- **Доступное EPS** – количество обрабатываемых в секунду событий, которое поддерживается лицензией.
- **Текущее EPS** – текущее среднее количество событий в секунду, которое обрабатывает KUMA.
- **Лицензионный ключ** – уникальная буквенно-цифровая последовательность.
- **Компания** – название компании, купившей лицензию.
- **Имя клиента** – имя клиента, купившего лицензию.
- **Модули** – модули, доступные для лицензии.

Удаление лицензионного ключа в веб-интерфейсе программы

Вы можете удалить добавленный лицензионный ключ из KUMA (например, если вам нужно заменить текущий лицензионный ключ другим). После удаления лицензионного ключа программа перестает получать и обрабатывать события. Эта работа возобновится при добавлении лицензионного ключа.

Только пользователи с ролью администратора (см. раздел "Роли пользователей" на стр. 57) могут удалять лицензионные ключи.

► *Чтобы удалить лицензионный ключ:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Лицензия**.

   Откроется окно с условиями лицензии KUMA.

2. Нажмите на значок  на лицензии, которую требуется удалить.

   Откроется окно подтверждения.

3. Подтвердите удаление лицензионного ключа.

Лицензионный ключ удален из программы.

kaspersky

Процедура приемки

Перед вводом программы в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

В этом разделе

Проверка целостности файлов KUMA 54

Безопасное состояние 54

Проверка правильной установки и работоспособности программы 55

Проверка целостности файлов KUMA

Целостность компонентов программы проверяется с помощью набора скриптов, основанных на инструменте integrity_checker, расположенных в директории /opt/kaspersky/kuma/integrity/bin. При проверке целостности используются xml-файлы манифестов из директории /opt/kaspersky/kuma/integrity/manifest/*, подписанные криптографической сигнатурой "Лаборатории Касперского".

Для запуска инструмента проверки целостности необходима учетная запись с root-правами.

Проверка целостности выполняется раздельно для компонентов KUMA, и должна выполняться раздельно на серверах с соответствующими компонентами. При проверке целостности также проверяется целостность использованного xml-файла.

► *Чтобы проверить целостность файлов компонентов:*

1. Перейдите в директорию, содержащую набор скриптов с помощью следующей команды:

   ```
   cd /opt/kaspersky/kuma/integrity/bin
   ```

2. Выполните команду из таблицы ниже, в зависимости от того, целостность какого компонента KUMA вы хотите проверить:

Таблица 2. Команды для проверки целостности компонентов KUMA

Команда	Проверяемые компоненты (исполняемые файлы)
`./check_all.sh`	Компоненты Ядра KUMA и Хранилища
`./check_core.sh`	Компоненты Ядра KUMA
`./check_collector.sh`	Компоненты Коллектора KUMA
`./check_correlator.sh`	Компоненты Коррелятора KUMA
`./check_storage.sh`	Компоненты Хранилища
`./check_kuma_exe.sh <полный путь к файлу`	Агент KUMA для Windows

`kuma.exe без указания имени файла>`	Стандартное расположение исполняемого файла агента на устройстве Window: C:\Program Files\Kaspersky Lab\KUMA\

Результат проверки каждого компонента отображается в следующем формате:

- В случае, если скрипт проверяет целостность более одного компонента – название компонента
- Блок Summary описывает количество проверенных объектов со статусом проверки: целостность не подтверждена/объект пропущен/целостность подтверждена
  - Manifests – количество обработанных файлов манифеста.
  - Files – количество обработанных файлов KUMA.
  - Directories – при проверке целостности KUMA не используется.
  - Registries – при проверке целостности KUMA не используется.
  - Registry values – при проверке целостности KUMA не используется.
- Результат проверки целостности компонента:
  - SUCCEEDED – целостность подтверждена.
  - FAILED – целостность нарушена.

Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если выполняются следующие условия:

- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу (см. раздел "Приложение. Значения параметров программы в сертифицированной конфигурации" на стр. 531).

Проверка правильной установки и работоспособности программы

После успешного запуска команд для установки системы перейти по URL адресу `https://<IP-адрес или FQDN сервера Ядра KUMA>:<порт, используемый сервером Ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7220)`. В результате открывается экран авторизации веб-консоли KUMA, что говорит о правильной установке программы.

На экране авторизации ввести корректные учетные данные (логин и пароль). В результате открывается веб-консоль KUMA, которая содержит разделы:

- Панель мониторинга
- Алерты
- Инциденты
- События
- Активы
- Отчеты

- Ресурсы
- Диспетчер задач
- Параметры
- Состояние источников
- Метрики

Открытие веб-консоли KUMA после авторизации говорит о работоспособности программы.

kaspersky

Разделение доступа к функциям программы по пользовательским ролям

Если пользователь не зарегистрирован в списке пользователей KUMA, он не может открыть веб-интерфейс KUMA.

В этом разделе

Роли пользователей 57

Управление пользователями 69

Роли пользователей

Пользователи (см. раздел «Управление пользователями» на стр. 69) KUMA могут иметь следующие роли:

- *Главный администратор* – эта роль предназначена для пользователей, отвечающих за функционирование основных систем KUMA. Например, они устанавливают системные компоненты, выполняют обслуживание, работают с сервисами, создают резервные копии и добавляют пользователей в систему. Эти пользователи имеют полный доступ к KUMA.
- *Администратор* – эта роль предназначена для пользователей, отвечающих за функционирование систем KUMA, принадлежащих определенным тенантам.
- *Аналитик* – эта роль предназначена для пользователей, ответственных за настройку системы KUMA для получения и обработки событий определенного тенанта. Они также создают и настраивают правила корреляции.
- *Оператор* – эта роль предназначена для пользователей, которые сталкиваются с непосредственными угрозами безопасности определенного тенанта. Пользователь с ролью оператор посредством REST API видит ресурсы на общем тенанте.

Таблица 3. Права пользователей

Раздел веб-интерфейса и действия	Главный администратор	Администратор	Аналитик	Оператор	Комментарий
Отчеты					
Просматривать и изменять шаблоны и отчеты	есть	есть	есть	нет	Аналитик может: Просмотреть и изменить шаблоны/отчеты, которые создал сам. Просмотреть отчеты, которые были отправлены аналитику на почту. Просмотреть

					предустановленные шаблоны.
Формировать отчеты	есть	есть	есть	нет	Аналитик может генерировать отчеты, которые создал сам и предустановленные (из шаблона и из отчета). Аналитик не может генерировать отчеты, которые были отправлены аналитику на почту.
Выгружать сформированные отчеты	есть	есть	есть	нет	Аналитик может выгружать: Отчеты, которые создал сам. Предустановленные отчеты. Отчеты, которые получил по почте.
Удалять шаблоны и сформированные отчеты	есть	есть	есть	нет	Аналитик может удалить шаблоны и отчеты, которые создал сам. Аналитик не может удалять: Предустановленные шаблоны. Отчеты, которые пришли ему на почту. Предустановленные шаблоны и отчеты может удалять только главный администратор.
Изменять настройки формирования отчетов	есть	есть	есть	нет	Аналитик может изменять настройки генерации отчетов, которые создал сам, и предустановленные.
Дублировать шаблон отчета	есть	есть	есть	нет	Аналитик может дублировать шаблоны отчетов, которые создал сам, и предустановленные.
Панель мониторинга					
Просматривать данные на панели мониторинга и менять макеты	есть	есть	есть	есть	
Добавлять макеты	есть	есть	есть	нет	В том числе добавлять виджеты в макет.

Изменять и переименовывать макеты	есть	есть	есть	нет	В том числе добавлять, изменять и удалять виджеты. Аналитик может изменять/переименовывать предустановленные макеты и макеты, созданные своей учетной записью.
Удалять макеты	есть	есть	есть	нет	Администратор тенанта может удалять макеты в доступных ему тенантах. Аналитик может удалять макеты, созданные своей учетной записью. Предустановленные макеты может удалять только главный администратор.
Ресурсы → Сервисы и **Ресурсы → Сервисы → Активные сервисы**					
Просматривать список активных сервисов	есть	есть	есть	нет	Только главный администратор может просматривать и удалять пространства у хранилища. Права доступа не зависят от выбранных в меню тенантов.
Просматривать содержимое активного листа	есть	есть	есть	нет	
Импортировать/экспортировать/очищать содержимое активного листа	есть	есть	есть	нет	
Создавать набор ресурсов для сервисов	есть	есть	есть	нет	Аналитик не может создавать хранилища.
Создавать сервис в разделе Ресурсы - Сервисы - Активные сервисы	есть	есть	нет	нет	
Удалять сервисы	есть	есть	нет	нет	
Перезапускать сервисы	есть	есть	нет	нет	
Обновлять параметры	есть	есть	есть	нет	

сервисов					
Сбрасывать сертификаты	есть	есть	нет	нет	Пользователь с ролью администратор может сбрасывать сертификаты сервисов только в доступных ему тенантах.
Ресурсы → Ресурсы					
Просматривать список ресурсов	есть	есть	есть	нет*	Аналитики не могут просматривать список ресурсов секретов, однако эти ресурсы доступны им при создании сервисов.
Добавлять ресурсы	есть	есть	есть	нет	Аналитики не могут добавлять ресурсы секретов.
Изменять ресурсы	есть	есть	есть	нет	Аналитики не могут изменять ресурсы секретов.
Создавать/редактировать/удалять ресурсы в общем тенанте	есть	нет	нет	нет	
Удалять ресурсы	есть	есть	есть	нет	Аналитики не могут удалять ресурсы секретов.
Импортировать ресурсы	есть	есть	есть	нет	Импортировать ресурсы в общий тенант может только главный администратор.
Экспортировать ресурсы	есть	есть	есть	нет	В том числе ресурсы из общего тенанта.
Просматривать/редактировать черновики коллектора или коррелятора	есть	есть	есть	нет	Пользователю доступны только свои черновики вне зависимости от выбранного тенанта, список черновиков формируется по принадлежности к пользователю.
Состояние источников → Список источников событий					
Просматривать источники событий	есть	есть	есть	есть	
Изменять источники событий	есть	есть	есть	нет	Редактировать наименование источника, назначать политику мониторинга, отключать

					политику мониторинга.
Удалять источники событий	есть	есть	есть	нет	
Состояние источников → Политики мониторинга					
Просматривать политики мониторинга	есть	есть	есть	есть	
Создавать политики мониторинга	есть	есть	есть	нет	
Изменять политики мониторинга	есть	есть	есть	нет	Только главный администратор может редактировать предустано вленные политики мониторинга.
Удалять политики мониторинга	есть	есть	есть	нет	Предустановленные полит ики недоступны для удаления.
Активы					
Просматривать активы и категории активов	есть	есть	есть	есть	Включая категории общего тенанта.
Добавлять/редактироват ь/удалять категории активов	есть	есть	есть	нет	В рамках доступного пользователю тенанта.
Добавлять категории активов в общем тенанте	есть	нет	нет	нет	В том числе редактировать и удалять категории общего тенанта.
Привязывать активы к категории активов общего тенанта	есть	есть	есть	нет	
Добавлять активы	есть	есть	есть	нет	
Изменять активы	есть	есть	есть	нет	
Удалять активы	есть	есть	есть	нет	
Импортировать активы из Kaspersky Security Center	есть	есть	есть	нет	
Запускать задачи на активах в Kaspersky Security Center	есть	есть	есть	нет	
Запускать задачи на активах Kaspersky Endpoint Detection and Response	есть	есть	есть	нет	

Алерты					
Просматривать список алертов	есть	есть	есть	есть	
Изменять уровень важности алертов	есть	есть	есть	есть	
Открывать детали алертов	есть	есть	есть	есть	
Назначать ответственных пользователей	есть	есть	есть	есть	
Закрывать алерты	есть	есть	есть	есть	
Добавлять комментарий к алертам	есть	есть	есть	есть	
Привязывать событие к алертам	есть	есть	есть	есть	
Отвязывать событие от алертов	есть	есть	есть	есть	
Изменять и удалять чужие фильтры	есть	есть	нет	нет	
Инциденты					
Просматривать список инцидентов	есть	есть	есть	есть	
Создавать пустые инциденты	есть	есть	есть	есть	
Создавать вручную инциденты из алертов	есть	есть	есть	есть	
Изменять уровень важности инцидентов	есть	есть	есть	есть	
Открывать детали инцидентов	есть	есть	есть	есть	В деталях инцидента отображаются данные только тех тенантов, к которым у пользователя есть доступ.
Назначать исполнителей	есть	есть	есть	есть	
Закрывать инциденты	есть	есть	есть	есть	
Добавлять комментарии к инцидентам	есть	есть	есть	есть	
Привязывать алерты к инцидентам	есть	есть	есть	есть	
Отвязывать алерты от инцидентов	есть	есть	есть	есть	

Изменять и удалять чужие фильтры	есть	есть	нет	нет	
Экспортировать инциденты в НКЦКИ	есть	есть	есть	есть	
События					
Просматривать список событий	есть	есть	есть	есть	
Выполнять поиск событий	есть	есть	есть	есть	
Открывать детали событий	есть	есть	есть	есть	
Открывать статистику	есть	есть	есть	есть	
Провозить ретроспективную проверку	есть	есть	есть	нет	
Выгружать события в TSV-файл	есть	есть	есть	есть	
Изменять и удалять чужие фильтры	есть	есть	нет	нет	
Запускать ktl-обогащение	есть	есть	есть	нет	
Запускать задачи на активах Kaspersky Endpoint Detection and Response в деталях событий	есть	есть	есть	нет	
Параметры → Пользователи					Раздел доступен только главному администратору.
Увидеть список пользователей	есть	нет	нет	нет	
Добавить пользователя	есть	нет	нет	нет	
Изменить пользователя	есть	нет	нет	нет	
Увидеть данные своего профиля	есть	есть	есть	есть	
Изменить данные своего профиля	есть	есть	есть	есть	Роль пользователя недоступна для изменения.
Параметры → LDAP-сервер					
Просматривать параметры подключения к LDAP	есть	есть	нет	нет	
Изменять параметры	есть	есть	нет	нет	

подключения к LDAP					
Параметры → Тенанты					Раздел доступен только главному администратору.
Просматривать список тенантов	есть	нет	нет	нет	
Добавлять тенантов	есть	нет	нет	нет	
Изменять тенантов	есть	нет	нет	нет	
Отключать тенантов	есть	нет	нет	нет	
Параметры → Доменная авторизация					Раздел доступен только главному администратору.
Просматривать параметры подключения к Active directory	есть	нет	нет	нет	
Изменять параметры подключения к Active directory	есть	нет	нет	нет	
Добавлять фильтры по ролям для тенантов	есть	нет	нет	нет	
Параметры → Общие					Раздел доступен только главному администратору.
Просматривать параметры подключения к SMTP	есть	нет	нет	нет	
Изменять параметры подключения к SMTP	есть	нет	нет	нет	
Параметры → Лицензия					Раздел доступен только главному администратору.
Просматривать список добавленных лицензионных ключей	есть	нет	нет	нет	
Добавлять лицензионные ключи	есть	нет	нет	нет	
Удалять лицензионные ключи	есть	нет	нет	нет	
Параметры → Kaspersky Security Center					
Просматривать список Kaspersky Security Center-серверов, с которыми выполнена интеграция	есть	есть	нет	нет	
Добавлять подключения	есть	есть	нет	нет	

к Kaspersky Security Center					
Удалять подключения к Kaspersky Security Center	есть	есть	нет	нет	
Параметры → Kaspersky CyberTrace					Раздел доступен только главному администратору.
Просматривать параметры интеграции с CyberTrace	есть	нет	нет	нет	
Изменять параметры интеграции с CyberTrace	есть	нет	нет	нет	
Параметры → IRP / SOAR					Раздел доступен только главному администратору.
Просматривать параметры интеграции с IRP / SOAR	есть	нет	нет	нет	
Изменять параметры интеграции с IRP / SOAR	есть	нет	нет	нет	
Параметры → Kaspersky Threat Lookup					Раздел доступен только главному администратору.
Просматривать параметры интеграции с Threat Lookup	есть	нет	нет	нет	
Изменять параметры интеграции с Threat Lookup	есть	нет	нет	нет	
Параметры → Алерты					
Просматривать параметры	есть	есть	есть	нет	
Изменять параметры	есть	есть	есть	нет	
Параметры → Инциденты → Автоматическая привязка алертов к инцидентам					
Увидеть настройки	есть	нет	нет	нет	
Изменить настройки	есть	нет	нет	нет	
Параметры → Инциденты → Типы инцидентов					
Просматривать	есть	есть	нет	нет	

справочник категорий					
Просматривать карточки категорий	есть	есть	нет	нет	
Добавлять категории	есть	есть	нет	нет	Доступно, если у пользователя есть роль администратора хотя бы в одном тенанте.
Изменять категории	есть	есть	нет	нет	Доступно, если у пользователя есть роль администратора хотя бы в одном тенанте.
Удалять категории	есть	есть	нет	нет	Доступно, если у пользователя есть роль администратора хотя бы в одном тенанте.
Параметры → НКЦКИ					
Просматривать параметры	есть	нет	нет	нет	
Изменять параметры	есть	нет	нет	нет	
Параметры → Иерархия					
Просматривать параметры	есть	нет	нет	нет	
Изменять параметры	есть	нет	нет	нет	
Просматривать инцидентов дочернего узла	есть	есть	есть	есть	
Метрики					
Открывать метрики	есть	нет	нет	нет	
Диспетчер задач					
Просматривать список своих задач	есть	есть	есть	есть	Раздел и задачи не имеют привязки к тенанту. Задачи доступны только создавшему их пользователю.
Завершать свои задачи	есть	есть	есть	есть	
Перезапускать свои задачи	есть	есть	есть	есть	
Просматривать список всех задач	есть	нет	нет	нет	
Завершать любые задачи	есть	нет	нет	нет	

Перезапускать любые задачи	есть	нет	нет	нет	
CyberTrace					Раздел не отображается в веб-интерфейсе, если не настроена интеграция с CyberTrace в разделе Параметры → CyberTrace.
Открывать раздел	есть	нет	нет	нет	
Доступ к данным тенантов					
Доступ к тенантам	есть	есть	есть	есть	Пользователь имеет доступ к главному тенанту, если его название указано в блоках параметров ролей учетной записи пользователя. Уровень доступа зависит от того, в какой из ролей указан тенант Права доступа к главному тенанту не означают доступ ко всем тенантам, а только к данным этого тенанта.
Главный тенант	есть	есть	есть	есть	Общий тенант используется для хранения общих ресурсов, которые должны быть доступны для всех тенантов. Сервисы не могут принадлежать общему тенанту, но в них могут использоваться принадлежащие общему тенанту ресурсы. При этом такие сервисы принадлежат к своему тенанту. События, алерты и инциденты не могут быть общими. Права доступа к общему тенанту: чтение и запись – только главный администратор; чтение – остальные пользователи, включая пользователей с правами доступа к главному

					тенанту.
Общий тенант	есть	есть	есть	есть	Пользователь имеет доступ к главному тенанту, если его название указано в блоках параметров ролей учетной записи пользователя. Уровень доступа зависит от того, в какой из ролей указан тенант Права доступа к главному тенанту не дают доступ к другим тенантам.

kaspersky

Управление пользователями

Доступ к KUMA может иметь несколько пользователей. Пользователям присваиваются роли пользователей (на стр. 57), которые влияют на задачи, которые пользователи могут выполнять. У разных тенантов (см. раздел "О тенантах" на стр. 25) у одного и того же пользователя могут быть разные роли.

Вы можете создать или изменить учетные записи пользователя в разделе веб-интерфейса KUMA **Параметры → Пользователи**. Пользователи также создаются в программе автоматически, если включена интеграция KUMA с Active directory (см. раздел "Авторизация с помощью доменных учетных записей" на стр. 110) и пользователь входит в веб-интерфейс KUMA с помощью своей доменной учетной записи в первый раз.

Таблица учетных записей отображается в окне **Пользователи** веб-интерфейса KUMA. Пользователей можно искать с помощью поля **Поиск**. Вы можете отсортировать таблицу по столбцу **Данные о пользователе**, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.

Учетные записи можно создать (см. раздел "Создание пользователя" на стр. 69), изменить (см. раздел "Редактирование пользователя" на стр. 70) или выключить. При изменении учетных записей (как своей (см. раздел "Редактирование своей учетной записи" на стр. 71), так и чужих) для них можно сгенерировать API-токен.

По умолчанию выключенные учетные записи не отображаются в таблице пользователей, но их можно просмотреть, нажав на столбец **Данные о пользователе** и установив флажок **Выключенные пользователи**.

► *Чтобы выключить пользователя,*

В разделе веб-интерфейса KUMA **Параметры → Пользователи** поставьте флажок напротив нужного пользователя и нажмите **Выключить пользователя**.

В этом разделе

Создание пользователя 69

Редактирование пользователя 70

Редактирование своей учетной записи 71

Создание пользователя

► *Чтобы создать учетную запись пользователя:*

1. Откройте раздел веб-интерфейса KUMA **Параметры → Пользователи**.

   В правой части раздела **Параметры** отобразится таблица **Пользователи**.

2. Нажмите на кнопку **Добавить пользователя** и задайте параметры, как описано ниже.

   - **Имя** (обязательно) – введите имя пользователя. Длина должна быть от 1 до 128 символов Юникода.
   - **Логин** (обязательно) – введите уникальный логин учетной записи пользователя. Длина должна быть от 3 до 64 символов (допускается использование только символов a–z, A–Z, 0–9, . \ - _).

- **Адрес электронной почты** (обязательно) – введите уникальный адрес электронной почты пользователя. Адрес электронной почты должен быть действительным.
- **Новый пароль** (обязательно) – введите пароль для учетной записи пользователя. Требования к паролю:
  - длина от 8 до 128 символов;
  - требуется как минимум один символ в нижнем регистре;
  - требуется как минимум один символ в верхнем регистре;
  - требуется как минимум одна цифра;
  - требуется как минимум один специальный символ: !, @, #, %, ^, &, *.
- **Подтверждение пароля** (обязательно) – повторите пароль.
- **Выключен** – установите этот флажок, если хотите выключить учетную запись пользователя. По умолчанию этот флажок снят.
- В блоке параметров **Тенанты для ролей** с помощью кнопок **Добавить поле** укажите, какие роли (см. раздел "Роли пользователей" на стр. 57) и в каких тенантах (см. раздел "О тенантах" на стр. 25) будет исполнять пользователь. В разных тенантах можно иметь разные роли, в одном тенанте можно иметь только одну роль.
- **Получать уведомления по почте** – установите этот флажок, если хотите, чтобы пользователь получал SMTP-уведомления (см. раздел "Подключение к SMTP-серверу" на стр. 407) от KUMA.
- Установите флажок **Может взаимодействовать с НКЦКИ**, если хотите, чтобы пользователь мог экспортировать инциденты в НКЦКИ (см. раздел "Экспорт инцидентов в НКЦКИ" на стр. 317). Установить флажок может только пользователь с ролью главный администратор.
- Установите флажок **Группа главных администраторов**, если хотите присвоить пользователю роль главного администратора. Пользователи с ролью главного администратора могут изменять параметры других учетных записей пользователей. По умолчанию этот флажок снят.

3. Нажмите **Сохранить**.

Учетная запись пользователя создана и отображается в таблице **Пользователи**.

Редактирование пользователя

► *Чтобы отредактировать пользователя:*

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Пользователи**.

   В правой части раздела **Параметры** отобразится таблица **Пользователи**.

2. Выберите нужного пользователя и в открывшейся в правой части области деталей пользователя измените требуемые параметры.
   - **Имя** (обязательно) – измените имя пользователя. Длина должна быть от 1 до 128 символов Юникода.
   - **Логин** (обязательно) – введите уникальный логин учетной записи пользователя. Длина должна быть от 3 до 64 символов (допускается использование только символов a–z, A–Z, 0–9, . \ - _).
   - **Адрес электронной почты** (обязательно) – введите уникальный адрес электронной почты пользователя. Адрес электронной почты должен быть действительным.

- **Выключен** – установите этот флажок, если хотите выключить учетную запись пользователя. По умолчанию этот флажок снят.
- В блоке параметров **Тенанты для ролей** с помощью кнопок **Добавить поле** укажите, какие роли (см. раздел "Роли пользователей" на стр. 57) и в каких тенантах (см. раздел "О тенантах" на стр. 25) будет исполнять пользователь. В разных тенантах можно иметь разные роли, в одном тенанте можно иметь только одну роль.
- **Получать уведомления по почте** – установите этот флажок, если хотите, чтобы пользователь получал SMTP-уведомления (см. раздел "Подключение к SMTP-серверу" на стр. 407) от KUMA.
- Установите флажок **Может взаимодействовать с НКЦКИ**, если хотите, чтобы пользователь мог экспортировать инциденты в НКЦКИ (см. раздел "Экспорт инцидентов в НКЦКИ" на стр. 317). Установить флажок может только пользователь с ролью главный администратор.
- Установите флажок **Группа главных администраторов**, если хотите присвоить пользователю роль главного администратора. Пользователи с ролью главного администратора могут изменять параметры других учетных записей пользователей. По умолчанию этот флажок снят.

3. Если требуется изменить пароль, нажмите на кнопку **Изменить пароль** и в открывшемся окне заполните поля, описанные ниже. По завершении нажмите **ОК**.
   - **Действующий пароль** (обязательно) – введите действующий пароль своей учетной записи.
   - **Новый пароль** (обязательно) – введите пароль для учетной записи пользователя. Требования к паролю:
     - длина от 8 до 128 символов;
     - требуется как минимум один символ в нижнем регистре;
     - требуется как минимум один символ в верхнем регистре;
     - требуется как минимум одна цифра;
     - требуется как минимум один специальный символ: !, @, #, %, ^, &, *.
   - **Подтверждение пароля** (обязательно) – повторите пароль.
4. При необходимости сгенерируйте API-токен (см. раздел "Создание токена" на стр. 414) с помощью кнопки **Сгенерировать токен**. При нажатии на эту кнопку отображается окно создания токена.
5. При необходимости настройте доступные пользователю операции (см. раздел "Настройка прав доступа к API" на стр. 414) через REST API с помощью кнопки **Права доступа через API**.
6. Нажмите **Сохранить**.

Учетная запись пользователя изменена.

Редактирование своей учетной записи

► *Чтобы отредактировать свою учетную запись:*

1. Откройте веб-интерфейс KUMA, в левом нижнем углу окна нажмите на имя учетной записи пользователя и в открывшемся меню нажмите на кнопку **Профиль**.

   Откроется окно **Пользователь** с параметрами вашей учетной записи.
2. Измените нужные параметры:
   - **Имя** (обязательно) – введите имя пользователя. Длина должна быть от 1 до 128 символов Юникода.

- **Логин** (обязательно) – введите уникальный логин учетной записи пользователя. Длина должна быть от 3 до 64 символов (допускается использование только символов a–z, A–Z, 0–9, . \ - _).

  Адрес электронной почты (обязательно) – введите уникальный адрес электронной почты пользователя. Адрес электронной почты должен быть действительным.

- **Получать уведомления по почте** – установите этот флажок, если хотите получать SMTP-уведомления (см. раздел "Подключение к SMTP-серверу" на стр. 407) от KUMA.

- **Отображать непечатаемые символы** – установите этот флажок, если хотите, чтобы в веб-интерфейсе KUMA отображались непечатаемые символы: пробелы, знаки табуляции, перенос на новую строку.

  Пробелы и знаки табуляции отображаются во всех полях ввода, кроме **Описание**, в ресурсах нормализаторов, правил корреляции, фильтров и коннекторов, а также в SQL-запросах на поиск событий в разделе **События**.

  Пробелы отображаются в виде точек.

  Знак табуляции отображается в виде тире в ресурсах нормализаторов, правил корреляции, фильтров и коннекторов. В других полях знак табуляции отображается в виде одной или двух точек.

  Символ переноса на новую строку отображается во всех полях ввода, поддерживающих многострочный ввод. Например, в строке поиска событий (см. раздел "Создание SQL-запроса вручную" на стр. 345).

  Если флажок **Отображать непечатаемые символы** установлен, отображение непечатаемых символов можно включать и выключать, нажимая клавиши **CTRL/COMMAND+***.

3. Если требуется изменить пароль, нажмите на кнопку **Изменить пароль** и в открывшемся окне заполните поля, описанные ниже. По завершении нажмите **ОК**.

   - **Действующий пароль** (обязательно) – введите действующий пароль своей учетной записи.
   - **Новый пароль** (обязательно) – введите пароль для учетной записи пользователя. Требования к паролю:
     - длина от 8 до 128 символов;
     - требуется как минимум один символ в нижнем регистре;
     - требуется как минимум один символ в верхнем регистре;
     - требуется как минимум одна цифра;
     - требуется как минимум один специальный символ: !, @, #, %, ^, &, *.
   - **Подтверждение пароля** (обязательно) – повторите пароль.

4. При необходимости сгенерируйте API-токен (см. раздел "Создание токена" на стр. 414) с помощью кнопки **Сгенерировать токен**. При нажатии на эту кнопку отображается окно создания токена.

5. При необходимости настройте доступные операции (см. раздел "Настройка прав доступа к API" на стр. 414) через REST API с помощью кнопки **Права доступа через API**.

6. Нажмите **Сохранить**.

Ваша учетная запись отредактирована.

kaspersky

Интеграция с другими решениями

В этом разделе описано, как интегрировать KUMA с другими приложениями для расширения возможностей программы.

В этом разделе

Интеграция с Kaspersky Security Center 73
Интеграция с Kaspersky Endpoint Detection and Response 80
Интеграция с Kaspersky CyberTrace 81
Интеграция с Kaspersky Threat Intelligence Portal 87
Интеграция с R-Vision Incident Response Platform 90
Интеграция с Active Directory 102
Интеграция с НКЦКИ 114
Интеграция с Security Vision Incident Response Platform 117
Интеграция с Kaspersky Industrial CyberSecurity for Networks 124

Интеграция с Kaspersky Security Center

Вы можете настроить интеграцию с выбранными серверами Kaspersky Security Center для одного, нескольких или всех тенантов KUMA. Если интеграция с Kaspersky Security Center включена, вы можете импортировать информацию об активах (см. раздел "Импорт информации об активах из Kaspersky Security Center" на стр. 384), защищаемых этой программой, управлять активами с помощью задач (см. раздел "Работа с задачами Kaspersky Security Center" на стр. 77), а также импортировать события (см. раздел "Импорт событий из базы Kaspersky Security Center" на стр. 79) из базы событий Kaspersky Security Center.

Предварительно вам требуется убедиться, что на требуемом сервере Kaspersky Security Center разрешено входящее соединение для сервера с KUMA.

Настройка интеграции KUMA с Kaspersky Security Center включает следующие этапы:

1. Создание в Консоли администрирования Kaspersky Security Center учетной записи пользователя.

   Данные этой учетной записи используются при создании секрета для установки соединения с Kaspersky Security Center. Вам не требуется назначать в Kaspersky Security Center специальные права доступа для этой учетной записи.

   Подробнее о создании учетной записи и назначении прав пользователю см. в *справке Kaspersky Security Center*.

2. Создание секрета (см. раздел "Секреты" на стр. 226) с типом credentials для соединения с Kaspersky Security Center.
3. Настройка параметров интеграции (см. раздел "Настройка параметров интеграции с Kaspersky Security Center" на стр. 74) с Kaspersky Security Center.

4. Создание подключения к серверу Kaspersky Security Center (см. раздел "Создание подключения к Kaspersky Security Center" на стр. 75) для импорта информации об активах.

   Если вы хотите импортировать в KUMA информацию об активах, зарегистрированных на серверах Kaspersky Security Center, вам требуется создать отдельное подключение к каждому серверу Kaspersky Security Center для каждого выбранного тенанта.

   Если для тенанта выключена интеграция или отсутствует подключение к Kaspersky Security Center, при попытке импорта информации об активах в веб-интерфейсе KUMA отобразится ошибка. Процесс импорта при этом не запускается.

В этом разделе

Настройка параметров интеграции с Kaspersky Security Center 74

Добавление тенанта в список тенантов для интеграции с Kaspersky Security Center 75

Создание подключения к Kaspersky Security Center 75

Изменение подключения к Kaspersky Security Center 76

Удаление подключения к Kaspersky Security Center 77

Работа с задачами Kaspersky Security Center 77

Импорт событий из базы Kaspersky Security Center 79

Настройка параметров интеграции с Kaspersky Security Center

► *Чтобы настроить параметры интеграции с Kaspersky Security Center:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Выберите тенант, для которого вы хотите настроить параметры интеграции с Kaspersky Security Center.

   Откроется окно **Интеграция с Kaspersky Security Center**.

3. Для флажка **Выключено** выполните одно из следующих действий:

   - Снимите флажок, если вы хотите включить интеграцию с Kaspersky Security Center для этого тенанта.
   - Установите флажок, если хотите выключить интеграцию с Kaspersky Security Center для этого тенанта.

   По умолчанию флажок снят.

4. В поле **Период обновления данных** укажите период времени, по истечении которого KUMA обновляет данные об устройствах Kaspersky Security Center.

   Интервал указывается в часах. Вы можете указать только целое число.

   По умолчанию временной интервал составляет 12 часов.

5. Нажмите на кнопку **Сохранить**.

Параметры интеграции с Kaspersky Security Center для выбранного тенанта будут настроены.

Если в списке тенантов отсутствует нужный вам тенант, вам требуется добавить его в список (см. раздел "Добавление тенанта в список тенантов для интеграции с Kaspersky Security Center" на стр. 75).

Добавление тенанта в список тенантов для интеграции с Kaspersky Security Center

► *Чтобы добавить тенант в список тенантов для интеграции с Kaspersky Security Center:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.
2. Нажмите на кнопку **Добавить тенант**.

   Откроется окно **Интеграция с Kaspersky Security Center**.
3. В раскрывающемся списке **Тенант** выберите тенант, который вам требуется добавить.
4. Нажмите **Сохранить**.

Выбранный тенант будет добавлен в список тенантов для интеграции с Kaspersky Security Center.

Создание подключения к Kaspersky Security Center

► *Чтобы создать подключение к Kaspersky Security Center:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.
2. Выберите тенант, для которого вы хотите создать подключение к Kaspersky Security Center.
3. Нажмите на кнопку **Добавить подключение** и укажите значения для следующих параметров:
   - **Название** (обязательно) – имя подключения. Имя может включать от 1 до 128 символов Юникода.
   - **URL** (обязательно) – URL сервера Kaspersky Security Center в формате hostname:port или IPv4:port.
   - В раскрывающемся списке **Секрет** выберите ресурс секрета с учетными данными Kaspersky Security Center или создайте новый ресурс секрета (см. раздел "Добавление секрета при создании подключения" на стр. 76).

     Выбранный секрет можно изменить, нажав на кнопку  .
   - **Выключено** – состояние подключения к выбранному серверу Kaspersky Security Center. Если флажок установлен, подключение к выбранному серверу неактивно. В этом случае вы не можете использовать это подключение для соединения с сервером Kaspersky Security Center.

     По умолчанию флажок снят.
4. Если вы хотите, чтобы программа KUMA импортировала только активы, которые подключены к подчиненным серверам или включены в группы:

   a. Нажмите на кнопку **Загрузить иерархию**.

b. Установите флажки рядом с именами подчиненных серверов и групп, из которых вы хотите импортировать информацию об активах.

c. Если вы хотите импортировать активы только из новых групп, установите флажок **Импортировать активы из новых групп**.

Если ни один флажок не установлен, при импорте выгружается информация обо всех активах выбранного сервера Kaspersky Security Center.

5. Нажмите на кнопку **Сохранить**.

Подключение к серверу Kaspersky Security Center будет создано. Его можно использовать для импорта информации об активах (см. раздел "Импорт информации об активах из Kaspersky Security Center" на стр. 384) из Kaspersky Security Center в KUMA и для создания задач, связанных с активами (см. раздел "Работа с задачами Kaspersky Security Center" на стр. 77), в Kaspersky Security Center из KUMA.

Добавление секрета при создании подключения

1. Нажмите на кнопку  .

   Откроется окно секрета.

2. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будут принадлежать учетные данные Kaspersky Security Center.

   c. В раскрывающемся списке **Тип** выберите **credentials**.

   d. В полях **Пользователь** и **Пароль** введите учетные данные вашего сервера Kaspersky Security Center.

   e. В поле **Описание** можно добавить описание секрета.

3. Нажмите **Сохранить**.

Изменение подключения к Kaspersky Security Center

► *Чтобы изменить подключение к Kaspersky Security Center:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Выберите тенант, для которого вы хотите настроить параметры интеграции с Kaspersky Security Center.

   Откроется окно **Интеграция с Kaspersky Security Center**.

3. Нажмите на подключение с Kaspersky Security Center, которое вы хотите изменить.

   Откроется окно с параметрами выбранного подключения к Kaspersky Security Center.

4. Измените значения необходимых параметров.

5. Нажмите на кнопку **Сохранить**.

Подключение к Kaspersky Security Center будет изменено.

Удаление подключения к Kaspersky Security Center

► *Чтобы удалить подключение к Kaspersky Security Center:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.

2. Выберите тенант, для которого вы хотите настроить параметры интеграции с Kaspersky Security Center.

   Откроется окно **Интеграция с Kaspersky Security Center**.

3. Выберите подключение Kaspersky Security Center, которое вы хотите удалить.
4. Нажмите на кнопку **Удалить**.

Подключение к Kaspersky Security Center будет удалено.

Работа с задачами Kaspersky Security Center

После импорта информации об активах Kaspersky Security Center вы можете управлять этими активами с помощью задач. Задачи запускаются в веб-интерфейсе KUMA. Вы можете запускать задачи вручную из раздела **Активы** веб-интерфейса программы или автоматически с помощью правил реагирования (см. раздел "Правила реагирования" на стр. 217) в процессе корреляции (см. раздел "Коррелятор" на стр. 23).

Подробнее о задачах Kaspersky Security Center см. в *справке Kaspersky Security Center*.

В веб-интерфейсе KUMA вы можете запустить только те задачи Kaspersky Security Center, название которых начинается с <kuma> (без учета регистра).

В этом разделе

Запуск задач Kaspersky Security Center вручную 77

Запуск задач Kaspersky Security Center автоматически 78

Проверка статуса задач Kaspersky Security Center 79

Запуск задач Kaspersky Security Center вручную

► *Чтобы запустить задачу Kaspersky Security Center вручную:*

1. В разделе **Активы** веб-интерфейса KUMA выберите активы, импортированные из Kaspersky Security Center.

   Откроется окно **Информация об активе**.

2. Нажмите на кнопку **Реагирование KSC**.

Кнопка отображается, если подключение к Kaspersky Security Center, к которому принадлежит выбранный актив, включено.

3. В открывшемся окне **Выберите задачу** установите флажки рядом с задачами, которые вы хотите запустить, и нажмите на кнопку **Запустить**.

Kaspersky Security Center запускает выбранные задачи.

Некоторые типы задач доступны только для определенных активов.
Информация об уязвимостях и программном обеспечении доступна только для активов с операционной системой Windows.

Запуск задач Kaspersky Security Center автоматически

Корреляторы могут запускать задачи Kaspersky Security Center автоматически. При выполнении определенных условий коррелятор активирует правила реагирования, содержащие список задач Kaspersky Security Center для запуска и определения соответствующих активов.

► *Чтобы настроить ресурс реагирования, который может использоваться корреляторами для автоматического запуска задач Kaspersky Security Center:*

1. Выберите раздел веб-интерфейса KUMA **Ресурсы** → **Реагирование**.
2. Нажмите кнопку **Добавить реагирование** и задайте параметры, как описано ниже:
   - В поле **Имя** введите имя ресурса для его идентификации.
   - В раскрывающемся списке **Тип** выберите **ksctasks** (задачи Kaspersky Security Center).
   - В раскрывающемся списке **Задача Kaspersky Security Center** выберите задачи, запускаемые при срабатывании коррелятора, связанного с этим ресурсом реагирования.

     Вы можете выбрать несколько задач. При активации реагирования из списка задач выбирается только первая задача, соответствующая выбранному активу. Остальные подходящие задачи игнорируются. Если требуется запустить несколько задач при выполнении одного условия, нужно создать несколько правил реагирования.
   - В поле **Поле события** выберите поля события, которые вызовут срабатывание корреляторов. Возможные значения:
     - SourceAssetID.
     - DestinationAssetID.
     - DeviceAssetID.
3. При необходимости в поле **Рабочие процессы** укажите количество процессов реагирования, которые можно запускать одновременно.
4. При необходимости в блоке параметров **Фильтр** задайте условия, при соответствии которым события будут обрабатываться создаваемым ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или создать новый фильтр.

   Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

5. Нажмите **Сохранить**.

Ресурс реагирования создан. Теперь его можно связать с коррелятором, который будет вызывать его, запуская тем самым задачу Kaspersky Security Center.

Проверка статуса задач Kaspersky Security Center

В веб-интерфейсе KUMA можно проверить, была ли запущена задача Kaspersky Security Center или завершен ли поиск событий из коллектора, который прослушивает события Kaspersky Security Center.

► *Чтобы выполнить проверку статуса задач Kaspersky Security Center:*

1. Выберите раздел KUMA **Ресурсы** → **Активные сервисы**.
2. Выберите коллектор, настроенный на получение событий с сервера Kaspersky Security Center, и нажмите на кнопку **Перейти к событиям**.

Откроется новая закладка браузера в разделе **События** KUMA. В таблице отобразятся события с сервера Kaspersky Security Center. Статус задач отображается в столбце **Название**.

Поля событий Kaspersky Security Center:

- **Name** (Название) – статус или тип задачи.
- **Message** (Сообщение) – сообщение о задаче или событии.
- **FlexString<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, полученного от Kaspersky Security Center. Например, `FlexString1Label=TaskName`.
- **FlexString<номер>** (Настраиваемое поле <номер>) – значение атрибута, указанного в поле поля FlexString<номер>Label. Например, `FlexString1=Download updates`.
- **DeviceCustomNumber<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, относящегося к состоянию задачи. Например, `DeviceCustomNumber1Label=TaskOldState`.
- **DeviceCustomNumber<номер>** (Настраиваемое поле <номер>) – значение, относящееся к состоянию задачи. Например, `DeviceCustomNumber1=1` означает, что задача выполняется.
- **DeviceCustomString<номер>Label** (Заголовок настраиваемого поля <номер>) – название атрибута, относящегося к обнаруженной уязвимости: например, название вируса, уязвимого приложения.
- **DeviceCustomString<номер>** (Настраиваемое поле <номер>) – значение, относящееся к обнаруженной уязвимости. Например, пары атрибут-значение `DeviceCustomString1Label=VirusName` и `DeviceCustomString1=EICAR-Test-File` означают, что обнаружен тестовый вирус EICAR.

Импорт событий из базы Kaspersky Security Center

В KUMA можно получать события непосредственно из SQL-базы Kaspersky Security Center. Получение событий производится с помощью коллектора (см. раздел "Коллектор" на стр. 20), в котором используются доступные в поставке ресурсы коннектора (см. раздел "Коннекторы" на стр. 169) [OOTB] KSC SQL и нормализатора (см. раздел "Нормализаторы" на стр. 158) [OOTB] KSC from SQL.

► *Чтобы создать коллектор для получения событий Kaspersky Security Center:*

1. Запустите мастер установки коллектора одним из следующих способов:
   - В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Подключить источник**.
   - В веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** нажмите **Добавить коллектор**.
2. На шаге 2 (см. раздел "Шаг 2. Транспорт" на стр. 238) мастера установки выберите коннектор [OOTB] KSC SQL:
   - В поле **URL** укажите строку подключения к серверу в следующем формате:

     `sqlserver://user:password@kscdb.example.com:1433/KAV`

     где:
     - `user` – учетная запись с правами public и db_datareader к нужной базе данных;
     - `password` – пароль учетной записи;
     - `kscdb.example.com:1433` – адрес и порт сервера базы данных;
     - `KAV` – название базы данных.
   - В поле **Запрос** укажите запрос к базе данных, исходя из потребности получать определенные события.

     Пример запроса к SQL-базе Kaspersky Security Center (см. раздел "Пример запроса к SQL базе Kaspersky Security Center" на стр. 180)
3. На шаге 3 (см. раздел "Шаг 3. Парсинг событий" на стр. 239) мастера установки выберите нормализатор [OOTB] KSC from SQL.
4. Остальные параметры укажите в соответствии вашими требованиями к коллектору.

В результате выполнения шагов мастера в веб-интерфейсе KUMA создается сервис коллектора, с помощью которого вы можете импортировать события из SQL-базы Kaspersky Security Center.

Интеграция с Kaspersky Endpoint Detection and Response

Kaspersky Endpoint Detection and Response (далее также KEDR) – функциональный блок программы Kaspersky Anti Targeted Attack Platform, обеспечивающий защиту активов локальной сети организации.

Вы можете настроить интеграцию KUMA с Kaspersky Endpoint Detection and Response, чтобы управлять действиями по реагированию на угрозы на активах, подключенных к серверам Kaspersky Endpoint Detection and Response, и активах Kaspersky Security Center. Команды на выполнение операций поступают на сервер Kaspersky Endpoint Detection and Response, после чего она передает их программе Kaspersky Endpoint Agent, установленной на активах. Также вы можете импортировать события Kaspersky Endpoint Detection and Response, отмеченные правилами TAA (IOA), в KUMA.

При интеграции KUMA с Kaspersky Endpoint Detection and Response вы можете выполнять следующие операции на активах Kaspersky Endpoint Detection and Response с Kaspersky Endpoint Agent:

- Управлять сетевой изоляцией активов.
- Управлять правилами запрета.
- Запускать программы.

kaspersky

Управление действиями по реагированию доступно только при наличии лицензии Kaspersky Symphony XDR.

За инструкцией по настройке интеграции вам требуется обратиться к вашему аккаунт-менеджеру или в службу технической поддержки.

Интеграция с Kaspersky CyberTrace

Kaspersky CyberTrace (далее CyberTrace) – это инструмент, который объединяет потоки данных об угрозах с решениями SIEM. Он обеспечивает пользователям мгновенный доступ к данным аналитики, повышая их осведомленность при принятии решений, связанных с безопасностью.

Вы можете интегрировать CyberTrace с KUMA одним из следующих способов:

- Интегрировать функцию поиска индикаторов CyberTrace (см. раздел "Интеграция поиска по индикаторам CyberTrace" на стр. 81) для обогащения событий KUMA информацией потоков данных CyberTrace.
- Интегрировать в KUMA веб-интерфейс CyberTrace целиком (см. раздел "Интеграция интерфейса CyberTrace" на стр. 84), чтобы обеспечить полный доступ к CyberTrace.

  Интеграция с веб-интерфейсом CyberTrace доступна только в том случае, если ваша лицензия CyberTrace включает многопользовательскую функцию.

В этом разделе

Интеграция поиска по индикаторам CyberTrace 81
Интеграция интерфейса CyberTrace 84

Интеграция поиска по индикаторам CyberTrace

Интеграция функции поиска по индикаторам CyberTrace состоит из следующих этапов:

a. **Настройка CyberTrace для приема и обработки запросов от KUMA (см. раздел "Настройка CyberTrace для приема и обработки запросов" на стр. 82)**

   Вы можете настроить интеграцию с KUMA сразу после установки CyberTrace в мастере первоначальной настройки или позднее в веб-интерфейсе CyberTrace.

b. **Создание правила обогащения событий в KUMA (см. раздел "Создание правил обогащения событий" на стр. 83)**

После завершения всех этапов интеграции требуется перезапустить коллектор, отвечающий за получение событий, которые вы хотите обогатить информацией из CyberTrace.

kaspersky

В этом разделе

Настройка CyberTrace для приема и обработки запросов 82
Создание правил обогащения событий 83

Настройка CyberTrace для приема и обработки запросов

Вы можете настроить CyberTrace для приема и обработки запросов от KUMA сразу после установки в мастере первоначальной настройки или позднее в веб-интерфейсе программы.

► *Чтобы настроить CyberTrace для приема и обработки запросов в мастере первоначальной настройки:*

1. Дождитесь запуска мастера первоначальной настройки CyberTrace после установки программы.

   Откроется окно **Welcome to Kaspersky CyberTrace**.
2. В раскрывающемся списке **<select SIEM>** выберите тип SIEM-системы, от которой вы хотите получать данные, и нажмите на кнопку **Next**.

   Откроется окно **Connection Settings**.
3. Выполните следующие действия:
   a. В блоке параметров **Service listens on** выберите вариант **IP and port**.
   b. В поле **IP address** введите `0.0.0.0`.
   c. В поле **Port** введите `9999`.
   d. В нижнем поле **IP address or hostname** укажите `127.0.0.1`.

      Остальные значения оставьте по умолчанию.
   e. Нажмите на кнопку **Next**.

   Откроется окно **Proxy Settings**.
4. Если в вашей организации используется прокси-сервер, укажите параметры соединения с ним. Если нет, оставьте все поля незаполненными и нажмите на кнопку **Next**.

   Откроется окно **Licensing Settings**.
5. В поле **Kaspersky CyberTrace license key** добавьте лицензионный ключ для программы CyberTrace.
6. В поле **Kaspersky Threat Data Feeds certificate** добавьте сертификат, позволяющий скачивать с серверов обновлений списки данных (data feeds), и нажмите на кнопку **Next**.

CyberTrace будет настроен.

► *Чтобы настроить CyberTrace для приема и обработки запросов в веб-интерфейсе программы:*

1. В окне веб-интерфейса программы CyberTrace выберите раздел **Settings** – **Service**.
2. В блоке параметров **Connection Settings** выполните следующие действия:
   a. Выберите вариант **IP and port**.

b. В поле **IP address** введите `0.0.0.0`.

c. В поле **Port** введите `9999`.

3. В блоке параметров **Web interface** в поле **IP address or hostname** введите `127.0.0.1`.
4. В верхней панели инструментов нажмите на кнопку **Restart Feed Service**.
5. Выберите раздел **Settings** – **Events format**.
6. В поле **Alert events format** введите `%Date% alert=%Alert%%RecordContext%`.
7. В поле **Detection events format** введите `Category=%Category%|MatchedIndicator=%MatchedIndicator%%RecordContext%`.
8. В поле **Records context format** введите `|%ParamName%=%ParamValue%`.
9. В поле **Actionable fields context format** введите `%ParamName%:%ParamValue%`.

CyberTrace будет настроен.

После обновления конфигурации CyberTrace требуется перезапустить сервер CyberTrace.

Создание правил обогащения событий

► *Чтобы создать правила обогащения (на стр. 194) событий:*

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Правила обогащения** и в левой части окна выберите или создайте папку (см. раздел "Создание, переименование, перемещение и удаление папок ресурсов" на стр. 130), в которую требуется поместить новый ресурс.

   Отобразится список доступных правил обогащения.

2. Нажмите кнопку **Добавить правило обогащения**, чтобы создать новый ресурс.

   Откроется окно правила обогащения.

3. Укажите параметры правила обогащения:

   a. В поле **Название** введите уникальное имя ресурса. Название должно содержать от 1 до 128 символов Юникода.

   b. В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот ресурс.

   c. В раскрывающемся списке **Тип источника** выберите **cybertrace**.

   d. Укажите **URL** сервера CyberTrace, к которому вы хотите подключиться. Например, *example.domain.com:9999*.

   e. При необходимости укажите в поле **Количество подключений** максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

   f. В поле **Запросов в секунду** введите количество запросов к серверу CyberTrace, которое сможет выполнять KUMA в секунду. Значение по умолчанию: `1000`.

   g. В поле **Время ожидания** укажите время в секундах, в течение которого KUMA должна ожидать ответа от сервера CyberTrace. Событие не будет отправлено в коррелятор, пока не истечет время ожидания или не будет получен ответ. Если ответ получен до истечения времени

ожидания, он добавляется в поле события `TI`, и обработка события продолжается. Значение по умолчанию: `30`.

h. В блоке параметров **Сопоставление** требуется указать поля событий, которые следует отправить в CyberTrace на проверку, а также задать правила сопоставления полей событий KUMA с типами индикаторов CyberTrace:

- В столбце **Поле KUMA** выберите поле, значение которого требуется отправить в CyberTrace.
- В столбце **Индикатор CyberTrace** выберите тип индикатора CyberTrace для каждого выбранного поля:
  - **ip**
  - **url**
  - **hash**

В таблице требуется указать как минимум одну строку. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки  – удалить.

i. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию логирование выключено.

j. При необходимости в поле **Описание** добавьте до 256 символов Юникода, описывающих ресурс.

k. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом правила обогащения. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

4. Нажмите **Сохранить**.

Создано правило обогащения.

Интеграция поиска по индикаторам CyberTrace настроена. Созданное правило обогащения можно добавить к коллектору (см. раздел "Создание коллектора" на стр. 235). Требуется перезапустить (см. раздел "Перезапуск сервиса" на стр. 231) коллекторы KUMA, чтобы применить новые параметры.

Если какие-либо из полей CyberTrace в области деталей события содержат "`[{`" или "`}]`", это означает, что информация из потока данных об угрозах из CyberTrace была обработана некорректно и некоторые данные, возможно, не отображаются. Информацию из потока данных об угрозах можно получить, скопировав из события KUMA значение поля **TI indicator** событий и выполнив поиск по этому значению на портале CyberTrace в разделе индикаторов. Вся информация будет отображаться в разделе CyberTrace **Indicator context**.

Интеграция интерфейса CyberTrace

Вы можете интегрировать веб-интерфейс CyberTrace в веб-интерфейс KUMA. Когда эта интеграция включена, в веб-интерфейсе KUMA появляется раздел **CyberTrace**, в котором предоставляется доступ к веб-интерфейсу CyberTrace. Интеграция настраивается в разделе **Параметры** → **Kaspersky CyberTrace** веб-интерфейса KUMA.

► *Чтобы интегрировать веб-интерфейс CyberTrace в KUMA:*

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите кнопку **Добавить секрет**, чтобы создать новый секрет. Этот ресурс используется для хранения учетных данных для подключения к серверу CyberTrace.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета. Название должно содержать от 1 до 128 символов Юникода.

   b. В раскрывающемся списке **Тенант** выберите, к какому тенанту относится этот ресурс.

   c. В раскрывающемся списке **Тип** выберите **credentials**.

   d. В полях **Пользователь** и **Пароль** введите учетные данные для вашего сервера CyberTrace.

   e. При необходимости в поле **Описание** добавьте до 256 символов Юникода, описывающих ресурс.

4. Нажмите **Сохранить**.

   Учетные данные сервера CyberTrace сохранены и могут использоваться в других ресурсах KUMA.

5. Откройте раздел веб-интерфейс KUMA **Параметры** → **Kaspersky CyberTrace**.

   Откроется окно с параметрами интеграции CyberTrace.

6. Измените необходимые параметры:

   - **Выключено** – снимите этот флажок, если хотите включить интеграцию веб-интерфейса CyberTrace в веб-интерфейс KUMA.
   - **Адрес сервера** (обязательно) – введите адрес сервера CyberTrace в формате `hostname:port`.
   - **Порт** (обязательно) – введите порт сервера CyberTrace.

7. В раскрывающемся списке **Секрет** выберите ресурс секрета, который вы создали ранее.

8. Нажмите **Сохранить**.

CyberTrace теперь интегрирован с KUMA: раздел **CyberTrace** отображается в веб-интерфейсе KUMA.

Если для работы в веб-интерфейсе программы вы используете браузер Mozilla Firefox, данные в разделе **CyberTrace** могут не отображаться. В таком случае очистите кеш браузера и настройте отображение данных (см. ниже).

Чтобы настроить отображение данных в разделе **CyberTrace**:

1. В строке браузера введите FQDN веб-интерфейса KUMA с номером порта 7222: https://kuma.example.com:7222. Не рекомендуется в качестве адреса сервера указывать IP-адрес.

   Отобразится окно с предупреждением о вероятной угрозе безопасности.

2. Нажмите на кнопку **Подробнее**.

3. В нижней части окна нажмите на кнопку **Принять риск и продолжить**.

Для URL-адреса веб-интерфейса KUMA будет создано исключение.

4. В строке браузера введите URL-адрес веб-интерфейса KUMA с номером порта 7220.
5. Перейдите в раздел **CyberTrace**.

Данные отобразятся в разделе.

Обновление списка запрещенных объектов CyberTrace (Internal TI)

Если веб-интерфейс CyberTrace интегрирован в веб-интерфейс KUMA, можно обновлять список запрещенных объектов CyberTrace или **Internal TI** данными из событий KUMA.

► *Чтобы обновить Internal TI в CyberTrace:*

1. Откройте область деталей события в таблице событий, окне алертов или окне корреляционного события и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла.

   Откроется контекстное меню.

2. Выберите **Добавить в Internal TI CyberTrace**.

Выбранный объект добавлен в список запрещенных объектов в CyberTrace.

kaspersky

Интеграция с Kaspersky Threat Intelligence Portal

Портал Kaspersky Threat Intelligence Portal https://tip.kaspersky.com/help/Doc_data/ThreatLookup.htm объединяет все знания Лаборатории Касперского о киберугрозах и их взаимосвязи в единую мощную веб-службу. При интеграции с KUMA он помогает пользователям KUMA быстрее принимать обоснованные решения, предоставляя им данные о веб-адресах, доменах, IP-адресах, данных WHOIS / DNS.

Доступ к Kaspersky Threat Intelligence Portal предоставляется на платной основе. Лицензионные сертификаты создаются специалистами Лаборатории Касперского. Чтобы получить сертификат для Kaspersky Threat Intelligence Portal, вашему персональному техническому менеджеру Лаборатории Касперского.

В этом разделе

Инициализация интеграции 87

Запрос данных от Kaspersky Threat Intelligence Portal 88

Просмотр данных от Kaspersky Threat Intelligence Portal 89

Обновление данных от Kaspersky Threat Intelligence Portal 89

Инициализация интеграции

► *Чтобы интегрировать Kaspersky Threat Intelligence Portal в KUMA:*

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов (см. раздел "Секреты" на стр. 226).

2. Нажмите кнопку **Добавить секрет**, чтобы создать новый секрет. Этот ресурс используется для хранения данных вашей учетной записи Kaspersky Threat Intelligence Portal.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** выберите имя для добавляемого секрета.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.

   c. В раскрывающемся списке **Тип** выберите **ktl**.

   d. В полях **Пользователь** и **Пароль** введите данные своей учетной записи Kaspersky Threat Intelligence Portal.

   e. В поле **Описание** можно добавить описание секрета.

4. Загрузите ключ сертификата Kaspersky Threat Intelligence Portal:

   a. Нажмите **Загрузить PFX** и выберите PFX-файл с сертификатом.

      Имя выбранного файла отображается справа от кнопки **Загрузить PFX**.

b. В поле **Пароль PFX** введите пароль для PFX-файла.

5. Нажмите **Сохранить**.

   Ваши учетные данные Kaspersky Threat Intelligence Portal сохранены и могут использоваться в других ресурсах KUMA.

6. В разделе **Параметры** веб-интерфейса KUMA откройте закладку **Kaspersky Threat Lookup**.

   Отобразится список доступных подключений.

7. Убедитесь, что флажок **Выключено** снят.

8. В раскрывающемся списке **Секрет** выберите ресурс секрета, который вы создали ранее.

   Можно создать новый секрет (см. раздел "Секреты" на стр. 226), нажав на кнопку со значком плюса. Созданный секрет будет сохранен в разделе **Ресурсы → Секреты**.

9. При необходимости в раскрывающемся списке **Прокси-сервер** выберите ресурс прокси-сервера.

10. Нажмите **Сохранить**.

Процесс интеграции Kaspersky Threat Intelligence Portal с KUMA завершен.

После интеграции Kaspersky Threat Intelligence Portal и KUMA в области деталей события (см. раздел "Просмотр информации о событии" на стр. 353) можно запрашивать сведения о хостах, доменах, URL-адресах, IP-адресах и хешах файлов (MD5, SHA1, SHA256).

Запрос данных от Kaspersky Threat Intelligence Portal

► *Чтобы запросить данные от Kaspersky Threat Intelligence Portal:*

1. Откройте область деталей (см. раздел "Просмотр информации о событии" на стр. 353) события в таблице событий, окне алертов (см. раздел "Просмотр информации об алерте" на стр. 333) или окне корреляционного события (см. раздел "Открытие окна корреляционного события" на стр. 357) и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла.

   В правой части экрана откроется область **Обогащение Threat Lookup**.

2. Установите флажки рядом с типами данных, которые нужно запросить.

   Если ни один из флажков не установлен, запрашиваются все данные.

3. В поле **Максимальное количество записей в каждой группе данных** введите количество записей для выбранного типа данных, которое вы хотите получить. Значение по умолчанию: `10`.

4. Нажмите **Запрос**.

Задача *ktl* создана. По ее завершении события дополняются данными из Kaspersky Threat Intelligence Portal, которые можно просмотреть (см. раздел "Просмотр данных от Kaspersky Threat Intelligence Portal" на стр. 89) в таблице событий, окне алерта или окне корреляционного события.

kaspersky

Просмотр данных от Kaspersky Threat Intelligence Portal

► *Чтобы просмотреть данные из Kaspersky Threat Intelligence Portal,*

Откройте область деталей события (см. раздел "Просмотр информации о событии" на стр. 353) в таблице событий, окне алертов (см. раздел "Просмотр информации об алерте" на стр. 333) или окне корреляционного события (см. раздел "Открытие окна корреляционного события" на стр. 357) и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла, для которого вы ранее запрашивали данные (см. раздел "Запрос данных от Kaspersky Threat Intelligence Portal" на стр. 88) от Kaspersky Threat Intelligence Portal.

В правой части экрана откроется область деталей (см. раздел "Просмотр информации о событии" на стр. 353) с данными из Kaspersky Threat Intelligence Portal с указанием времени последнего обновления этих данных.

Информация, полученная от Kaspersky Threat Intelligence Portal, кешируется. Если нажать на домен, веб-адрес, IP-адрес или хеш файла в области деталей события, для которого у KUMA уже есть доступная информация, вместо окна **Обогащение Threat Lookup** отобразятся данные из Kaspersky Threat Intelligence Portal https://tip.kaspersky.com/help/Doc_data/ThreatLookup.htm с указанием времени их получения. Эти данные можно обновить (см. раздел "Обновление данных от Kaspersky Threat Intelligence Portal" на стр. 89).

Обновление данных от Kaspersky Threat Intelligence Portal

► *Чтобы обновить данные, полученные от Kaspersky Threat Intelligence Portal:*

1. Откройте область деталей события (см. раздел "Просмотр информации о событии" на стр. 353) в таблице событий, окне алертов (см. раздел "Просмотр информации об алерте" на стр. 333) или окне корреляционного события (см. раздел "Открытие окна корреляционного события" на стр. 357) и нажмите ссылку на домене, веб-адресе, IP-адресе или хеш-коде файла, для которого вы ранее запрашивали данные (см. раздел "Запрос данных от Kaspersky Threat Intelligence Portal" на стр. 88) от Kaspersky Threat Intelligence Portal.
2. Нажмите **Обновить** в области деталей события с данными, полученными с портала Kaspersky Threat Intelligence Portal.

   В правой части экрана откроется область **Обогащение Threat Lookup**.
3. Установите флажки рядом с типами данных, которые вы хотите запросить.

   Если ни один из флажков не установлен, запрашиваются все данные.
4. В поле **Максимальное количество записей в каждой группе данных** введите количество записей для выбранного типа данных, которое вы хотите получить. Значение по умолчанию: `10`.
5. Нажмите **Обновить**.

   Создается задача *KTL* и запрашиваются новые данные, полученные из Kaspersky Threat Intelligence Portal.
6. Закройте окно **Обогащение Threat Lookup** и область подробной информации о KTL.
7. Откройте область подробной информации о событии из таблицы событий, окна алертов или окна корреляционных событий и перейдите по ссылке, соответствующей домену, веб-адресу, IP-адресу или хешу файла, для которого вы обновили информацию на Kaspersky Threat Intelligence Portal, и выберите **Показать информацию из Threat Lookup**.

В правой части экрана откроется область деталей с данными из Kaspersky Threat Intelligence Portal с указанием времени.

kaspersky

Интеграция с R-Vision Incident Response Platform

R-Vision Incident Response Platform (далее R-Vision IRP) – это программная платформа для автоматизации мониторинга, обработки и реагирования на инциденты информационной безопасности. Она объединяет данные о киберугрозах из различных источников в единую базу данных для дальнейшего анализа и расследования, что позволяет облегчить реагирование на инциденты.

R-Vision IRP можно интегрировать с KUMA. Когда интеграция включена, создание алерта (см. раздел "Об алертах" на стр. 27) в KUMA приводит к созданию инцидента в R-Vision IRP. Алерт KUMA и инцидент R-Vision IRP взаимосвязаны (см. раздел "Работа с алертами с помощью R-Vision IRP" на стр. 100): при обновлении статуса инцидента в R-Vision IRP статус соответствующего алерта KUMA также меняется.

Интеграция R-Vision IRP и KUMA настраивается в обоих приложениях.

Таблица 4. Сопоставление полей алерта KUMA и инцидента R-Vision IRP при передаче данных по API

Поле алерта KUMA	Поле инцидента R-Vision IRP
`firstSeen`	`detection`
`priority`	`level`
`correlationRuleName`	`description`
`events` (в виде json-файла)	`files`

В этом разделе

Настройка интеграции в KUMA 90

Настройка интеграции в R-Vision IRP 92

Работа с алертами с помощью R-Vision IRP 100

Настройка интеграции в KUMA

В этом разделе описывается интеграция KUMA с R-Vision IRP на стороне KUMA.

Интеграция в KUMA настраивается в разделе веб-интерфейса KUMA **Параметры** → **IRP / SOAR**.

► *Чтобы настроить интеграцию с R-Vision IRP:*

1. Откройте раздел веб-интерфейса KUMA **Ресурсы** → **Секреты**.

   Отобразится список доступных секретов.

2. Нажмите кнопку **Добавить секрет**, чтобы создать новый секрет. Этот ресурс будет использоваться для хранения токена для API-запросов в R-Vision IRP.

   Откроется окно секрета.

3. Введите данные секрета:

   a. В поле **Название** укажите имя для добавляемого секрета. Длина названия должна быть от 1 до 128 символов Юникода.

   b. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый ресурс.

   c. В раскрывающемся списке **Тип** выберите **token**.

   d. В поле **Токен** введите свой API-токен для R-Vision IRP.

      Токен можно узнать в веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Общие** → **API**.

   e. При необходимости в поле **Описание** добавьте описание секрета. Длина описания должна быть от 1 до 256 символов Юникода.

4. Нажмите **Сохранить**.

   API-токен для R-Vision IRP сохранен и теперь может использоваться в других ресурсах KUMA.

5. Откройте раздел веб-интерфейса KUMA **Параметры** → **IRP / SOAR**.

   Откроется окно с параметрами интеграции R-Vision IRP.

6. Измените необходимые параметры:

   - **Выключено** – установите этот флажок, если хотите выключить интеграцию R-Vision IRP с KUMA.
   - В раскрывающемся списке **Секрет** выберите ресурс секрета, созданный ранее.

     Можно создать новый секрет (см. раздел "Секреты" на стр. 226), нажав на кнопку со значком плюса. Созданный секрет будет сохранен в разделе **Ресурсы** → **Секреты**.
   - **URL** (обязательно) – URL хоста сервера R-Vision IRP.
   - **Название поля для размещения идентификаторов алертов KUMA** (обязательно) – имя поля R-Vision IRP, в которое будет записываться идентификатор алерта KUMA.
   - **Название поля для размещения URL алертов KUMA** (обязательно) – имя поля R-Vision IRP, в которое будет помещаться ссылка на алерт KUMA.
   - **Категория** (обязательно) – категория алерта R-Vision IRP, который создается при получении данных об алерте от KUMA.
   - **Поля событий KUMA для отправки в IRP / SOAR** (обязательно) – раскрывающийся список для выбора полей событий (см. раздел "Модель данных нормализованного события" на стр. 471) KUMA, которые следует отправлять в R-Vision IRP.
   - Группа настроек **Уровень важности** (обязательно) – используется для сопоставления значений уровня важности (см. раздел "Об уровне важности" на стр. 29) KUMA со значениями уровня важности R-Vision IRP.

7. Нажмите **Сохранить**.

В KUMA теперь настроена интеграция с R-Vision IRP. Если интеграция также настроена в R-Vision IRP (см. раздел "Настройка интеграции в R-Vision IRP" на стр. 92), при появлении алертов в KUMA информация о них будет отправляться в R-Vision IRP для создания инцидента. В разделе **Информация об алерте** в веб-интерфейсе KUMA отображается ссылка в R-Vision IRP.

Если вы работаете с несколькими тенантами (см. раздел "Работа с тенантами" на стр. 301) и хотите интегрироваться с R-Vision IRP, названия тенантов должны соответствовать коротким названиям компаний в R-Vision IRP.

Настройка интеграции в R-Vision IRP

В этом разделе описывается интеграция KUMA с R-Vision IRP на стороне R-Vision IRP.

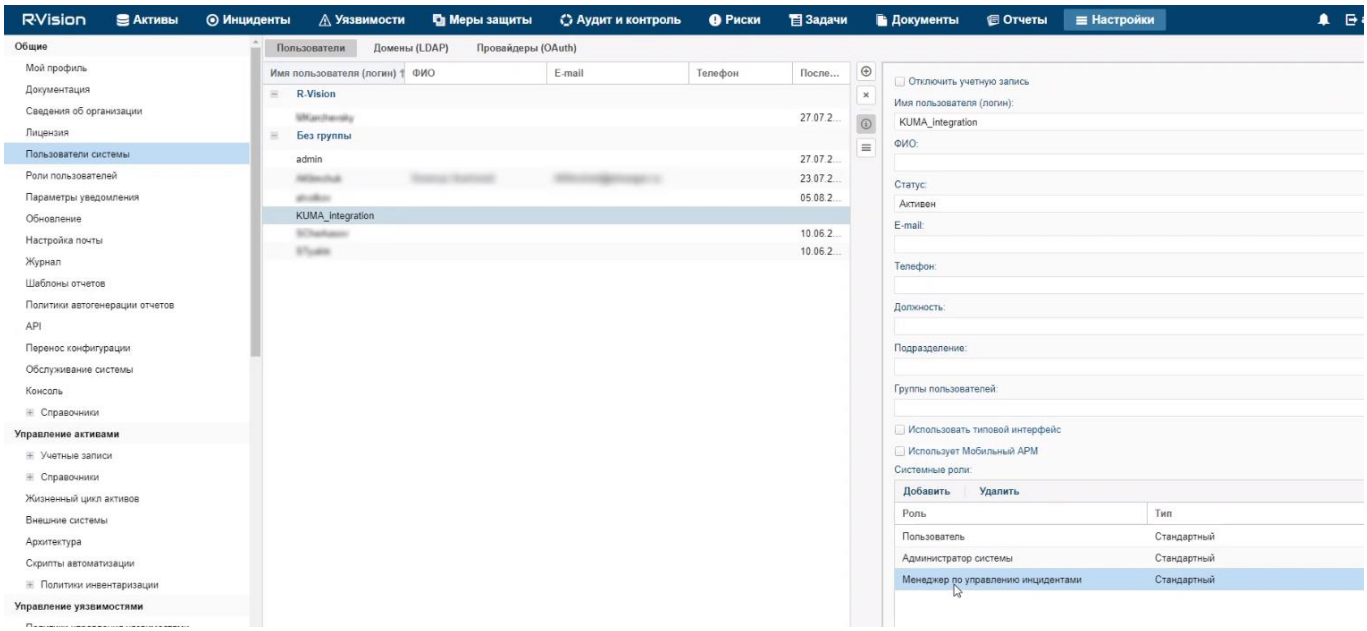
Интеграция в R-Vision IRP настраивается в разделе **Настройки** веб-интерфейса R-Vision IRP. Подробнее о настройке R-Vision IRP см. в документации этой программы.

Настройка интеграции с KUMA состоит из следующих этапов:

- Настройка роли пользователя R-Vision IRP

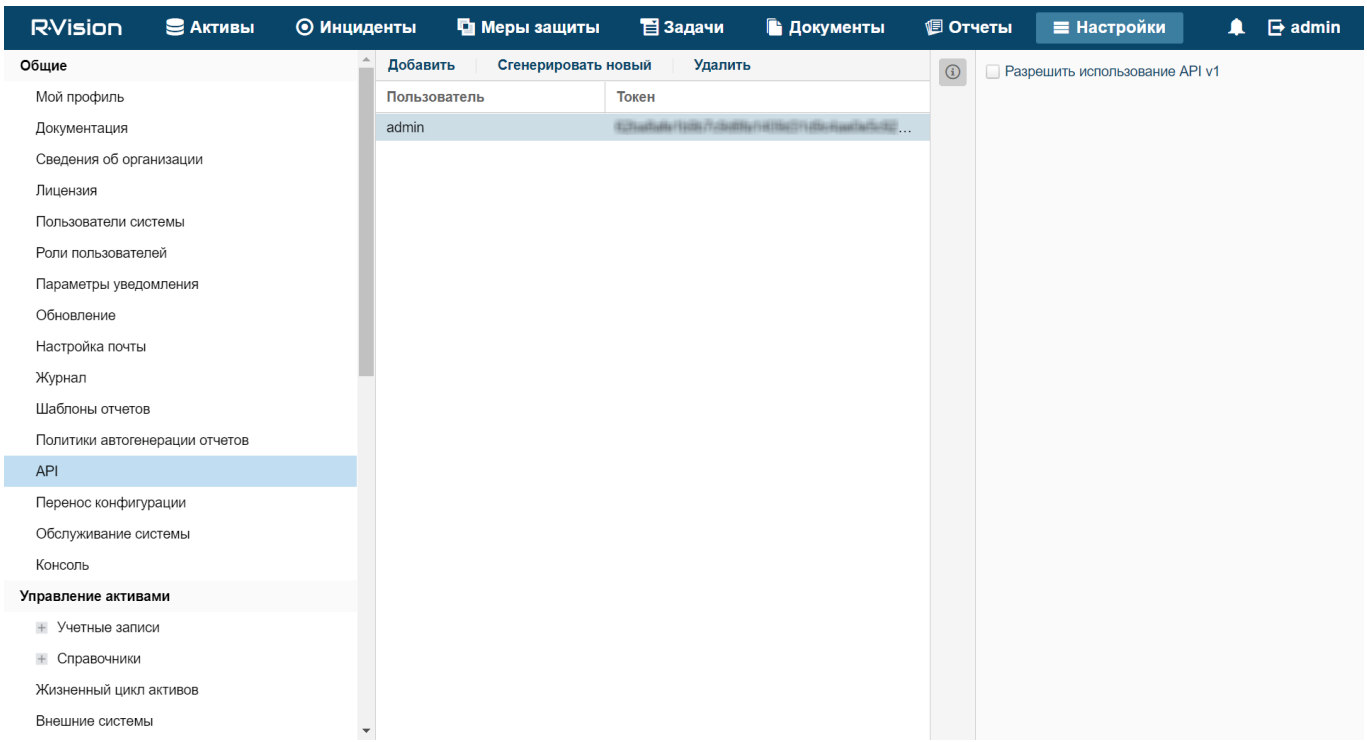
  1. Присвойте используемому для интеграции пользователю R-Vision IRP системную роль **Менеджер по управлению инцидентами**. Роль можно присвоить в веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Общие** → **Пользователи системы**, выбрав нужного пользователя. Роль добавляется в блоке параметров **Системные роли**.

     Пользователь R-Vision IRP с ролью Менеджер по управлению инцидентами



  2. Убедитесь, что API-токен используемого для интеграции пользователя R-Vision IRP указан в секрете в веб-интерфейсе KUMA (см. раздел "Настройка интеграции в KUMA" на стр. 90). Токен отображается в веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Общие** → **API**.

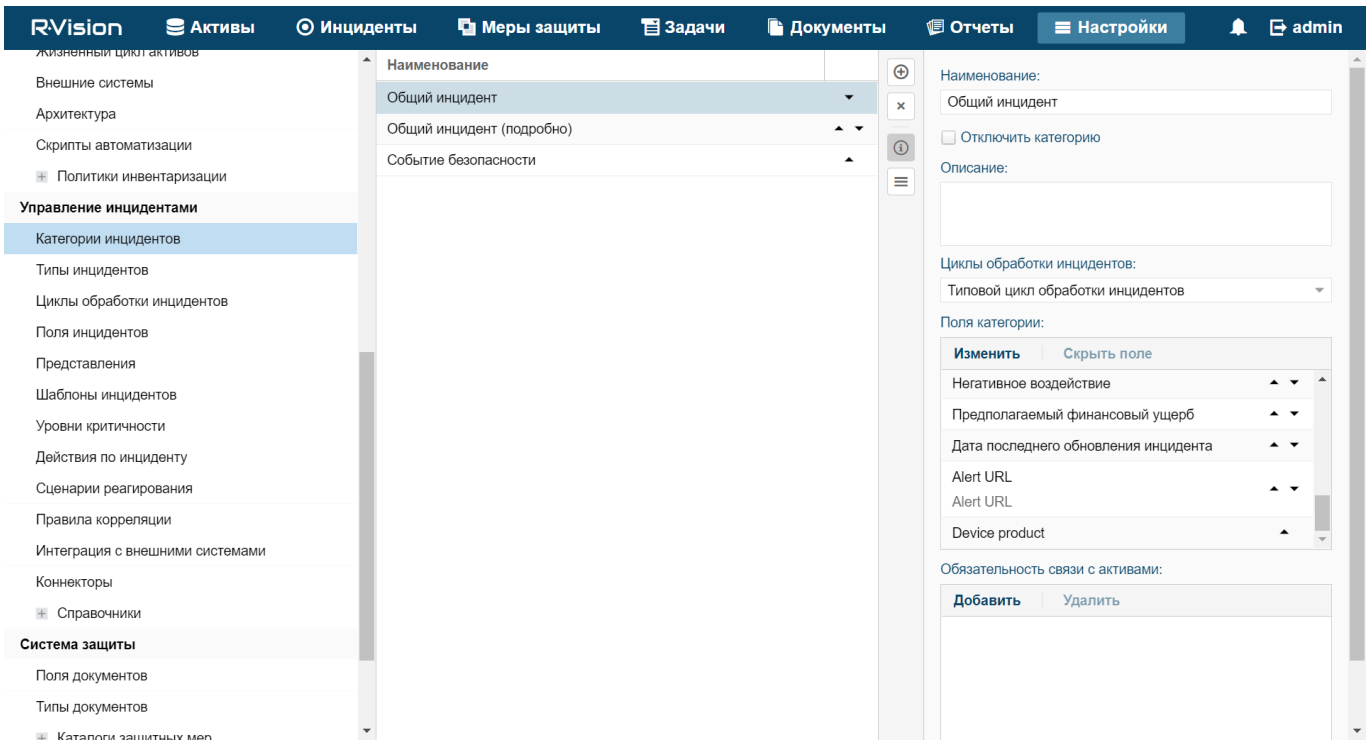
API-токен в R-Vision IRP



- Настройка полей инцидентов R-Vision IRP и алертов KUMA

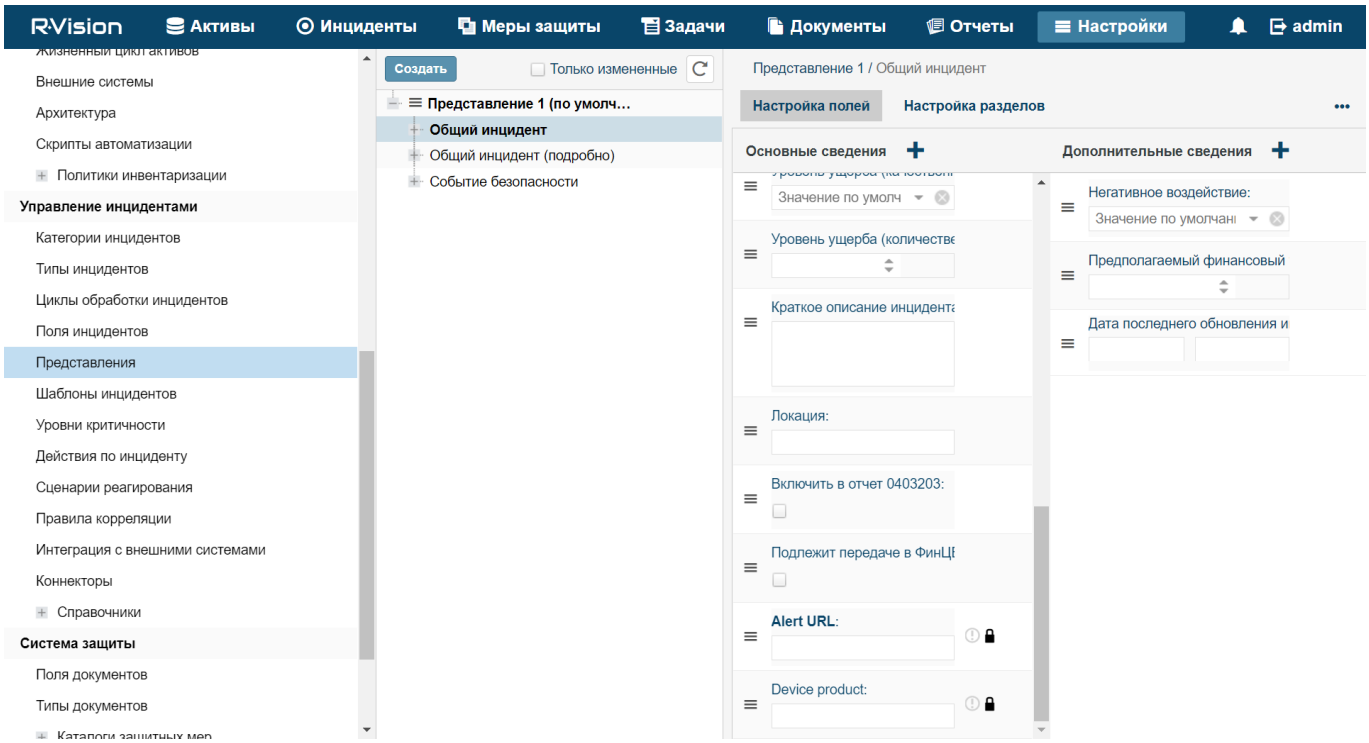
  1. Добавьте поля инцидента ALERT_ID и ALERT_URL (см. раздел "Добавление полей инцидента ALERT_ID и ALERT_URL" на стр. 95).
  2. Настройте категорию инцидентов R-Vision IRP, создаваемых по алертам KUMA. Это можно сделать в веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Категории инцидентов**. Добавьте новую или измените существующую категорию инцидентов, указав в блоке параметров **Поля категорий** созданные ранее поля инцидентов `Alert ID` и `Alert URL`. Поле `Alert ID` можно сделать скрытым.

Категории инцидентов с данными из алертов KUMA



3. Запретите редактирование ранее созданных полей инцидентов `Alert ID` и `Alert URL`. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Представления** выберите категорию инцидентов R-Vision IRP, которые будут создаваться по алертам KUMA, и установите рядом с полями `Alert ID` и `Alert URL` значок замка.

   Поле Alert URL недоступно для редактирования



- Создание коллектора и коннектора в R-Vision IRP

  1. Создайте коллектор R-Vision IRP для взаимодействия с KUMA (см. раздел "Создание коллектора в R-Vision IRP" на стр. 97).
  2. Создайте и настройте коннектор R-Vision IRP для отправки в KUMA API-запросов на закрытие алертов (см. раздел "Создание коннектора в R-Vision IRP" на стр. 97).

- Создание правила на закрытие алерта в KUMA

  Создайте правило на отправку в KUMA запроса на закрытие алерта (см. раздел "Создание правила на закрытие алерта в KUMA при закрытии инцидента в R-Vision IRP" на стр. 99) при закрытии инцидента в R-Vision IRP.

В R-Vision IRP теперь настроена интеграция с KUMA. Если интеграция также настроена в KUMA (см. раздел "Настройка интеграции в KUMA" на стр. 90), при появлении алертов в KUMA информация о них будет отправляться в R-Vision IRP для создания инцидента. В разделе **Информация об алерте** в веб-интерфейсе KUMA отображается ссылка в R-Vision IRP.

В этом разделе

Добавление полей инцидента ALERT_ID и ALERT_URL 95

Создание коллектора в R-Vision IRP 97

Создание коннектора в R-Vision IRP 97

Создание правила на закрытие алерта в KUMA при закрытии инцидента в R-Vision IRP 99

Добавление полей инцидента ALERT_ID и ALERT_URL

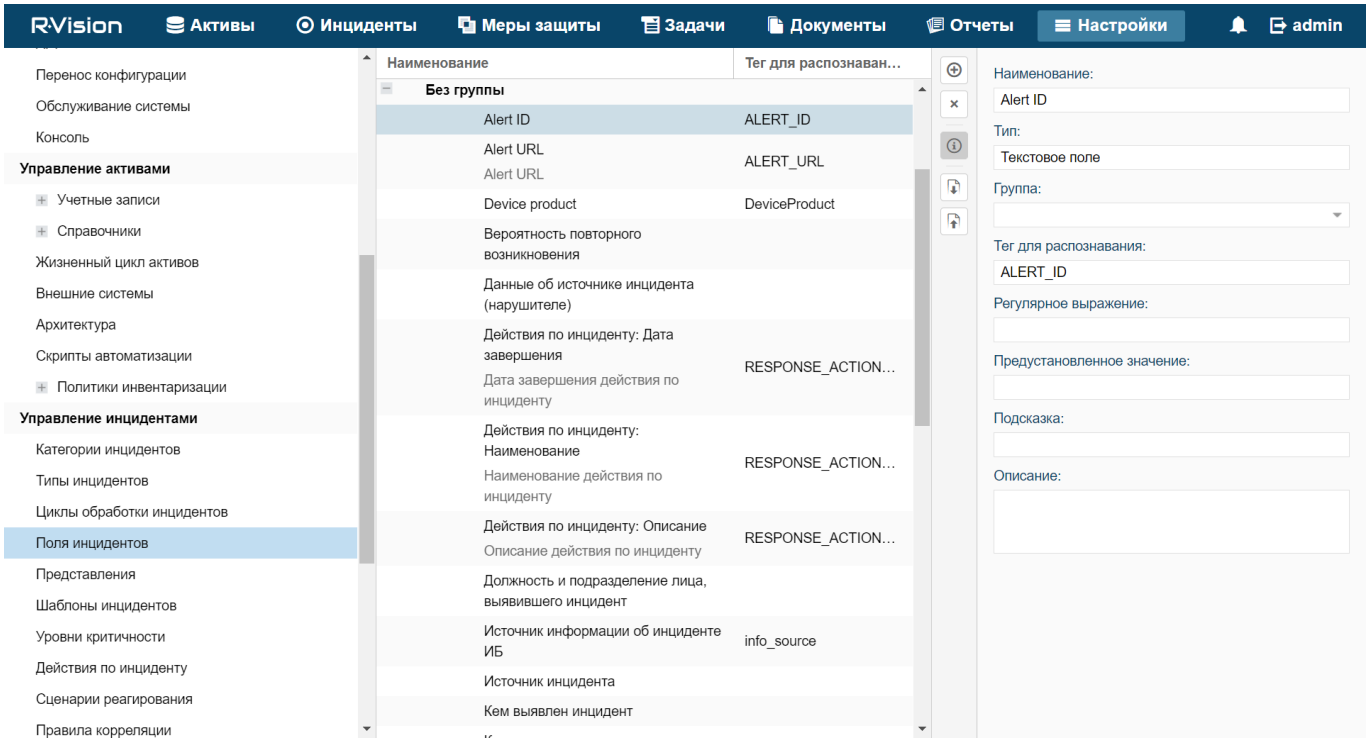
► *Чтобы добавить в R-Vision IRP поле инцидента ALERT_ID:*

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Поля инцидентов** выберите группу полей **Без группы**.
2. Нажмите на значок плюса в правой части экрана.

   В правой части экрана отобразится область параметров создаваемого поля инцидента.
3. В поле **Наименование** введите название поля, например `Alert ID`.
4. В раскрывающемся списке **Тип** выберите **Текстовое поле**.
5. В поле **Тег для распознавания** введите `ALERT_ID`.

Поле ALERT_ID добавлено в инцидент R-Vision IRP.

Поле ALERT_ID



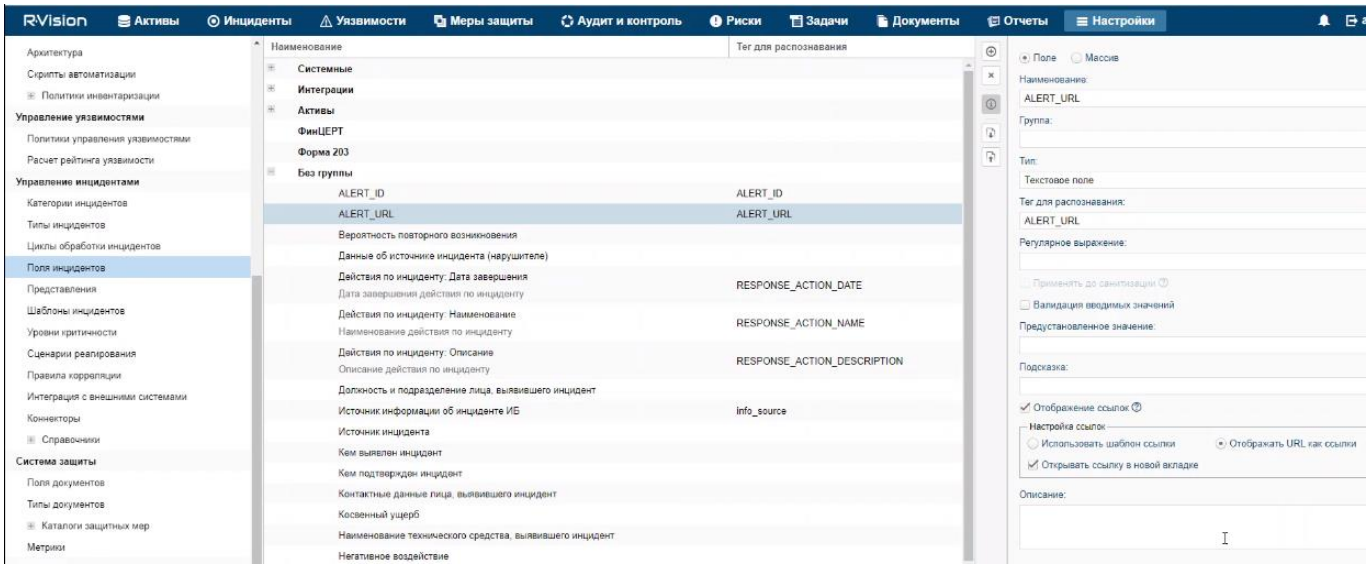
► *Чтобы добавить в R-Vision IRP поле инцидента ALERT_URL:*

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Поля инцидентов** выберите группу полей **Без группы**.
2. Нажмите на значок плюса в правой части экрана.

   В правой части экрана отобразится область параметров создаваемого поля инцидента.
3. В поле **Наименование** введите название поля, например `Alert URL`.
4. В раскрывающемся списке **Тип** выберите **Текстовое поле**.
5. В поле **Тег для распознавания** введите `ALERT_URL`.
6. Установите флажки **Отображение ссылок** и **Отображать URL как ссылки**.

Поле ALERT_URL добавлено в инцидент R-Vision IRP.

Поле ALERT_URL



При необходимости аналогичным образом можно настроить отображение других данных из алерта KUMA в инциденте R-Vision IRP.

Создание коллектора в R-Vision IRP

► *Чтобы создать коллектор в R-Vision IRP:*

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Asset Management** → **System components** нажмите на значок плюса.
2. В поле **Название** укажите название коллектора (например, `Main collector`).
3. В поле **Адрес коллектора** введите IP-адрес или название хоста, где установлена R-Vision IRP (например, `127.0.0.1`).
4. В поле **Порт** введите значение `3001`.
5. Установите флажки **Default collector** и **Use for reaction**.
6. Нажмите **Добавить**.

Коллектор R-Vision IRP создан.

Создание коннектора в R-Vision IRP

► *Чтобы создать коннектор в R-Vision IRP:*

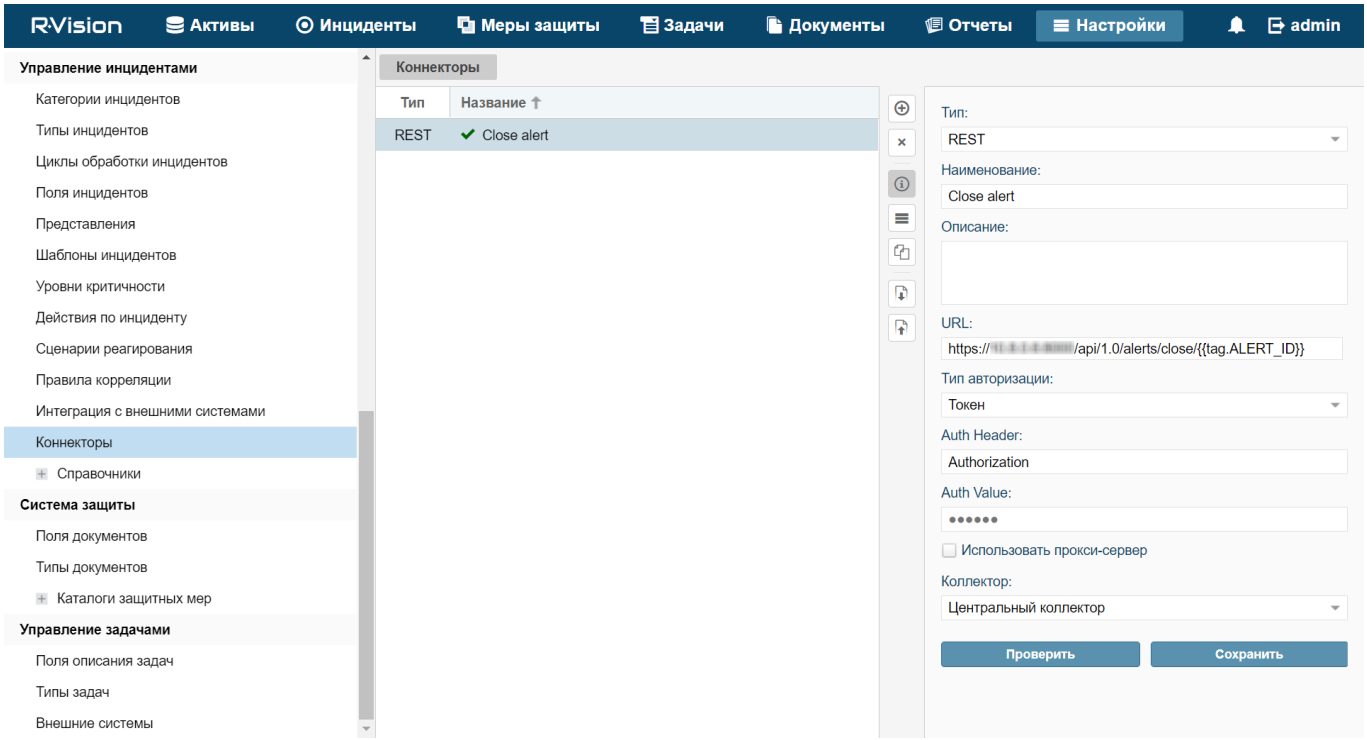
1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Коннекторы** нажмите на значок плюса.
2. В раскрывающемся списке **Тип** выберите **REST**.
3. В поле **Название** укажите название коннектора, например, `KUMA`.
4. В поле **URL** введите API-запрос (см. раздел "REST API" на стр. 413) на закрытие алерта (см. раздел "Закрытие алертов" на стр. 428) в формате `<FDQN сервера Ядра KUMA>:<Порт, используемый для API-запросов (по умолчанию 7223)>/api/v1/alerts/close`.

Пример: `https://kuma-example.com:7223/api/v1/alerts/close`

5. В раскрывающемся списке **Тип авторизации** выберите **Токен**.
6. В поле **Auth header** введите значение `Authorization`.
7. В поле **Auth value** введите токен главного администратора KUMA.

   Токен главного администратора KUMA можно получить в веб-интерфейсе KUMA в разделе **Параметры** → **Пользователи**.
8. В раскрывающемся списке **Коллектор** выберите ранее созданный коллектор (см. раздел "Создание коллектора в R-Vision IRP" на стр. 97).
9. Нажмите **Сохранить**.

Коннектор R-Vision IRP создан.



После того как коннектор создан, требуется настроить отправку API-запросов на закрытие алертов в KUMA.

► *Чтобы настроить отправку API-запросов в R-Vision IRP:*

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Коннекторы** откройте созданный коннектор для редактирования.
2. В раскрывающемся списке типа запросов выберите **POST**.
3. В поле **Params** введите API-запрос (см. раздел "REST API" на стр. 413) на закрытие алерта (см. раздел "Закрытие алертов" на стр. 428) в формате `<FDQN сервера Ядра KUMA>:<Порт, используемый для API-запросов (по умолчанию 7223)>/api/v1/alerts/close`.

   Пример, `https://kuma-example.com:7223/api/v1/alerts/close`
4. На закладке **HEADERS** добавьте следующие ключи и их значения:
   - Ключ `Content-Type`; значение: `application/json`.

- Ключ `Authorization`; значение: `Bearer <токен главного администратора KUMA>`.

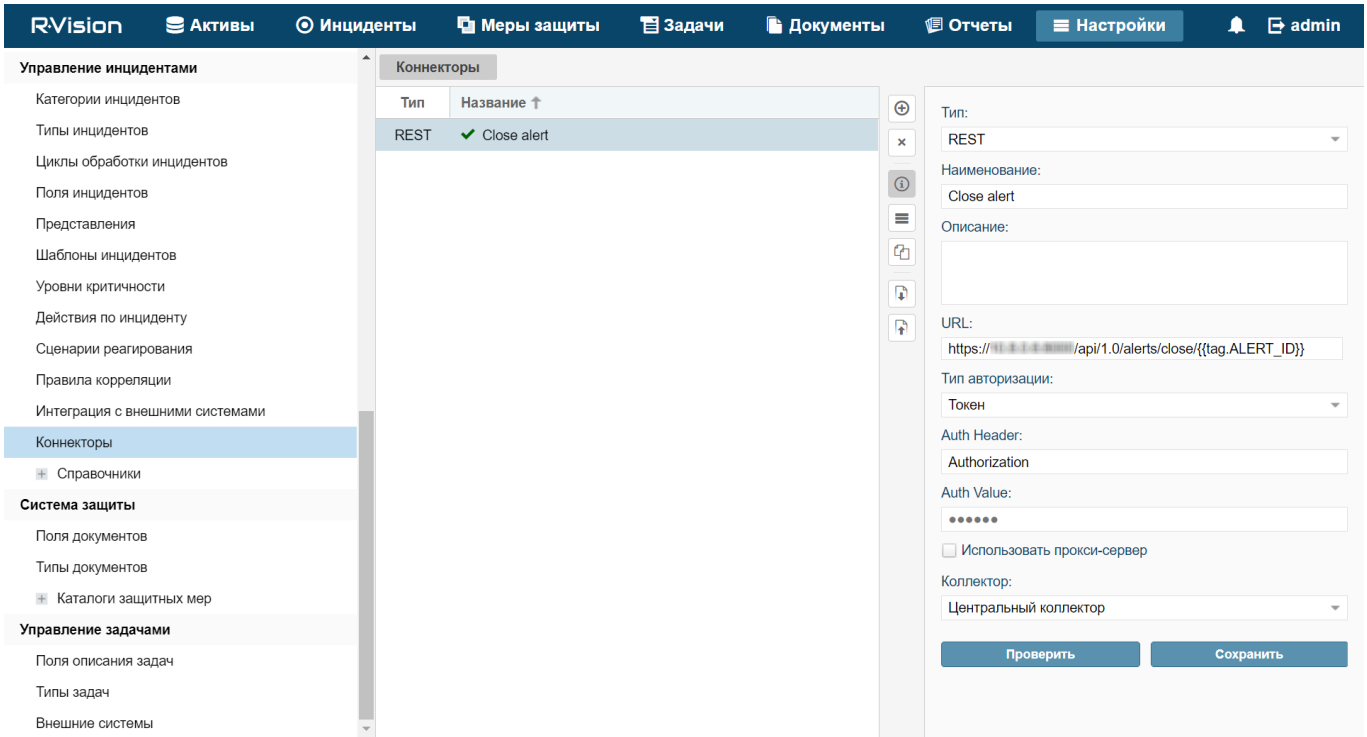
  Токен главного администратора KUMA можно получить в веб-интерфейсе KUMA в разделе **Параметры** → **Пользователи**.

5. На закладке **BODY** → **Raw** введите содержание тела API-запроса (см. раздел "Закрытие алертов" на стр. 428):

```
{
    "id":"{{tag.ALERT_ID}}"
    "reason":"<комментарий, который будет добавлен к алерту в KUMA при закрытии. Например, Responded to alert from R-Vision>"
}
```

6. Нажмите **Сохранить**.

Коннектор R-Vision IRP настроен.



Создание правила на закрытие алерта в KUMA при закрытии инцидента в R-Vision IRP

► *Чтобы создать правило на отправку в KUMA запроса на закрытие алерта при закрытии инцидента в R-Vision IRP:*

1. В веб-интерфейсе R-Vision IRP в разделе **Настройки** → **Управление инцидентами** → **Сценарии реагирования** нажмите на значок плюса.
2. В поле **Название** введите название создаваемого правила, например `Close alert`.
3. В раскрывающемся списке **Группа** выберите **Все сценарии**.

4. В блоке параметров **Критерии автоматического запуска** нажмите **Добавить** и в открывшемся окне введите условия срабатывания правила:

   a. В раскрывающемся списке **Тип** выберите **Значение поля**.

   b. В раскрывающемся списке **Поле** выберите **Статус инцидента**.

   c. Установите флажок напротив статуса **Закрыт**.

   d. Нажмите **Добавить**.

   Условия срабатывания правила добавлены. Правило будет срабатывать при закрытии инцидента.

5. В блоке параметров **Действия по инциденту** нажмите **Добавить** → **Run connector** и в открывшемся окне выберите коннектор, который следует выполнить при срабатывании правила:

   a. В раскрывающемся списке **Коннектор** выберите ранее созданный коннектор (см. раздел "Создание коннектора в R-Vision IRP" на стр. 97).

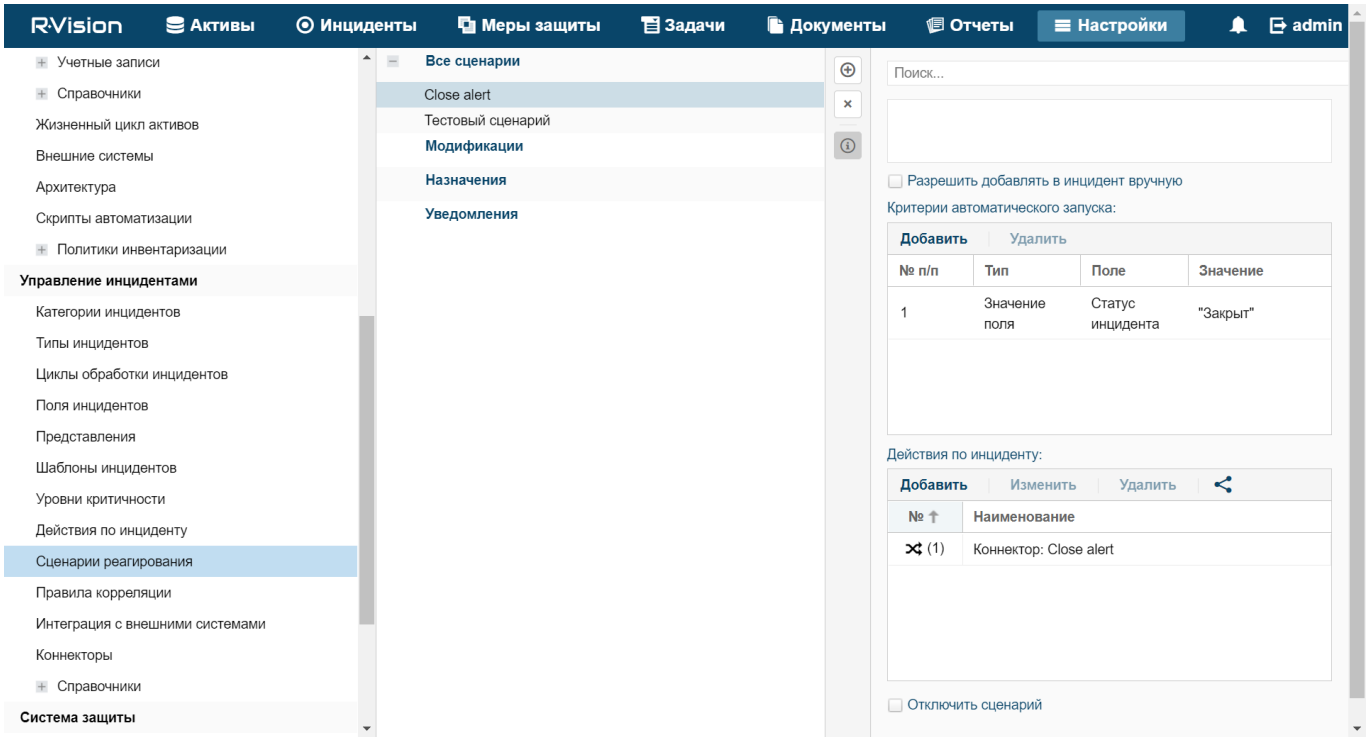
   b. Нажмите **Добавить**.

   Коннектор добавлен в правило.

6. Нажмите **Добавить**.

Правило на отправку в KUMA запроса на закрытие алерта при закрытии инцидента в R-Vision IRP создано.

Правило сценария R-Vision IRP



Работа с алертами с помощью R-Vision IRP

После того как интеграция KUMA и R-Vision IRP настроена, данные об алертах (см. раздел "Об алертах" на стр. 27) KUMA поступают в R-Vision IRP. Изменение параметров алертов в KUMA отражается в R-Vision

IRP. Изменение статусов алертов в KUMA или R-Vision IRP, кроме закрытия, также отражается в другой системе.

Если настроена интеграция KUMA и R-Vision IRP, вы можете выполнять следующее:

- Передавать сведения о киберугрозах из KUMA в R-Vision IRP

  Из KUMA в R-Vision IRP автоматически передаются сведения об обнаруженных алертах. При этом в R-Vision IRP создается инцидент.

  В R-Vision IRP передаются следующие сведения об алерте KUMA:

  - идентификатор;
  - название;
  - статус;
  - дата первого события, относящегося к алерту;
  - дата последнего обнаружения, относящегося к алерту;
  - имя учетной записи или адрес электронной почты специалиста по безопасности, назначенного для обработки алерта;
  - уровень важности алерта;
  - категория инцидента R-Vision IRP, соответствующего алерту KUMA;
  - иерархический список событий, связанных с алертом;
  - список активов, как внутренних, так и внешних, связанных с алертом;
  - список пользователей, связанных с алертом;
  - журнал изменений алерта;
  - ссылка на алерт в KUMA.
- Расследовать киберугрозы в KUMA

  Первоначальная обработка алерта производится в KUMA. Специалист по безопасности может уточнять и менять любые параметры алерта, кроме идентификатора и названия. Внесенные изменения отражаются в карточке инцидента R-Vision IRP.

  Если киберугроза признается ложной и алерт закрывается в KUMA, соответствующий ему инцидент R-Vision IRP также автоматически закрывается.
- Закрывать инциденты в R-Vision IRP

  После необходимых работ по инциденту и фиксации хода расследования в R-Vision IRP инцидент закрывается. Соответствующий алерт KUMA также автоматически закрывается.
- Открывать ранее закрытые инциденты

  Если в процессе мониторинга обнаруживается, что инцидент не был решен полностью или обнаруживаются дополнительные сведения, такой инцидент снова открывается в R-Vision IRP. При этом в KUMA алерт остается закрытым.

  Специалист по безопасности с помощью ссылки может перейти из инцидента R-Vision IRP в соответствующий алерт в KUMA и изменить его параметры, кроме идентификатора, названия и статуса. Внесенные изменения отражаются в карточке инцидента R-Vision IRP.

  Дальнейший анализ происходит в R-Vision IRP. Когда расследование завершено и инцидент в R-Vision IRP снова закрыт, статус соответствующего алерта в KUMA не меняется: алерт остается закрытым.

- Запрашивать дополнительные сведения из системы-источника в рамках сценария реагирования или вручную

  Если в процессе анализа в R-Vision IRP возникает необходимость получить дополнительные сведения из KUMA, в R-Vision IRP можно сформировать требуемый поисковый запрос (например, запрос телеметрии, репутации, сведений о хосте) к KUMA. Запрос передается с помощью REST API KUMA (см. раздел "REST API" на стр. 413), ответ фиксируется в карточке инцидента R-Vision IRP для дальнейшего анализа и вывода в отчет.

  Действия выполняются в такой же последовательности на этапе автоматической обработки, если нет возможности сразу сохранить всю информацию по инциденту при импорте.

Интеграция с Active Directory

KUMA можно интегрировать с используемыми в вашей организации службами Active Directory®.

Вы можете настроить подключение к службе каталогов Active Directory по протоколу LDAP (см. раздел "Подключение по протоколу LDAP" на стр. 102). Это позволит использовать информацию из Active Directory в правилах корреляции для обогащения событий и алертов, а также для аналитики.

Если вы настроите соединение с сервером контроллера домена, это позволит использовать доменную авторизацию (см. раздел "Авторизация с помощью доменных учетных записей" на стр. 110). В этом случае вы сможете привязать группы пользователей из Active Directory к фильтрам ролей KUMA. Пользователи, принадлежащие к этим группам, смогут войти в веб-интерфейс KUMA, используя свои доменные учетные данные, и получат доступ к разделам программы в соответствии с назначенной ролью.

Рекомендуется предварительно создать в Active Directory группы пользователей, которым вы хотите предоставить возможность проходить авторизацию с помощью доменной учетной записи в веб-интерфейсе KUMA. В свойствах учетной записи пользователя в Active Directory обязательно должен быть указан адрес электронной почты.

В этом разделе

Подключение по протоколу LDAP 102

Авторизация с помощью доменных учетных записей 110

Подключение по протоколу LDAP

Подключения по протоколу LDAP создаются и управляются в разделе **Параметры** → **LDAP-сервер** веб-интерфейса KUMA. В разделе **Интеграция с LDAP-сервером по тенантам** отображаются тенанты (см. раздел "О тенантах" на стр. 25), для которых созданы подключения по протоколу LDAP. Тенанты можно создать или удалить (см. раздел "Добавление тенанта в список тенантов для интеграции с LDAP-сервером" на стр. 104).

Если выбрать тенант, откроется окно **Интеграция с LDAP-сервером**, в котором отображается таблица с существующими LDAP-подключениями. Подключения можно создать (см. раздел "Создание подключения к LDAP-серверу" на стр. 104) или изменить (см. раздел "Изменение подключения к LDAP-серверу" на

стр. 107). В этом же окне можно изменить частоту (см. раздел "Изменение частоты обновления данных" на стр. 107) обращения к LDAP-серверам и установить срок хранения устаревших данных.

После включения интеграции информация об учетных записях Active Directory становится доступной в окне алертов (см. раздел "Работа с алертами" на стр. 330), в окне с подробной информацией о событиях корреляции (см. раздел "Открытие окна корреляционного события" на стр. 357), а также окне инцидентов (см. раздел "Просмотр информации об инциденте" на стр. 310). При выборе имени учетной записи в разделе **Связанные пользователи** откроется окно **Информация об учетной записи** с данными, импортированными из Active Directory.

Данные из LDAP можно также использовать при обогащении событий в коллекторах (см. раздел "Шаг 6. Обогащение событий" на стр. 245) и в аналитике (см. раздел "Аналитика" на стр. 273).

Импортируемые атрибуты Active Directory (см. раздел "Импортируемые атрибуты Active Directory" на стр. 109)

В этом разделе

Включение и выключение LDAP-интеграции 103
Добавление тенанта в список тенантов для интеграции с LDAP-сервером 104
Создание подключения к LDAP-серверу 104
Создание копии подключения к LDAP-серверу 106
Изменение подключения к LDAP-серверу 107
Изменение частоты обновления данных 107
Изменение срока хранения данных 108
Запуск задач на обновление данных об учетных записях 108
Удаление подключения к LDAP-серверу 109
Импортируемые атрибуты Active Directory 109

Включение и выключение LDAP-интеграции

Можно включить или выключить сразу все LDAP-подключения тенанта, а можно включить или выключить только определенное LDAP-подключение.

► *Чтобы включить или отключить все LDAP-подключения тенанта:*

1. Откройте раздел **Параметры** → **LDAP-сервер** веб-интерфейса KUMA и выберите тенант, у которого вы хотите включить или выключить все подключения к LDAP.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.
2. Установите или снимите флажок **Выключено**.
3. Нажмите **Сохранить**.

► *Чтобы включить или отключить определенное LDAP-подключение:*

1. Откройте раздел **Параметры** → **LDAP-сервер** веб-интерфейса KUMA и выберите тенант, у которого вы хотите включить или выключить подключение к LDAP.

Откроется окно **Интеграция с LDAP-сервером**.

2. Выберите нужное подключение и в открывшемся окне установите или снимите флажок **Выключено**.
3. Нажмите **Сохранить**.

Добавление тенанта в список тенантов для интеграции с LDAP-сервером

► *Чтобы добавить тенант в список тенантов для интеграции с LDAP-сервером:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.
2. Нажмите на кнопку **Добавить тенант**.

   Отобразится окно **Интеграция с LDAP-сервером**.
3. В раскрывающемся списке **Тенант** выберите тенант, который вам требуется добавить.
4. Нажмите **Сохранить**.

Выбранный тенант добавлен в список тенантов для интеграции с LDAP-сервером.

► *Чтобы добавить тенант из списка тенантов для интеграции с LDAP-сервером:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **LDAP-сервер**.

   Отобразится таблица **Интеграция с LDAP-сервером по тенантам**.
2. Установите флажок рядом с тенантом, который необходимо удалить, и нажмите на кнопку **Удалить**.
3. Подтвердите удаление тенанта.

Выбранный тенант удален из списка тенантов для интеграции с LDAP-сервером.

Создание подключения к LDAP-серверу

► *Чтобы создать LDAP-подключение к Active Directory:*

1. Откройте раздел **Параметры** → **LDAP-сервер** веб-интерфейса KUMA.
2. Выберите или создайте тенант (см. раздел "Добавление тенанта в список тенантов для интеграции с LDAP-сервером" на стр. 104), для которого хотите создать подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.
3. Нажмите на кнопку **Добавить подключение**.

   Откроется окно **Параметры подключения**.
4. Добавьте секрет с учетными данными для подключения к серверу Active Directory. Для этого выполните следующие действия:

   a. Если вы добавили секрет ранее, в раскрывающемся списке **Секрет** выберите существующий ресурс секрета (тип **credentials**).

      Выбранный секрет можно изменить, нажав на кнопку  .

   b. Если вы хотите создать новый секрет, нажмите на кнопку  .

      Откроется окно **Секрет**.

c. В поле **Название** (обязательно) введите название ресурса: от 1 до 128 символов Юникода.

d. В полях **Пользователь** и **Пароль** (обязательно) введите учетные данные для подключения к серверу Active Directory.

Вы можете указать имя пользователя в одном из следующих форматов: <имя пользователя>@<домен> или <домен><имя пользователя>.

e. В поле **Описание** введите описание ресурса: до 256 символов Юникода.

f. Нажмите на кнопку **Сохранить**.

5. В поле **Название** (обязательно) введите уникальное имя LDAP-подключения.

Длина должна быть от 1 до 128 символов Юникода.

6. В поле **URL** (обязательно) введите адрес контроллера домена в формате `<hostname или IP-адрес сервера>:<порт>`.

> Вы можете указать через запятую адреса нескольких серверов с контроллерами домена на случай, если один из них будет недоступен. Все указанные серверы должны находиться в одном домене.

7. Если вы хотите использовать TLS-шифрование для соединения с контроллером домена, в раскрывающемся списке **Тип** выберите один из следующих вариантов:

- **startTLS**.

  При использовании метода startTLS сначала устанавливается незащищенное соединение по порту 389, а затем отправляется запрос на шифрование. Если команда STARTTLS завершается с ошибкой, соединение обрывается.

  > Убедитесь, что порт 389 открыт. В противном случае соединение с контроллером домена будет невозможно.

- **ssl**.

  При использовании SSL сразу устанавливается шифрованное соединение по порту 636.

- **незащищенный**.

При использовании шифрованного соединения невозможно указать IP-адрес в качестве URL.

8. Если на предыдущем шаге вы включили TLS-шифрование, добавьте TLS-сертификат. Для этого выполните следующие действия:

a. Если вы загрузили сертификат ранее, выберите его в раскрывающемся списке **Сертификат**.

Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.

b. Если вы хотите загрузить новый сертификат, справа от списка **Сертификат** нажмите на кнопку  .

Откроется окно **Секрет**.

c. В поле **Название** введите название, которое будет отображаться в списке сертификатов после его добавления.

d. По кнопке **Загрузить файл сертификата** добавьте файл с сертификатом Active Directory. Поддерживаются открытые ключи сертификата X.509 в Base64.

e. Если требуется, укажите любую информацию о сертификате в поле **Описание**.

f. Нажмите на кнопку **Сохранить**.

Сертификат будет загружен и отобразится в списке **Сертификат**.

9. В поле **Время ожидания в секундах** укажите, сколько времени требуется ожидать ответа от сервера контроллера домена.

   Если в поле **URL** указано несколько адресов, то KUMA будет ждать ответа от первого сервера указанное количество секунд. Если за это время ответ не будет получен, программа обратится к следующему указанному серверу и т.д. Если ни один из указанных серверов не ответит в течение заданного времени, подключение будет прервано с ошибкой.

10. В поле **База поиска (Base DN)** введите базовое отличительное имя каталога, в котором должен выполняться поисковый запрос.

11. Установите флажок **Выключено**, если не хотите использовать это LDAP-подключение.

    По умолчанию флажок снят.

12. Нажмите на кнопку **Сохранить**.

LDAP-подключение к Active Directory создано и отображается в окне **Интеграция с LDAP-сервером**.

Информация об учетных записях из Active Directory будет запрошена сразу после сохранения подключения, а затем будет обновляться с указанной периодичностью (см. раздел "Изменение частоты обновления данных" на стр. 107).

Если вы хотите использовать одновременно несколько LDAP-подключений для одного тенанта, вам нужно убедиться, что адрес контроллера домена, указанный в каждом из этих подключений, является уникальным. В противном случае KUMA позволяет включить только одно из этих подключений. Порт при проверке адреса контроллера домена на уникальность не проверяется.

Создание копии подключения к LDAP-серверу

Вы можете создать LDAP-подключение, скопировав уже существующее подключение. В этом случае в созданное подключение дублируются все параметры исходного подключения.

► *Чтобы скопировать LDAP-подключение:*

1. Откройте раздел **Параметры** → **LDAP-сервер** веб-интерфейса KUMA и выберите тенант, для которого вы хотите скопировать подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером**.

2. Выберите нужное подключение.

3. В открывшемся окне **Параметры подключения** нажмите на кнопку **Дублировать подключение**.

   Отобразится окно создания нового подключения. К названию подключения будет добавлено слово `копия`.

4. Если требуется, измените нужные параметры.

5. Нажмите на кнопку **Сохранить**.

Создано новое подключение.

Если вы хотите использовать одновременно несколько LDAP-подключений для одного тенанта, вам нужно убедиться, что адрес контроллера домена, указанный в каждом из этих подключений, является уникальным. В противном случае KUMA позволяет включить только одно из этих подключений. Порт при проверке адреса контроллера домена на уникальность не проверяется.

Изменение подключения к LDAP-серверу

► *Чтобы изменить подключение к LDAP-серверу:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **LDAP-сервер**.

   Откроется окно **Интеграция с LDAP-сервером по тенантам**.

2. Выберите тенант, для которого вы хотите изменить подключение к LDAP-серверу.

   Откроется окно **Интеграция с LDAP-сервером**.

3. Нажмите на подключение с LDAP-серверу, которое вы хотите изменить.

   Откроется окно с параметрами выбранного подключения к LDAP-серверу.

4. Измените значения необходимых параметров.

5. Нажмите на кнопку **Сохранить**.

Подключение к LDAP-серверу изменено. Перезапустите сервисы (см. раздел "Перезапуск сервиса" на стр. 231) KUMA, использующие обогащение данными LDAP-серверов, чтобы изменения вступили в силу.

Изменение частоты обновления данных

KUMA обращается к LDAP-серверу для обновления данных об учетных записях. Это происходит в следующих случаях:

- Сразу после создания нового подключения.
- Сразу после изменения параметров существующего подключения.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов.
- При создании пользователем задачи на обновление данных (см. раздел "Запуск задач на обновление данных об учетных записях" на стр. 108) об учетных записях.

При обращении к LDAP-серверам создается задача в разделе **Диспетчер задач** веб-интерфейса KUMA.

► *Чтобы изменить расписание обращений KUMA к LDAP-серверам:*

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **LDAP-сервер** → **Интеграция с LDAP-сервером по тенантам**.

2. Выберите нужный тенант.

   Откроется окно **Интеграция с LDAP-сервером**.

3. В поле **Период обновления данных** укажите требуемую частоту в часах. Значение по умолчанию – 12.

Расписание обращений изменено.

Изменение срока хранения данных

Полученные данные об учетных записях, если сведения о них перестают поступать от сервера Active Directory, по умолчанию хранятся в KUMA в течение 90 дней. По прошествии этого срока данные удаляются.

После удаления данных об учетных записях в KUMA новые и существующие события не обогащаются этой информацией. Информация об учетных записях также будет недоступна в алертах. Если вы хотите просматривать информацию об учетных записях на протяжении всего времени хранения алерта, требуется установить срок хранения данных об учетных записях больше, чем срок хранения алерта.

► *Чтобы изменить срок хранения данных об учетных записях:*

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **LDAP-сервер** → **Интеграция с LDAP-сервером по тенантам**.
2. Выберите нужный тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. В поле **Время хранения данных** укажите количество дней, в течение которого требуется хранить полученные от LDAP-сервера данные.

Срок хранения данных об учетных записях изменен.

Запуск задач на обновление данных об учетных записях

После создания подключения к серверу Active Directory задачи на получение данных об учетных записях (см. раздел "Изменение частоты обновления данных" на стр. 107) создаются автоматически. Это происходит в следующих случаях:

- Сразу после создания нового подключения.
- Сразу после изменения параметров существующего подключения.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов. Расписание можно изменить.

Задачи на обновление данных об учетных записях можно создать вручную. Загрузить данные можно для всех подключений требуемого тенанта, так и для одного подключения.

► *Чтобы запустить задачу на обновление данных об учетных записях для всех LDAP-подключений тенанта:*

1. Откройте в веб-интерфейсе KUMA разделе **Параметры** → **LDAP-сервер** → **Интеграция с LDAP-сервером по тенантам**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. Нажмите на кнопку **Импортировать учетные записи**.

В разделе **Диспетчер задач** веб-интерфейса KUMA добавлена задача (см. раздел "Просмотр таблицы задач" на стр. 405) на получение данных об учетных записях выбранного тенанта.

► *Чтобы запустить задачу на обновление данных об учетных записях для одного LDAP-подключения тенанта:*

1. Откройте в веб-интерфейсе KUMA разделе **Параметры** → **LDAP-сервер** → **Интеграция с LDAP-сервером по тенантам**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с LDAP-сервером**.
3. Выберите требуемое подключение к LDAP-серверу.

   Откроется окно **Параметры подключения**.
4. Нажмите на кнопку **Импортировать учетные записи**.

В разделе **Диспетчер задач** веб-интерфейса KUMA добавлена задача (см. раздел "Просмотр таблицы задач" на стр. 405) на получение данных об учетных записях из выбранного подключения тенанта.

Удаление подключения к LDAP-серверу

► *Чтобы удалить LDAP-подключения к Active Directory:*

1. Откройте раздел **Параметры** → **LDAP-сервер** веб-интерфейса KUMA и выберите тенант, которому принадлежит нужное подключение к LDAP.

   Откроется окно **Интеграция с LDAP-сервером**.
2. Нажмите на подключение LDAP, которое вы хотите удалить, а затем нажмите на кнопку **Удалить**.
3. Подтвердите удаление подключения.

LDAP-подключение к Active Directory удалено.

Импортируемые атрибуты Active Directory

Из Active Directory можно запросить следующие атрибуты учетных записей:

- `accountExpires`
- `badPasswordTime`
- `cn`
- `co`
- `company`
- `department`
- `description`
- `displayName` (по этому атрибуту события можно искать при корреляции)
- `distinguishedName` (по этому атрибуту события можно искать при корреляции)
- `division`

- employeeID
- givenName
- l
- lastLogon
- lastLogonTimestamp
- mail (по этому атрибуту события можно искать при корреляции)
- mailNickname
- managedObjects
- manager
- memberOf (по этому атрибуту события можно искать при корреляции)
- mobile
- name
- objectCategory
- objectGUID (этот атрибут запрашивается из Active Directory всегда)
- objectSid
- physicalDeliveryOfficeName
- pwdLastSet
- sAMAccountName (по этому атрибуту события можно искать при корреляции)
- sAMAccountType
- sn (по этому атрибуту события можно искать при корреляции)
- streetAddress
- telephoneNumber
- title
- userAccountControl (по этому атрибуту события можно искать при корреляции)
- userPrincipalName (по этому атрибуту события можно искать при корреляции)
- whenChanged
- whenCreated

Авторизация с помощью доменных учетных записей

Для того чтобы пользователи могли проходить авторизацию в веб-интерфейсе KUMA с помощью своих доменных учетных данных, требуется выполнить следующие этапы настройки.

a. **Включить доменную авторизацию, если она отключена (см. раздел "Включение и выключение доменной авторизации" на стр. 111)**

По умолчанию доменная авторизация включена, но подключение к домену не настроено.

b. **Настроить соединение с контроллером домена (см. раздел "Настройка соединения с контроллером домена" на стр. 112)**

   Вы можете подключиться только к одному домену.

c. **Добавить группы ролей пользователей (см. раздел "Добавление групп ролей пользователей" на стр. 114)**

   Вы можете указать для каждой роли KUMA группу Active Directory. Пользователи из этой группы, пройдя авторизацию с помощью своих доменных учетных данных, будут получать доступ к веб-интерфейсу KUMA в соответствии с указанной ролью.

   При этом программа проверяет соответствие группы пользователя в Active Directory указанному фильтру в порядке следования ролей в веб-интерфейсе KUMA: оператор → аналитик → администратор тенанта → главный администратор. При первом совпадении пользователю присваивается роль и дальнейшая проверка не осуществляется. Если для пользователя указано две группы в одном тенанте, то будет использована роль с наименьшими правами. Если указано несколько групп для разных тенантов, то в каждом тенанте пользователю будет присвоена указанная роль.

Если вы выполнили все этапы настройки, но пользователь не может авторизоваться в веб-интерфейсе KUMA с помощью своей доменной учетной записи, рекомендуется проверить конфигурацию на наличие следующих проблем:

- В свойствах учетной записи пользователя в Active Directory не указан адрес электронной почты. В этом случае при первой авторизации пользователя отобразится сообщение об ошибке и учетная запись KUMA не будет создана.
- Локальная учетная запись KUMA с адресом электронной почты, указанным в свойствах доменной учетной записи, уже существует. В этом случае при попытке авторизации с помощью доменной учетной записи пользователь получит сообщение об ошибке.
- Доменная авторизация отключена (см. раздел "Включение и выключение доменной авторизации" на стр. 111) в параметрах KUMA.
- Допущена ошибка при вводе группы ролей (см. раздел "Добавление групп ролей пользователей" на стр. 114).
- Доменное имя пользователя содержит пробел.

В этом разделе

Включение и выключение доменной авторизации 111

Настройка соединения с контроллером домена 112

Добавление групп ролей пользователей 114

Включение и выключение доменной авторизации

По умолчанию доменная авторизация включена, но подключение к домену Active Directory не настроено. Если после настройки подключения вы хотите временно приостановить доменную авторизацию, вы можете отключить ее в веб-интерфейсе KUMA, не удаляя заданные ранее значения параметров. При необходимости вы сможете в любой момент включить авторизацию снова.

► *Чтобы включить или отключить доменную авторизацию пользователей в веб-интерфейсе KUMA:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Доменная авторизация**.
2. Выполните одно из следующих действий:
   - Если вы хотите выключить доменную авторизацию, в верхней части рабочей области установите флажок **Выключено**.
   - Если вы хотите включить доменную авторизацию, в верхней части рабочей области снимите флажок **Выключено**.
3. Нажмите на кнопку **Сохранить**.

Доменная авторизация будет включена или отключена.

Настройка соединения с контроллером домена

Вы можете подключиться только к одному домену Active Directory. Для этого требуется настроить соединение с контроллером домена.

► *Чтобы настроить соединение с контроллером домена Active Directory:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Доменная авторизация**.
2. В блоке параметров **Подключение** в поле **База поиска (Base DN)** введите DistinguishedName корневой записи для поиска групп доступа в службе каталогов Active Directory.
3. В поле **URL** укажите адрес контроллера домена в формате `<hostname или IP-адрес сервера>:<порт>`.

   Вы можете указать через запятую адреса нескольких серверов с контроллерами домена на случай, если один из них будет недоступен. Все указанные серверы должны находиться в одном домене.

4. Если вы хотите использовать TLS-шифрование для соединения с контроллером домена, в раскрывающемся списке **Режим TLS** выберите один из следующих вариантов:
   - **startTLS**.

     При использовании метода startTLS сначала устанавливается незащищенное соединение по порту 389, а затем отправляется запрос на шифрование. Если команда STARTTLS завершается с ошибкой, соединение обрывается.

     Убедитесь, что порт 389 открыт. В противном случае соединение с контроллером домена будет невозможно.

   - **ssl**.

     При использовании SSL сразу устанавливается шифрованное соединение по порту 636.

   - **незащищенный**.

   При использовании шифрованного соединения невозможно указать IP-адрес в качестве URL.
5. Если на предыдущем шаге вы включили TLS-шифрование, добавьте TLS-сертификат:

- Если вы загрузили сертификат ранее, выберите его в раскрывающемся списке **Секрет**.

  Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.

- Если вы хотите загрузить новый сертификат, справа от списка **Секрет** нажмите на кнопку  . В открывшемся окне в поле **Название** введите название, которое будет отображаться в списке сертификатов после его добавления. Добавьте файл с сертификатом Active Directory (поддерживаются открытые ключи сертификата X.509 в Base64), нажав на кнопку **Загрузить файл сертификата**. Нажмите на кнопку **Сохранить**.

  Сертификат будет загружен и отобразится в списке **Секрет**.

6. В поле **Время ожидания в секундах** укажите, сколько времени требуется ожидать ответа от сервера контроллера домена.

   Если в поле **URL** указано несколько адресов, то KUMA будет ждать ответа от первого сервера указанное количество секунд. Если за это время ответ не будет получен, программа обратится к следующему указанному серверу и так далее. Если ни один из указанных серверов не ответит в течение заданного времени, подключение будет прервано с ошибкой.

7. Если вы хотите настроить доменную авторизацию для пользователя с ролью главного администратора KUMA, в поле **Группа главных администраторов** укажите DistinguishedName группы Active Directory, в которой состоит пользователь.

   > Если для пользователя указано две группы в одном тенанте, то будет использована роль с наименьшими правами.

   Пример ввода фильтра: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`

8. Нажмите на кнопку **Сохранить**.

Соединение с контроллером домена Active Directory будет настроено. Для работы доменной авторизации требуется также добавить группы для ролей пользователей KUMA (см. раздел "Добавление групп ролей пользователей" на стр. 114).

Вы также можете проверить соединение для введенных ранее параметров соединения с контроллером домена.

► *Чтобы проверить соединение с контроллером домена:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Доменная авторизация**.
2. В блоке параметров **Проверка подключения** выберите нужный секрет в поле **Данные аутентификации**.

   При необходимости вы можете создать новый секрет, нажав на кнопку  , или изменить параметры существующего секрета, нажав на кнопку  .

3. Нажмите на кнопку **Тест**.

Отобразится всплывающее уведомление с результатами теста. Во всплывающем уведомлении отображается сообщение: **Подключение установлено**. Если соединение установить не удалось, то отображается причина отсутствия соединения.

Добавление групп ролей пользователей

Вы можете указать группы только для тех ролей, для которых требуется настроить доменную авторизацию. Остальные поля можно оставить пустыми.

► *Чтобы добавить группы ролей пользователей:*

1. В веб-интерфейсе программы выберите раздел **Параметры** → **Доменная авторизация**.
2. В блоке параметров **Группы ролей** нажмите на кнопку **Добавить группы ролей**.
3. В раскрывающемся списке **Тенант** выберите, для пользователей какого тенанта вы хотите настроить доменную авторизацию.
4. Укажите DistinguishedName группы Active Directory, пользователи которой должны иметь возможность пройти авторизацию со своими доменными учетными данными, в полях для следующих ролей:
   - **Оператор**.
   - **Аналитик**.
   - **Администратор**.

   Пример ввода группы: `CN=KUMA team,OU=Groups,OU=Clients,DC=test,DC=domain`.

   Вы можете указать для каждой роли только одну группу Active Directory. Если вам нужно указать несколько групп, то для каждой группы требуется повторить шаги 2–4, указывая при этом тот же тенант.
5. Если требуется, повторите шаги 2–4 для каждого тенанта, для которого вы хотите настроить доменную авторизацию с ролями оператор, аналитик или администратор тенанта.
6. Нажмите на кнопку **Сохранить**.

Группы ролей пользователей будут добавлены. Заданные параметры будут применены после следующего входа пользователя в веб-интерфейс KUMA.

После первой авторизации пользователя информация о нем отобразится в разделе **Параметры** → **Пользователи**. Поля **Логин** и **Пароль**, полученные из Active Directory, недоступны для редактирования. Роль пользователя также будет недоступна для редактирования: для изменения роли потребуется изменить группы ролей пользователей. Изменения роли применяются после повторной авторизации пользователя. До истечения текущей сессии пользователь продолжает работу со старой ролью.

Если в свойствах учетной записи Active Directory изменяется имя или адрес электронной почты пользователя, требуется вручную внести эти изменения в учетную запись KUMA.

Интеграция с НКЦКИ

Вы можете создать в веб-интерфейсе KUMA подключение к Национальному координационному центру по компьютерным инцидентам (далее "НКЦКИ"). Это позволит вам экспортировать (см. раздел "Экспорт инцидентов в НКЦКИ" на стр. 317) в него инциденты (см. раздел "Об инцидентах" на стр. 28),

зарегистрированные в KUMA. Интеграция настраивается в разделе **Параметры** → **НКЦКИ** веб-интерфейса KUMA.

Интеграцию можно включить или выключить с помощью флажка **Выключено**.

► *Чтобы создать подключение к НКЦКИ:*

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **НКЦКИ**.
2. В поле **URL** введите URL, по которому доступен НКЦКИ.
3. В блоке параметров **Токен** создайте или выберите существующий ресурс секрета (см. раздел "Секреты" на стр. 226) с API-токеном, который был выдан вашей организации для подключения к НКЦКИ:
   - Если у вас уже есть секрет, его можно выбрать в раскрывающемся списке.
   - Если вы хотите создать новый секрет:
     a. Нажмите на кнопку + и укажите следующие параметры:
        - **Название** (обязательно) – уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.
        - **Токен** (обязательно) – токен, который был выдан вашей организации для подключения к НКЦКИ.
        - **Описание** – описание сервиса: до 256 символов Юникода.
     b. Нажмите **Сохранить**.

     Секрет с токеном для подключения к НКЦКИ создан. Он хранится в разделе **Ресурсы** → **Секреты** и принадлежит главному тенанту.

   Выбранный секрет можно изменить, нажав на кнопку  .
4. В раскрывающемся списке **Сфера деятельности компании** выберите сферу, в которой работает ваша организация.

   Доступные сферы деятельности компании (см. раздел "Сферы деятельности компании" на стр. 116)
5. В поле **Название компании** укажите название вашей компании. Эти данные будут передаваться в НКЦКИ при экспорте инцидентов.
6. С помощью раскрывающегося списка **Местоположение** укажите, где располагается ваша компания. Эти данные будут передаваться в НКЦКИ при экспорте инцидентов.
7. При необходимости в блоке параметров **Прокси-сервер** создайте или выберите существующий ресурс прокси-сервера, который должен использоваться при подключении к НКЦКИ.
8. Нажмите **Сохранить**.

KUMA интегрирована с НКЦКИ. Теперь вы можете экспортировать в него инциденты.

kaspersky

Доступные категории и типы инцидентов

Категория инцидента	Тип инцидента
Уведомление о компьютерном инциденте	Вовлечение контролируемого ресурса в инфраструктуру ВПО
	Замедление работы ресурса в результате DDoS-атаки
	Заражение ВПО
	Захват сетевого трафика
	Использование контролируемого ресурса для фишинга
	Компрометация учетной записи
	Несанкционированное изменение информации
	Несанкционированное разглашение информации
	Публикация на ресурсе запрещенной законодательством РФ информации
	Рассылка спам-сообщений с контролируемого ресурса
	Успешная эксплуатация уязвимости
Уведомление о компьютерной атаке	DDoS-атака
	Неудачные попытки авторизации
	Попытки внедрения ВПО
	Попытки эксплуатации уязвимости
	Публикация мошеннической информации
	Сетевое сканирование
	Социальная инженерия
Уведомление о наличии уязвимости	Уязвимый ресурс

Сферы деятельности компании

- Атомная энергетика
- Банковская сфера и иные сферы финансового рынка
- Горнодобывающая промышленность
- Государственная/муниципальная власть
- Здравоохранение
- Металлургическая промышленность

- Наука
- Оборонная промышленность
- Образование
- Ракетно-космическая промышленность
- Связь
- СМИ
- Топливно-энергетический комплекс
- Транспорт
- Химическая промышленность
- Иная

Интеграция с Security Vision Incident Response Platform

Security Vision Incident Response Platform (далее Security Vision IRP) – это программная платформа для автоматизации мониторинга, обработки и реагирования на инциденты информационной безопасности. Она объединяет данные о киберугрозах из различных источников в единую базу данных для дальнейшего анализа и расследования, что позволяет облегчить реагирование на инциденты.

Security Vision IRP можно интегрировать с KUMA. После настройки интеграции в Security Vision IRP можно выполнять следующие задачи:

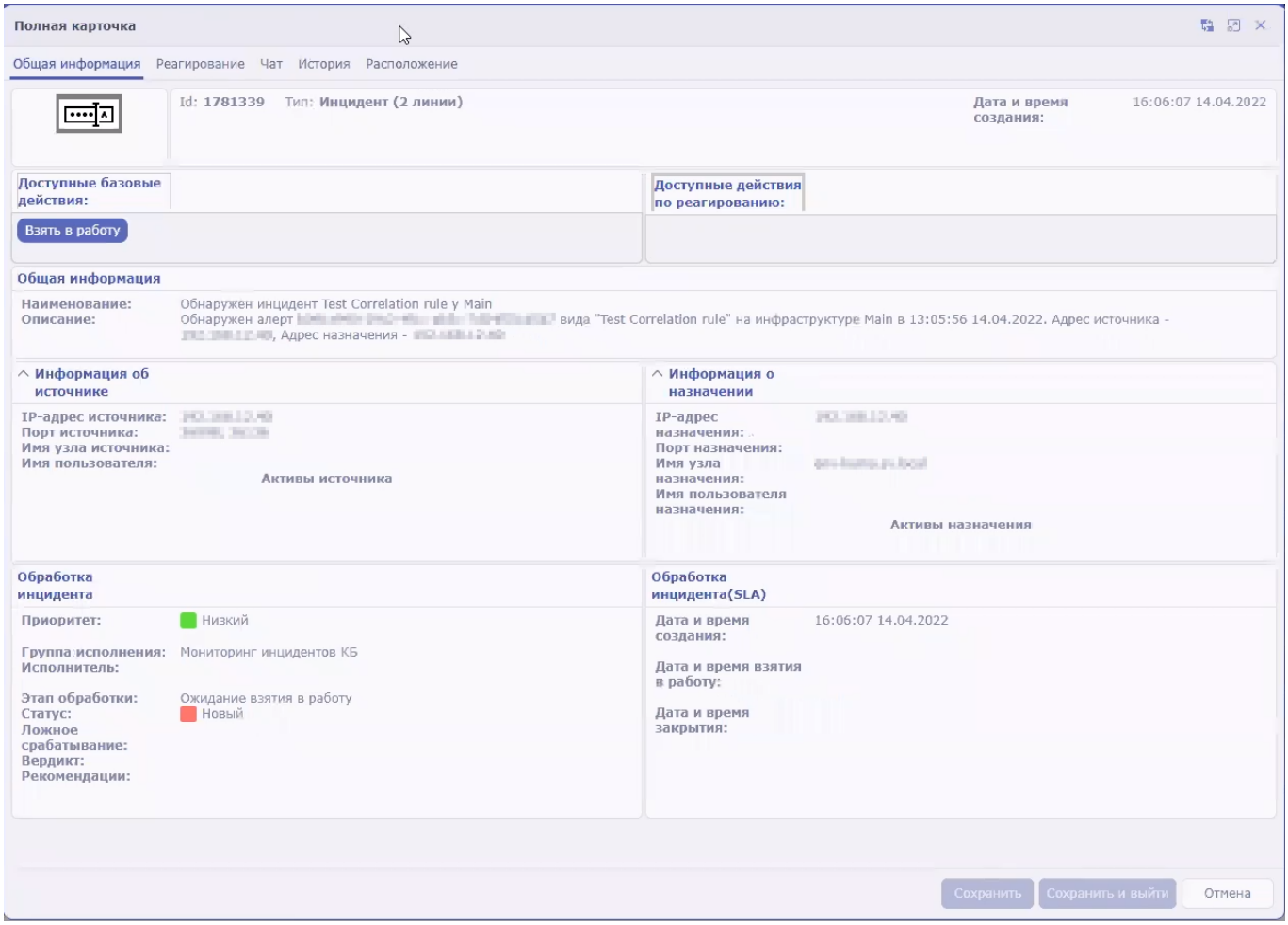
- Запрашивать из KUMA сведения об алертах (см. раздел "Об алертах" на стр. 27). При этом в Security Vision IRP по полученным данным создаются *инциденты*.
- Отправлять в KUMA запросы на закрытие алертов.

Интеграция реализована с помощью KUMA REST API (на стр. 413). На стороне Security Vision IRP интеграция осуществляется с помощью преднастроенного коннектора **Kaspersky KUMA** (см. раздел "**Импорт и настройка коннектора**" на стр. 120). О способах и условиях получения коннектора **Kaspersky KUMA** вы можете узнать у вашего поставщика Security Vision IRP.

Работа с инцидентами Security Vision IRP

Инциденты Security Vision IRP, созданные на основе данных об алертах KUMA, можно просмотреть в Security Vision IRP в разделе **Инциденты** → **Инциденты (2 линии)** → **Все инциденты (2 линии)**. В каждый инцидент Security Vision IRP записываются события, относящиеся к алертам KUMA. Импортированные события можно просмотреть на закладке **Реагирование**.

Алерт KUMA, импортированный в Security Vision IRP в качестве инцидента



См. также:

Об алертах 27

О событиях 25

REST API 413

В этом разделе:

Настройка интеграции в KUMA 119

Настройка интеграции в Security Vision IRP 119

kaspersky

Настройка интеграции в KUMA

Для того чтобы настроить интеграцию KUMA и Security Vision IRP необходимо настроить авторизацию API-запросов в KUMA. Для этого требуется создать токен для пользователя KUMA, от имени которого будут обрабатываться API-запросы на стороне KUMA.

Токен можно сгенерировать в профиле своей учетной записи (см. раздел "Редактирование своей учетной записи" на стр. 71). Пользователи с ролью главный администратор (см. раздел "Роли пользователей" на стр. 57) могут генерировать токены в учетных записях других пользователей (см. раздел "Редактирование пользователя" на стр. 70). Вы всегда можете сгенерировать новый токен.

► *Чтобы сгенерировать токен в профиле своей учетной записи:*

1. В веб-интерфейсе KUMA в левом нижнем углу окна нажмите на имя учетной записи пользователя и в открывшемся меню нажмите на кнопку **Профиль**.

   Откроется окно **Пользователь** с параметрами вашей учетной записи.
2. Нажмите на кнопку **Сгенерировать токен**.
3. В открывшемся окне скопируйте созданный токен. Он потребуется для настройки Security Vision IRP.

   При закрытии окна токен больше не отображается, и, если вы его не скопировали, потребуется сгенерировать новый токен.

Сгенерированный токен требуется указать в параметрах коннектора Security Vision IRP (см. раздел "Импорт и настройка коннектора" на стр. 120).

См. также:

Настройка интеграции в Security Vision IRP 119

Настройка интеграции в Security Vision IRP

Настройка интеграции в Security Vision IRP заключается в импорте и настройки коннектора (см. раздел "Импорт и настройка коннектора" на стр. 120). При необходимости можно также изменить другие параметры Security Vision IRP, связанные с обработкой данных KUMA (см. раздел "Настройка обработчика, расписания и рабочего процесса" на стр. 123): например, расписание обработки данных и рабочий процесс.

Более подробные сведения о настройке Security Vision IRP см. в документации продукта.

См. также:

Настройка интеграции в KUMA..... 119

В этом разделе:

Импорт и настройка коннектора 120

Настройка обработчика, расписания и рабочего процесса 123

Импорт и настройка коннектора

Добавление коннектора в Security Vision IRP

Интеграция Security Vision IRP и KUMA осуществляется с помощью коннектора **Kaspersky KUMA**. О способах и условиях получения коннектора **Kaspersky KUMA** вы можете узнать у вашего поставщика Security Vision IRP..

► *Чтобы импортировать коннектор **Kaspersky KUMA** в Security Vision IRP:*

1. В Security Vision IRP откройте раздел **Настройки** → **Коннекторы** → **Коннекторы**.

   Отобразится список коннекторов, добавленных в Security Vision IRP.

2. В верхней части экрана нажмите на кнопку импорта и выберите zip-архив с коннектором **Kaspersky KUMA**.

Коннектор импортирован в Security Vision IRP и готов к настройке.

Настройка в коннекторе подключения к KUMA

Для использования коннектора нужно настроить его подключение к KUMA.

► *Чтобы настроить в Security Vision IRP подключение к KUMA с помощью коннектора **Kaspersky KUMA**:*

1. В Security Vision IRP откройте раздел **Настройки** → **Коннекторы** → **Коннекторы**.

   Отобразится список коннекторов, добавленных в вашу Security Vision IRP.

2. Выберите коннектор **Kaspersky KUMA**.

   Отобразятся общие параметры коннектора.

3. В разделе **Параметры коннектора** нажмите на кнопку **Редактировать**.

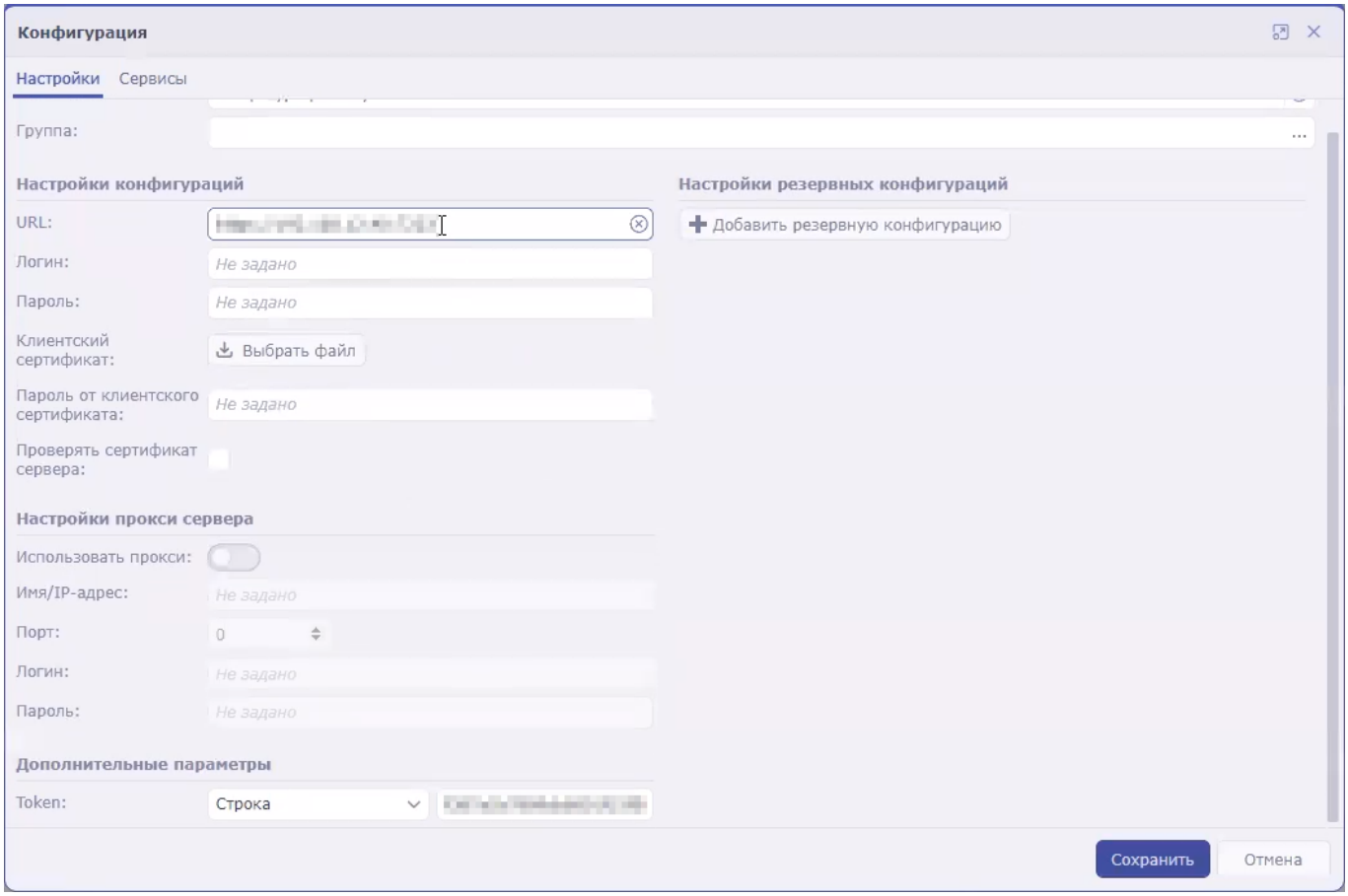
   Отобразится конфигурация коннектора.

4. В поле **URL** укажите адрес и порт KUMA. Например, `kuma.example.com:7223`.

5. В поле **Token** укажите API-токен пользователя KUMA (см. раздел "Настройка интеграции в KUMA" на стр. 119).

Подключение к KUMA настроено в коннекторе Security Vision IRP.

Настройки коннектора Security Vision IRP



Настройка в коннекторе Security Vision IRP команд для взаимодействия с KUMA

С помощью Security Vision IRP можно получать сведения об алертах KUMA (или *инцидентах* в терминологии Security Vision IRP), а также отправлять запросы на их закрытие. Для выполнения этих действий в коннекторе Security Vision IRP нужно настроить соответствующие команды.

В инструкциях ниже описано, как добавить команды на получение и закрытие алертов, однако при необходимости реализовать более сложную логику взаимодействия Security Vision IRP и KUMA вы можете аналогичным образом создать команды с другими API-запросами.

► *Чтобы настроить команду на получение из KUMA сведений об алертах:*

1. В Security Vision IRP откройте раздел **Настройки** → **Коннекторы** → **Коннекторы**.

   Отобразится список коннекторов, добавленных в Security Vision IRP.
2. Выберите коннектор **Kaspersky KUMA**.

   Отобразятся общие настройки коннектора.
3. Нажмите на кнопку **+Команда**.

   Откроется окно создания команды.
4. Укажите параметры команды для получения алертов:
   - В поле **Наименование** введите название команды: `Получение инцидентов`.

- В раскрывающемся списке **Тип запроса** выберите **GET**.
- В поле **Вызываемый метод** введите API-запрос на поиск алертов (см. раздел "Поиск алертов" на стр. 422): `api/v1/alerts/?withEvents&status=new`
- В разделе **Заголовки запроса** в поле **Название** укажите `authorization`, а в поле **Значение** укажите **Bearer <token>**.
- В раскрывающемся списке **Тип контента** выберите **application/json**.

5. Сохраните команду и закройте окно.

Команда коннектора настроена. При этой команды коннектор Security Vision IRP будет запрашивать в KUMA сведения обо всех алертах со статусом **Новый** и всех относящихся к ним событиях. Полученные данные будут передаваться в обработчик Security Vision IRP, который на их основе будет создавать инциденты Security Vision IRP. Если алерт уже был импортирован в Security Vision IRP, но в нем появились новые данные, сведения о нем будут обновлены в Security Vision IRP.

► *Чтобы настроить команду на закрытие алертов KUMA:*

1. В Security Vision IRP откройте раздел **Настройки → Коннекторы → Коннекторы**.

   Отобразится список коннекторов, добавленных в Security Vision IRP.

2. Выберите коннектор **Kaspersky KUMA**.

   Отобразятся общие настройки коннектора.

3. Нажмите на кнопку **+Команда**.

   Отобразится окно создания команды.

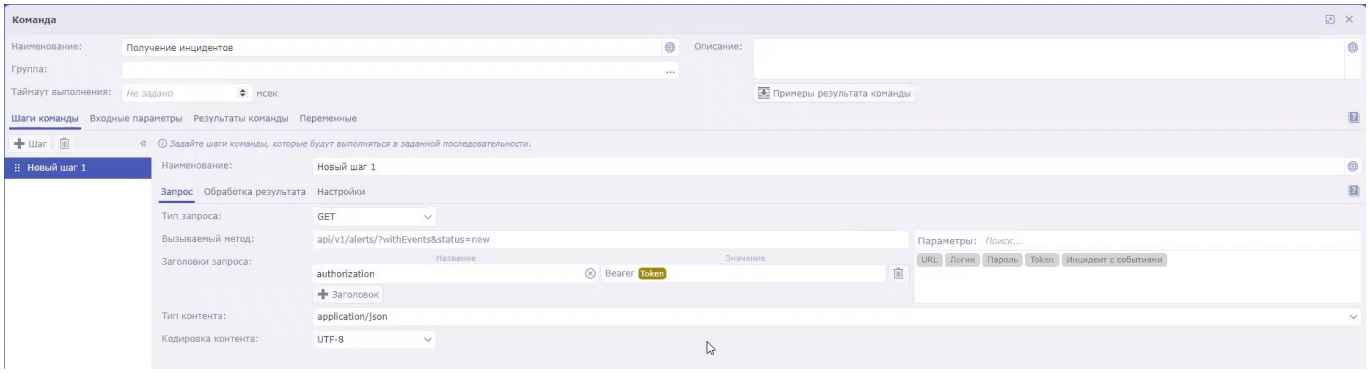
4. Укажите параметры команды для получения алертов:
   - В поле **Наименование** введите название команды: `Закрытие инцидента`.
   - В раскрывающемся списке **Тип запроса** выберите **POST**.
   - В поле **Вызываемый метод** введите API-запрос на закрытие алерта (см. раздел "Закрытие алертов" на стр. 428): `api/v1/alerts/close`
   - В поле **Запрос** введите содержимое отправляемого API-запроса: `{"id":"<Идентификатор алерта>","reason":"responded"}`

     Можно создать несколько команд для разных причин закрытия алертов: responded, incorrect data, incorrect correlation rule (см. раздел "Обработка алертов" на стр. 335).
   - В разделе **Заголовки запроса** в поле **Название** укажите `authorization`, а в поле **Значение** укажите **Bearer <token>**.
   - В раскрывающемся списке **Тип контента** выберите **application/json**.

5. Сохраните команду и закройте окно.

Команда коннектора настроена. При выполнении этой команды в Security Vision IRP будет закрыт инцидент, а в KUMA будет закрыт соответствующий ему алерт.

Создание команд в Security Vision IRP



После настройки коннектора Security Vision IRP алерты KUMA будут поступать в платформу в виде инцидентов Security Vision IRP. Далее необходимо настроить обработку инцидентов в Security Vision IRP (см. раздел "Настройка обработчика, расписания и рабочего процесса" на стр. 123) в соответствии с существующей в вашей организации политикой безопасности.

Настройка обработчика, расписания и рабочего процесса

Обработчик Security Vision IRP

Обработчик Security Vision IRP принимает от коннектора Security Vision IRP данные об алертах KUMA и создает на их основе инциденты Security Vision IRP. Для обработки используется предустановленный обработчик **KUMA (Инциденты)**. Настройки обработчика **KUMA (Инциденты)** доступны в Security Vision IRP в разделе **Настройки** → **Обработка событий** → **Обработчики событий**:

- Правила обработки алертов KUMA можно просмотреть в настройках обработчика на закладке **Нормализация**.
- Действия при создании новых объектов можно просмотреть в настройках обработчика на закладке **Действия** для создания объектов типа **Инцидент (2 линии)**.

Расписание запуска обработчика

Запуск коннектора (см. раздел "Импорт и настройка коннектора" на стр. 120) и обработчика выполняется по предустановленному расписанию **KUMA**. Настройка этого расписания доступна в Security Vision IRP в разделе **Настройки** → **Обработка событий** → **Расписание**:

- В блоке параметров **Настройки коннектора** можно настроить параметры запуска коннектора.
- В блоке параметров **Настройки обработки** можно настроить параметры запуска обработчика.

Рабочий процесс Security Vision IRP

Жизненный цикл инцидентов Security Vision IRP, созданных на основе алертов KUMA, проходит по преднастроенному процессу **Обработка инц. (2 линии)**. Настройка рабочего процесса доступна в Security Vision IRP в разделе **Настройки** → **Рабочие процессы** → **Шаблоны рабочих процессов**: выберите процесс **Обработка инц. (2 линии)** и нажмите на транзакцию или состояние, которое необходимо изменить.

kaspersky

Интеграция с Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks https://ics.kaspersky.ru/ (далее "KICS for Networks") – программа для защиты инфраструктуры промышленных предприятий от угроз информационной безопасности и для обеспечения непрерывности технологических процессов. Программа анализирует трафик промышленной сети для выявления отклонений в значениях технологических параметров, обнаружения признаков сетевых атак, контроля работы и текущего состояния устройств в сети.

KICS for Networks версии 4.0 и выше можно интегрировать с KUMA. После настройки интеграции в KUMA можно выполнять следующие задачи:

- Импортировать из KICS for Networks в KUMA сведения об активах.
- Отправлять из KUMA в KICS for Networks команды на изменение статусов активов.

> В отличие от KUMA, в KICS for Networks активы называются устройствами.

Интеграцию KICS for Networks и KUMA необходимо настроить на стороне обеих программ:

1. В KICS for Networks необходимо создать коннектор KUMA и сохранить файл свертки этого коннектора (см. раздел "Настройка интеграции в KICS for Networks" на стр. 124).
2. В KUMA с помощью файла свертки коннектора создается подключение к KICS for Networks (см. раздел "Настройка интеграции в KUMA" на стр. 125).

> Описываемая в этом разделе интеграция касается импорта сведений об активах. KICS for Networks можно также настроить на отправку событий в KUMA. Для этого необходимо в KICS for Networks создать коннектор типа SIEM/Syslog, а на стороне KUMA – настроить коллектор.

В этом разделе

Настройка интеграции в KICS for Networks 124
Настройка интеграции в KUMA 125
Включение и выключение интеграции с KICS for Networks 126
Изменение частоты обновления данных 126
Особенности импорта информации об активах из KICS for Networks 126
Изменение статуса актива KICS for Networks 127

kaspersky

Настройка интеграции в KICS for Networks

Интеграция поддерживается с KICS for Networks версий 4.0 и выше.

Настройку интеграции KICS for Networks и KUMA рекомендуется проводить после завершения режима обучения правилам контроля процесса. Подробнее см. в документации KICS for Networks https://support.kaspersky.com/KICSforNetworks/3.1/ru-RU/195603.htm.

На стороне KICS for Networks настройка интеграции заключается в создании *коннектора типа KUMA*. В KICS for Networks коннекторы – это специальные программные модули, которые обеспечивают обмен данными KICS for Networks со сторонними системами, в том числе с KUMA. Подробнее о создании коннекторов см. в документации KICS for Networks https://support.kaspersky.com/KICSforNetworks/3.1/ru-RU/136497.htm.

При добавлении в KICS for Networks коннектора автоматически создается *файл свертки* для этого коннектора. Это зашифрованный файл конфигурации для подключения к KICS for Networks, который используется при настройке интеграции на стороне KUMA (см. раздел "Настройка интеграции в KUMA" на стр. 125).

Настройка интеграции в KUMA

Настройку интеграции KICS for Networks и KUMA рекомендуется проводить после завершения режима обучения правилам контроля процесса. Подробнее см. в документации KICS for Networks https://support.kaspersky.com/KICSforNetworks/3.1/ru-RU/195603.htm.

► *Чтобы настроить в KUMA интеграцию с KICS for Networks:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Industrial CyberSecurity for Networks**.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks по тенантам**.

2. Выберите или создайте тенант, для которого хотите создать интеграцию с KICS for Networks.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.

3. Нажмите на поле **Файл свертки** и выберите файл свертки коннектора (см. раздел "Настройка интеграции в KICS for Networks" на стр. 124), созданный в KICS for Networks.

4. В поле **Пароль файла свертки** введите пароль файла свертки.

5. Установите флажок **Включить реагирование**, если вы хотите изменять статусы активов KICS for Networks с помощью правил реагирования KUMA.

6. Нажмите **Сохранить**.

В KUMA настроена интеграция с KICS for Networks, в окне отображается IP-адрес узла, на котором будет работать коннектор KICS for Networks, а также его идентификатор.

Включение и выключение интеграции с KICS for Networks

► *Чтобы включить или выключить для тенанта интеграцию с KICS for Networks:*

1. Откройте раздел **Параметры** → **Kaspersky Industrial CyberSecurity for Networks** веб-интерфейса KUMA и выберите тенант, у которого вы хотите включить или выключить интеграцию с KICS for Networks.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.

2. Установите или снимите флажок **Выключено**.
3. Нажмите **Сохранить**.

Изменение частоты обновления данных

KUMA обращается к KICS for Networks для обновления сведений об активах. Это происходит в следующих случаях:

- Сразу после создания новой интеграции.
- Сразу после изменения параметров существующей интеграции.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 3 часа.
- При создании пользователем задачи на обновление данных об активах.

При обращении к KICS for Networks создается задача в разделе **Диспетчер задач** веб-интерфейса KUMA.

► *Чтобы изменить расписание импорта сведений об активах KICS for Networks:*

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Kaspersky Industrial CyberSecurity for Networks**.
2. Выберите нужный тенант.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.

3. В поле **Период обновления данных** укажите требуемую частоту в часах. Значение по умолчанию – 3.

Расписание импорта изменено.

См. также:

Особенности импорта информации об активах из KICS for Networks 126

Особенности импорта информации об активах из KICS for Networks

Импорт активов

Активы импортируются в соответствии с правилами импорта активов (см. раздел "Добавление активов" на стр. 381). Импортируются только активы со статусами **Разрешенное** и **Неразрешенное**.

Активы KICS for Networks идентифицируются по комбинации следующих параметров:

- IP-адрес экземпляра KICS for Networks, с которым настроена интеграция.
- Идентификатор коннектора KICS for Networks, с помощью которого настроена интеграция.
- Идентификатор, присвоенный активу (или "устройству") в экземпляре KICS for Networks.

Импорт сведений об уязвимостях

При импорте активов в KUMA также поступают сведения об активных уязвимостях KICS for Networks. Если в KICS for Networks уязвимость была помечена как устраненная или незначительная, сведения о ней удаляются из KUMA при следующем импорте.

Сведения об уязвимостях активов отображаются в окне **Информация об активе** в блоке параметров **Уязвимости** на языке локализации KICS for Networks.

В KICS for Networks уязвимости называются рисками и разделяются на несколько типов. В KUMA импортируются все типы рисков.

Срок хранения импортированных данных

Если сведения о ранее импортированном активе перестают поступать из KICS for Networks, актив удаляется по прошествии 30 дней.

Изменение статуса актива KICS for Networks

После настройки интеграции вы можете менять статусы активов KICS for Networks из KUMA. Статусы можно менять автоматически и вручную.

Статусы активов можно менять, только если вы включили реагирование (см. раздел "Настройка интеграции в KUMA" на стр. 125) в настройках подключения к KICS for Networks.

Изменение статуса актива KICS for Networks вручную

Пользователи с ролями (см. раздел "Роли пользователей" на стр. 57) Главный Администратор, Администратор и Аналитик в доступных им тенантах могут вручную менять статусы активов, импортированных из KICS for Networks.

► *Чтобы вручную изменить статус актива KICS for Networks:*

1. В разделе **Активы** веб-интерфейса KUMA нажмите на актив, который вы хотите изменить.

   В правой части окна откроется область **Информация об активе**.

2. В раскрывающемся списке **Статус KICS for Networks** выберите статус, который необходимо присвоить активу KICS for Networks. Доступны статусы *Разрешенное* или *Неразрешенное*.

Статус актива изменен. Новый статус отображается в KICS for Networks и в KUMA.

Изменение статуса актива KICS for Networks автоматически

Автоматическое изменение статусов активов KICS for Networks реализовано с помощью правил реагирования (см. раздел "Правила реагирования для KICS for Networks" на стр. 219). Правила необходимо добавить в коррелятор (см. раздел "Создание коррелятора" на стр. 252), который будет определять условия их срабатывания.

kaspersky

Ресурсы KUMA

Ресурсы – это компоненты KUMA, которые содержат параметры для реализации различных функций: например, установления связи с заданным веб-адресом или преобразования данных по определенным правилам. Из этих компонентов, как из частей конструктора, собираются наборы ресурсов для сервисов (на стр. 235), на основе которых в свою очередь создаются сервисы (см. раздел "Сервисы KUMA" на стр. 229) KUMA.

Ресурсы содержатся в разделе веб-интерфейса KUMA **Ресурсы** в блоке **Ресурсы**. Доступные типы ресурсов:

- **Правила корреляции** (на стр. 134) – в ресурсах этого типа содержатся правила определения в событиях закономерностей, указывающих на угрозы. Если условия, заданные в этих ресурсах, выполняются, создается корреляционное событие.
- **Нормализаторы** (на стр. 158) – в ресурсах этого типа содержатся правила для приведения поступающих событий к формату, принятому в KUMA (см. раздел "Модель данных нормализованного события" на стр. 471). После обработки в нормализаторе "сырое" событие становится нормализованным и может обрабатываться другими ресурсами и сервисами KUMA.
- **Коннекторы** (на стр. 169) – в ресурсах этого типа содержатся параметры для установления сетевых подключений.
- **Правила агрегации** (на стр. 194) – в ресурсах этого типа содержатся правила для объединения нескольких однотипных базовых событий в одно агрегационное событие.
- **Правила обогащения** (на стр. 194) – в ресурсах этого типа содержатся правила для дополнения событий информацией из сторонних источников.
- **Точки назначения** (на стр. 199) – в ресурсах этого типа содержатся параметры для пересылки событий в пункт дальнейшей обработки или хранения.
- **Фильтры** (на стр. 212) – в ресурсах этого типа содержатся условия для отсева или выделения отдельных событий из потока событий.
- **Реагирование** (см. раздел "**Правила реагирования**" на стр. 217) – ресурсы этого типа используются в корреляторах для выполнения скриптов или запуска задач Kaspersky Security Center при выполнении определенных условий.
- **Шаблоны уведомлений** (на стр. 220) – ресурсы этого типа используются при рассылке уведомлений (см. раздел "Уведомления KUMA" на стр. 410) о новых алертах.
- **Активные листы** (на стр. 224) – ресурсы этого типа используются корреляторами для динамической работы с данными при анализе событий по правилам корреляции.
- **Словари** (на стр. 225) – ресурсы этого типа используются для хранения ключей и их значений, которые могут потребоваться другим ресурсам и сервисам KUMA.
- **Прокси-серверы** (на стр. 226) – в ресурсах этого типа содержатся параметры использования прокси-серверов.
- **Секреты** (на стр. 226) – ресурсы этого типа используются для безопасного хранения конфиденциальной информации (например, учетных данных), которые должны использоваться KUMA для взаимодействия с внешними службами.

При нажатии на тип ресурса открывается окно, в котором отображается таблица с имеющимися ресурсами этого типа. Таблица содержит следующие столбцы:

- **Название** – имя ресурса. Может использоваться для поиска и сортировки ресурсов.

- **Последнее обновление** – дата и время последнего обновления ресурса. Может использоваться для сортировки ресурсов.
- **Создал** – имя пользователя, создавшего ресурс.
- **Описание** – описание ресурса.

Ресурсы можно расположить по папкам (см. раздел "Создание, переименование, перемещение и удаление папок ресурсов" на стр. 130). В левой части каждого окна отображается структура папок, причем количество и названия корневых папок соответствуют созданным в KUMA тенантам. Когда папка выбрана, содержащиеся в ней ресурсы отображаются в таблице в правой части окна.

Ресурсы можно создавать, редактировать, копировать, перемещать между папками и удалять (см. раздел "Создание, дублирование, перемещение, редактирование и удаление ресурсов" на стр. 131). Ресурсы можно также экспортировать и импортировать (см. раздел "Экспорт и импорт ресурсов" на стр. 132).

В этом разделе

Операции с ресурсами 129
Правила корреляции 134
Нормализаторы 158
Коннекторы 169
Правила агрегации 194
Правила обогащения 194
Точки назначения 199
Фильтры 212
Правила реагирования 217
Шаблоны уведомлений 220
Активные листы 224
Словари 225
Прокси-серверы 226
Секреты 226

Операции с ресурсами

Вы можете управлять ресурсами KUMA: создавать, перемещать, копировать, редактировать и удалять ресурсы, а также импортировать и экспортировать их. Перечисленные операции доступны для всех ресурсов, вне зависимости от типа ресурса.

Ресурсы KUMA располагаются в папках. Вы можете добавлять, переименовывать, перемещать и удалять папки ресурсов.

kaspersky

В этом разделе

Создание, переименование, перемещение и удаление папок ресурсов 130
Создание, дублирование, перемещение, редактирование и удаление ресурсов 131
Экспорт и импорт ресурсов 132

Создание, переименование, перемещение и удаление папок ресурсов

Папки можно создавать, переименовывать, перемещать и удалять.

► *Чтобы создать папку:*

1. Выберите в дереве папку, в которой требуется новая папка.
2. Нажмите на кнопку **Добавить папку**.

Папка будет создана.

► *Чтобы переименовать папку:*

1. Найдите нужную папку в структуре папок.
2. Наведите курсор на название папки.

   Рядом с названием папки появится значок ⋯.
3. В раскрывающемся списке ⋯ выберите **Переименовать**.

   Название папки станет доступным для редактирования.
4. Введите новое название папки и нажмите **ENTER**.

   Название папки не может быть пустым.

Папка будет переименована.

► *Чтобы переместить папку,*

Нажмите название папки и перетащите ее в требуемое место в структуре папок.

Папки невозможно переместить из одного тенанта в другой

► *Чтобы удалить папку:*

1. Найдите нужную папку в структуре папок.
2. Наведите курсор на название папки.

Рядом с названием папки появится значок ⋯.

3. В раскрывающемся списке ⋯ выберите **Удалить**.

   Появится окно подтверждения.

4. Нажмите **ОК**.

Папка будет удалена.

> Программа не удаляет папки, которые содержат файлы или подпапки.

Создание, дублирование, перемещение, редактирование и удаление ресурсов

Вы можете создавать, перемещать, копировать, редактировать и удалять ресурсы.

► *Чтобы создать ресурс:*

1. В разделе **Ресурсы** → **<тип ресурса>** выберите или создайте папку, в которую требуется добавить новый ресурс.

   Корневые папки соответствуют тенантам. Чтобы ресурс был доступен определенному тенанту, его следует создать в папке этого тенанта.

2. Нажмите кнопку **Добавить <тип ресурса>**.

   Откроется окно для настройки параметров выбранного типа ресурсов. Доступные параметры зависят от типа ресурса.

3. Введите уникальное имя ресурса в поле **Название**.
4. Укажите обязательные параметры (они отмечены красной звездочкой).
5. При желании укажите дополнительные параметры (это необязательное действие).
6. Нажмите **Сохранить**.

Ресурс будет создан и доступен для использования в сервисах и других ресурсах.

► *Чтобы переместить ресурс в новую папку:*

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.
2. Установите флажки рядом с ресурсами, которые вы хотите переместить. Можно выбрать сразу несколько ресурсов.

   Рядом с выбранными ресурсами отобразится значок ⠿.

3. Перетащите ресурсы в нужную папку с помощью значка ⠿.

Ресурсы будут перемещены в новые папки.

> Вы можете перемещать ресурсы только в папки того тенанта, в рамках которого были созданы ресурсы. Перемещение ресурсов в папки другого тенанта недоступно.

► *Чтобы скопировать ресурс:*

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.
2. Установите флажок рядом с ресурсом, которые вы хотите скопировать, и нажмите **Дублировать**.

   Отображается окно с параметрами ресурса, который вы выбрали для копирования. Доступные параметры зависят от типа ресурса.

   В поле **Название** отображается `<название выбранного ресурса> - копия`.
3. Измените нужные параметры.
4. Введите уникальное имя в поле **Название**.
5. Нажмите **Сохранить**.

Копия ресурса будет создана.

► *Чтобы изменить ресурс:*

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.
2. Выберите ресурс.

   Отображается окно с параметрами выбранного ресурса. Доступные параметры зависят от типа ресурса.
3. Измените нужные параметры.
4. Нажмите **Сохранить**.

Ресурс будет обновлен. Если этот ресурс используется в сервисе, перезапустите сервис (см. раздел "Перезапуск сервиса" на стр. 231), чтобы он задействовал новые параметры.

► *Чтобы удалить ресурс:*

1. В разделе **Ресурсы** → **<тип ресурса>** найдите требуемый ресурс в структуре папок.
2. Установите флажок рядом с ресурсом, которые вы хотите удалить, и нажмите **Удалить**.

   Откроется окно подтверждения.
3. Нажмите **ОК**.

Ресурс будет удален.

Экспорт и импорт ресурсов

Вы можете экспортировать и импортировать ресурсы.

► *Чтобы экспортировать ресурсы:*

1. В разделе **Ресурсы** → **<тип ресурса>** нажмите на значок  .
2. В раскрывающемся списке выберите **Экспортировать ресурсы**.

   Откроется окно **Экспортировать ресурсы** с деревом всех доступных ресурсов.
3. В поле **Пароль** введите пароль, который необходимо использовать для защиты экспортируемых данных.

4. В раскрывающемся списке **Тенант** выберите тенант, ресурсы которого вы хотите экспортировать.
5. Установите флажки рядом с ресурсами, которые вы хотите экспортировать.

   Если выбранные ресурсы связаны с другими ресурсами, эти ресурсы также будут экспортированы.
6. Нажмите на кнопку **Экспортировать**.

Ресурсы в защищенном паролем файле сохранятся на вашем компьютере в зависимости от настроек вашего браузера. Ресурсы секретов экспортируются пустыми.

► *Чтобы импортировать ресурсы:*

1. В раскрывающемся списке  выберите **Импортировать ресурсы**.

   Откроется окно **Импорт ресурсов**.
2. В поле **Пароль** введите пароль для файла, который вы хотите импортировать.
3. В раскрывающемся списке **Тенант** выберите тенант, которому будут принадлежать импортируемые ресурсы.
4. Нажмите на кнопку **Выбрать файл** и укажите файл с ресурсами, которые вы хотите импортировать.

   В окне **Импорт ресурсов** отображается дерево всех доступных ресурсов в выбранном файле.
5. Выберите ресурсы, которые хотите импортировать.
6. Нажмите на кнопку **Импортировать**.
7. Разрешите конфликты (см. ниже) между импортированными и существующими ресурсами, если они возникли. Подробнее о конфликтах ресурсов см. ниже.
   a. Если имя любого из импортированных ресурсов совпадает с именем уже существующего ресурса, открывается окно **Конфликты** с таблицей, в которой отображаются тип и имя конфликтующих ресурсов. Разрешите отображаемые конфликты:
      - Если вы хотите заменить существующий ресурс новым, нажмите **Заменить**.

        Нажмите **Заменить все**, чтобы заменить все конфликтующие ресурсы.
      - Если вы хотите оставить существующий ресурс, нажмите **Пропустить**.

        Нажмите **Пропустить все**, чтобы сохранить все существующие ресурсы.
   b. Нажмите на кнопку **Устранить**.

Ресурсы импортируются в KUMA. Ресурсы секретов импортируются пустыми.

О разрешении конфликтов

Когда ресурсы импортируются в KUMA, программа сравнивает их с существующими ресурсами, проверяя их *название*, *тип* и параметр *guid* (идентификатор):

- Если *имя* и *тип* импортируемого ресурса совпадают с параметрами существующего ресурса, имя импортированного ресурса автоматически изменяется.
- Если идентификаторы двух ресурсов совпадают, возникает конфликт, который должен разрешить пользователь. Такая ситуация может возникнуть, когда вы импортируете ресурсы на тот же сервер KUMA, с которого они были экспортированы.

При разрешении конфликта вы можете либо *заменить существующий ресурс* импортированным, либо *оставить существующий ресурс*.

Некоторые ресурсы связаны между собой (например, для ресурса коннектора требуется ресурс подключения): такие ресурсы экспортируются и импортируются вместе. Если во время импорта возникает конфликт, и вы выбираете замену существующего ресурса новым, все связанные с ним ресурсы также будут автоматически заменены импортированными ресурсами, даже если вы выбрали для них **Пропустить**.

При импорте все ресурсы импортируются в один тенант, даже если при экспорте они принадлежали разным тенантам (например, если связанный ресурс находился в общем тенанте).

Правила корреляции

Ресурсы правила корреляции используются в сервисах (см. раздел "Сервисы KUMA" на стр. 229) коррелляторов (см. раздел "Коррелятор" на стр. 23) для распознавания определенных последовательностей обрабатываемых событий (см. раздел "О событиях" на стр. 25) и выполнения определенных действий после распознавания: например, создание корреляционных событий или алертов, взаимодействие с активным листом.

Доступные параметры правила корреляции зависят от выбранного типа. Типы правил корреляции:

- standard (см. раздел "Правила корреляции типа standard" на стр. 135) – используется для поиска корреляций между несколькими событиями. Ресурсы этого типа могут создавать корреляционные события.

  Этот тип ресурсов используется для определения сложных закономерностей в последовательности событий. Для более простых комбинаций следует использовать другие типы правил корреляции, которые требуют меньше ресурсов.

- simple (см. раздел "Правила корреляции типа simple" на стр. 139) – используется для создания событий корреляции при обнаружении определенного события.

- operational (см. раздел "Правила корреляции типа operational" на стр. 142) – используется для операций с активными листами. Этот тип ресурсов не может создавать корреляционные события.

Для этих ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов (см. раздел "Редактирование своей учетной записи" на стр. 71).

Если правило корреляции используется в корреляторе и по нему был создан алерт, то при изменении ресурса правила корреляции существующий алерт не будет изменен, даже если перезапустить сервис коррелятора. Например, если у правила корреляции было изменено название, название алерта останется прежним. Если существующий алерт закрыть, то новый алерт будет создан уже с учетом изменений ресурса правила корреляции.

В этом разделе

Правила корреляции типа standard 135

Правила корреляции типа simple 139

Правила корреляции типа operational 142

Переменные в коррелляторах 144

kaspersky

Правила корреляции типа standard

Правила корреляции типа **standard** используются для определения сложных закономерностей в обрабатываемых событиях.

Поиск закономерностей происходит с помощью контейнеров (см. раздел "Контейнеры" на стр. 138)

Окно ресурса правила корреляции содержит следующие закладки параметров:

- **Общие** – используется для указания основных параметров ресурса правила корреляции. На этой закладке можно выбрать тип правила корреляции.
- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа ресурса.
- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У ресурса правила корреляции должен быть хотя бы один триггер. Доступные параметры зависят от выбранного типа ресурса.

Закладка Общие

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.
- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **standard**, если хотите создать правило корреляции типа standard.
- **Группирующие поля** (обязательно) – поля событий, которые должны быть сгруппированы в контейнере. Хеш-код значений выбранных полей используется в качестве ключа контейнера. Если срабатывает селектор (см. ниже), отобранные поля копируются в корреляционное событие.
- **Уникальные поля** – поля событий, которые должны быть отправлены в контейнер. Если задан этот параметр, в контейнер будут отправляться только уникальные поля. Хеш-код значений отобранных полей используется в качестве ключа контейнера. Если срабатывает правило корреляции, отобранные поля копируются в корреляционное событие.
- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. Значение по умолчанию: 100.

  Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Время жизни контейнера, сек.** (обязательно) – время жизни контейнера в секундах. Этот таймер запускается при создании контейнера (когда он получает первое событие). Время жизни не обновляется, и когда оно истекает, срабатывает триггер **По истечении времени жизни контейнера** из группы настроек **Действия**, а контейнер удаляется. Триггеры **На каждом срабатывании правила** и **На последующих срабатываниях правила** могут срабатывать более одного раза в течение времени жизни контейнера.
- **Политика хранения базовых событий** – этот раскрывающийся список используется, чтобы определить, какие базовые события должны быть сохранены в корреляционном событии:

  - **first** (значение по умолчанию) – поместить в корреляционное событие первое базовое событие из коллекции событий, инициировавшей создание корреляционного события.
  - **last** – поместить в корреляционное событие последнее базовое событие из коллекции событий, инициировавшей создание корреляционного события.
  - **all** – поместить в корреляционное событие все базовые события из коллекции событий, инициировавшей создание корреляционного события.
- **Уровень важности** – базовый коэффициент, используемый для определения уровня важности правила корреляции. Значение по умолчанию: **Низкий**.
- **Сортировать по** – в этом раскрывающемся списке можно выбрать поле события, по которому селекторы правила корреляции будут отслеживать изменение ситуации. Это может пригодиться, если, например, вы захотите настроить правило корреляции на срабатывание при последовательном возникновении нескольких типов событий.
- **Описание** – описание ресурса. До 256 символов Юникода.

Закладка Селекторы

В ресурсе типа **standard** может быть несколько селекторов. Селекторы можно добавлять с помощью кнопки **Добавить селектор** и удалять с помощью кнопки **Удалить селектор**. Селекторы можно перемещать с помощью кнопки  .

Для каждого селектора доступны две закладки **Параметры** и **Локальные переменные**.

Закладка **Параметры** содержит следующие параметры:

- **Название** (обязательно) – уникальное имя группы событий, удовлетворяющее условиям селектора. Название используется для идентификации событий в объединяющем фильтре. Должно содержать от 1 до 128 символов Юникода.
- **Порог срабатывания селектора (количество событий)** (обязательно) – количество событий, которое необходимо получить для срабатывания селектора.
- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий ресурс фильтра (см. раздел "Фильтры" на стр. 212) или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

  Фильтрация по данным из поля события Extra (см. раздел "Поиск по данным поля события Extra" на стр. 215)
- **Обнуление** – этот флажок должен быть установлен, если правило корреляции НЕ должно срабатывать при получении селектором определенного количества событий. По умолчанию этот флажок снят.

На закладке **Локальные переменные** с помощью кнопки **Добавить переменную** можно объявлять переменные (см. раздел "Переменные в корреляторах" на стр. 144), которые будут действовать в пределах этого правила корреляции.

Закладка Действия

В ресурсе типа **standard** может быть несколько триггеров.

- **На первом срабатывании правила** – этот триггер срабатывает, когда контейнер регистрирует первое в течение срока своей жизни срабатывание селектора.

- **На последующих срабатываниях правила** – этот триггер срабатывает, когда контейнер регистрирует в течение срока своей жизни второе и последующие срабатывания селектора.
- **На каждом срабатывании правила** – этот триггер срабатывает каждый раз, когда контейнер регистрирует срабатывание селектора.
- **По истечении времени жизни контейнера** – этот триггер срабатывает по истечении времени жизни контейнера и используется в связке с селектором с установленным флажком **Обнуление**. То есть триггер срабатывает, если в течение заданного времени ситуация, обнаруженная правилом корреляции, не разрешается.

Каждый триггер представлен в виде группы настроек со следующими доступными параметрами:

- **Отправить событие на дальнейшую обработку** – если этот флажок установлен, корреляционное событие будет отправлено на пост-обработку: на обогащение, для реагирования и в точки назначения.
- **Отправить событие снова в коррелятор** – если этот флажок установлен, созданное корреляционное событие будет обрабатываться текущим ресурсом правила корреляции. Это позволяет достичь иерархической корреляции.

  Если установлены оба флажка, правило корреляции будет отправлено сначала на пост-обработку, а затем в селекторы текущего правила корреляции.

- **Не создавать алерт** – если этот флажок установлен, алерт не будет создаваться при срабатывании этого правила корреляции.
- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами (см. раздел "Активные листы" на стр. 224). С помощью кнопок **Добавить действие с активным листом** и **Удалить действие с активным листом** можно добавлять и удалять операции с активными листами.

  Доступные параметры:

  - **Название** (обязательно) – этот раскрывающийся список используется для выбора ресурсов активного листа.
  - **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:
    - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
    - **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.
    - **Удалить** – удалить запись из активного листа.
  - **Ключевые поля** (обязательно) – это список полей события, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

    Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в веб-интерфейсе KUMA.

- **Сопоставление** (требуется для операций **Получить** и **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.

  Левое поле используется для указания поля активного листа. Средний раскрывающийся список используется для выбора полей событий. Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.

- Группа параметров **Обогащение** – вы можете менять значения полей корреляционных событий, используя правила обогащения, аналогичные ресурсам правил обогащения (см. раздел "Правила обогащения" на стр. 194). Эти правила обогащения хранятся в ресурсе правила корреляции, в котором они были созданы. Можно создать более одного правила обогащения. Правила обогащения можно добавлять или удалять с помощью кнопок **Добавить обогащение** и **Удалить обогащение**.
  - **Тип источника** – в этом раскрывающемся списке можно выбрать тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

    Доступные типы обогащения:

    - константа (см. раздел "Обогащение, тип константа" на стр. 195)
    - словарь (см. раздел "Обогащение, тип словарь" на стр. 196)
    - событие (см. раздел "Обогащение, тип событие (для нормализатора)" на стр. 197)
    - шаблон (см. раздел "Обогащение, тип шаблон" на стр. 197)
  - **Отладка** – с помощью этого раскрывающегося списка можно включить логирование операций сервиса (см. раздел "Журналы KUMA" на стр. 408).
  - **Описание** – описание ресурса. До 256 символов Юникода.
  - Блок параметров **Фильтр** – позволяет выбрать, какие события будут отправляться на обогащение. Настройка происходит, как описано выше.
- Группа параметров **Изменение категорий** – используется для изменения категорий активов, указанных в событии. Правил категоризации может быть несколько: их можно добавить или удалить с помощью кнопок **Добавить категоризацию** или **Удалить категоризацию**. Активам можно добавлять или удалять только реактивные категории.
  - **Действие** – этот раскрывающийся список используется для выбора операции над категорией:
    - **Добавить** – присвоить категорию активу.
    - **Удалить** – отвязать актив от категории.
  - **Поле события** – поле события, в котором указан актив, над которым будет совершена операция.
  - **Идентификатор категории** – с помощью кнопки  можно выбрать категорию, над которой будет совершена операция. При нажатии на нее открывается окно **Выбор категорий**, где отображается дерево категорий.

Контейнеры

Контейнеры правила корреляции – это временные хранилища данных, которые используются ресурсами правила корреляции при определении необходимости создания корреляционных событий. Эти контейнеры выполняет следующие функции:

- Группируют события, которые были отобраны фильтрами в группе настроек **Селекторы** ресурса правила корреляции. События группируются по полям, которые указываются пользователем в поле **Группирующие поля**.
- Определяют момент, когда должно сработать правило корреляции, меняя соответствующим образом события, сгруппированные в контейнере.
- Выполняют действия, указанные в группе настроек **Действия**.
- Создают корреляционные события.

Доступные состояния контейнера:

- `Пусто` – в контейнере нет событий. Это может произойти только в момент своего создания при срабатывании правила корреляции.
- `Частичное совпадение` – в контейнере есть некоторые из ожидаемых событий (события восстановления не учитываются).
- `Полное совпадение` – в корзине есть все ожидаемые события (события восстановления не учитываются). При достижении этого состояния:
  - Срабатывает правило корреляции
  - События удаляются из контейнера
  - Счетчик срабатываний контейнера обновляется
  - Контейнера переводится в состояние `Пусто`
- `Ложное совпадение` – такое состояние контейнера возможно в следующих случаях:
  - когда было достигнуто состояние `Полное совпадение`, но объединяющий фильтр возвратил значение false.
  - когда при установленном флажке **Обнуление** были получены события восстановления.

  Когда это условие достигается, правило корреляции не срабатывает. События удаляются из контейнера, счетчик срабатываний обновляется, контейнер переводится в состояния `Пусто`.

Правила корреляции типа simple

Правила корреляции типа **simple** используются для определения простых последовательностей событий.

Окно ресурса правила корреляции содержит следующие закладки параметров:

- **Общие** – используется для указания основных параметров ресурса правила корреляции. На этой закладке можно выбрать тип правила корреляции.
- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа ресурса.
- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У ресурса правила корреляции должен быть хотя бы один триггер. Доступные параметры зависят от выбранного типа ресурса.

Закладка Общие

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.
- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **simple**, если хотите создать правило корреляции типа simple.
- **Наследуемые поля** (обязательно) – поля событий, по которым отбираются события. При срабатывания селектора (см. ниже) эти поля будут записаны в корреляционное событие.
- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. Значение по умолчанию: 100.

  Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Уровень важности** – базовый коэффициент, используемый для определения уровня важности правила корреляции. Значение по умолчанию: `Низкий`.
- **Описание** – описание ресурса. До 256 символов Юникода.

Закладка Селекторы

В ресурсе типа **simple** может быть только один селектор, для которого доступны закладки **Параметры** и **Локальные переменные**.

Закладка **Параметры** содержит параметры с блоком параметров **Фильтр**:

- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий ресурс фильтра (см. раздел "Фильтры" на стр. 212) или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

  Фильтрация по данным из поля события Extra (см. раздел "Поиск по данным поля события Extra" на стр. 215)

На закладке **Локальные переменные** с помощью кнопки **Добавить переменную** можно объявлять переменные (см. раздел "Переменные в корреляторах" на стр. 144), которые будут действовать в пределах этого правила корреляции.

Закладка Действия

В ресурсе типа **simple** может быть только один триггер: **На каждом событии**. Он активируется каждый раз, когда срабатывает селектор.

Доступные параметры триггера:

- **Отправить событие на дальнейшую обработку** – если этот флажок установлен, корреляционное событие будет отправлено на пост-обработку: на обогащение, для реагирования и в точки назначения.

- **Отправить событие снова в коррелятор** – если этот флажок установлен, созданное корреляционное событие будет обрабатываться текущим ресурсом правила корреляции. Это позволяет достичь иерархической корреляции.

  Если установлены оба флажка, правило корреляции будет отправлено сначала на пост-обработку, а затем в селекторы текущего правила корреляции.

- **Не создавать алерт** – если этот флажок установлен, алерт не будет создаваться при срабатывании этого правила корреляции.
- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами (см. раздел "Активные листы" на стр. 224). С помощью кнопок **Добавить действие с активным листом** и **Удалить действие с активным листом** можно добавлять и удалять операции с активными листами.

  Доступные параметры:

  - **Название** (обязательно) – этот раскрывающийся список используется для выбора ресурсов активного листа.
  - **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:
    - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.
    - **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.
    - **Удалить** – удалить запись из активного листа.
  - **Ключевые поля** (обязательно) – это список полей события, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

    Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в веб-интерфейсе KUMA.

  - **Сопоставление** (требуется для операций **Получить** и **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.

    Левое поле используется для указания поля активного листа. Средний раскрывающийся список используется для выбора полей событий. Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.
- Группа параметров **Обогащение** – вы можете менять значения полей корреляционных событий, используя правила обогащения, аналогичные ресурсам правил обогащения (см. раздел "Правила обогащения" на стр. 194). Эти правила обогащения хранятся в ресурсе правила корреляции, в котором они были созданы. Можно создать более одного правила обогащения. Правила обогащения можно добавлять или удалять с помощью кнопок **Добавить обогащение** и **Удалить обогащение**.
  - **Тип источника** – в этом раскрывающемся списке можно выбрать тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

    Доступные типы обогащения:

    - константа (см. раздел "Обогащение, тип константа" на стр. 195)
    - словарь (см. раздел "Обогащение, тип словарь" на стр. 196)
    - событие (см. раздел "Обогащение, тип событие (для нормализатора)" на стр. 197)
    - шаблон (см. раздел "Обогащение, тип шаблон" на стр. 197)
  - **Отладка** – с помощью этого раскрывающегося списка можно включить логирование операций сервиса (см. раздел "Журналы KUMA" на стр. 408).
  - **Описание** – описание ресурса. До 256 символов Юникода.
  - Блок параметров **Фильтр** – позволяет выбрать, какие события будут отправляться на обогащение. Настройка происходит, как описано выше.
- Группа параметров **Изменение категорий** – используется для изменения категорий активов, указанных в событии. Правил категоризации может быть несколько: их можно добавить или удалить с помощью кнопок **Добавить категоризацию** или **Удалить категоризацию**. Активам можно добавлять или удалять только реактивные категории.
  - **Действие** – этот раскрывающийся список используется для выбора операции над категорией:
    - **Добавить** – присвоить категорию активу.
    - **Удалить** – отвязать актив от категории.
  - **Поле события** – поле события, в котором указан актив, над которым будет совершена операция.
  - **Идентификатор категории** – с помощью кнопки  можно выбрать категорию, над которой будет совершена операция. При нажатии на нее открывается окно **Выбор категорий**, где отображается дерево категорий.

Правила корреляции типа operational

Правила корреляции типа **operational** используются для работы с активными листами.

Окно ресурса правила корреляции содержит следующие закладки параметров:

- **Общие** – используется для указания основных параметров ресурса правила корреляции. На этой закладке можно выбрать тип правила корреляции.
- **Селекторы** – используется для определения условий, которым должны удовлетворять обрабатываемые события для срабатывания правила корреляции. Доступные параметры зависят от выбранного типа ресурса.
- **Действия** – используется для установки триггеров, срабатывающих при выполнении условий, заданных в группе настроек **Селекторы**. У ресурса правила корреляции должен быть хотя бы один триггер. Доступные параметры зависят от выбранного типа ресурса.

Закладка Общие

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – тенант, которому принадлежит правило корреляции.

- **Тип** (обязательно) – раскрывающийся список для выбора типа правила корреляции. Выберите **operational**, если хотите создать правило корреляции типа operational.
- **Частота срабатываний** – максимальное количество срабатываний правила корреляции в секунду. Значение по умолчанию: 100.

  Если правила корреляции, в которых реализована сложная логика обнаружения закономерностей, не срабатывают, причиной могут быть особенности подсчета срабатываний правила в KUMA. Попробуйте увеличить значение **Частота срабатываний**, например, до `1000000`.

- **Описание** – описание ресурса. До 256 символов Юникода.

Закладка Селекторы

В ресурсе типа **operational** может быть только один селектор, для которого доступны закладки **Параметры** и **Локальные переменные**.

Закладка **Параметры** содержит параметры с блоком параметров **Фильтр**:

- **Фильтр** (обязательно) – используется для установки критериев определения событий, из-за которых будет срабатывать селектор. В раскрывающемся списке можно выбрать существующий ресурс фильтра (см. раздел "Фильтры" на стр. 212) или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

  Фильтрация по данным из поля события Extra (см. раздел "Поиск по данным поля события Extra" на стр. 215)

На закладке **Локальные переменные** с помощью кнопки **Добавить переменную** можно объявлять переменные (см. раздел "Переменные в корреляторах" на стр. 144), которые будут действовать в пределах этого правила корреляции.

Закладка Действия

В ресурсе типа **operational** может быть только один триггер: **На каждом событии**. Он активируется каждый раз, когда срабатывает селектор.

Доступные параметры триггера:

- Группа параметров **Обновление активных листов** – используется для назначения триггера на одну или несколько операций с активными листами (см. раздел "Активные листы" на стр. 224). С помощью кнопок **Добавить действие с активным листом** и **Удалить действие с активным листом** можно добавлять и удалять операции с активными листами.

  Доступные параметры:

  - **Название** (обязательно) – этот раскрывающийся список используется для выбора ресурсов активного листа.
  - **Операция** (обязательно) – этот раскрывающийся список используется для выбора операции, которую необходимо выполнить:
    - **Получить** – получить запись активного листа и записать значения указанных полей в корреляционное событие.

  - **Установить** – записать значения указанных полей корреляционного события в активный лист, создав новую или обновив существующую запись активного листа. При обновлении записи активного листа данные объединяются, и только указанные поля перезаписываются.
  - **Удалить** – удалить запись из активного листа.
- **Ключевые поля** (обязательно) – это список полей события, используемые для создания записи активного листа. Этот список также используется в качестве ключа записи активного листа.

  Ключ записи активного листа зависит только от состава полей и не зависит от порядка их отображения в веб-интерфейсе KUMA.

- **Сопоставление** (требуется для операций **Получить** и **Установить**) – используется для сопоставления полей активного листа с полями событий. Можно установить более одного правила сопоставления.

  Левое поле используется для указания поля активного листа. Средний раскрывающийся список используется для выбора полей событий. Правое поле можно использовать для назначения константы полю активного листа, если была выбрана операция **Установить**.

Переменные в корреляторах

Если для покрытия каких-то сценариев обеспечения безопасности недостаточно отслеживания значений в полях событий, активных листах или словарях, вы можете воспользоваться глобальными и локальными *переменными*. С их помощью можно выполнять различные действия над поступающими в корреляторы значениями, реализуя сложную логику выявления угроз. Переменные можно объявить в коррелляторе (см. раздел "Коррелятор" на стр. 23) (*глобальные переменные*) или в правиле корреляции (*локальные переменные*), присвоив им какую-либо функцию (см. раздел "Функции переменных" на стр. 146), а затем обращаться к ним из правил корреляции, как к обычным полям событий, получая в ответ результат срабатывания функции.

Область применения переменных:

- При поиске группирующих или уникальных значений полей в правилах корреляции.
- В селекторах правил корреляции в фильтрах условий, при которых должно срабатывать правило корреляции.
- При обогащении корреляционных событий. В качестве типа источника следует выбирать **Событие**.
- При наполнении активных листов значениями.

К переменным можно обращаться так же, как к полям события, предваряя их название символом $.

В этом разделе

Свойства переменных 145
Требования к переменным 145
Функции переменных 146
Объявление переменных 156
Требования к наименованию переменных 157

kaspersky

Свойства переменных

Свойства глобальных и локальных переменных различаются.

Глобальные переменные:

- Глобальные переменные объявляются (см. раздел "Шаг 2. Глобальные переменные" на стр. 254) на уровне коррелятора и действуют только в пределах этого коррелятора.
- К глобальным переменным коррелятора можно обращаться из всех правил корреляции, которые в нем указаны.
- В правилах корреляции типа standard (см. раздел "Правила корреляции типа standard" на стр. 135) одна и та же глобальная переменная в каждом селекторе может принимать разные значения.
- Невозможно переносить глобальные переменные между разными корреляторами.

Локальные переменные:

- Локальные переменные объявляются (см. раздел "Объявление переменных" на стр. 156) на уровне правила корреляции и действуют только в пределах этого правила.
- В правилах корреляции типа standard (см. раздел "Правила корреляции типа standard" на стр. 135) областью действия локальной переменной является только тот селектор, в котором переменная была объявлена.
- Локальные переменные можно объявлять в любых типах правил корреляции.
- Невозможно переносить локальные переменные между правилами или селекторами.
- Локальная переменная не может быть использована в качестве глобальной переменной.

Требования к переменным

Добавляя функцию (см. раздел "Функции переменных" на стр. 146) переменной необходимо сначала указать название функции, а затем в круглых скобках перечислить ее параметры. Исключением являются простейшие математические операции (сложение, вычитание, умножение, деление), при их использовании скобками обозначается приоритет выполнения операций.

Требования к названиям функций:

- Должно быть уникально в рамках коррелятора.
- Должно содержать от 1 до 128 символов Юникода.
- Не может начинаться с символа $.
- Должно быть написано в camelCase или CamelCase.

Особенности указания функций переменных:

- Последовательность указания параметров имеет значение.
- Параметры передаются через запятую: `,`.
- Строковые параметры передаются в одинарных кавычках: `'`.
- Наименования полей событий и переменные указываются без кавычек.
- При обращении к переменной как параметру перед ее названием необходимо добавлять символ `$`.
- Ставить пробел между параметрами необязательно.

- Во всех функциях, где в качестве параметров допускается использование переменной, допускается создавать вложенные функции.

Функции переменных

Операции с активными листами и словарями

Функция "active_list"

Получение информации из активного листа о значении в указанном столбце.

Необходимо указать параметры в следующей последовательности:

1. название активного листа;
2. название столбца активного листа;
3. ключ записи активного листа.

   В качестве ключа записи активного листа используется название одного или нескольких полей события.

Пример использования	Результат выполнения
`active_list('exampleActiveList, 'score', SourceAddress,SourceUserName)`	Получение данных из активного листа `exampleActiveList` из записи `SourceAddress,SourceUserName` из столбца `score`.

Функция "table_dict"

Получение информации о значении в указанном столбце словаря типа таблица.

Необходимо указать параметры в следующей последовательности:

1. название словаря;
2. название столбца словаря;
3. ключ строки словаря.

Пример использования	Результат выполнения
`table_dict('exampleTableDict', 'office', SourceUserName)`	Получение данных из словаря `exampleTableDict` из строки с ключом `SourceUserName` из столбца `office`.

Функция "dict"

Получение информации о значении в указанном столбце словаря типа словарь.

Необходимо указать параметры в следующей последовательности:

1. название словаря;
2. ключ строки словаря.

Пример использования	Результат выполнения
`dict('exampleDictionary', SourceAddress)`	Получение данных из словаря `exampleDictionary` из строки с ключом `SourceAddress`.

Операции со строками

Функция "len"

Возвращает число символов в строке.

Строку можно передать строкой, названием поля или переменной.

Примеры использования
`len('SomeText')`
`len(Message)`
`len($otherVariable)`

Функция "to_lower"

Перевод символов в строке в нижний регистр.

Строку можно передать строкой, названием поля или переменной.

Примеры использования
`to_lower(SourceUserName)`
`to_lower('SomeText')`
`to_lower($otherVariable)`

Функция "to_upper"

Перевод символов в строке в верхний регистр. Строку можно передать строкой, названием поля или переменной.

Примеры использования
`to_upper(SourceUserName)`
`to_upper('SomeText')`
`to_upper($otherVariable)`

Функция "append"

Добавление символов в конец строки.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;

2. добавляемая строка.

Строки можно передать строкой, названием поля или переменной.

Примеры использования	Результат использования
`append(Message, '123')`	Строка из поля `Message`, в конце которой добавлена строка `123`.
`append($otherVariable, 'text')`	Строка из переменной `otherVariable`, в конце которой добавлена строка `text`.
`append(Message, $otherVariable)`	Строка из поля `Message`, в конце которой добавлена строка из переменной `otherVariable`.

Функция "prepend"

Добавление символов в начало строки.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;
2. добавляемая строка.

Строки можно передать строкой, названием поля или переменной.

Примеры использования	Результат использования
`append(Message, '123')`	Строка из поля `Message`, в начало которой добавлена строка `123`.
`append($otherVariable, 'text')`	Строка из переменной `otherVariable`, в начало которой добавлена строка `text`.
`append(Message, $otherVariable)`	Строка из поля `Message`, в начало которой добавлена строка из переменной `otherVariable`.

Функция "substring"

Возвращает подстроку из строки.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;
2. позиция начала подстроки (натуральное число или 0);
3. (необязательно) позиция конца подстроки.

Строки можно передать строкой, названием поля или переменной. Если номер позиции больше, чем длина строки исходных данных, возвращается пустая строка.

Примеры использования	Результат использования
`substring(Message, 2)`	Возвращает часть строки из поля `Message`: от 3 символа до конца.
`substring($otherVariable, 2, 5)`	Возвращает часть строки из переменной `otherVariable`: от 3 до 6 символа.
`substring(Message, 0, len(Message) - 1)`	Возвращает всю строку из поля `Message`, кроме последнего символа.

Функция "tr"

Убирает из начала и конца строки указанные символы.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;
2. (необязательно) строка, которую следует удалить из начала и конца исходной строки.

Строки можно передать строкой, названием поля или переменной. Если строку на удаление не указать, в начале и в конце исходной строки будут удалены пробелы.

Примеры использования	Результат использования
`tr(Message)`	В начале и в конце строки из поля `Message` удалены пробелы.
`tr($otherVariable, '_')`	Если переменной `otherVariable` соответствует значение `_test_`, будет возвращена строка `test`.
`tr(Message, '@example.com')`	Если в поле события `Message` находится строка `user@example.com`, будет возвращена строка `user`.

Функция "replace"

Замена в строке всех вхождений последовательности символов A на последовательность символов B.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;
2. строка поиска: последовательность символов, подлежащая замене;
3. строка замены: последовательность символов, на которую необходимо заменить строку поиска.

Строки можно передать строкой, названием поля или переменной.

Примеры использования	Результат использования
`replace(Name, 'UserA', 'UserB')`	Возвращается строка из поля события `Name`, в которой все вхождения `UserA` заменены на `UserB`.
`replace($otherVariable, ' text ', '_text_')`	Возвращается строка из переменной `otherVariable`, в которой все вхождения `' text '` заменены на `'_text_'`.

Функция "regexp_replace"

Замена в строке последовательности символов, удовлетворяющих регулярному выражению, на последовательность символов и группы захвата регулярного выражения.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;
2. строка поиска: регулярное выражение;
3. строка замены: последовательность символов, на которую необходимо заменить строку поиска, и идентификаторы групп захвата регулярного выражения.

Строки можно передать строкой, названием поля или переменной. Допускается использовать неименованные группы захвата.

Примеры использования	Результат использования
`regexp_replace(SourceAddress, '([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3})', 'newIP: $1.$2.$3.10')`	Возвращается строка из поля события `SourceAddress`, в которой перед IP-адресами вставлен текст `newIP`. Также последние цифры адреса заменены на `10`.

Функция "regexp_capture"

Получение из исходной строки результата, удовлетворяющего условию регулярного выражения.

Необходимо указать параметры в следующей последовательности:

1. исходная строка;
2. строка поиска: регулярное выражение.

Строки можно передать строкой, названием поля или переменной. Допускается использовать неименованные группы захвата.

Примеры использования	Примеры значений	Результат использования
`regexp_replace(Message, '(\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}\\.\\d{1,3})')`	`Message = 'Access from 192.168.1.1 session 1'` `Message = 'Access from 45.45.45.45 translated address 192.168.1.1 session 1'`	`'192.168.1.1'` `'45.45.45.45'`

Операции с метками времени

Функция now

Получение временной метки в формате epoch. Запускается без аргументов.

Примеры использования
`now()`

Функция "extract_from_timestamp"

Получение атомарных представлений времени (в виде год, месяц, день, час, минута, секунда, день недели) из полей и переменных со временем в формате epoch.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Обозначение атомарного представления времени. Параметр регистрозависимый.

   Возможные варианты обозначения атомарного времени:

   - y – год в виде числа.
   - M – месяц, числовое обозначение.
   - d – число месяца.
   - wd – день недели: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday.
   - h – часы в 24-часовом формате.
   - m – минуты.
   - s – секунды.
3. (необязательно) Обозначение часового пояса. Если параметр не указан, время высчитывается в формате UTC.

Примеры использования
`extract_from_timestamp(Timestamp, 'wd')`
`extract_from_timestamp(Timestamp, 'h')`
`extract_from_timestamp($otherVariable, 'h')`
`extract_from_timestamp(Timestamp, 'h', 'Europe/Moscow')`

Функция "parse_timestamp"

Представление времени из формата RFC3339 (например, "2022-05-24 00:00:00", "2022-05-24 00:00:00+0300) в формат epoch.

Примеры использования
`parse_timestamp(Message)`
`parse_timestamp($otherVariable)`

Функция "format_timestamp"

Представление времени из формата epoch в формат RFC3339.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Обозначение формата времени: RFC3339.
3. (необязательно) Обозначение часового пояса. Если параметр не указан, время высчитывается в формате UTC.

Примеры использования
`format_timestamp(Timestamp, 'RFC3339')`
`format_timestamp($otherVariable, 'RFC3339')`
`format_timestamp(Timestamp, 'RFC3339', 'Europe/Moscow')`

Функция "truncate_timestamp"

Округление времени в формате epoch. После округления время возвращается в формате epoch. Время округляется в меньшую сторону.

Параметры необходимо указать в следующей последовательности:

1. Поле события, имеющего тип timestamp, или переменная.
2. Параметр округления:
   - 1s – округление до секунд;
   - 1m – округление до минут;
   - 1h – округление до часов;
   - 24h – округление до суток.

3. (необязательно) Обозначение часового пояса. Если параметр не указан, время высчитывается в формате UTC.

Примеры использования	Примеры округляемых значений	Результат использования
`truncate_timestamp(Timestamp, '1m')`	1654631774175 (7 June 2022 г., 19:56:14.175)	1654631760000 (7 June 2022 г., 19:56:00)
`truncate_timestamp($otherVariable, '1h')`	1654631774175 (7 June 2022 г., 19:56:14.175)	1654628400000 (7 June 2022 г., 19:00:00)
`truncate_timestamp(Timestamp, '24h', 'Europe/Moscow')`	1654631774175 (7 June 2022 г., 19:56:14.175)	1654560000000 (7 June 2022 г., 0:00:00)

Функция "time_diff"

Получение интервала времени между двумя метками времени в формате epoch.

Параметры необходимо указать в следующей последовательности:

1. Время конца отрезка. Поле события, имеющего тип timestamp, или переменная.
2. Время начала отрезка. Поле события, имеющего тип timestamp, или переменная.
3. Представление временного интервала:
   - ms – в миллисекундах;
   - s – в секундах;
   - m – в минутах;
   - h – в часах;
   - d – в днях.

Примеры использования
`time_diff(EndTime, StartTime, 's')`
`time_diff($otherVariable, Timestamp, 'h')`
`time_diff(Timestamp, DeviceReceiptTime, 'd')`

Математические операции

Представлены как простейшими математическими операциями, так и функциями.

Простейшие математические операции

Операции:

- сложение;
- вычитание;
- умножение;
- деление;
- деление по модулю.

Использование круглых скобок определяет последовательность действий

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- вещественные числа.

  При делении по модулю в качестве аргументов можно использовать только натуральные числа.

Ограничения использования:

- деление на ноль возвращает ноль;
- математические операции между числами и строками возвращают ноль;
- целые числа, полученные в результате операций, возвращаются без точки.

Примеры использования **(Type=3; otherVariable=2; Message=text)**	**Результат использования**
`Type + 1`	4
`$otherVariable - Type`	-1
`2 * 2.5`	5
`2 / 0`	0
`Type * Message`	0
`(Type + 2) * 2`	10
`Type % $otherVariable`	1

Функция "round"

Округление чисел.

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования `(DeviceCustomFloatingPoint1=7.75; DeviceCustomFloatingPoint2=7.5 otherVariable=7.2)`	Результат использования
`round(DeviceCustomFloatingPoint1)`	8
`round(DeviceCustomFloatingPoint2)`	8
`round($otherVariable)`	7

Функция "ceil"

Округление чисел в большую сторону.

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования `(DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)`	Результат использования
`ceil(DeviceCustomFloatingPoint1)`	8
`ceil($otherVariable)`	9

Функция "floor"

Округление чисел в меньшую сторону.

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования `(DeviceCustomFloatingPoint1=7.15; otherVariable=8.2)`	Результат использования
`floor(DeviceCustomFloatingPoint1)`	7
`floor($otherVariable)`	8

Функция "abs"

Получение числа по модулю.

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования `(DeviceCustomNumber1=-7; otherVariable=-2)`	Результат использования
`abs(DeviceCustomFloatingPoint1)`	7
`abs($otherVariable)`	2

Функция "pow"

Возведение числа в степень.

Параметры необходимо указать в следующей последовательности:

1. База. Вещественные числа.
2. Степень. Натуральные числа.

Доступные аргументы:

- числовые поля события;
- числовые переменные;
- числовые константы.

Примеры использования
`pow(DeviceCustomNumber1, DeviceCustomNumber2)`
`pow($otherVariable, DeviceCustomNumber1)`

Объявление переменных

Для объявления переменных их необходимо добавить в коррелятор или правило корреляции.

► *Чтобы добавить глобальную переменную в существующий коррелятор:*

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Корреляторы** выберите набор ресурсов нужного коррелятора.

   Откроется мастер установки коррелятора (см. раздел "Запуск мастера установки коррелятора" на стр. 253).
2. Выберите шаг мастера установки **Глобальные переменные**.
3. Нажмите на кнопку **Добавить переменную** и укажите следующие параметры:
   - В окне **Переменная** введите название переменной.

Требования к наименованию переменных (см. раздел "Требования к наименованию переменных" на стр. 157)

- В окне **Значение** введите функцию переменной.

  Описание функций переменных (см. раздел "Функции переменных" на стр. 146).

Переменных можно добавить несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

4. Выберите шаг мастера установки **Проверка параметров** и нажмите **Сохранить**.

Глобальная переменная добавлена в коррелятор. К ней можно обращаться, как к полю события, указывая перед названием переменной символ $. Переменная будет использоваться при корреляции после перезапуска (см. раздел "Перезапуск сервиса" на стр. 231) сервиса коррелятора.

► *Чтобы добавить локальную переменную в существующее правило корреляции:*

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Правила корреляции** выберите ресурс нужного правила корреляции.

   Откроется окно параметров правила корреляции. Параметры правила корреляции можно также открыть из коррелятора (см. раздел "Запуск мастера установки коррелятора" на стр. 253), в которое оно было добавлено, перейдя на шаг мастера установки **Корреляция**.

2. Откройте закладку **Селекторы**.
3. В селекторе откройте закладку **Локальные переменные**, нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

   - В окне **Переменная** введите название переменной.

     Требования к наименованию переменных (см. раздел "Требования к наименованию переменных" на стр. 157)

   - В окне **Значение** введите функцию переменной.

     Описание функций переменных (см. раздел "Функции переменных" на стр. 146).

   Переменных можно добавить несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

   Для правил корреляции типа standard (см. раздел "Правила корреляции типа standard" на стр. 135) повторите этот шаг для каждого селектора, в которым вы хотите объявить переменные.

4. Нажмите **Сохранить**.

Локальная переменная добавлена в правило корреляции. К ней можно обращаться, как к полю события, указывая перед названием переменной символ $. Переменная будет использоваться при корреляции после перезапуска (см. раздел "Перезапуск сервиса" на стр. 231) сервиса коррелятора.

Добавленные переменные можно изменить или удалить. Если правило корреляции обращается к необъявленной переменной (например, если ее название было изменено), в качестве результата возвращается пустая строка.

Требования к наименованию переменных

- Должно быть уникально в рамках коррелятора.
- Должно содержать от 1 до 128 символов Юникода.
- Не может начинаться с символа $.

- Должно быть написано в camelCase или CamelCase.

Нормализаторы

Ресурсы нормализатора используются для приведения "сырых" событий (см. раздел "О событиях" на стр. 25) из различных форматов к модели данных событий KUMA (см. раздел "Модель данных нормализованного события" на стр. 471). Это превращает "сырые" события в нормализованные, которые уже могут обрабатываться другими ресурсами (см. раздел "Ресурсы KUMA" на стр. 128) и сервисами (см. раздел "Сервисы KUMA" на стр. 229) KUMA.

Ресурс нормализатора состоит из *основного* и необязательных *дополнительных нормализаторов*. Данные передаются по древовидной структуре нормализаторов в зависимости от заданных *условий*, что позволяет настроить сложную логику обработки событий.

Ресурс нормализатора создается в несколько этапов:

a. **Создание основного нормализатора**

   Основной нормализатор создается с помощью кнопки **Добавить парсинг событий**. Ввод параметров нормализатора (см. раздел "Параметры нормализатора" на стр. 159) завершается нажатием кнопки **ОК**.

   Созданный основной нормализатор отображается в виде темного кружка. Можно нажать на кружок, чтобы открыть параметры нормализатора для редактирования. При наведении на кружок отображается значок плюса: при нажатии на него можно добавить дополнительные нормализаторы.

b. **Создание условий для использования дополнительного нормализатора**

   При нажатии на нормализаторе значка плюса откроется окно **Добавление дополнительного нормализатора**, в котором вы можете определить условия (см. раздел "Условие передачи данных в дополнительный нормализатор" на стр. 164), при которых данные будут поступать в новый нормализатор.

c. **Создание дополнительного нормализатора**

   При завершении предыдущего этапа открывается окно создания дополнительного нормализатора. Ввод параметров нормализатора (см. раздел "Параметры нормализатора" на стр. 159) завершается нажатием кнопки **ОК**.

   Созданный дополнительный нормализатор отображается в виде темного блока, на котором указаны условия, при котором этот нормализатор будет задействован (см. этап 2). Условия можно изменить, наведя указатель мыши на дополнительный нормализатор и нажав кнопу с изображением карандаша.

   Если навести указатель мыши на дополнительный нормализатор, отобразится кнопка со значком плюса, с помощью которой можно создать новый дополнительный нормализатор. С помощью кнопки со значком корзины нормализатор можно удалить.

   Если требуется создать больше дополнительных нормализаторов, повторите этапы 2 и 3.

d. **Завершение создания ресурса нормализатора**

   Создание ресурса нормализатора завершается нажатием кнопки **Сохранить**.

Для этих ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов (см. раздел "Редактирование своей учетной записи" на стр. 71).

Если изменить или удалить преобразования в ресурсе нормализатора (см. раздел "Нормализаторы" на стр. 158) в существующем наборе ресурсов (см. раздел "Наборы ресурсов для сервисов" на стр. 235) для коллектора (см. раздел "Создание коллектора" на стр. 235), правки в нормализаторе не сохранятся, а сам ресурс может быть поврежден. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, правки необходимо вносить непосредственно в ресурс в разделе веб-интерфейса **Ресурсы** → **Нормализаторы**.

См. также:

Требования к переменным.....145

Параметры нормализатора

Окно нормализатора содержит две закладки: **Схема нормализации** и **Обогащение**.

Схема нормализации

Эта закладка используются для указания основных параметров нормализатора, а также определения правил приведения событий к формату KUMA.

Доступные параметры:

- **Название** (обязательно) – имя нормализатора. Должно содержать от 1 до 128 символов Юникода. Название основного нормализатора будет использоваться в качестве названия ресурса нормализатора.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.

  Этот параметр недоступен для дополнительных нормализаторов.
- **Метод парсинга** (обязательно) – выпадающий список для выбора типа входящих событий. В зависимости от выбора можно будет воспользоваться преднастроенными правилами сопоставления полей событий или же задать свои собственные правила. При выборе некоторых методов парсинга могут стать доступны дополнительные параметры, требуемые для заполнения.

  Доступные методы парсинга:

  - json (см. раздел "Нормализатор, тип json" на стр. 162)
  - cef (см. раздел "Нормализатор, тип cef" на стр. 161)
  - regexp (см. раздел "Нормализатор, тип regexp" на стр. 163)
  - syslog (см. раздел "Нормализатор, тип syslog" на стр. 163)
  - csv (см. раздел "Нормализатор, тип csv" на стр. 161)
  - kv (см. раздел "Нормализатор, тип kv" на стр. 162)
  - xml (см. раздел "Нормализатор, тип xml" на стр. 164)
  - netflow5 (см. раздел "Нормализатор, тип netflow5" на стр. 162)
  - netflow9 (см. раздел "Нормализатор, тип netflow9" на стр. 162)
  - sflow5 (см. раздел "Нормализатор, тип sflow5" на стр. 163)

  - ipfix (см. раздел "Нормализатор, тип ipfix" на стр. 162)
  - sql (см. раздел "Нормализатор, тип sql" на стр. 163)
- **Хранить исходное событие** (обязательно) – с помощью этого раскрывающегося списка можно указать, надо ли сохранять исходное "сырое" событие во вновь созданном нормализованном событии. Доступные значения:
  - **Не хранить** – не сохранять исходное событие. Это значение используется по умолчанию.
  - **При возникновении ошибок** – сохранять исходное событие в поле `Raw` нормализованного события, если в процессе парсинга возникли ошибки. Это значение удобно использовать при отладке сервиса: в этом случае появление у событий непустого поля `Raw` будет являться признаком неполадок.

    Если поля с названиями `*Address` или `*Date*` не соответствуют правилам нормализации, такие поля игнорируются. При этом не возникает ошибка нормализации и значения полей не попадают в поле `Raw` нормализованного события, даже если был указан параметр **Хранить исходное событие → При возникновении ошибок**.
  - **Всегда** – сохранять сырое событие в поле `Raw` нормализованного события.

  Этот параметр недоступен для дополнительных нормализаторов.
- **Сохранить дополнительные поля** (обязательно) – в этом раскрывающемся списке можно выбрать, хотите ли вы сохранять поля и их значения, для которых не настроены правила сопоставления (см. ниже). Эти данные сохраняются в поле события **Extra** в виде массива. Нормализованные события можно искать (см. раздел "Создание SQL-запроса вручную" на стр. 345) и фильтровать по данным, хранящимся в поле **Extra**.

  Фильтрация по данным из поля события Extra (см. раздел "Поиск по данным поля события Extra" на стр. 215)

  По умолчанию дополнительные поля не сохраняются.
- **Описание** – описание ресурса: до 256 символов Юникода.

  Этот параметр недоступен для дополнительных нормализаторов.
- **Примеры событий** – в это поле можно поместить пример данных, которые вы хотите обработать. Пример событий можно также загрузить из файла формата tsv, csv или txt с помощью кнопки **Загрузить из файла**.

  Этот параметр недоступен для метода парсинга sFlow5.
- Блок параметров **Сопоставление** – здесь можно настроить сопоставление полей исходного события с полями события в формате KUMA (см. раздел "Модель данных нормализованного события" на стр. 471):
  - **Исходные данные** – столбец для названий полей исходного события, которые вы хотите преобразовать в поля события KUMA.

    Если рядом с названиями полей в столбце **Исходные данные** нажать на кнопку  , откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

    Доступные преобразования (см. раздел "Преобразования" на стр. 168)
  - **Поле KUMA** – раскрывающийся список для выбора требуемых полей событий KUMA. Поля можно искать, вводя в поле их названия.

- **Подпись** – в этом столбце можно добавить уникальную пользовательскую метку полям событий, которые начинаются с DeviceCustom*.

Новые строки таблицы можно добавлять с помощью кнопки **Добавить строку**. Строки можно удалять по отдельности с помощью кнопки ✕ или все сразу с помощью кнопки **Очистить все**.

Если вы загрузили данные в поле **Примеры событий**, в таблице отобразится столбец **Примеры** с примерами значений, переносимых из поля исходного события в поле события KUMA.

Обогащение

Эта закладка используются для дополнения полей нормализованного события другими данными с помощью правил обогащения, аналогичным правилам в ресурсах правил обогащения (см. раздел "Правила обогащения" на стр. 194). Эти правила хранятся в ресурсе нормализатора, в котором они были созданы. Правил обогащения может быть несколько. Обогащения создаются с помощью кнопки **Добавить обогащение**.

Параметры, доступные в блоке параметров правила обогащения:

- **Тип источника** (обязательно) – раскрывающийся список для выбора типа обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

  Доступные типы источников обогащения:

  - константа (см. раздел "Обогащение, тип константа" на стр. 195)
  - словарь (см. раздел "Обогащение, тип словарь" на стр. 196)
  - событие (см. раздел "Обогащение, тип событие (для нормализатора)" на стр. 197)
  - шаблон (см. раздел "Обогащение, тип шаблон" на стр. 197)
- **Целевое поле** (обязательно) – раскрывающийся список для выбора поля события KUMA, в которое следует поместить данные.

Нормализатор, тип cef

Этот метод парсинга используется для обработки данных в формате CEF.

При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

Нормализатор, тип csv

Этот метод парсинга используется для создания собственных правил обработки данных в формате CSV.

При выборе этого метода необходимо в поле **Разделитель** указать один из возможных разделителей значений:

- `\n` (используется по умолчанию)
- `\t`
- `\0`

Нормализатор, тип ipfix

Этот метод парсинга используется для обработки данных в формате IPFIX.

При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

В правилах сопоставления по умолчанию для типа **netflow** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow в закладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

Нормализатор, тип json

Этот метод парсинга используется для обработки данных в формате JSON.

Нормализатор, тип kv

Этот метод парсинга используется для обработки данных в формате ключ-значение.

При выборе этого метода необходимо указать значения в следующих обязательных полях:

- **Разделитель пар** – укажите символ, которые будет служит разделителем пар ключ-значение. По умолчанию используется символ перевода строки, однако допускается указать любое односимвольное (1 байт) значение при условии, что символ не будет совпадать с разделителем значений.
- **Разделитель значений** – укажите символ, который будет служить разделителем между ключом и значением. По умолчанию используется символ "=", однако допускается указать любое односимвольное (1 байт) значение при условии, что символ не будет совпадать с разделителем пар ключ-значение.

Нормализатор, тип netflow5

Этот метод парсинга используется для обработки данных в формате NetFlow v5.

При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

В правилах сопоставления по умолчанию для типа **netflow** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow в закладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

Нормализатор, тип netflow9

Этот метод парсинга используется для обработки данных в формате NetFlow v9.

При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

В правилах сопоставления по умолчанию для типа **netflow** тип протокола не указывается в полях событий KUMA. При парсинге данных в формате NetFlow в закладке нормализатора **Обогащение** следует создать правило обогащения данных типа **constant**, добавляющее значение `netflow` в целевое поле `DeviceProduct`.

Нормализатор, тип regexp

Этот метод парсинга используется для создания собственных правил обработки данных в формате JSON.

В поле блока параметров **Нормализация** необходимо добавить регулярное выражение (синтаксис RE2) с именованными группами захвата: имя группы и ее значение будут считаться полем и значением "сырого" события, которое можно будет преобразовать в поле события формата KUMA.

► *Чтобы добавить правила обработки событий:*

1. Скопируйте в поле **Примеры событий** пример данных, которые вы хотите обработать. Это необязательный, но рекомендуемый шаг.
2. В поле блока параметров **Нормализация** добавьте регулярное выражение с именованными группами захвата в синтаксисе RE2, например "(?P<name>regexp)".

   Можно добавить несколько регулярных выражений с помощью кнопки **Добавить регулярное выражение**. При необходимости удалить регулярное выражение, воспользуйтесь кнопкой ✕.
3. Нажмите на кнопку **Перенести названия полей в таблицу**.

   Имена групп захвата отображаются в столбце **Поле KUMA** таблицы **Сопоставление**. Теперь в столбце напротив каждой группы захвата можно выбрать соответствующее ей поле KUMA или, если вы именовали группы захвата в соответствии с форматом CEF, можно воспользоваться автоматическим сопоставлением CEF, поставив флажок **Использовать синтаксис CEF при нормализации**.

Правила обработки событий добавлены.

Нормализатор, тип sflow5

Этот метод парсинга используется для обработки данных в формате sFlow5.

При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

Нормализатор, тип sql

Этот метод парсинга используется для обработки данных в формате SQL.

Нормализатор, тип syslog

Этот метод парсинга используется для обработки данных в формате syslog.

При выборе этого метода можно воспользоваться преднастроенными правилами преобразования событий в формат KUMA, нажав на кнопку **Применить сопоставление по умолчанию**.

Нормализатор, тип xml

Этот метод парсинга используется для обработки данных в формате XML.

При выборе этого метода в блоке параметров **Атрибуты XML** можно указать ключевые атрибуты, которые следует извлекать из тегов. Если в структуре XML в одном теге есть атрибуты с разными значениями, можно определить нужное значение, указав ключ к нему в столбце **Исходные данные** таблицы **Сопоставление**.

► *Чтобы добавить ключевые атрибуты XML,*

нажмите на кнопку **Добавить поле** и в появившемся окне укажите путь к нужному атрибуту.

Можно добавить несколько атрибутов. Атрибуты можно удалить по одному с помощью значка с крестиком или все сразу с помощью кнопки **Сбросить**.

Если ключевые атрибуты XML не указаны, при сопоставлении полей уникальный путь к значению XML будет представлен последовательностью тегов.

Условие передачи данных в дополнительный нормализатор

Окно **Добавление дополнительного нормализатора** используется для определения условий, при которых данные будут попадать в дополнительный нормализатор.

Доступные параметры:

- **Поля, которые следует передать в нормализатор** – используется для указания полей события в том случае, если вы хотите отправлять в дополнительный нормализатор только события с определенными полями.

  Если оставить это поле пустым, в дополнительный нормализатор для обработки будет передано событие целиком.

- **Нормализовать, если поле события имеет определенное значение** – используется для указания полей события, если вы хотите отправлять в дополнительный нормализатор только события, в которых определенным полям присвоены определенные значения. Значение указывается в поле **Значение условия**.

  Обрабатываемые этими условиями данные можно предварительно преобразовать, если нажать на кнопку : откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

  Доступные преобразования (см. раздел "Преобразования" на стр. 168)

kaspersky

Предустановленные нормализаторы

В поставку KUMA включены перечисленные в таблице ниже нормализаторы.

Наименование нормализатора	Источник событий	Тип	Комментарий
[OOTB] 1C EventJournal Normalizer	Журнал регистрации 1С.	xml	
[OOTB] 1C TechJournal Normalizer	Технологический журнал 1С.	regexp	
[OOTB] Apache Access Syslog (Common or Combined Log Format)	Apache access.log в формате Common or Combined Log Format), с Syslog-заголовком.	syslog	
[OOTB] Apache Access file (Common or Combined Log Format)	Apache access.log в формате Common or Combined Log Format).	regexp	Чтение файла.
[OOTB] BIND Syslog	Журналы DNS сервера BIND, с заголовком Syslog.	syslog	
[OOTB] BIND file	Журналы DNS сервера BIND.	regexp	Чтение файла.
[OOTB] Bastion SKDPU-GW	ИТ Бастион Система СКДПУ.	syslog	
[OOTB] CEF	События в формате CEF от произвольных источников.	cef	
[OOTB] Checkpoint Syslog CEF by CheckPoint	Checkpoint, нормализация на основании вендорской схемы представления событий в формат CEF.	syslog	
[OOTB] Checkpoint Syslog basic	Пользовательское сопоставление полей Checkpoint, нормализация в зависимости от типа устройства.	syslog	
[OOTB] Cisco Basic	Cisco ASA базовый набор событий.	syslog	
[OOTB] Cisco ASA Extended v 0.1	Cisco ASA базовый расширенный набор событий.	syslog	
[OOTB] Cisco WSA AccessFile	Прокси-сервер Cisco WSA, файл access.log.	regexp	Чтение файла.

[OOTB] Continent SQL	Континент АПКШ, запросы к БД, таблицы AlertLog, PacketLog, ServerAccessLog, SystemLog.	sql	
[OOTB] CyberTrace	События Kaspersky CyberTrace.	regexp	
[OOTB] DNS Windows	Журналы DNS сервера Windows.	regexp	Чтение файла.
[OOTB] Dovecot Syslog	Журналы POP3/IMAP сервера dovecpt.	syslog	
[OOTB] Exchange CSV	Журналы MTA сервера Exchange.	csv	Чтение файла.
[OOTB] FortiGate KV	Журналы FortiGate в формате Key-Value.	regexp	
[OOTB] Fortimail	Журналы почтовой системы Fortimail.	regexp	
[OOTB] FreeIPA	Журналы службы каталогов Free IPA.	json	
[OOTB] Huawei USG Basic	Журналы основных модулей USG.	syslog	
[OOTB] IIS Log File Format	Журналы Microsoft IIS.	regexp	Чтение файла.
[OOTB] IPFIX	События Netflow формата IPFIX.	ipfix	
[OOTB] InfoWatch Traffic Monitor	DLP система Traffic Monitor компании InfoWatch.	sql	
[OOTB] Juniper - JUNOS	Журналы сетевого оборудования Juniper.	regexp	
[OOTB] KATA	Kaspersky Anti Target Attack.	cef	
[OOTB] KICS4Net v2.x	Kaspersky Industrial Cyber Security v 2.x.	cef	
[OOTB] KICS4Net v3.x	Kaspersky Industrial Cyber Security v 3.x.	syslog	
[OOTB] KSC	Kaspersky Security Center.	cef	Пассивное получение событий от KSC: KUMA прослушивает порт, KSC отправляет события.
[OOTB] KSC from SQL	Kaspersky Security Center, запросы к БД MS SQL.	sql	Активное получение событий из KSC: KUMA получает события из БД KSC.
[OOTB] KSMG	Kaspersky Security Mail	syslog	

	Gateway.		
[OOTB] KWTS (KV)	Журналы KWTS в случае их отправки в формате Key-Value.	syslog	
[OOTB] Linux audit and iptables Syslog	События linux.	syslog	
[OOTB] Linux audit.log file	События linux.	regexp	Чтение файла.
[OOTB] MS DHCP file	Журналы DHCP сервера Windows.	csv	Чтение файла.
[OOTB] NetFlow v5	События Netflow v5.	netflow5	
[OOTB] NetFlow v9	События Netflow v9.	netflow9	
[OOTB] Nginx regexp	Журнал Nginx.	regexp	
[OOTB] PA-NGFW (Syslog-CSV)	Журналы Palo Alto в формате CSV.	csv	Предпочтительный вариант отправки журналов - формат CEF. Отправка журналов в csv, только если отправка в CEF невозможна.
[OOTB] PTsecurity NAD	Network Anomaly Detection компании Positive Technologies.	syslog	
[OOTB] PT WAF	Web Application Firewall компании Positive Technologies.	syslog	
[OOTB] SecretNet SQL	Secret Net 7.	sql	
[OOTB] Squid access Syslog	Журналы access.log прокси-сервера Squid.	syslog	Получение по Syslog.
[OOTB] Squid access.log file	Журналы access.log прокси-сервера Squid.	regexp	Чтение из файла.
[OOTB] Syslog	События в формате Syslog от произвольных источников.	syslog	
[OOTB] Syslog-CEF	События в формате CEF от произвольных источников, с заголовком Syslog.	syslog	
[OOTB] Unbound Syslog	Журналы DNS сервера unbount.	syslog	
[OOTB] VMWare Horizon - Syslog	Журналы VMWare Horizon. Получение по Syslog.	syslog	
[OOTB] VipNet Coordinator Syslog	Журналы VipNet Coordinator.	syslog	
[OOTB] Windows Basic	Базовый набор событий	xml	

	Windows Security.		
[OOTB] Windows Extended v.0.3	Расширенный набор событий Windows.	xml	
[OOTB] pfSense Syslog	События pfSence.	syslog	
[OOTB] pfSense w/o hostname	Пользовательский нормализатор события pfSence (некорректный формат Syslog заголовка).	regexp	
[OOTB[Syslog] Continent IPS/IDS & TLS	Континент СОВ, TSL.	syslog	Получение по Syslog.
[OOTB][regexp] Continent IPS/IDS & TLS	Континент СОВ, TSL.	regexp	Чтение файла.

Преобразования

Преобразования – это изменения, которые можно применить к значению до того, как оно будет записано в поле события. Тип преобразования выбирается в раскрывающемся списке.

Доступные преобразования:

- **lower** – используется для перевода всех символов значения в нижний регистр
- **upper** – используется для перевода всех символов значения в верхний регистр
- **regexp** – используется для применения к значению регулярного выражения RE2. Поле, в которое следует добавить регулярное выражение, появляется, когда выбран этот тип преобразования.
- **substring** – используется для извлечения символов в диапазоне позиций, указанном в полях **Начало** и **Конец**. Эти поля появляются, когда выбран данный тип преобразования.
- **replace** – используется для замены указанной последовательности символов на другую последовательность символов. Когда выбран этот тип преобразования, появляются новые поля:
  - **Символы на замену** – в этом поле вы можете указать последовательность символов, которую следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.
- **trim** – используется для удаления одновременно с начала и с конца значения поля события символов, указанных в поле **Символы**. Это поле появляется при выборе данного типа преобразования. Например, если для значения `Microsoft-Windows-Sismon` выполнить преобразование **trim** со значением `Micromon`, то получается значение `soft-Windows-Sys`.
- **append** – используется для добавления в конец значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.
- **prepend** – используется для добавления к началу значения поля события символов, указанных в поле **Константа**. Это поле появляется при выборе данного типа преобразования.

- **replace with regexp** – используется для замены результатов регулярного выражения RE2 на последовательность символов.
  - **Выражение** – в этом поле вы можете указать регулярное выражение, результаты которого следует заменить.
  - **Чем заменить** – в этом поле вы можете указать последовательность символов, которая должна использоваться вместо заменяемой последовательности символов.

Коннекторы

Ресурсы коннекторов используются для установления соединений между сервисами (см. раздел "Сервисы KUMA" на стр. 229) KUMA, сетевыми активами и / или другими службами.

В программе доступны следующие типы коннекторов:

- internal – используется для установления связи между сервисами KUMA.
- tcp – используется для связи по протоколу TCP. Доступен для Windows- и Linux-агентов.
- udp – используется для связи по протоколу UDP. Доступен для Windows- и Linux-агентов.
- netflow – используется для установления соединений NetFlow.
- sflow – используется для установления соединений SFlow.
- nats – используется для коммуникации через NATS. Доступен для Windows- и Linux-агентов.
- kafka – используется для коммуникации с помощью kafka. Доступен для Windows- и Linux-агентов.
- http – используется для связи по протоколу HTTP. Доступен для Windows- и Linux-агентов.
- sql – используется для связи с базой данных и СУБД.

  Программа поддерживает работу со следующими типами баз данных SQL:
  - SQLite.
  - MsSQL.
  - MySQL.
  - PostgreSQL.
  - Cockroach.
  - Firebird.
- file – используется для получения данных из любого текстового файла. Доступен для Linux-агентов.
- diode – используется для однонаправленной передачи данных в промышленных ICS-сетях с использованием диодов данных (см. раздел "Передача в KUMA событий из изолированных сегментов сети" на стр. 366).
- ftp – используется для получения данных по протоколу File Transfer Protocol. Доступен для Windows- и Linux-агентов.
- nfs – используется для получения данных по протоколу Network File System. Доступен для Windows- и Linux-агентов.
- wmi – используется для получения данных с помощью Windows Management Instrumentation. Доступен для Windows-агентов.

- wec – используется для получения данных с помощью Windows Event Collector. Доступен для Windows-агентов.
- snmp – используется для получения данных с помощью Simple Network Management Protocol. Доступен для Windows- и Linux-агентов.

В этом разделе

Просмотр параметров коннектора 170
Добавление коннектора 170
Параметры коннекторов 171

Просмотр параметров коннектора

► *Чтобы просмотреть параметры коннектора:*

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коннекторы**.
2. В структуре папок выберите папку, в которой располагается нужный вам коннектор.
3. Выберите коннектор, параметры которого вы хотите просмотреть.

Параметры коннекторов отображаются на двух вкладках: **Основные параметры** и **Дополнительные параметры**. Подробное описание параметров каждого коннектора см. в разделе *Параметры коннекторов* (на стр. 171).

Добавление коннектора

Вы можете включить отображение непечатаемых символов (см. раздел "Редактирование своей учетной записи" на стр. 71) для всех полей ввода, кроме поля **Описание**.

► *Чтобы добавить коннектор:*

1. В веб-интерфейсе KUMA перейдите в раздел **Ресурсы** → **Коннекторы**.
2. В структуре папок выберите папку, в которой должен располагаться ресурс.

   Корневые папки соответствуют тенантам. Для того, чтобы ресурс был доступен определенному тенанту, его следует создать в папке этого тенанта.

   Если в дереве папок отсутствует требуемая папка, вам нужно создать ее.

   По умолчанию добавляемые коннекторы создаются в папке **Общий**.
3. Нажмите на кнопку **Добавить коннектор**.
4. Укажите параметры для выбранного типа коннектора.

Параметры, которые требуется указать для каждого типа коннектора, приведены в разделе *Параметры коннекторов* (на стр. 171).

5. Нажмите на кнопку **Сохранить**.

Параметры коннекторов

Этот раздел содержит описание параметров всех поддерживаемых KUMA типов коннекторов.

В этом разделе

Тип internal 171
Тип tcp 172
Тип udp 173
Тип netflow 173
Тип sflow 174
Тип nats 174
Тип kafka 176
Тип http 178
Тип sql 179
Тип file 185
Тип diode 187
Тип ftp 188
Тип nfs 189
Тип wmi 190
Тип wec 191
Тип snmp 192

Тип internal

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** (обязательно) – URL, с которым необходимо установить связь.

    Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
  - **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:
  - **Прокси-сервер** – раскрывающийся список, в котором можно выбрать ресурс прокси-сервера (см. раздел "Прокси-серверы" на стр. 226).
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408).

    По умолчанию указывается значение **Выключено**.

Тип tcp

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
  - **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то по умолчанию используется значение: `\n`.
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:
  - **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Режим TLS** – использование шифрования TLS:
    - **Выключено** (по умолчанию) – не использовать шифрование TLS.
    - **Включено** – использовать шифрование, но без верификации.
    - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы (см. раздел "Изменение корневого сертификата" на стр. 46) и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

    При использовании TLS невозможно указать IP-адрес в качестве URL.
  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

Тип udp

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
  - **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то события не разделяются.
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:
  - **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
  - **Рабочие процессы** – используется для установки числа рабочих процессов для коннектора. Значение по умолчанию: 1.
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

Тип netflow

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** (обязательно) – URL, с которым необходимо установить связь.
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:
  - **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
  - **Рабочие процессы** – используется для установки числа рабочих процессов для коннектора. Значение по умолчанию: 1.

- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

Тип sflow

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** (обязательно) – URL, с которым требуется установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:
  - **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.
  - **Рабочие процессы** – используется для установки количества рабочих процессов для коннектора. Значение по умолчанию: 1.
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
  - **Отладка** – раскрывающийся список, позволяющий включить логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

Тип nats

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** (обязательно) – URL, с которым необходимо установить связь.
  - **Топик** (обязательно) – тема сообщений NATS. Должно содержать от 1 до 255 символов Юникода.

- **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то события не разделяются.
- **Описание** – описание ресурса: до 256 символов Юникода.

- Закладка **Дополнительные параметры**:
  - **Размер буфера** – используется для установки размера буфера коннектора. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
  - **Идентификатор группы** – параметр GroupID для сообщений NATS. Должно содержать от 1 до 255 символов Юникода. Значение по умолчанию: `io.nats`.
  - **Рабочие процессы** – используется для установки числа рабочих процессов для коннектора. Значение по умолчанию: 1.
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Идентификатор хранилища** – идентификатор хранилища NATS.
  - **Режим TLS** – использование шифрования TLS:
    - **Выключено** (по умолчанию) – не использовать шифрование TLS.
    - **Включено** – использовать шифрование, но без верификации сертификата.
    - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы (см. раздел "Изменение корневого сертификата" на стр. 46) и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
    - **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

      Создание сертификата, подписанного центром сертификации (см. раздел "Нестандартный CA" на стр. 175)

    При использовании TLS невозможно указать IP-адрес в качестве URL.
  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

Нестандартный CA

Для использования этого режима TLS необходимо выполнить следующие действия на сервере Ядра KUMA (в примерах команд ниже используется OpenSSL):

1. Создать ключ, который будет использоваться центром сертификации.

   Пример команды: `openssl genrsa -out ca.key 2048`

2. Создать сертификат для только что созданного ключа.

Пример команды: `openssl req -new -x509 -days 365 -key ca.key -subj "/CN=<общее имя хоста центра сертификации>" -out ca.crt`

3. Создать приватный ключ и запрос на его подписание в центре сертификации.

   Пример команды: `openssl req -newkey rsa:2048 -nodes -keyout server.key -subj "/CN=общее имя хоста сервера KUMA>" -out server.csr`

4. Создать сертификат, подписанный центром сертификации. Необходимо включить в subjectAltName доменные имена или IP-адреса сервера, для которого создается сертификат.

   Пример команды: `openssl x509 -req -extfile <(printf "subjectAltName=DNS:domain1.ru,DNS:domain2.com,IP:192.168.0.1") -days 365 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt`

5. Полученный сертификат `server.crt` следует загрузить в веб-интерфейсе KUMA в секрет типа **certificate**, который затем следует выбрать в раскрывающемся списке **Нестандартный CA**.

Тип kafka

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port.
  - **Топик** – тема сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, ".", "_", "-".
  - **Авторизация** – необходимость агентам проходить авторизацию при подключении к коннектору:
    - **выключена** (по умолчанию).
    - **PFX**.

      При выборе этого варианта требуется сформировать сертификат с закрытым ключом в формате PKCS#12-контейнера во внешнем центре сертификации, экспортировать сертификат из хранилища и загрузить его в веб-интерфейс KUMA в виде PFX-секрета.

      Добавить PFX-секрет (на стр. 177)
    - **обычная**.

      При выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору.

      Добавить секрет (см. раздел "Добавление секрета" на стр. 177)
  - **Идентификатор группы** – параметр GroupID для сообщений Kafka. Должен содержать от 1 до 255 следующих символов: a–z, A–Z, 0–9, ".", "_", "-".
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:

- **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то события не разделяются.
- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
- **Режим TLS** – использование шифрования TLS:
  - **Выключено** (по умолчанию) – не использовать шифрование TLS.
  - **Включено** – использовать шифрование, но без верификации сертификата.
  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы (см. раздел "Изменение корневого сертификата" на стр. 46) и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
  - **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

    Создание сертификата, подписанного центром сертификации (см. раздел "Нестандартный CA" на стр. 175)

  При использовании TLS невозможно указать IP-адрес в качестве URL.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

1. Если вы загрузили PFX-сертификат ранее, выберите его в раскрывающемся списке **Секрет**.

   Если ранее не было добавлено ни одного сертификата, в раскрывающемся списке отобразится **Нет данных**.

2. Если вы хотите добавить новый сертификат, справа от списка **Секрет** нажмите на кнопку  .

   Откроется окно **Секрет**.
3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.
4. По кнопке **Загрузить PFX** выберите файл, в который вы экспортировали сертификат с закрытым ключом, в формате PKCS#12-контейнера.
5. В поле **Пароль** введите пароль для защиты сертификата, заданный в мастере экспорта сертификата.
6. Нажмите на кнопку **Сохранить**.

Сертификат будет добавлен и отобразится в списке **Секрет**.

Добавление секрета

1. Если вы создали секрет ранее, выберите его в раскрывающемся списке **Секрет**.

   Если ранее не было добавлено ни одного секрета, в раскрывающемся списке отобразится **Нет данных**.

2. Если вы хотите добавить новый секрет, справа от списка **Секрет** нажмите на кнопку  .

   Откроется окно **Секрет**.
3. В поле **Название** введите название, под которым секрет будет отображаться в списке доступных.
4. В полях **Пользователь** и **Пароль** введите данные учетной записи, под которой агент будет подключаться к коннектору.
5. Если требуется, в поле **Описание** добавьте любую дополнительную информацию о секрете.
6. Нажмите на кнопку **Сохранить**.

Секрет будет добавлен и отобразится в списке **Секрет**.

Тип http

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.
  - **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то события не разделяются.
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Режим TLS** – использование шифрования TLS:
    - **Выключено** (по умолчанию) – не использовать шифрование TLS.
    - **Включено** – использовать шифрование, но без верификации.
    - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы (см. раздел "Изменение корневого сертификата" на стр. 46) и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

    При использовании TLS невозможно указать IP-адрес в качестве URL.
  - **Прокси-сервер** – раскрывающийся список, в котором можно выбрать ресурс прокси-сервера (см. раздел "Прокси-серверы" на стр. 226).
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

kaspersky

Тип sql

KUMA поддерживает работу с несколькими типами баз данных (на стр. 185).

При создании коннектора вам требуется задать значения для общих параметров коннектора и индивидуальных параметров подключения к базе данных.

Для коннектора на закладке **Основные параметры** вам требуется задать значения следующих параметров:

- **Название** (обязательно) – уникальное имя ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тип** (обязательно) – **sql**.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Запрос по умолчанию** (обязательно) – SQL-запрос, который выполняется при подключении к базе данных.
- **Интервал запросов, сек.** – интервал выполнения SQL-запросов. Указывается в секундах.

  Значение по умолчанию: 10 секунд.
- **Описание** – описание ресурса: до 256 символов Юникода.

Для подключения к базе данных на закладке **Основные параметры** вам требуется задать значения следующих параметров:

- **URL** (обязательно) – секрет, в котором хранится список URL-адресов для подключения к базе данных.

  При необходимости вы можете изменить (на стр. 184) или создать секрет (на стр. 182).

  > При создании подключений могут некорректно обрабатываться строки с учетными данными, содержащими специальные символы. Если при создании подключения возникает ошибка, но вы уверены в том, что значения параметров корректны, укажите специальные символы в процентной кодировке.

  Коды специальных символов (см. раздел "Процентная кодировка" на стр. 182)
- **Столбец идентификатора** (обязательно) – название столбца, содержащего идентификатор для каждой строки таблицы.
- **Начальное значение идентификатора** (обязательно) – значение в столбце идентификатора, по которому будет определена строка, с которой требуется начать считывание данных из SQL-таблицы.
- **Запрос** – поле для дополнительного SQL-запроса. Запрос, указанный в этом поле, выполняется вместо запроса по умолчанию.

В SQL-запросах поддерживается последовательный запрос сведений из базы данных. Например, если в поле **Запрос** указать запрос `select * from <название таблицы с данными> where id > <плейсхолдер>`, то при первом обращении к таблице в качестве значения плейсхолдера будет использоваться значение поля **Начальное значение идентификатора**. При этом в сервисе, в котором используется SQL-коннектор, сохраняется идентификатор последней прочитанной записи, и во время следующего обращения к базе данных в качестве значения плейсхолдера в запросе будет использоваться идентификатор этой записи.

Примеры SQL-запросов

- **Интервал запросов, сек.** – интервал выполнения SQL-запросов. Интервал, указанный в этом поле, используется вместо интервала, указанного по умолчанию для коннектора.

  Указывается в секундах. Значение по умолчанию: 10 секунд.

Для коннектора на закладке **Дополнительные параметры** вам требуется задать значения следующих параметров:

- **Кодировка символов** – кодировка символов. Значение по умолчанию: `UTF-8`.

  KUMA обрабатывает ответы SQL в кодировке UTF-8. Вы можете настроить SQL-сервер на отправку сообщений в кодировке UTF-8 или изменить кодировку входящих сообщений на стороне KUMA.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

В рамках одного коннектора вы можете создать подключение (на стр. 185) для нескольких поддерживаемых баз данных.

Оператор UNION не поддерживается коннекторами типа SQL.

Примеры SQL-запросов

SQLite, Firebird – `select * from table_name where id > ?`

MsSQL – `select * from table_name where id > @p1`

MySQL – `select * from table_name where id > %s`

PostgreSQL, Cockroach – `select * from table_name where id > $1`

Oracle – `select * from table_name where id > :val`

Пример запроса к SQL базе Kaspersky Security Center

SELECT ev.event_id AS externalId, ev.severity AS severity, ev.task_display_name AS taskDisplayName,

```
        ev.product_name AS product_name, ev.product_version AS product_version,
         ev.event_type As deviceEventClassId, ev.event_type_display_name As event_subcode, ev.descr As msg,
CASE
      WHEN ev.rise_time is not NULL THEN
DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.rise_time )
         ELSE ev.rise_time
      END
   AS endTime,
   CASE
      WHEN ev.registration_time is not NULL
         THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),ev.registration_time )
         ELSE ev.registration_time
      END
   AS kscRegistrationTime,
   cast(ev.par7 as varchar(4000)) as sourceUserName,
   hs.wstrWinName as dHost,
   hs.wstrWinDomain as strNtDom, serv.wstrWinName As kscName,
      CAST(hs.nIp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +
   CAST(hs.nIp / 256 / 256 % 256 AS VARCHAR) + '.' +
   CAST(hs.nIp / 256 % 256 AS VARCHAR) + '.' +
   CAST(hs.nIp % 256 AS VARCHAR) AS sourceAddress,
   serv.wstrWinDomain as kscNtDomain,
      CAST(serv.nIp / 256 / 256 / 256 % 256 AS VARCHAR) + '.' +
   CAST(serv.nIp / 256 / 256 % 256 AS VARCHAR) + '.' +
   CAST(serv.nIp / 256 % 256 AS VARCHAR) + '.' +
   CAST(serv.nIp % 256 AS VARCHAR) AS kscIP,
   CASE
   WHEN virus.tmVirusFoundTime is not NULL
         THEN DATEADD(hour,DATEDIFF(hour,GETUTCDATE(),GETDATE()),virus.tmVirusFoundTime )
         ELSE ev.registration_time
      END
   AS virusTime,
   virus.wstrObject As filePath,
```

```
    virus.wstrVirusName as virusName,
    virus.result_ev as result
FROM KAV.dbo.ev_event as ev
LEFT JOIN KAV.dbo.v_akpub_host as hs ON ev.nHostId = hs.nId
INNER JOIN KAV.dbo.v_akpub_host As serv ON serv.nId = 1
Left Join KAV.dbo.rpt_viract_index as Virus on ev.event_id = virus.nEventVirus
where registration_time >= DATEADD(minute, -191, GetDate())
```

Процентная кодировка

Символ	Представление символа в процентной кодировке
!	%21
#	%23
$	%24
%	%25
&	%26
'	%27
(	%28
)	%29
*	%2A
+	%2B
,	%2C
/	%2F
:	%3A
;	%3B
=	%3D
?	%3F
@	%40
[	%5B
]	%5D
\	%5C

Следующие специальные символы не поддерживаются в паролях доступа к базам SQL: пробел, [,], :, /, #, %, \.

1. Нажмите на кнопку  .

   Откроется окно секрета.

2. Укажите значения для следующих параметров:

   a. **Название** – имя добавляемого секрета.

   b. **Тип** – **urls**.

      Значение установлено по умолчанию, его редактирование недоступно.

   c. **URL** – URL-адрес базы данных.

      Вам требуется учитывать, что для подключения к каждому типу базы данных используется свой формат URL-адреса.

      Доступные форматы URL-адресов:

      - Для SQLite:
        - `sqlite3://file:<file_path>`

        В качестве плейсхолдера используется знак вопроса: ?.

      - Для MsSQL:
        - `sqlserver://<user>:<password>@<server:port>/<instance_name>?database=<database>` (рекомендуется)
        - `sqlserver://<user>:<password>@<server>?database=<database>&encrypt=disable`

        В качестве плейсхолдера используются символы @p1.

      - Для MySQL:
        - `mysql://<user>:<password>@tcp(<server>:<port>)/<database>`

        В качестве плейсхолдера используются символы %s.

      - Для PostgreSQL:
        - `postgres://<user>:<password>@<server>/<database>?sslmode=disable`

        В качестве плейсхолдера используются символы $1.

      - Для Cockroach:
        - `postgres://<user>:<password>@<server>:<port>/<database>?sslmode=disable`

        В качестве плейсхолдера используются символы $1.

- Для Firebird:
  - `firebirdsql://<user>:<password>@<server>:<port>/<database>`

    В качестве плейсхолдера используется знак вопроса: ?.

d. **Описание** – любая дополнительная информация.

3. При необходимости нажмите на кнопку **Добавить** и укажите дополнительный URL-адрес.

   В этом случае при недоступности одного URL-адреса программа подключается к следующему URL-адресу, указанному в списке адресов.

4. Нажмите на кнопку **Сохранить**.

1. Нажмите на кнопку  .

   Откроется окно секрета.

2. Укажите значения для параметров, которые требуется изменить.

   Вы можете изменить значения для следующих параметров:

   a. **Название** – имя добавляемого секрета.

   b. **URL** – URL-адрес базы данных.

      Вам требуется учитывать, что для подключения к каждому типу базы данных используется свой формат URL-адреса.

      Доступные форматы URL-адресов:

      - Для SQLite:
        - `sqlite3://file:<file_path>`

          В качестве плейсхолдера используется знак вопроса: ?.

      - Для MsSQL:
        - `sqlserver://<user>:<password>@<server:port>/<instance_name>?database=<database>` (рекомендуется)
        - `sqlserver://<user>:<password>@<server>?database=<database>&encrypt=disable`

          В качестве плейсхолдера используются символы @p1.

      - Для MySQL:
        - `mysql://<user>:<password>@tcp(<server>:<port>)/<database>`

          В качестве плейсхолдера используются символы %s.

      - Для PostgreSQL:

- `postgres://<user>:<password>@<server>/<database>?sslmode=disable`

В качестве плейсхолдера используются символы $1.

- Для Cockroach:
  - `postgres://<user>:<password>@<server>:<port>/<database>?sslmode=disable`

В качестве плейсхолдера используются символы $1.

- Для Firebird:
  - `firebirdsql://<user>:<password>@<server>:<port>/<database>`

В качестве плейсхолдера используется знак вопроса: ?.

c. **Описание** – любая дополнительная информация.

3. При необходимости нажмите на кнопку **Добавить** и укажите дополнительный URL-адрес.

   В этом случае при недоступности одного URL-адреса программа подключается к следующему URL-адресу, указанному в списке адресов.

4. Нажмите на кнопку **Сохранить**.

► *Чтобы создать подключение для нескольких баз данных SQL:*

1. Нажмите на кнопку **Добавить подключение**.
2. Задайте значение для параметров **URL**, **Столбец идентификатора**, **Начальное значение идентификатора**, **Запрос**, **Интервал запросов, сек**.
3. Повторите шаги 1–2 для каждого требуемого подключения.

   Программа поддерживает работу со следующими типами баз данных SQL:

   - SQLite.
   - MsSQL.
   - MySQL.
   - PostgreSQL.
   - Cockroach.
   - Firebird.

kaspersky

Тип file

Тип **file** используется для получения данных из любого текстового файла. Одна строка файла считается одним событием. Разделители между строк: \n. Коннектор этого типа доступен для Linux-агентов.

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** (обязательно) – полный путь до файла, с которым требуется выполнять взаимодействие. Например, `/var/log/*som?[1-9].log`.

    Шаблоны масок для файлов и директорий (см. раздел "Шаблоны масок" на стр. 186)

    Ограничения при использовании префиксов к путям файлов (см. раздел "Коннектор, тип file - ограничения" на стр. 187)
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

Шаблоны масок

Маски:

- '*' – соответствует любой последовательности символов;
- '[' ['^'] { диапазон символов } ']' – класс символов (не должен быть пустым);
- '?' – соответствует любому одиночному символу;
- c – соответствует символу c (c != '*', '?', '\\', '[');
- '\\' c – соответствует символу c.

Диапазоны символов:

- c – соответствует символу c (c != '\\', '-', ']');
- '\\' c – соответствует символу c;
- lo '-' hi – соответствует символу c для lo <= c <= hi.

Примеры:

- /var/log/*som?[1-9].log
- /mnt/dns_logs/*/dns.log
- /mnt/proxy/access*.log

kaspersky

Коннектор, тип file - ограничения

Префиксы, которые невозможно использовать при указании путей к файлам:

- /*
- /bin
- /boot
- /dev
- /etc
- /home
- /lib
- /lib64
- /proc
- /root
- /run
- /sys
- /tmp
- /usr/*
- /usr/bin/
- /usr/local/*
- /usr/local/sbin/
- /usr/local/bin/
- /usr/sbin/
- /usr/lib/
- /usr/lib64/
- /var/*
- /var/lib/
- /var/run/
- /opt/kaspersky/kuma/

Файлы по указанным ниже путям доступны:

- /opt/kaspersky/kuma/clickhouse/logs/
- /opt/kaspersky/kuma/mongodb/log/
- /opt/kaspersky/kuma/victoria-metrics/log/

kaspersky

Тип diode

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **Директория с событиями от диода данных** (обязательно) – полный путь до директории на сервере коллектора KUMA, в которую диод данных перемещает файлы с событиями из изолированного сегмента сети. После считывания коннектором файлы удаляются из директории. Путь может содержать до 255 символов Юникода.

    Ограничения при использовании префиксов к путям (см. раздел "Коннектор, тип file - ограничения" на стр. 187)
  - **Разделитель** – используется для указания символа, определяющего границу между событиями. Доступные значения: `\n`, `\t`, `\0`. Если разделитель не задан (выбрано пустое значение), то по умолчанию используется значение: `\n`.

    Этот параметр должен совпадать ресурсах коннектор и точка назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:
  - **Рабочие процессы** – количество служб, обрабатывающих очередь запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
  - **Интервал запросов, сек.** – регулярность считывания файлов из директории с событиями от диода данных. Значение по умолчанию: 2. Значение указывается в секундах.
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

    Этот параметр должен совпадать ресурсах коннектор и точка назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

Тип ftp

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** (обязательно) – Действительный URL файла или маски файлов, который начинается со схемы 'ftp://'. Для маски файлов допустимо использование * ? [...].

    Шаблоны масок для файлов (см. раздел "Шаблоны масок" на стр. 186)

    Если в URL не содержится порт ftp сервера, подставляется 21 порт.
  - **Учетные данные для URL** – для указания логина и пароля к FTP серверу. При отсутствии логина и пароля строка остается пустой.
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

Тип nfs

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** (обязательно) – путь до удаленной директории в формате nfs://host/path.
  - **Маска имени файла** (обязательно) – маска, по которой фильтруются файлы с событиями. Допустимо использование масок "`*`", "`?`", "`[...]`".
  - **Интервал запросов, сек.** – интервал опроса. Промежуток времени, через который перечитываются файлы с удаленной системы. Значение указывается в секундах. По умолчанию указано значение: 0.
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:

- **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

Тип wmi

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **URL** (обязательно) – URL создаваемого коллектора, например `kuma-collector.example.com:7221`.

    При создании коллектора для получения данных с помощью Windows Management Instrumentation автоматически создается агент (см. раздел "Об агентах" на стр. 29), который будет получать необходимые данные на удаленной машине и перенаправлять их в сервис коллектора. В поле **URL** требуется указать адрес этого коллектора. URL известен заранее, если вы знаете, на каком сервере планируете установить сервис, но это поле можно заполнить и после завершения мастера установки, скопировав данные из раздела **Ресурсы** → **Активные сервисы**.
  - **Описание** – описание ресурса: до 256 символов Юникода.
  - **Учетные данные по умолчанию** – раскрывающийся список, в котором выбирать значение не требуется. Учетные данные для подключения к хостам необходимо указывать в таблице **Удаленные хосты** (см. ниже).
  - В таблице **Удаленные хосты** перечисляются удаленные устройства Windows, к которым требуется установить подключение. Доступные столбцы:
    - **Хост** (обязательно) – IP-адрес или доменное имя устройства, с которого необходимо принимать данные. Например, "machine-1.example.com".
    - **Домен** (обязательно) – название домена, в котором расположено удаленное устройство. Например, "example.com"
    - **Тип журналов** – раскрывающийся список для выбора названия журналов Windows, которые требуется получить. По умолчанию в списке отображаются только предварительно настроенные журналы, но вы можете расширить список пользовательскими журналами, введя их название в поле **Журналы Windows**, а затем нажав **ENTER**. Конфигурация сервисов и ресурсов KUMA может потребовать дополнительных изменений для правильной обработки настраиваемых журналов.

      Журналы, доступные по умолчанию:

      - Application
      - ForwardedEvents

- Security
- System
- HardwareEvents

- **Секрет** – учетные данные для доступа к удаленному устройству Windows с правами на чтение журналов. Если оставить это поле пустым, то будут использоваться учетные данные из секрета, выбранного в раскрывающемся списке Учетные данные, используемые по умолчанию. Логин в ресурсе секрета (см. раздел "Секреты" на стр. 226) необходимо указывать без домена, значение домена для доступа к хосту берется из столбца **Домен** таблицы **Удаленные хосты**.

  Можно выбрать ресурс секрета в раскрывающемся списке или создать его с помощью кнопки  . Выбранный секрет можно изменить, нажав на кнопку  .

- Закладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

Получение событий с удаленной машины

Условия для получения событий с удаленной машины Windows с агентом KUMA:

- Для запуска агента KUMA на удаленной машине необходимо использовать учетную запись с правами Log on as a service.
- Для получения событий от агента KUMA необходимо использовать учетную запись с правами Event Log Readers. Для серверов домена может быть создана одна такая учетная запись, чтобы через групповую политику ее права на чтение логов можно было распространить на все серверы и рабочие станции домена.
- На удаленных машинах Windows необходимо открыть следующие TCP-порты 135, 445, 49152-65535.
- На удаленных машинах требуется запустить следующие службы:
  - Remote Procedure Call (RPC)
  - RPC Endpoint Mapper

Тип wec

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.

- **URL** (обязательно) – URL создаваемого коллектора, например `kuma-collector.example.com:7221`.

  При создании коллектора для получения данных с помощью Windows Event Collector автоматически создается агент (см. раздел "Об агентах" на стр. 29), который будет получать необходимые данные на удаленной машине и перенаправлять их в сервис коллектора. В поле **URL** требуется указать адрес этого коллектора. URL известен заранее, если вы знаете, на каком сервере планируете установить сервис, но это поле можно заполнить и после завершения мастера установки, скопировав данные из раздела **Ресурсы** → **Активные сервисы**.

- **Описание** – описание ресурса: до 256 символов Юникода.
- **Журналы Windows** (обязательно) – в этом раскрывающемся списке необходимо выбрать названия журналов Windows, которые требуется получить. По умолчанию в списке отображаются только предварительно настроенные журналы, но вы можете расширить список пользовательскими журналами, введя их название в поле **Журналы Windows**, а затем нажав **ENTER**. Конфигурация сервисов и ресурсов KUMA может потребовать дополнительных изменений для правильной обработки настраиваемых журналов.

  Преднастроенные журналы:

  - Application
  - ForwardedEvents
  - Security
  - System
  - HardwareEvents

- Закладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

Для запуска агента KUMA на удаленной машине необходимо использовать учетную запись с правами Log on as a service.
Для получения событий необходимо использовать учетную запись с правами Event Log Readers. Для серверов домена может быть создана одна такая учетная запись, чтобы через групповую политику ее права на чтение логов можно было распространить на все серверы и рабочие станции домена.

Тип snmp

Доступен для Windows- и Linux-агентов. Поддерживаемые версии протокола:

- snmpV1
- snmpV2
- snmpV3

При создании этого типа коннектора вам требуется указать значения для следующих параметров:

- Закладка **Основные параметры**:
  - **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
  - **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
  - **Тип** (обязательно) – тип коннектора.
  - **Версия SNMP** (обязательно) – в этом раскрывающемся списке можно выбрать версию используемого протокола.
  - **Хост** (обязательно) – имя хоста или его IP-адрес. Доступные форматы: hostname, IPv4, IPv6.
  - **Порт** (обязательно) – порт для подключения к хосту. Обычно используются значения 161 или 162.

  С помощью параметров **Версия SNMP**, **Хост** и **Порт** определяется одно подключение к SNMP-ресурсу. Таких подключений в одном коннекторе можно создать несколько, добавляя новые с помощью кнопки **SNMP-ресурс**. Удалить подключения можно с помощью кнопки  .
  - **Секрет** (обязательно) – раскрывающийся список для выбора ресурса секрета (см. раздел "Секреты" на стр. 226), в котором хранятся учетные данные для подключения через Simple Network Management Protocol. Тип секрета должен соответствовать версии SNMP. При необходимости секрет можно создать в окне создания коннектора с помощью кнопки  .

    Выбранный секрет можно изменить, нажав на кнопку  .
  - В таблице **Данные источника** можно задать правила именования получаемых данных, по которым идентификаторы объектов OID будут преобразовываться в ключи, с которыми сможет взаимодействовать нормализатор. Доступные столбцы таблицы:
    - **Название параметра** (обязательно) – произвольное название для типа данных. Например, "Имя узла" или "Время работы узла".
    - **OID** (обязательно) – уникальный идентификатор, который определяет, где искать требуемые данные на источнике событий. Например, "1.3.6.1.2.1.1.5".
    - **Ключ** (обязательно) – уникальный идентификатор, возвращается в ответ на запрос к устройству со значением запрошенного параметра. Например, "sysName". К этому ключу можно обращаться при нормализации данных.
  - **Описание** – описание ресурса: до 256 символов Юникода.
- Закладка **Дополнительные параметры**:
  - **Кодировка символов** – параметр для установки кодировки символов. Значение по умолчанию: `UTF-8`.
  - **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
  - **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.

kaspersky

Правила агрегации

Ресурсы правил агрегации используются для объединения повторяющихся событий.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Предел событий** – количество событий, которое должно быть получено для того, чтобы сработало правило агрегации и события были объединены. Значение по умолчанию: `100`.
- **Время ожидания событий** (обязательно) – время (в секундах), в течение которого получаются события для объединения. По истечении этого срока правило агрегирования срабатывает и создается новое событие. Значение по умолчанию: `60`.
- **Описание** – описание ресурса: до 256 символов Юникода.
- **Группирующие поля** (обязательно) – в этом раскрывающемся списке можно выбрать поля, по которым будут определяться однотипные события.
- **Уникальные поля** – в этом раскрывающемся списке можно выбрать поля, наличие которых выведет событие из процесса агрегации даже при наличие полей, указанных в разделе **Группирующие поля**.
- **Поля суммы** – в этом раскрывающемся списке можно выбрать поля, значения которых при агрегации будут суммироваться.
- **Фильтр** – блок параметров, в котором можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Не используйте в ресурсах правил агрегации фильтры с операндом **TI** или операторами **TIDetect** и **inActiveDirectoyGroup**. Поля Active Directory, для которых используется оператор **inActiveDirectoyGroup,** появляются на этапе обогащения, то есть после выполнения правил агрегации.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Правила обогащения

Ресурсы правил обогащения используются для обновления полей событий.

Доступные параметры ресурсов правил обогащения:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип источника данных** (обязательно) – выпадающий список для выбора типа входящих событий. В зависимости от выбранного типа отображаются дополнительные параметры:
  - константа (см. раздел "Обогащение, тип константа" на стр. 195)

  - словарь (см. раздел "Обогащение, тип словарь" на стр. 196)
  - событие (см. раздел "Обогащение, тип событие (для ресурса обогащения)" на стр. 196)
  - шаблон (см. раздел "Обогащение, тип шаблон" на стр. 197)
  - dns (см. раздел "Обогащение, тип dns" на стр. 196)
  - cybertrace (см. раздел "Обогащение, тип cybertrace" на стр. 195)
  - часовой пояс (см. раздел "Обогащение, тип часовой пояс" на стр. 197)
  - геоданные (см. раздел "Обогащение, тип геоданные" на стр. 198)
- **Отладка** – с помощью этого раскрывающегося списка можно включить логирование операций сервиса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию логирование выключено.
- **Описание** – описание ресурса: до 256 символов Юникода.
- **Фильтр** – блок параметров, в котором можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Обогащение, тип константа

Этот тип обогащения используется, если в поле события необходимо добавить константу. Параметры этого типа обогащения:

- В поле **Константа** укажите значение, которое следует добавить в поле события. Значение должно состоять не более чем из 255 символов Юникода. Если оставить это поле пустым, существующее значение поля события будет удалено.
- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Обогащение, тип cybertrace

Этот тип обогащения используется для добавления в поля события сведений из потоков данных CyberTrace (см. раздел "Интеграция с Kaspersky CyberTrace" на стр. 81).

Доступные параметры:

- **URL** (обязательно) – в этом поле можно указать URL сервера CyberTrace, которому вы хотите отправлять запросы.
- **Количество подключений** – максимальное количество подключений к серверу CyberTrace, которые может одновременно установить KUMA. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Запросов в секунду** – максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.
- **Время ожидания** – время ожидания отклика от сервера CyberTrace в секундах. Значение по умолчанию: `30`.

- **Сопоставление** (обязательно) – этот блок параметров содержит таблицу сопоставления полей событий KUMA с типами индикаторов CyberTrace. В столбце **Поле KUMA** указаны названия полей событий KUMA (см. раздел "Модель данных нормализованного события" на стр. 471), а в столбце **Индикатор CyberTrace** указаны типы индикаторов CyberTrace.

  Доступные типы индикаторов CyberTrace:

  - **ip**
  - **url**
  - **hash**

  В таблице сопоставления требуется указать как минимум одну строку. С помощью кнопки **Добавить строку** можно добавить строку, а с помощью кнопки ✕ – удалить.

Обогащение, тип словарь

Этот тип обогащения используется, если в поле события необходимо добавить значение из словаря (см. раздел "Словари" на стр. 225).

При выборе этого типа в раскрывающемся списке **Название словаря** необходимо выбрать словарь, из которого будут браться значения, а в блоке параметров **Ключевые поля** с помощью кнопки **Добавить поле** требуется выбрать поля события, значения которых будут использоваться для выбора записи словаря.

Обогащение, тип dns

Этот тип обогащения используется для отправки запросов на DNS-сервер частной сети для преобразования IP-адресов в доменные имена или наоборот.

Доступные параметры:

- **URL** – в этом поле можно указать URL DNS-сервера, которому вы хотите отправлять запросы. С помощью кнопки **Добавить URL** можно указать несколько URL.
- **Запросов в секунду** – максимальное количество запросов к серверу в секунду. Значение по умолчанию: `1000`.
- **Рабочие процессы** – максимальное количество запросов в один момент времени. Значение по умолчанию: `1`.
- **Количество задач** – максимальное количество одновременно выполняемых запросов. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Срок жизни кеша** – время жизни значений, хранящихся в кеше. Значение по умолчанию: `60`.
- **Кеш отключен** – с помощью этого раскрывающегося списка можно включить или отключить кеширование. По умолчанию кеширование включено.

Обогащение, тип событие (для ресурса обогащения)

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- В блоке параметров **Преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA. Тип преобразования можно выбрать в раскрывающемся списке. С помощью кнопок **Добавить преобразование** и **Удалить** можно добавить или удалить преобразование. Порядок преобразований имеет значение.

  Доступные преобразования (см. раздел "Преобразования" на стр. 168)

Обогащение, тип событие (для нормализатора)

Этот тип обогащения используется, если в поле события необходимо записать значение другого поля события. Параметры этого типа обогащения:

- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.
- В раскрывающемся списке **Исходное поле** выберите поле события, значение которого будет записано в целевое поле.
- Если нажать на кнопку  , откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

  Доступные преобразования (см. раздел "Преобразования" на стр. 168)

Обогащение, тип шаблон

Этот тип обогащения используется, если в поле события необходимо записать значение, полученное при обработке шаблонов Go. Параметры этого типа обогащения:

- В поле **Шаблон** поместите шаблон Go https://pkg.go.dev/text/template.

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это название поля события, значение которого должно быть передано в скрипт.

  Пример: `Атака на {{.DestinationAddress}} со стороны {{.SourceAddress}}`.
- В раскрывающемся списке **Целевое поле** выберите поле события KUMA, в которое следует поместить данные.

Обогащение, тип часовой пояс

Этот тип обогащения используется в коллекторах (см. раздел "Коллектор" на стр. 20) и корреляторах (см. раздел "Коррелятор" на стр. 23) для присваивания событию определенного часового пояса. Сведения о часовом поясе могут пригодиться при поиске событий, случившихся в нетипичное время, например ночью.

При выборе этого типа обогащения в раскрывающемся списке **Часовой пояс** необходимо выбрать требуемую временную зону.

Убедитесь, что требуемый часовой пояс установлен на сервере сервиса, использующего обогащение. Например, это можно сделать с помощью команды `timedatectl list-timezones`, которая показывает все установленные на сервере часовые пояса. Подробнее об установке часовых поясов смотрите в документации используемой вами операционной системы.

При обогащении события в поле события DeviceTimeZone (см. раздел "Модель данных нормализованного события" на стр. 471) записывается смещение времени выбранного часового пояса относительно всемирного координированного времени (UTC) в формате +-`чч:мм`. Например, если выбрать временную зону **Asia/Yekaterinburg** в поле DeviceTimeZone будет записано значение `+05:00`. Если в обогащаемом событии есть значение поля DeviceTimeZone, оно будет перезаписано.

По умолчанию, если в обрабатываемом событии не указан часовой пояс и не настроены правила обогащения по часовому поясу, событию присваивается часовой пояс сервера, на котором установлен сервис (коллектор или коррелятор), обрабатывающий событие. При изменении времени сервера сервис необходимо перезапустить (см. раздел "Перезапуск сервиса" на стр. 231).

Допустимые форматы времени при обогащении поля DeviceTimeZone (см. раздел "Допустимые форматы времени" на стр. 198)

Допустимые форматы времени

При обработке в коллекторе поступающих "сырых" событий следующие форматы времени могут быть автоматически приведены к формату +-чч:мм:

Формат времени в обрабатываемом событии	Пример
+-чч:мм	-07:00
+-ччмм	-0700
+-чч	-07

Если формат даты в поле `DeviceTimeZone` отличается от указанных выше, при обогащении события сведениями о часовом поясе в поле записывается часовой пояс серверного времени коллектора. Вы можете создать особые правила нормализации (см. раздел "Нормализаторы" на стр. 158) для нестандартных форматов времени.

Обогащение, тип геоданные

Этот тип обогащения используется для добавления в поля событий сведений о географическом расположении IP-адресов. Подробнее о привязке IP-адресов к географическим данным (см. раздел "Работа с геоданными" на стр. 361).

При выборе этого типа в блоке параметров **Сопоставление геоданных с полями события** необходимо указать, из какого поля события будет считан IP-адрес, а также выбрать требуемые атрибуты геоданных и определить поля событий, в которые геоданные будут записаны:

1. В раскрывающемся списке **Поле события с IP-адресом** выберите поле события, из которого считывается IP-адрес. По этому IP-адресу будет произведен поиск соответствий по загруженным в KUMA геоданным.

С помощью кнопки **Добавить поле события с IP-адресом** можно указать несколько полей события с IP-адресами, по которым требуется обогащение геоданными. Удалить добавленные таким образом поля событий можно с помощью кнопки **Удалить поле события с IP-адресом**.

При выборе полей события `SourceAddress`, `DestinationAddress` и `DeviceAddress` становится доступна кнопка **Применить сопоставление по умолчанию**. С ее помощью можно добавить преднастроенные пары соответствий (см. раздел "Сопоставление геоданных по умолчанию" на стр. 364) атрибутов геоданных и полей события.

2. Для каждого поля события, откуда требуется считать IP-адрес, выберите тип геоданных и поле события, в которое следует записать геоданные.

   С помощью кнопки **Добавить атрибут геоданных** вы можете добавить пары полей **Атрибут геоданных** – **Поле события для записи**. Так вы можете настроить запись разных типов геоданных одного IP-адреса в разные поля события. Пары полей можно удалить с помощью значка ✕.

   - В поле **Атрибут геоданных** выберите, какие географические сведения, соответствующие считанному IP-адресу, необходимо записать в событие. Доступные атрибуты геоданных: **Страна**, **Регион**, **Город**, **Долгота**, **Широта**.
   - В поле **Поле события для записи** выберите поле события, в которое необходимо записать выбранный атрибут геоданных.

   Вы можете записать одинаковые атрибуты геоданных в разные поля событий. Если вы настроите запись нескольких атрибутов геоданных в одно поле события, событие будет обогащено последним по очереди сопоставлением.

Точки назначения

Ресурсы точек назначения для получения событий и их последующей отправки в другие сервисы. Параметры точек назначения указываются на двух закладках: **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа точки назначения:

- **nats** (см. раздел "**Тип nats**" на стр. 200) – используется для коммуникации через NATS.
- **tcp** (см. раздел "**Тип tcp**" на стр. 201) – используется для связи по протоколу TCP.
- **http** (см. раздел "**Тип http**" на стр. 203) – используется для связи по протоколу HTTP.
- **diode** (см. раздел "**Тип diode**" на стр. 204) – используется для передачи событий с помощью диода данных (см. раздел "Передача в KUMA событий из изолированных сегментов сети" на стр. 366).
- **kafka** (см. раздел "**Тип kafka**" на стр. 206) – используется для коммуникаций с помощью kafka.
- **file** (см. раздел "**Тип file**" на стр. 208) – используется для записи в файл.
- **storage** (см. раздел "**Тип storage**" на стр. 209) – используется для передачи данных в хранилище.
- **correlator** (см. раздел "**Тип correlator**" на стр. 210) – используется для передачи данных в коррелятор.

kaspersky

В этом разделе

Тип nats 200
Тип tcp 201
Тип http 203
Тип diode 204
Тип kafka 206
Тип file 208
Тип storage 209
Тип correlator 210

Тип nats

Тип **nats** используется для коммуникации через NATS.

Доступные параметры:

Закладка Основные параметры**:**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип коннектора.
- **URL** (обязательно) – URL, с которым необходимо установить связь.
- **Топик** (обязательно) – тема сообщений NATS. Должно содержать от 1 до 255 символов Юникода.
- **Разделитель** – используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- **Авторизация** – тип авторизации при подключении к указанному URL:
  - **выключена** (по умолчанию).
  - **обычная**.

    При выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору.

    Добавить секрет (см. раздел "Добавление секрета" на стр. 177)
- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка Дополнительные параметры**:**

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.
- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
- **Идентификатор хранилища** – идентификатор хранилища NATS.
- **Режим TLS** – использование шифрования TLS:
  - **Выключено** (по умолчанию) – не использовать шифрование TLS.
  - **Включено** – использовать шифрование, но без верификации сертификата.
  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы (см. раздел "Изменение корневого сертификата" на стр. 46) и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
  - **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

    Создание сертификата, подписанного центром сертификации (см. раздел "Нестандартный CA" на стр. 175)

  При использовании TLS невозможно указать IP-адрес в качестве URL.
- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.
- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.
- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.
- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Тип tcp

Тип **tcp** используется для связи по протоколу TCP.

Доступные параметры:

Закладка Основные параметры**:**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип коннектора.
- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port. С помощью кнопки **URL** можно добавить несколько адресов, если в вашу лицензию KUMA включен модуль High Level Availability.
- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка Дополнительные параметры**:**

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.
- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
- **Режим TLS** – использование шифрования TLS:
  - **Выключено** (по умолчанию) – не использовать шифрование TLS.
  - **Включено** – использовать шифрование, но без верификации сертификата.
  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы (см. раздел "Изменение корневого сертификата" на стр. 46) и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

  При использовании TLS невозможно указать IP-адрес в качестве URL.
- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.
- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.
- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Тип http

Тип **http** используется для связи по протоколу HTTP.

Доступные параметры:

Закладка Основные параметры**:**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип коннектора.
- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port. С помощью кнопки **URL** можно добавить несколько адресов, если в вашу лицензию KUMA включен модуль High Level Availability.
- **Авторизация** – тип авторизации при подключении к указанному URL:
  - **выключена** (по умолчанию).
  - **обычная**.

    При выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору.

    Добавить секрет (см. раздел "Добавление секрета" на стр. 177)
- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка Дополнительные параметры**:**

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.
- **Прокси-сервер** – раскрывающийся список для выбора ресурса прокси-сервера (см. раздел "Прокси-серверы" на стр. 226).
- Размер буфера – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.
- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
- **Режим TLS** – использование шифрования TLS:
  - **Выключено** (по умолчанию) – не использовать шифрование TLS.

- **Включено** – использовать шифрование, но без верификации сертификата.
- **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы (см. раздел "Изменение корневого сертификата" на стр. 46) и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
- **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

  Создание сертификата, подписанного центром сертификации (см. раздел "Нестандартный CA" на стр. 175)

При использовании TLS невозможно указать IP-адрес в качестве URL.

- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:
  - **Любой**
  - **Сначала первый**
  - **По очереди**
- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- **Путь** – путь, который необходимо добавить для URL-запроса. Например, если указать путь `/input`, а в качестве URL ввести `10.10.10.10`, то от точки назначения будут исходить запросы `10.10.10.10/input`.
- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.
- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- Вы можете установить проверки работоспособности, используя поля **Путь проверки работоспособности** и **Ожидание проверки работоспособности**. Вы также можете отключить проверку работоспособности, установив флажок **Проверка работоспособности отключена**.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.
- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.
- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Тип diode

Тип **diode** используется для передачи событий с помощью диода данных (см. раздел "Передача в KUMA событий из изолированных сегментов сети" на стр. 366).

Доступные параметры:

Закладка Основные параметры**:**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип коннектора.
- **Директория, из которой диод данных получает события** (обязательно) – директория, откуда диод данных перемещает события. Путь может содержать до 255 символов Юникода.

  Ограничения при использовании префиксов к путям на серверах Windows (см. раздел "Ограничения на Windows" на стр. 206)

  Ограничения при использовании префиксов к путям на серверах Linux (см. раздел "Коннектор, тип file - ограничения" на стр. 187)
- **Временная директория** – директория, в которой события готовятся для передачи диоду данных.

  События собираются в файл по истечении времени ожидания (по умолчанию 10 секунд) или при переполнении буфера. В качестве названия файла с событиями используется хеш-сумма (SHA-256) содержимого файла. Подготовленный файл перемещается в директорию, указанную в поле **Директория, из которой диод данных получает события**.

  Временная директория не должна совпадать с директорией, из которой диод данных получает события.
- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка Дополнительные параметры**:**

- **Сжатие** – можно использовать сжатие Snappy. По умолчанию сжатие **Выключено**.

  Этот параметр должен совпадать ресурсах коннектор и точка назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.
- **Размер буфера** – используется для установки размера буфера. По умолчанию размер равен 64 МБ. Не может быть больше 64 МБ.
- **Время ожидания** – поле, в котором можно указать интервал (в секундах) между перемещением данных из временной директории в директорию для диода данных. Значение по умолчанию: `10`.
- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

  Этот параметр должен совпадать ресурсах коннектор и точка назначения, используемых для передачи событий из изолированного сегмента сети с помощью диода данных.
- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.
- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.
- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.
- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Ограничения на Windows

На серверах Windows необходимо указывать абсолютные пути к директориям. Невозможно использовать директории, названия которых соответствуют указанным ниже регулярным выражениям:

- `^[a-zA-Z]:\\Program Files`
- `^[a-zA-Z]:\\Program Files \(x86\)`
- `^[a-zA-Z]:\\Windows`
- `^[a-zA-Z]:\\Program Files\\Kaspersky Lab\\KUMA`

Тип kafka

Тип **kafka** используется для коммуникаций с помощью kafka.

Доступные параметры:

Закладка Основные параметры**:**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип коннектора.
- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port. С помощью кнопки **URL** можно добавить несколько адресов, если в вашу лицензию KUMA включен модуль High Level Availability.
- **Топик** (обязательно) – тема сообщений NATS. Должно содержать от 1 до 255 символов Юникода.
- **Разделитель** – используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- **Авторизация** – тип авторизации при подключении к указанному URL:
  - **выключена** (по умолчанию).
  - **PFX**.

При выборе этого варианта требуется сформировать сертификат с закрытым ключом в формате PKCS#12-контейнера во внешнем центре сертификации, экспортировать сертификат из хранилища и загрузить его в веб-интерфейс KUMA в виде PFX-секрета.

Добавить PFX-секрет (на стр. 177)

- **обычная**.

  При выборе этого варианта требуется указать секрет, содержащий данные учетной записи пользователя для авторизации при подключении к коннектору.

  Добавить секрет (см. раздел "Добавление секрета" на стр. 177)

- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка Дополнительные параметры**:**

- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.
- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
- **Режим TLS** – использование шифрования TLS:
  - **Выключено** (по умолчанию) – не использовать шифрование TLS.
  - **Включено** – использовать шифрование, но без верификации сертификата.
  - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы (см. раздел "Изменение корневого сертификата" на стр. 46) и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.
  - **Нестандартный CA** – использовать шифрование с верификацией сертификата, подписанного центром сертификации. Секрет с сертификатом выбирается в раскрывающемся списке **Нестандартный CA**, который отображается при выборе этого пункта.

    Создание сертификата, подписанного центром сертификации (см. раздел "Нестандартный CA" на стр. 175)

  При использовании TLS невозможно указать IP-адрес в качестве URL.
- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.
- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.
- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Тип file

Тип **file** используется для записи в файл.

Доступные параметры:

Закладка Основные параметры**:**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип коннектора.
- **URL** (обязательно) – путь к файлу, в который необходимо записать события.

  Ограничения при использовании префиксов к путям файлов (см. раздел "Коннектор, тип file - ограничения" на стр. 187)
- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка Дополнительные параметры**:**

- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.
- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
- **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.
- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.
- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.

- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Тип storage

Тип **storage** используется для передачи данных в хранилище.

Доступные параметры:

Закладка Основные параметры**:**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип коннектора.
- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port.

  С помощью кнопки **URL** можно добавить несколько адресов, при этом ваша лицензия KUMA может не включать модуль High Level Availability.

  Поле **URL** можно заполнить автоматически с помощью раскрывающегося списка **Копировать URL сервиса**, в котором отображаются активные сервисы (см. раздел "Сервисы KUMA" на стр. 229) выбранного типа.
- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка Дополнительные параметры**:**

- **Прокси-сервер** – раскрывающийся список для выбора ресурса прокси-сервера (см. раздел "Прокси-серверы" на стр. 226).
- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.
- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:
  - **Любой**
  - **Сначала первый**
  - **По очереди**
- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.

- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Ожидание проверки работоспособности** – время ожидания проверки работоспособности в секундах.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.
- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.
- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Тип correlator

Тип **correlator** используется для передачи данных в коррелятор.

Доступные параметры:

Закладка Основные параметры**:**

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Переключатель **Выключено** – используется в том случае, если события не нужно отправляться в точку назначения. По умолчанию отправка событий включена.
- **Тип** (обязательно) – тип коннектора.
- **URL** (обязательно) – URL, с которым необходимо установить связь. Доступные форматы: hostname:port, IPv4:port, IPv6:port, :port. С помощью кнопки **URL** можно добавить несколько адресов, если в вашу лицензию KUMA включен модуль High Level Availability.

  Поле **URL** можно заполнить автоматически с помощью раскрывающегося списка **Копировать URL сервиса**, в котором отображаются активные сервисы (см. раздел "Сервисы KUMA" на стр. 229) выбранного типа.
- **Описание** – описание ресурса: до 256 символов Юникода.

Закладка Дополнительные параметры**:**

- **Прокси-сервер** – раскрывающийся список для выбора ресурса прокси-сервера (см. раздел "Прокси-серверы" на стр. 226).
- **Размер буфера** – используется для установки размера буфера. Значение по умолчанию: 16 Кб; максимальное: 64 Кб.
- **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.

- **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
- **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:
  - **Любой**
  - **Сначала первый**
  - **По очереди**
- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.
- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- **Ожидание проверки работоспособности** – время ожидания проверки работоспособности в секундах.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.
- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.
- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

kaspersky

Фильтры

Ресурсы фильтров используются для выбора событий на основе определенных пользователем условий.

> Это неверно только тогда, когда фильтры используются в сервисе коллектор (на стр. 20), где они выбирают все события, которые НЕ удовлетворяют условиям фильтра.

Фильтры можно использовать в сервисах коллектора (см. раздел "Создание коллектора" на стр. 235), ресурсах правил обогащения (см. раздел "Правила обогащения" на стр. 194), ресурсах правил агрегации (см. раздел "Правила агрегации" на стр. 194), ресурсах правил реагирования (см. раздел "Правила реагирования" на стр. 217), ресурсах правил корреляции (см. раздел "Правила корреляции" на стр. 134) и ресурсах точек назначения (см. раздел "Точки назначения" на стр. 199): либо как отдельные ресурсы фильтра, либо как встроенные фильтры, которые хранятся в сервисе или ресурсе, где они были созданы.

Для этих ресурсов в полях ввода, кроме поля **Описание**, можно включить отображение непечатаемых символов (см. раздел "Редактирование своей учетной записи" на стр. 71).

Доступные параметры ресурсов фильтра:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода. Встроенные фильтры создаются в других ресурсах или сервисах и не имеют имен.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- Блок параметров **Условия** – здесь вы можете сформулировать критерии фильтрации, создав условия фильтрации и группы фильтров, а также добавив существующие ресурсы фильтров.

  С помощью кнопки **Добавить группу** можно добавить группу фильтров. Можно переключать групповые операторы между **И**, **ИЛИ**, **НЕ**. В группы фильтров можно добавить группы, условия и существующие ресурсы фильтров.

  С помощью кнопки **Добавить фильтр** можно добавить существующий ресурс фильтра, который следует выбрать в раскрывающемся списке **Выберите фильтр**.

  С помощью кнопки **Добавить условие** можно добавить строку с полями для определения условия (см. ниже).

  Условия, группы и фильтры можно удалить с помощью кнопки ✕.

Параметры условий:

- **Если** (обязательно) – в этом раскрывающемся списке можно указать, требуется ли использовать инвертированную функцию оператора
- **Левый операнд** и **Правый операнд** (обязательно) – используются для указания значений, которые будет обрабатывать оператор. Доступные типы зависят от выбранного оператора.

  Операнды фильтров (см. раздел "Операнды фильтров" на стр. 213)
- **Оператор** (обязательно) – используется для выбора оператора условия.

  В этом же раскрывающемся списке можно установить флажок **без учета регистра**, если требуется, чтобы оператор игнорировал регистр значений. Флажок игнорируется, если выбраны операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

  Операторы фильтров (см. раздел "Операторы фильтров" на стр. 215)

Доступные типы операндов зависят от того, является ли операнд левым (L) или правым (R).

Таблица 5. Доступные типы операндов для левого (L) и правого (R) операндов

Оператор	Тип "поле события"	Тип "активный лист"	Тип "словарь"	Тип "константа"	Тип "список"	Тип "TI"
=	L,R	L,R	L,R	R	R	L,R
>	L,R	L,R	L,R	R		L,R
>=	L,R	L,R	L,R	R		L,R
<	L,R	L,R	L,R	R		L,R
<=	L,R	L,R	L,R	R		L,R
contains	L,R	L,R	L,R	R	R	L,R
startsWith	L,R	L,R	L,R	R	R	L,R
endsWith	L,R	L,R	L,R	R	R	L,R
match	L	L	L	R	R	L
inSubnet	L,R	L,R	L,R	R	R	L,R
inCategory	L	L	L	R	R	
inActiveDirectoryGroup	L	L	L	R	R	
inActiveList		L				
TIDetect						

kaspersky

Операнды фильтров

- **Поле события** – используется для присвоения операнду значения поля события. Дополнительные параметры:
  - **поле события** (обязательно) – этот раскрывающийся список используется для выбора поля, из которого следует извлечь значение операнда.
- **Активный лист** – используется для присвоения операнду значения записи активного листа (см. раздел "Активные листы" на стр. 224). Дополнительные параметры:
  - **название активного листа** (обязательно) – этот раскрывающийся список используется для выбора активного листа.
  - **ключевые поля** (обязательно) – это список полей событий, используемых для создания записи активного листа и служащих ключом записи активного листа.
  - **поле** (требуется, если не выбран оператор **inActiveList**) – используется для ввода имени поля активного листа, из которого следует извлечь значение операнда.
- **Словарь** – используется для присвоения значения операнду значения из ресурса словарь (см. раздел "Словари" на стр. 225). Дополнительные параметры:
  - **словарь** (обязательно) – этот раскрывающийся список используется для выбора словаря.
  - **ключевые поля** (обязательно) – это список полей событий, используемых для формирования ключа значения словаря.
- **Константа** – используется для присвоения операнду пользовательского значения. Дополнительные параметры:
  - **значение** (обязательно) – здесь вы вводите константу, которую хотите присвоить операнду.
- **Таблица** – используется для присвоения операнду нескольких пользовательских значений. Дополнительные параметры:
  - **словарь** (обязательно) – этот раскрывающийся список используется для выбора словаря типа **Таблица**.
  - **ключевые поля** (обязательно) – это список полей событий, используемых для формирования ключа значения словаря.
- **Список** – используется для присвоения операнду нескольких пользовательских значений. Дополнительные параметры:
  - **значение** (обязательно) – здесь вы вводите список констант, которые хотите назначить операнду. Когда вы вводите значение в поле и нажимаете **ENTER**, значение добавляется в список, и вы можете ввести новое значение.
- **TI** – используется для чтения данных CyberTrace об угрозах (TI) из событий. Дополнительные параметры:
  - **канал** (обязательно) – в этом поле указывается категория угрозы CyberTrace.
  - **ключевые поля** (обязательно) – этот раскрывающийся список используется для выбора поля события с индикаторами угроз CyberTrace.
  - **поле** (обязательно) – в этом поле указывается поле фида CyberTrace с индикаторами угроз.

kaspersky

Операторы фильтров

- **=** – левый операнд равен правому операнду.
- **<** – левый операнд меньше правого операнда.
- **<=** – левый операнд меньше или равен правому операнду.
- **>** – левый операнд больше правого операнда.
- **>=** – левый операнд больше или равен правому операнду.
- **inSubnet** – левый операнд (IP-адрес) находится в подсети правого операнда (подсети).
- **contains** – левый операнд содержит значения правого операнда.
- **startsWith** – левый операнд начинается с одного из значений правого операнда.
- **endsWith** – левый операнд заканчивается одним из значений правого операнда.
- **match** – левый операнд соответствует регулярному выражению правого операнда. Используются регулярные выражения RE2.
- **inActiveList** – этот оператор имеет только один операнд. Его значения выбираются в поле **Ключевые поля** и сравниваются с записями активного листа, выбранного в раскрывающемся списке активных листов.
- **inCategory** – активу в левом операнде назначена по крайней мере одна из категорий активов правого операнда.
- **inActiveDirectoryGroup** – учетная запись Active Directory в левом операнде принадлежит одной из групп Active Directory в правом операнде.
- **TIDetect** – этот оператор используется для поиска событий с данными CyberTrace Threat Intelligence (TI). Этот оператор можно использовать только на событиях, прошедших обогащение данными из CyberTrace Threat Intelligence, то есть только в коллекторах на этапе выбора точки назначения и в корреляторах.

Поиск по данным поля события Extra

Условия для фильтров по данным из поля события **Extra**:

- Условие – **Если**.
- Левый операнд – **поле события**.
- В поле события вы можете указать одно из следующих значений:
  - Поле **Extra**.
  - Значение из поля Extra в следующем формате:

    `Extra.<название поля>`

    Например, `Extra.app`.

    > Значение этого типа указывается вручную.

  - Значение из массива, записанного в поле **Extra**, в следующем формате:

`Extra.<название поля>.<элемент массива>`

Например, `Extra.array.0`.

Нумерация значений в массиве начинается с 0.

Значение этого типа указывается вручную.

- Оператор – =.
- Правый операнд – **константа**.
- Значение – значение, по которому требуется фильтровать события.

Создание фильтра в ресурсах

1. В раскрывающемся списке **Фильтр** выберите **Создать**.
2. Если вы хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**.

   В этом случае вы сможете использовать созданный фильтр в разных сервисах.

   По умолчанию флажок снят.
3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов Юникода.
4. В блоке параметров **Условия** задайте условия, которым должны соответствовать события:
   a. Нажмите на кнопку **Добавить условие**.
   b. В раскрывающихся списках **Левый операнд** и **Правый операнд** укажите параметры поиска.

      В зависимости от источника данных, выбранного в поле **Правый операнд**, могут отобразиться поля дополнительных параметров (см. раздел "Фильтры" на стр. 212), с помощью которых вам нужно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.
   c. В раскрывающемся списке **оператор** выберите нужный вам оператор.

      Операторы фильтров (см. раздел "Операторы фильтров" на стр. 215)
   d. При необходимости установите флажок **без учета регистра**. В этом случае оператор игнорирует регистр значений.

      Действие флажка не распространяется на операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**.

      По умолчанию флажок снят.
   e. Если вы хотите добавить отрицательное условие, в раскрывающемся списке **Если** выберите **Если не**.
   f. Вы можете добавить несколько условий или группу условий.
5. Если вы добавили несколько условий или групп условий, выберите условие отбора (и, или, не), нажав на кнопку **И**.
6. Если вы хотите добавить уже существующие фильтры, которые выбираются в раскрывающемся списке **Выберите фильтр**, нажмите на кнопку **Добавить фильтр**.

Параметры вложенного фильтра можно просмотреть, нажав на кнопку  .

Правила реагирования

Вы можете настроить автоматическое выполнение задач Kaspersky Security Center, действий по реагированию Kaspersky Endpoint Detection and Response и запуска пользовательского скрипта при получении событий, для которых настроены правила реагирования.

Автоматическое выполнение задач Kaspersky Security Center, Kaspersky Endpoint Detection and Response и KICS for Networks по правилам реагирования доступно при интеграции с перечисленными программами (см. раздел "Интеграция с другими решениями" на стр. 73).

В этом разделе

Правила реагирования для Kaspersky Security Center 217

Правила реагирования для пользовательского скрипта 218

Правила реагирования для KICS for Networks 219

Правила реагирования для Kaspersky Security Center

Вы можете настроить правила реагирования для автоматического запуска задач на активах Kaspersky Security Center. Например, вы можете настроить автоматический запуск антивирусной проверки или обновление базы данных.

При создании и изменении (см. раздел "Создание, дублирование, перемещение, редактирование и удаление ресурсов" на стр. 131) правил реагирования для Kaspersky Security Center вам требуется задать значения для следующих параметров:

- **Название** (обязательно) – уникальное имя ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – **ksctasks**.

  Доступно при интеграции KUMA с Kaspersky Security Center (см. раздел "Интеграция с Kaspersky Security Center" на стр. 73).

- **Задача Kaspersky Security Center** (обязательно) – название задачи Kaspersky Security Center, которую требуется запустить. Задачи должны быть созданы заранее, и их названия должны начинаться со слова "`KUMA `". Например, "`KUMA antivirus check`".

  Регистр не имеет значения.

- **Поле события** (обязательно) – определяет поле события для актива, для которого нужно запустить задачу Kaspersky Security Center. Возможные значения:

  - SourceAssetID.
  - DestinationAssetID.
  - DeviceAssetID.
- **Рабочие процессы** – количество процессов, которые сервис может запускать одновременно.

  По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
- **Описание** – вы можете добавить до 4000 символов Юникода, описывающих ресурс.
- **Фильтр** – используется для определения условий, при соответствии которым события будут обрабатываться ресурсом правила реагирования. В раскрывающемся списке можно выбрать существующий ресурс фильтра или создать новый фильтр.

Для отправки запросов в Kaspersky Security Center необходимо убедиться, что Kaspersky Security Center доступен по протоколу UDP.
Если ресурс правила реагирования принадлежит общему тенанту (см. раздел "О тенантах" на стр. 25), то в качестве доступных для выбора задач Kaspersky Security Center отображаются задачи от сервера Kaspersky Security Center, к которому подключен главный тенант.
Если в ресурсе правила реагирования выбрана задача, которая отсутствует на сервере Kaspersky Security Center, к которому подключен тенант, для активов этого тенанта задача не будет выполнена. Такая ситуация может возникнуть, например, когда два тенанта используют общий коррелятор (см. раздел "Правила принадлежности к тенантам" на стр. 302).

Правила реагирования для пользовательского скрипта

Вы можете создать скрипт с командами, которые требуется выполнить на сервере KUMA при обнаружении выбранных событий, и настроить правила реагирования для автоматического запуска этого скрипта. В этом случае программа запустит скрипт при получении событий, соответствующих правилам реагирования.

Файл скрипта хранится на сервере, где установлен сервис коррелятора (см. раздел "Установка коррелятора в сетевой инфраструктуре KUMA" на стр. 262), использующий ресурс реагирования: /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора (см. раздел "Получение идентификатора сервиса" на стр. 231)>/scripts. Пользователю `kuma` этого сервера требуются права на запуск скрипта.

При создании и изменении (см. раздел "Создание, дублирование, перемещение, редактирование и удаление ресурсов" на стр. 131) правил реагирования для произвольного скрипта вам требуется задать значения для следующих параметров:

- **Название** (обязательно) – уникальное имя ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – **script**.
- **Время ожидания** – количество секунд, в течение которого должно завершиться выполнение скрипта. Если это время превышено, выполнение скрипта прерывается.
- **Название скрипта** (обязательно) – имя файла скрипта.

Если ресурс реагирования прикреплен к сервису коррелятора, но в папке /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts файл скрипта отсутствует, коррелятор не будет работать.

- **Аргументы скрипта** – параметры или значения полей событий, которые необходимо передать скрипту.

  Если в скрипте производятся какие-либо действия с файлами, к ним следует указывать абсолютный путь.

  Параметры можно обрамлять кавычками (").

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это имя поля события, значение которого должно быть передано в скрипт.

  Пример: `-n "\"usr\": {{.SourceUserName}}"`

- **Рабочие процессы** – количество процессов, которые сервис может запускать одновременно.

  По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.

- **Описание** – вы можете добавить до 4000 символов Юникода, описывающих ресурс.

- **Фильтр** – используется для определения условий, при соответствии которым события будут обрабатываться ресурсом правила реагирования. В раскрывающемся списке можно выбрать существующий ресурс фильтра или создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Правила реагирования для KICS for Networks

Вы можете настроить правила реагирования для автоматического запуска действий по реагированию на активах KICS for Networks. Например, изменить статус актива в KICS for Networks.

При создании и изменении (см. раздел "Создание, дублирование, перемещение, редактирование и удаление ресурсов" на стр. 131) правил реагирования для KICS for Networks вам требуется задать значения для следующих параметров:

- **Название** (обязательно) – уникальное имя ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – **kics**.
- **Поле события** (обязательно) – поле события с активом, для которого нужно выполнить действия по реагированию. Возможные значения:
  - SourceAssetID.
  - DestinationAssetID.
  - DeviceAssetID.

- **Задача KICS for Networks** – действие по реагированию, которое требуется выполнить при получении данных, соответствующих фильтру. Доступны следующие типы действий по реагированию:
  - **Изменить статус актива на Разрешенное**.
  - **Изменить статус актива на Неразрешенное**.

  При срабатывании правила реагирования из KUMA в KICS for Networks будет отправлен API-запрос на изменение статуса указанного устройства на **Разрешенное** или **Неразрешенное**.
- **Рабочие процессы** – количество процессов, которые сервис может запускать одновременно.

  По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.
- **Описание** – вы можете добавить до 4000 символов Юникода, описывающих ресурс.
- **Фильтр** – используется для определения условий, при соответствии которым события будут обрабатываться ресурсом правила реагирования. В раскрывающемся списке можно выбрать существующий ресурс фильтра или создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Шаблоны уведомлений

Параметры ресурса

Ресурсы шаблонов уведомлений используются в уведомлениях (см. раздел "Уведомления KUMA" на стр. 410) о создании алертов.

Параметры ресурса шаблона уведомления:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тема** (обязательно) – тема электронного письма с уведомлением о создании алерта. В теме письма можно обращаться к полям алерта.

  Пример: `Новый алерт в KUMA: {{.CorrelationRuleName}}`. Вместо `{{.CorrelationRuleName}}` в теме письма с уведомлением будет подставлено название правила корреляции, содержащееся в поле алерта `CorrelationRuleName`.
- **Шаблон** (обязательно) – тело электронного письма с уведомлением о создании алерта. Шаблон поддерживает синтаксис, с помощью которого уведомление можно наполнить данными из алерта.

  Для удобства можно открыть текст письма в отдельном окне, нажав на значок  . При этом открывается окно **Шаблон**, в котором можно править текст письма с уведомлением. Сохранить изменения и закрыть окно можно с помощью кнопки **Сохранить**.

Синтаксис шаблона уведомления

В шаблоне можно обращаться к полям алерта (см. раздел "Модель данных алерта" на стр. 488), содержащим строку или число:

```
{{ .CorrelationRuleName }}
```

В письме будет отображаться название алерта, то есть содержимое поля `CorrelationRuleName`.

Некоторые поля алерта содержат массивы данных. Например, это поля алерта с относящимися к нему событиями (см. раздел "Модель данных нормализованного события" на стр. 471), активами (см. раздел "Модель данных актива" на стр. 491), учетными записями (см. раздел "Модель данных учетной записи" на стр. 499). К таким вложенным объектам можно обращаться с помощью функции **range**, которая последовательно обращается к полям 50 первых вложенных объектов. При обращении с помощью функции **range** к полю, в котором нет массива данных, возвращается ошибка. Пример:

```
{{ range .Assets }}
Устройство: {{ .DisplayName }}, дата создания: {{ .CreatedAt }}
{{ end }}
```

В письме будут отображаться значения полей `DeviceHostName` и `CreatedAt` из 50 связанных с алертом активов:

```
Устройство: <значение поля DisplayName из актива 1>, дата создания:
<значение поля CreatedAt из актива 1>
Устройство: <значение поля DisplayName из актива 2>, дата создания:
<значение поля CreatedAt из актива 2>
...
// Всего 50 строк
```

С помощью параметра **limit** можно ограничить количество объектов, возвращаемых функцией **range**:

```
{{ range (limit .Assets 5) }}
<strong>Устройство</strong>: {{ .DisplayName }},
<strong>Дата создания</strong>: {{ .CreatedAt }}
{{ end }}
```

В письме будут отображаться значения полей `DisplayName` и `CreatedAt` из 5 связанных с алертом активов, слова "Устройства" и "Дата создания" выделены HTML-тегами :

```
<strong>Устройство</strong>:  <значение поля DeviceHostName из актива 1>,
<strong>Дата создания</strong>: <значение поля CreatedAt из актива 1>
<strong>Устройство</strong>: <значение поля DeviceHostName из актива N>,
<strong>Дата создания</strong>: <значение поля CreatedAt из актива N>
...
// Всего 10 строк
```

Вложенные объекты могут иметь свои вложенные объекты. К ним можно обратиться с помощью вложенных функций **range**:

```
{{ range (limit .Events 5) }}
    {{ range (limit .Event.BaseEvents 10) }}
    Идентификатор сервиса: {{ .ServiceID }}
    {{ end }}
{{ end }}
```

В письме будет отображаться по десять идентификаторов сервисов (поле `ServiceID`) из базовых событий, относящихся к пяти корреляционным событиям алерта. Всего 50 строк. Обратите внимание, что обращение к событиям происходит через вложенную структуру EventWrapper, которая находится в алерте в поле Events. События доступны в поле Event этой структуры, что отражено в примере выше. Таким образом, если поле A содержит вложенную структуру [B] и в структуре [B] есть поле C, которое является строкой или числом, то чтобы обратиться к полю C необходимо указать путь {{ A.C }}.

Некоторые поля объектов содержат вложенные словари в формате "ключ - значение" (например, поле событий `Extra`). К ним можно обратиться с помощью функции **range** с переданными ей переменными: `range $placeholder1, $placeholder2 := .FieldName`. Значения переменных затем можно вызывать, указывая из названия. Пример:

```
{{ range (limit .Events 3) }}
    {{ range (limit .Event.BaseEvents 5) }}
    Список полей в поле события Extra: {{ range $name, $value := .Extra }}
{{ $name }} - {{ $value }} <br> {{ end }}
    {{ end }}
{{ end }}
```

В письме через HTML-тег
 будут отображаться пары "ключ - значение" из полей `Extra` базовых событий, принадлежащих корреляционным событиям. Вызываются данные из пяти базовых событий из каждого из трех корреляционных событий.

В шаблонах уведомлений можно использовать HTML-теги, выстраивая их в сложные структуры. Ниже приводится пример таблицы для полей корреляционного события:

```
<style type="text/css">
  TD, TH {
    padding: 3px;
    border: 1px solid black;
  }
</style>
<table>
  <thead>
    <tr>
        <th>Название сервиса</th>
        <th>Название корреляционного правила</th>
        <th>Версия устройства</th>
    </tr>
  </thead>
  <tbody>
    {{ range .Events }}
    <tr>
        <td>{{ .Event.ServiceName }}</td>
        <td>{{ .Event.CorrelationRuleName }}</td>
        <td>{{ .Event.DeviceVersion }}</td>
    </tr>
    {{ end }}
  </tbody>
</table>
```

С помощью функции **link_alert** в письмо с уведомлением можно вставить HTML-ссылку на алерт:

```
{{link_alert}}
```

В письме будет отображаться ссылка на окно алерта.

kaspersky

Активные листы

Ресурсы активных листов – это динамически обновляемые контейнеры данных, используемые коррелляторами (см. раздел "Коррелятор" на стр. 23) KUMA для чтения и записи информации при анализе событий по правилам корреляции (см. раздел "Правила корреляции" на стр. 134).

Один и тот же ресурс активного листа может быть использован разными сервисами коррелляторов, однако при этом для каждого коррелятора создается своя сущность активного листа. Таким образом, содержимое активных листов, используемых разными коррелляторами, различается, даже если идентификатор и название активных листов одинаковые. Содержимое активного листа можно открыть из окна активных сервисов (см. раздел "Окно активных листов коррелятора" на стр. 233).

Параметры ресурса активный лист:

- **Идентификатор** – идентификатор активного листа. Этот параметр отображается у созданных активных листов. Значение можно скопировать с помощью кнопки  .
- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Срок жизни** – время в секундах, в течение которого в активном листе будет храниться добавленная в него запись. Значение по умолчанию: `0`. Максимальный срок жизни: `31536000` (один год). При истечении срока жизни запись удаляется, при этом создается событие удаления записи из активного листа (см. ниже).
- **Описание** – вы можете добавить до 256 символов Юникода, описывающих ресурс.

В процессе корреляции при удалении записей из активных листов в коррелляторах создаются служебные события. Эти события существуют только в коррелляторах, они не перенаправляются в другие точки назначения. Правила корреляции (на стр. 134) можно настроить на отслеживание этих событий, чтобы с их помощью распознавать угрозы. Поля служебных событий удаления записи из активного листа описаны ниже.

Поле события	Значение или комментарий
`ID`	Идентификатор события
`Timestamp`	Время удаления записи, срок жизни которой истек
`Name`	`"active list record expired"`
`DeviceVendor`	`"Kaspersky"`
`DeviceProduct`	`"KUMA"`
`ServiceID`	Идентификатор коррелятора
`ServiceName`	Название коррелятора
`DeviceExternalID`	Идентификатор активного листа
`DevicePayloadID`	Ключ записи, чей срок жизни истек.
`BaseEventCount`	Увеличенное на единицу количество обновлений удаленной записи

kaspersky

Словари

Описание параметров

Словари – это ресурсы, в которых хранятся данные, которые могут использоваться другими ресурсами и сервисами KUMA.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Описание** – вы можете добавить до 256 символов Юникода, описывающих ресурс.
- **Тип** (обязательно) – тип словаря. От выбранного типа зависит формат данных, которые может содержать словарь:
  - В тип **Словарь** можно добавлять пары ключ–значение.

    Не рекомендуется добавлять в словари этого типа более 50 000 записей.

    > При добавлении в словарь строк с одинаковыми ключами каждая новая строка будет записана поверх уже существующий строки с тем же самым ключом. В итоге в словарь будет добавлена только одна строка.

  - В тип **Таблица** можно добавлять данные в виде сложных таблиц. С этим типом словарей можно взаимодействовать с помощью REST API (на стр. 413).
- Блок параметров **Значения** – содержит таблицу с данными словаря:
  - Для типа **Словарь** в блоке отображается перечень пар **Ключ** – **Значение**. Таблицу можно дополнять строками с помощью кнопки +. Удалить строки можно с помощью кнопки ×, которая отображается при наведении курсора мыши на нужную строку.
  - Для типа **Таблица** в блоке отображается таблица с данными. Таблицу можно дополнять строками и столбцами с помощью кнопки +. Удалить строки и столбцы можно с помощью кнопок ×, которые отображаются при наведении курсора мыши на нужную строку или заголовок нужного столбца. Заголовки столбцов доступны для редактирования.

  Если словарь содержит больше 5000 записей, они не отображаются в веб-интерфейсе KUMA. Для просмотра содержимого таких словарей содержимое необходимо экспортировать в формат CSV. Если CSV-файл отредактировать и снова импортировать в KUMA, ресурс словаря будет обновлен.

Импорт и экспорт словарей

Данные словарей можно импортировать или экспортировать в формате CSV (в кодировке UTF-8) с помощью кнопок **Импортировать CSV** и **Экспортировать CSV**.

Формат CSV-файла зависит от типа словаря:

- Тип **Словарь**:

  ```
  {КЛЮЧ},{ЗНАЧЕНИЕ}\n
  ```

- Тип **Таблица**:

```
{Заголовок столбца 1},{Заголовок столбца N},{Заголовок столбца N+1}\n
{Ключ1},{ЗначениеN},{ЗначениеN+1}\n
{Ключ2},{ЗначениеN},{ЗначениеN+1}\n
```

Ключи должны быть уникальными как для CSV-файла, так и для словаря. В таблицах ключи указываются в первом столбце. Ключ должен содержать от 1 до 128 символов Юникода.

Значения должны содержать от нуля до 256 символов Юникода.

При импорте содержимое словаря перезаписывается загружаемым файлом. При импорте в словарь также изменяется название ресурса, чтобы отразить имя импортированного файла.

При экспорте, если ключ или значение содержат символы запятой или кавычек (, и "), они заключаются в кавычки ("). Кроме того, символ кавычки (") экранируется дополнительной кавычкой ("").

Если в импортируемом файле обнаружены некорректные строки (например, неверные разделители), то при импорте в словарь такие строки будут проигнорированы, а при импорте в таблицу процесс импорта будет прерван.

Взаимодействие со словарями через API

С помощью REST API можно считывать (см. раздел "Получение словаря" на стр. 461) содержимое словарей типа **Таблица**, а также изменять (см. раздел "Обновление словаря в сервисах" на стр. 458) его, даже если эти ресурсы используются активными сервисами. Это позволяет, например, настроить обогащение событий данными из динамически изменяемых таблиц, выгружаемых из сторонних приложений.

Прокси-серверы

Ресурсы *прокси-сервера* используются для хранения параметров конфигурации прокси-серверов.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Брать URL из секрета** (обязательно) – раскрывающийся список для выбора ресурса секрета (см. раздел "Секреты" на стр. 226), в котором хранятся URL прокси-серверов. При необходимости секрет можно создать в окне создания прокси-сервера с помощью кнопки  . Выбранный секрет можно изменить, нажав на кнопку  .
- **Не использовать на доменах** – один или несколько доменов, к которым требуется прямой доступ.
- **Описание** – вы можете добавить до 256 символов Юникода, описывающих ресурс.

Секреты

Ресурсы *секрет* используются для безопасного хранения конфиденциальной информации, такой как логины и пароли, которые должны использоваться KUMA для взаимодействия с внешними службами.

Доступные параметры:

- **Название** (обязательно) – уникальное имя для этого типа ресурса. Должно содержать от 1 до 128 символов Юникода.
- **Тенант** (обязательно) – название тенанта, которому принадлежит ресурс.
- **Тип** (обязательно) – тип секрета.

  При выборе в раскрывающемся списке типа секрета отображаются параметры для настройки выбранного типа секрета. Эти параметры описаны ниже.
- **Описание** – вы можете добавить до 256 символов Юникода, описывающих ресурс.

В зависимости от типа секрета доступны различные поля для заполнения. Вы можете выбрать один из следующих типов секрета:

- **credentials** – тип секрета используется для хранения данных учетных записей, с помощью которых осуществляется подключение к внешним службам, например к SMTP-серверам. При выборе этого типа секрета требуется заполнить поля **Пользователь** и **Пароль**.
- **token** – тип секрета используется для хранения токенов для API-запросов. Токены используются, например, при подключении к IRP-системам. При выборе этого типа секрета требуется заполнить поле **Токен**.
- **ktl** – тип секрета используется для хранения данных учетной записи Kaspersky Threat Intelligence Portal. При выборе этого типа секрета требуется заполнить следующие поля:
  - **Пользователь** и **Пароль** (обязательные поля) – имя пользователя и пароль вашей учетной записи Kaspersky Threat Intelligence Portal.
  - **Файл обмена личной информацией - PKCS (.PFX)** (обязательно) – позволяет загрузить ключ сертификата Kaspersky Threat Intelligence Portal.
  - **Пароль PFX-файла** (обязательно) – пароль для доступа к ключу сертификата Kaspersky Threat Intelligence Portal.
- **urls** – тип секрета используется для хранения URL для подключения к базам SQL и прокси-серверам. В поле **Описание** требуется описать, для какого именно подключения вы используете секрет **urls**.

  Вы можете указать URL в следующих форматах: hostname:port, IPv4:port, IPv6:port, :port.
- **pfx** – тип секрета используется для импорта PFX-файла с сертификатами. При выборе этого типа секрета требуется заполнить следующие поля:
  - **Файл обмена личной информацией - PKCS (.PFX)** (обязательно) – используется для загрузки PFX-файла. Файл должен содержать сертификат и ключ. В PFX-файлы можно включать сертификаты, подписанными центрами сертификации, для проверки сертификатов сервера.
  - **Пароль PFX-файла** (обязательно) – используется для ввода пароля для доступа к ключу сертификата.
- **kata/edr** – тип секрета используется для хранения файла сертификата и закрытого ключа, требуемых при подключении к серверу Kaspersky Endpoint Detection and Response. При выборе этого типа секрета вам требуется загрузить следующие файлы:
  - Файл сертификата – сертификат сервера KUMA.

    Файл должен иметь формат PEM. Вы можете загрузить только один файл сертификата.
  - Закрытый ключ шифрования соединения – RSA-ключ сервера KUMA.

    Ключ должен быть без пароля и с заголовком PRIVATE KEY. Вы можете загрузить только один файл ключа.

Вы можете сгенерировать файлы сертификата и ключа по кнопке  .

- **snmpV1** – тип секрета используется для хранения значения **Уровень доступа** (например, `public` или `private`), которое требуется при взаимодействии по протоколу Simple Network Management Protocol.
- **snmpV3** – тип секрета используется для хранения данных, требуемого при взаимодействии по протоколу Simple Network Management Protocol. При выборе этого типа секрета требуется заполнить поля:
  - **Пользователь** – имя пользователя, указывается без домена.
  - **Уровень безопасности** – уровень безопасности пользователя:
    - **NoAuthNoPriv** – сообщения отправляются без аутентификации и без обеспечения конфиденциальности.
    - **AuthNoPriv** – сообщенияпосылаются с аутентификацией, но без обеспечения конфиденциальности.
    - **AuthPriv** – сообщения посылаются с аутентификацией и обеспечением конфиденциальности.

    В зависимости от выбранного уровня могут отобразиться дополнительные параметры.
  - **Пароль** – пароль пользователя. Это поле становится доступно при выборе уровней безопасности **AuthNoPriv** и **AuthPriv**.
  - **Протокол аутентификации** – доступны следующие протоколы: MD5, SHA, SHA224, SHA256, SHA384, SHA512. Это поле становится доступно при выборе уровней безопасности **AuthNoPriv** и **AuthPriv**.
  - **Протокол шифрования** – протокол, используемый для шифрования сообщений. Доступны следующие протоколы: DES, AES. Это поле становится доступно при выборе уровня безопасности **AuthPriv**.
  - **Пароль обеспечения безопасности** – пароль шифрования, который был указан при создании пользователя. Это поле становится доступно при выборе уровня безопасности **AuthPriv**.
- **cetrificate** – тип секрета используется для хранения файлов сертификатов. Файлы загружаются в ресурс с помощью кнопки **Загрузить файл сертификата**. Поддерживаются открытые ключи сертификата X.509 в Base64.

kaspersky

Сервисы KUMA

Сервисы – это основные компоненты KUMA (см. раздел "Архитектура программы" на стр. 19), с помощью которых осуществляется работа с событиями: получение, обработка, анализ и хранение. Каждый сервис состоит из двух частей, работающих вместе:

- Одна часть сервиса создается внутри веб-интерфейса KUMA на основе набора ресурсов для сервисов (см. раздел "Наборы ресурсов для сервисов" на стр. 235).
- Вторая часть сервиса устанавливается в сетевой инфраструктуре, где развернута система KUMA (см. раздел "Установка KUMA в производственной среде" на стр. 39), в качестве одного из ее компонентов. Серверная часть сервиса может состоять из нескольких экземпляров: например, сервисы одного и того же агента или хранилища могут быть установлены сразу на нескольких машинах.

  В серверной части сервисы KUMA располагаются в директории `/opt/kaspersky/kuma`.

Между собой части сервисов соединены с помощью идентификатора сервисов (см. раздел "Получение идентификатора сервиса" на стр. 231).

Типы сервисов:

- Коллекторы (см. раздел "Коллектор" на стр. 20) – используются для получения события и конвертации их в формат KUMA.
- Корреляторы (см. раздел "Коррелятор" на стр. 23) – используются для анализа событий и поиска заданных закономерностей.
- Хранилища (см. раздел "Хранилище" на стр. 24) – используются для хранения событий.
- Агенты (см. раздел "Об агентах" на стр. 29) – используются для получения событий на удаленных устройствах и пересылки их в коллекторы KUMA.

В веб-интерфейсе KUMA сервисы отображаются в разделе **Ресурсы** → **Активные сервисы** в виде таблицы. Таблицу сервисов можно обновить с помощью кнопки **Обновить** и сортировать по столбцам, нажимая на активные заголовки.

Столбцы таблицы:

- **Тип** – вид сервиса: **агент**, **коллектор**, **коррелятор**, **хранилище**.
- **Название** – название сервиса. При нажатии на название сервиса открываются его настройки.
- **Версия** – версия сервиса.
- **Тенант** – название тенанта, которому принадлежит сервис.
- **Полное доменное имя** – доменное имя сервера, на котором установлен сервис.
- **IP-адрес** – IP-адрес сервера, на котором установлен сервис.
- **Порт API** – номер порта для внутренних коммуникаций.
- **Статус** – статус сервиса:
  - Зеленый – сервис работает.
  - Красный – сервис не работает.

  - Желтый – этот статус применяется только к сервисам хранилища и означает, что нет соединения с узлами ClickHouse. Причина указывается в журнале сервиса (см. раздел "Журналы KUMA" на стр. 408), если было включено логирование.
- **Время работы** – как долго сервис работает.

С помощью кнопки **Добавить сервис** можно создавать новые сервисы (см. раздел "Создание сервисов" на стр. 46) на основе существующих наборов ресурсов для сервисов. В этом окне также можно перезапустить сервис или удалить его сертификат (см. раздел "Перезапуск сервиса" на стр. 231), скопировать идентификатор сервиса (см. раздел "Получение идентификатора сервиса" на стр. 231) или удалить сервис (см. раздел "Удаление сервиса" на стр. 232). Кроме того, в этом разделе можно просмотреть разделы хранилищ (см. раздел "Окно Разделы" на стр. 232) и активные листы коррелеторов (см. раздел "Окно активных листов коррелятора" на стр. 233).

Сервисы можно изменить, нажав на них в разделе **Ресурсы → Активные сервисы**. При этом открывается окно с набором ресурсов, на основе которых они были созданы. Сервис меняется путем изменения параметров наборе ресурсов. Изменения сохраняются с помощью кнопки **Сохранить** и вступают в силу после перезапуска сервиса.

Если изменить или удалить преобразования в ресурсе нормализатора (см. раздел "Нормализаторы" на стр. 158) в существующем наборе ресурсов (см. раздел "Наборы ресурсов для сервисов" на стр. 235) для коллектора (см. раздел "Создание коллектора" на стр. 235), правки в нормализаторе не сохранятся, а сам ресурс может быть поврежден. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, правки необходимо вносить непосредственно в ресурс в разделе веб-интерфейса **Ресурсы → Нормализаторы**.

В этом разделе

Инструменты сервисов 230
Наборы ресурсов для сервисов 235
Создание коллектора 235
Создание коррелятора 252
Создание агента 263
Создание хранилища 270

kaspersky

Инструменты сервисов

В этом разделе описываются инструменты по работе с сервисами, доступные в раздел веб-интерфейса KUMA **Ресурсы** → **Активные сервисы**.

В этом разделе

Получение идентификатора сервиса 231

Перезапуск сервиса 231

Удаление сервиса 232

Окно Разделы 232

Окно активных листов коррелятора 233

Поиск связанных событий 234

Получение идентификатора сервиса

Идентификатор сервиса используется для связи частей сервиса (см. раздел "Сервисы KUMA" на стр. 229) – расположенной внутри KUMA и установленной в сетевой инфраструктуре – в единый комплекс. Идентификатор присваивается сервису при его создании в KUMA, а затем используется при установке сервиса на сервер.

► *Чтобы получить идентификатор сервиса:*

1. Войдите в веб-интерфейс KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с сервисом, идентификатор которого вы хотите получить, и нажмите **Копировать идентификатор**.

Идентификатор сервиса помещен в буфер. Его можно использовать, например, для установки сервиса на сервере (см. раздел "Создание сервисов" на стр. 46).

Перезапуск сервиса

► *Чтобы перезапустить сервис:*

1. Войдите в веб-интерфейс KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с сервисом и выберите нужную опцию:
   - **Обновить параметры** – обновить конфигурацию работающего сервиса, не останавливая его. Например, так можно изменить настройки сопоставления полей или параметры точки назначения.
   - **Перезапустить** – остановить сервис и запустить его снова. Этот вариант используется для изменения таких параметров, как порт или тип коннектора.

     Агент KUMA для Windows может быть перезагружен, как описано выше, только если он запущен на удаленном компьютере. Если сервис на удаленном компьютере неактивен, при попытке перезагрузки из KUMA вы получите сообщение об ошибке. В этом случае следует перезапустить

сервис Агент KUMA для Windows на удаленном компьютере с Windows. Чтобы узнать, как перезапустить сервисы Windows, обратитесь к документации, относящейся к версии операционной системы вашего удаленного компьютера с Windows.

- **Сбросить сертификат** – удалить сертификаты, используемые сервисом для внутренней связи. Например, этот вариант подойдет при обновлении сертификата Ядра.

  При работе с агентами KUMA этот способ сброса сертификата доступен только для работающих агентов (с зеленым статусом). Для агентов с красным статусом сертификат необходимо менять вручную.

Сервис будет перезапущен.

Удаление сервиса

Перед удалением сервиса получите его идентификатор (см. раздел "Получение идентификатора сервиса" на стр. 231). Он потребуется, чтобы удалить сервис с сервера.

► *Чтобы удалить сервис:*

1. Войдите в веб-интерфейс KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным сервисом и нажмите **Удалить**.

   Откроется окно подтверждения.
3. Нажмите **ОК**.

Сервис удален из KUMA.

► *Чтобы удалить сервис с сервера:*

Удалите файл /usr/lib/systemd/system/kuma-<Тип сервиса: collector, correlator или storage >-<идентификатор сервиса>.service с сервера, на котором был установлен сервис.

Окно Разделы

Создав и установив сервис (см. раздел "Создание хранилища" на стр. 270) Хранилища (см. раздел "Хранилище" на стр. 24), вы можете просмотреть его разделы в таблице **Разделы**.

► *Чтобы открыть таблицу **Разделы**:*

1. Войдите в веб-интерфейс KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным хранилищем и нажмите **Смотреть разделы**.

Откроется таблица **Разделы**.

В таблице есть следующие столбцы:

- **Тенант** – название тенанта, которому принадлежат хранимые данные.
- **Дата** – дата создания раздела.

- **Пространство** – название раздела.
- **Размер** – размер раздела.
- **События** – количество хранимых событий.
- **Истекает** – дата, когда истекает срок действия пространства.

Вы можете удалять пространства.

► *Чтобы удалить пространство:*

1. Откройте таблицу **Разделы** (см. выше).
2. Откройте раскрывающийся список ••• слева от необходимого пространства.
3. Выберите **Удалить**.

   Откроется окно подтверждения.
4. Нажмите **ОК**.

Пространство удалено.

Окно активных листов коррелятора

В таблице **Активные листы коррелятора** можно просмотреть список активных листов, которые использует определенный коррелятор.

► *Чтобы открыть таблицу **Активные листы коррелятора**:*

1. Войдите в веб-интерфейс KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным коррелятором и нажмите **Смотреть активные листы**.

Откроется таблица **Активные листы коррелятора**.

В таблице есть следующие столбцы:

- **Название** – имя активного листа.
- **Записи** – количество записей в активном листе.
- **Размер на диске** – размер активного листа.
- **Каталог** – путь к активному листу на сервере коррелятора KUMA.

Активные листы можно просматривать, импортировать, экспортировать или очищать.

► *Чтобы просмотреть активный лист:*

Откройте таблицу **Активные листы коррелятора** (см. выше) и нажмите название требуемого активного листа.

Откроется таблица с содержимым активного листа. Если вы хотите просмотреть содержимое записи, нажмите на значение ее ключа (столбец **Ключ**). Если запись следует удалить, нажмите на значок . С помощью поля **Поиск** можно искать нужные записи.

► *Чтобы экспортировать активный лист:*

1. Откройте таблицу **Активные листы коррелятора** (см. выше).
2. Открой раскрывающийся список ••• слева от необходимого активного листа.
3. Нажмите **Экспортировать**.

Активный лист будет загружен в формате JSON используя настройки вашего браузера. Название загруженного файла соответствует названию активного листа.

► *Чтобы импортировать данные в активный лист:*

1. Откройте таблицу **Активные листы коррелятора** (см. выше).
2. Открой раскрывающийся список ••• слева от необходимого активного листа.
3. Нажмите **Импортировать**.

   Откроется окно импорта активного листа.
4. В поле **Файл** выберите файл, который требуется импортировать.
5. В раскрывающемся списке **Формат** выберите формат файла:
   - **csv**
   - **tsv**
   - **internal**
6. В поле **Ключевое поле** введите название столбца с ключами записей активного листа.
7. Нажмите **Импортировать**.

Данные из файла импортированы в активный лист.

Поиск связанных событий

Вы можете искать события, обработанные определенным коррелятором или коллектором.

► *Чтобы найти события, относящиеся к корреляторy или коллектору:*

1. Войдите в веб-интерфейс KUMA и откройте раздел **Ресурсы** → **Активные сервисы**.
2. Установите флажок рядом с нужным коррелятором или коллектором и нажмите **Перейти к событиям**.

Откроется новая закладка браузера с открытым разделом KUMA **События**, в котором будет отображаться таблица с событиями, отобранными по поисковому выражению `ServiceID = <идентификатор выбранного сервиса` (см. раздел "`Получение идентификатора сервиса`" на стр. 231)>.

kaspersky

Наборы ресурсов для сервисов

Наборы ресурсов для сервисов – это тип ресурсов, компонент KUMA, представляющий собой комплект настроек, на основе которых создаются и функционируют сервисы (см. раздел "Сервисы KUMA" на стр. 229) KUMA. Наборы ресурсов для сервисов собираются из ресурсов (см. раздел "Ресурсы KUMA" на стр. 128).

Ресурсы, объединяемые в набор ресурсов, должны принадлежать к тому же тенанту, что и создаваемый набор ресурсов. Исключением является общий тенант (см. раздел "О тенантах" на стр. 25): принадлежащие ему ресурсы можно использовать в наборах ресурсов других тенантов.

Наборы ресурсов для сервисов отображаются в разделе веб-интерфейса KUMA **Ресурсы** → **<Тип набора ресурсов для сервиса>**. Доступные типы:

- Коллекторы
- Корреляторы
- Хранилища
- Агенты

При выборе нужного типа открывается таблица с имеющимися наборами ресурсов для сервисов этого типа. Таблица содержит следующие столбцы:

- **Название** – имя набора ресурсов. Может использоваться для поиска и сортировки.
- **Последнее обновление** – дата и время последнего обновления набора ресурсов. Может использоваться для сортировки.
- **Создал** – имя пользователя, создавшего набор ресурсов.
- **Описание** – описание набора ресурсов.

Создание коллектора

Коллектор (на стр. 20) состоит из двух частей (см. раздел "Сервисы KUMA" на стр. 229): одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для получения событий.

Действия в веб-интерфейсе KUMA

Создание коллектора в веб-интерфейсе KUMA производится с помощью мастера установки, в процессе выполнения которого необходимые ресурсы (см. раздел "Ресурсы KUMA" на стр. 128) объединяются в набор ресурсов для коллектора (см. раздел "Наборы ресурсов для сервисов" на стр. 235), а по завершении мастера на основе этого набора ресурсов автоматически создается и сам сервис.

► *Чтобы создать коллектор в веб-интерфейсе KUMA,*

Запустите мастер установки коллектора:

- В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Подключить источник**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** нажмите **Добавить коллектор**.

В результате выполнения шагов мастера в веб-интерфейсе KUMA создается сервис коллектора.

В набор ресурсов для коллектора объединяются следующие ресурсы:

- коннектор (см. раздел "Коннекторы" на стр. 169);
- нормализатор (см. раздел "Нормализаторы" на стр. 158) (как минимум один);
- фильтры (на стр. 212) (при необходимости);
- правила агрегации (на стр. 194) (при необходимости);
- правила обогащения (на стр. 194) (при необходимости);
- точки назначения (на стр. 199) (как правило, две: задается отправка событий в коррелятор и хранилище).

Эти ресурсы можно подготовить заранее, а можно создать в процессе выполнения мастера установки.

Действия на сервере коллектора KUMA

Установка коллектора на сервер (см. раздел "Установка коллектора в сетевой инфраструктуре KUMA" на стр. 250), предназначенный для получения событий, на сервере требуется в запустить команду, которая отображается на последнем шаге мастера установки. При установке необходимо указать идентификатор (см. раздел "Получение идентификатора сервиса" на стр. 231), автоматически присвоенный сервису в веб-интерфейсе KUMA, а также используемый для связи порт.

Проверка установки

После создания коллектора рекомендуется убедиться (см. раздел "Проверка правильности установки коллектора" на стр. 251) в правильности его работы.

В этом разделе

Запуск мастера установки коллектора 236

Установка коллектора в сетевой инфраструктуре KUMA 250

Проверка правильности установки коллектора 251

Запуск мастера установки коллектора

Коллектор (на стр. 20) состоит из двух частей (см. раздел "Сервисы KUMA" на стр. 229): одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенной для получения событий. В мастере установки создается первая часть коллектора.

► *Чтобы запустить мастер установки коллектора:*

- В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Подключить источник**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** нажмите **Добавить коллектор**.

Следуйте указаниям мастера.

Шаги мастера, кроме первого и последнего, можно выполнять в произвольном порядке. Переключаться между шагами можно с помощью кнопок **Вперед** и **Назад**, а также нажимая на названия шагов в левой части окна.

По завершении мастера в веб-интерфейсе KUMA в разделе **Ресурсы** → **Коллекторы** создается набор ресурсов для коллектора (см. раздел "Наборы ресурсов для сервисов" на стр. 235), а в разделе **Ресурсы** → **Активные сервисы** добавляется сервис коллектора (см. раздел "Сервисы KUMA" на стр. 229).

В этом разделе

Шаг 1. Подключение источников событий 237
Шаг 2. Транспорт 238
Шаг 3. Парсинг событий 239
Шаг 4. Фильтрация событий 243
Шаг 5. Агрегация событий 244
Шаг 6. Обогащение событий 245
Шаг 7. Маршрутизация 246
Шаг 8. Проверка параметров 249

Шаг 1. Подключение источников событий

Это обязательный шаг мастера установки. На этом шаге указывается основные параметры коллектора: название и тенант, которому он будет принадлежать.

► *Чтобы задать основные параметры коллектора:*

- В поле **Название** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.

  При создании некоторых типов коллекторов вместе с ними автоматически создаются агенты, имеющие название "agent: <Название коллектора>, auto created". Если такой агент уже создавался ранее и не был удален, то коллектор с названием <Название коллектора> невозможно будет создать. В такой ситуации необходимо или указать другое название коллектора, или удалить ранее созданный агент.

- В раскрывающемся списке **Тенант** выберите тенант (см. раздел "О тенантах" на стр. 25), которому будет принадлежать коллектор. От выбора тенанта зависит, какие ресурсы будут доступны при его создании.

  Если вы с какого-либо последующего шага мастера установки вернетесь в это окно и выберите другой тенант, вам потребуется вручную изменить все ресурсы, которые вы успели добавить в сервис. В сервис можно добавлять только ресурсы из выбранного и общего тенантов.

- В поле **Рабочие процессы** при необходимости укажите количество процессов, которые может одновременно запускать сервис. По умолчанию количество рабочих процессов соответствует количеству vCPU сервера, на котором установлен сервис.

- При необходимости с помощью раскрывающегося списка **Отладка** включите логирование операций сервиса (см. раздел "Журналы KUMA" на стр. 408).
- В поле **Описание** можно добавить описание сервиса: до 256 символов Юникода.

Основные параметры коллектора заданы. Перейдите к следующему шагу мастера установки.

Шаг 2. Транспорт

Это обязательный шаг мастера установки. В закладке мастера установки **Транспорт** следует выбрать или создать ресурс коннектора (см. раздел "Коннекторы" на стр. 169), в параметрах которого будет определено, откуда сервис коллектора должен получать события (см. раздел "О событиях" на стр. 25).

► *Чтобы добавить в набор ресурсов существующий коннектор,*

Выберите в раскрывающемся списке **Коннектор** название нужного коннектора.

В закладке мастера установки **Транспорт** отобразятся параметры выбранного коннектора. Выбранный ресурс можно открыть для редактирования в новой вкладке браузера с помощью кнопки  .

► *Чтобы создать новый коннектор:*

1. Выберите в раскрывающемся списке **Коннектор** пункт **Создать**.
2. В раскрывающемся списке **Тип** выберите тип коннектора и укажите его параметры в закладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа коннектора:
   - internal (см. раздел "Тип internal" на стр. 171)
   - tcp (см. раздел "Тип tcp" на стр. 172)
   - udp (см. раздел "Тип udp" на стр. 173)
   - netflow (см. раздел "Тип netflow" на стр. 173)
   - sflow (см. раздел "Тип sflow" на стр. 174)
   - nats (см. раздел "Тип nats" на стр. 174)
   - kafka (см. раздел "Тип kafka" на стр. 176)
   - http (см. раздел "Тип http" на стр. 178)
   - sql (см. раздел "Тип sql" на стр. 179)
   - file (см. раздел "Тип file" на стр. 185)
   - ftp (см. раздел "Тип ftp" на стр. 188)
   - nfs (см. раздел "Тип nfs" на стр. 189)
   - wmi (см. раздел "Тип wmi" на стр. 190)
   - wec (см. раздел "Тип wec" на стр. 191)
   - snmp (см. раздел "Тип snmp" на стр. 192)

При использовании типа коннектора **tcp** или **upd** на этапе нормализации (см. раздел "Шаг 3. Парсинг событий" на стр. 239) в поле событий DeviceAddress, если она пустая, будут записаны IP-адреса устройств, с которых были получены события.

При использовании типа коннектора **wmi** или **wec** будут автоматически (см. раздел "Автоматически созданные агенты" на стр. 269) созданы агенты (см. раздел "Об агентах" на стр. 29) для приема событий Windows.

Рекомендуется использовать кодировку по умолчанию (то есть UTF-8) и применять другие параметры только при получении в полях событий битых символов.

Ресурс коннектора добавлен в набор ресурсов коллектора. Созданный ресурс доступен только в этом наборе ресурсов и не отображается в разделе веб-интерфейса **Ресурсы** → **Коннекторы**.

Перейдите к следующему шагу мастера установки.

Шаг 3. Парсинг событий

Это обязательный шаг мастера установки. В закладке мастера установки **Парсинг событий** следует выбрать или создать ресурс нормализатора (см. раздел "Нормализаторы" на стр. 158), в параметрах которого будут определены правила преобразования "сырых" событий в нормализованные (см. раздел "О событиях" на стр. 25). Можно добавить несколько нормализаторов и реализовать сложную логику обработки событий.

При создании нового нормализатора в мастере установки по умолчанию он будет сохранен в наборе ресурсов для коллектора и не сможет быть использован в других коллекторах. С помощью флажка **Сохранить нормализатор** вы можете создать отдельный ресурс (см. раздел "Ресурсы KUMA" на стр. 128).

Если изменить или удалить преобразования в ресурсе нормализатора (см. раздел "Нормализаторы" на стр. 158) в существующем наборе ресурсов (см. раздел "Наборы ресурсов для сервисов" на стр. 235) для коллектора (см. раздел "Создание коллектора" на стр. 235), правки в нормализаторе не сохранятся, а сам ресурс может быть поврежден. При необходимости изменить преобразования в нормализаторе, который уже является частью сервиса, правки необходимо вносить непосредственно в ресурс в разделе веб-интерфейса **Ресурсы** → **Нормализаторы**.

Добавление нормализатора

► *Чтобы добавить в набор ресурсов существующий нормализатор:*

1. Нажмите на кнопку **Добавить парсинг событий**.

   Откроется окно **Парсинг событий** с параметрами нормализатора и активной закладкой **Схема нормализации**.

2. В раскрывающемся списке **Нормализатор** выберите нужный нормализатор.

   В окне **Парсинг событий** отобразятся параметры выбранного нормализатора. Выбранный ресурс можно открыть для редактирования в новой вкладке браузера с помощью кнопки  .

3. Нажмите **ОК**.

В закладке мастера установки **Парсинг событий** отображается нормализатор в виде темного кружка. Можно нажать на кружок, чтобы открыть параметры нормализатора для редактирования. При

наведении на кружок отображается значок плюса: при нажатии на него можно добавить дополнительные нормализаторы (см. ниже).

► *Чтобы создать новый нормализатор:*

1. Выберите в раскрывающемся списке **Нормализатор** пункт **Создать**.

   Откроется окно **Парсинг событий** с параметрами нормализатора и активной закладкой **Схема нормализации**.

2. Если хотите сохранить нормализатор в качестве отдельного ресурса, установите флажок **Сохранить нормализатор**. По умолчанию флажок снят.

3. Введите в поле **Название** уникальное имя для нормализатора. Название должно содержать от 1 до 128 символов Юникода.

4. В раскрывающемся списке **Метод парсинга** выберите тип получаемых событий. В зависимости от выбора можно будет воспользоваться преднастроенными правилами сопоставления полей событий или же задать свои собственные правила. При выборе некоторых методов парсинга могут стать доступны дополнительные параметры, требуемые для заполнения.

   Доступные методы парсинга:

   - json (см. раздел "Нормализатор, тип json" на стр. 162)
   - cef (см. раздел "Нормализатор, тип cef" на стр. 161)
   - regexp (см. раздел "Нормализатор, тип regexp" на стр. 163)
   - syslog (см. раздел "Нормализатор, тип syslog" на стр. 163)
   - csv (см. раздел "Нормализатор, тип csv" на стр. 161)
   - kv (см. раздел "Нормализатор, тип kv" на стр. 162)
   - xml (см. раздел "Нормализатор, тип xml" на стр. 164)
   - netflow5 (см. раздел "Нормализатор, тип netflow5" на стр. 162)
   - netflow9 (см. раздел "Нормализатор, тип netflow9" на стр. 162)
   - ipfix (см. раздел "Нормализатор, тип ipfix" на стр. 162)
   - sql (см. раздел "Нормализатор, тип sql" на стр. 163) – этот метод становится доступным, только при использовании коннектора типа sql (см. раздел "Шаг 2. Транспорт" на стр. 238)

5. В раскрывающемся списке **Хранить исходное событие** укажите, надо ли сохранять исходное "сырое" событие во вновь созданном нормализованном событии. Доступные значения:

   - **Не хранить** – не сохранять исходное событие. Это значение используется по умолчанию.
   - **При возникновении ошибок** – сохранять исходное событие в поле `Raw` нормализованного события, если в процессе парсинга возникли ошибки. Это значение удобно использовать при отладке сервиса: в этом случае появление у событий непустого поля `Raw` будет являться признаком неполадок.
   - **Всегда** – сохранять сырое событие в поле `Raw` нормализованного события.

6. В раскрывающемся списке **Сохранить дополнительные поля** выберите, требуется ли сохранять поля исходного события в нормализованном событии, если для них не были настроены правила сопоставления (см. ниже). Данные сохраняются в поле события Extra. По умолчанию поля не сохраняются.

7. Скопируйте в поле **Примеры событий** пример данных, которые вы хотите обработать. Это необязательный, но рекомендуемый шаг.

   Пример событий можно также загрузить из файла формата tsv, csv или txt с помощью кнопки **Загрузить из файла**.

8. В таблице **Сопоставление** настройте сопоставление полей исходного события с полями события в формате KUMA (см. раздел "Модель данных нормализованного события" на стр. 471):

   a. В столбце **Исходные данные** укажите название поля исходного события, которое вы хотите преобразовать в поле события KUMA.

      Если рядом с названиями полей в столбце **Исходные данные** нажать на кнопку  , откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

      Доступные преобразования (см. раздел "Преобразования" на стр. 168)

   b. В столбце **Поле KUMA** в раскрывающемся списке выберите требуемое поле события KUMA. Поля можно искать, вводя в поле их названия.

   c. Если название поля события KUMA, выбранного на предыдущем шаге, начинается с DeviceCustom*, при необходимости в поле **Подпись** можно добавить уникальную пользовательскую метку.

   Новые строки таблицы можно добавлять с помощью кнопки **Добавить строку**. Строки можно удалять по отдельности с помощью кнопки  или все сразу с помощью кнопки **Очистить все**.

   Если вы загрузили данные в поле **Примеры событий**, в таблице отобразится столбец **Примеры** с примерами значений, переносимых из поля исходного события в поле события KUMA.

9. Нажмите **ОК**.

В закладке мастера установки **Парсинг событий** отображается нормализатор в виде темного кружка. Можно нажать на кружок, чтобы открыть параметры нормализатора для редактирования. При наведении на кружок отображается значок плюса: при нажатии на него можно добавить дополнительные нормализаторы (см. ниже).

Обогащение нормализованного события дополнительными данными

В только что созданные нормализованные события можно добавлять дополнительные данные, создавая в нормализаторе правила обогащения, аналогичные правилам в ресурсах правил обогащения (см. раздел "Правила обогащения" на стр. 194). Эти правила хранятся в ресурсе нормализатора, в котором они были созданы. Правил обогащения может быть несколько.

► *Чтобы добавить правила обогащения в нормализатор:*

1. Выберите нормализатор и в окне **Парсинг событий** перейдите на закладку **Обогащение**.
2. Нажмите на кнопку **Добавить обогащение**.

   Появится блок параметров правила обогащения. Блок параметров можно закрыть с помощью кнопки  .

3. В раскрывающемся списке **Тип источника** выберите тип обогащения. В зависимости от выбранного типа отобразятся дополнительные параметры, которые также потребуется заполнить.

   Доступные типы источников обогащения:

   - константа (см. раздел "Обогащение, тип константа" на стр. 195)
   - словарь (см. раздел "Обогащение, тип словарь" на стр. 196)

- событие (см. раздел "Обогащение, тип событие (для нормализатора)" на стр. 197)
- шаблон (см. раздел "Обогащение, тип шаблон" на стр. 197)

4. Нажмите **ОК**.

В нормализатор добавлены правила обогащения и окно **Парсинг событий** закрыто.

Создание структуры нормализаторов

Внутри нормализатора можно создать несколько дополнительных нормализаторов. Это позволяет настроить сложную логику обработки событий.

Последовательность создания нормализаторов имеет значение: события обрабатываются последовательно и их путь отображается в виде стрелочек.

► *Чтобы создать дополнительный нормализатор:*

- Создайте начальный нормализатор (см. выше).

  Созданный нормализатор отобразится в окне в виде темного кружка.

- Наведите указатель мыши на начальный нормализатор и нажмите на появившуюся кнопку со значком плюса.
- В открывшемся окне **Добавление дополнительного нормализатора** укажите условия, при которых данные будут попадать в дополнительный нормализатор:
  - Если вы хотите отправлять в дополнительный нормализатор только события с определенными полями, перечислите их в поле **Поля, которые следует передать в нормализатор**.
  - Если вы хотите отправлять в дополнительный нормализатор только события, в которых определенным полям присвоены определенные значения, задайте название поля события в поле **Нормализовать, если поле события имеет определенное значение**, а значение, которое должно ему соответствовать, – в поле **Значение условия**.

  Обрабатываемые этими условиями данные можно предварительно преобразовать, если нажать на кнопку : откроется окно **Преобразование**, в котором с помощью кнопки **Добавить преобразование** можно создать правила изменения исходных данных перед тем, как они будут записаны в поля событий KUMA.

  Доступные преобразования (см. раздел "Преобразования" на стр. 168)

- Нажмите **ОК**.

  Откроется окно **Парсинг событий**, в котором можно настроить правила обработки событий, как в начальном нормализаторе (см. выше). Параметр **Хранить исходное событие** недоступен. В поле **Примеры событий** отображаются значения, указанные при создании начального нормализатора.

- Укажите параметры дополнительного нормализатора по аналогии с параметрами начального нормализатора
- Нажмите **ОК**.

Дополнительный нормализатор отображается в виде темного блока, на котором указаны условия, при котором этот нормализатор будет задействован. Условия можно изменить, наведя указатель мыши на дополнительный нормализатор и нажав кнопу с изображением карандаша. Если навести указатель мыши на дополнительный нормализатор, отобразится кнопка со значком плюса, с помощью которой можно создать новый дополнительный нормализатор. С помощью кнопки со значком корзины нормализатор можно удалить.

Перейдите к следующему шагу мастера установки.

Шаг 4. Фильтрация событий

Это необязательный шаг мастера установки. В закладке мастера установки **Фильтрация событий** можно выбрать или создать ресурс фильтра (см. раздел "Фильтры" на стр. 212), в параметрах которого будут определены условия для отсева ненужных событий. В коллектор можно добавить более одного фильтра. Фильтры можно менять местами, перетягивая их мышью за значок , и удалять. Фильтры объединены оператором И.

► *Чтобы добавить в набор ресурсов коллектора существующий фильтр,*

Нажмите на кнопку **Добавить фильтр** и в раскрывающемся меню **Фильтр** выберите требуемый фильтр.

► *Чтобы добавить в набор ресурсов коллектора новый фильтр:*

1. Нажмите на кнопку **Добавить фильтр** и в раскрывающемся меню **Фильтр** выберите пункт **Создать**.
2. Если хотите сохранить фильтр в качестве отдельного ресурса, установите флажок **Сохранить фильтр**. Это может оказаться полезным, если вы решите использовать один и тот же фильтр в разных сервисах. По умолчанию флажок снят.
3. Если вы установили флажок **Сохранить фильтр**, в поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов Юникода.
4. В разделе **Условия** задайте условия, которым должны соответствовать отсеиваемые события:
   - С помощью кнопки **Добавить условие** добавляются условия фильтра, можно выбрать два значения (левый и правый операнды) и назначить операцию, которую вы хотите выполнить с выбранными значениями. Результат операции – Истина (True) или Ложь (False).
     - В раскрывающемся списке **оператор** необходимо выбрать функцию, которую должен выполнять фильтр.

       В этом же раскрывающемся списке можно установить флажок **без учета регистра**, если требуется, чтобы оператор игнорировал регистр значений. Флажок игнорируется, если выбраны операторы **InSubnet**, **InActiveList**, **InCategory**, **InActiveDirectoryGroup**. По умолчанию флажок снят.

       Операторы фильтров (см. раздел "Операторы фильтров" на стр. 215)
     - В раскрывающихся списках **Левый операнд** и **Правый операнд** необходимо выбрать, откуда поступят данные, с которыми произведет действие фильтр. В результате выбора появляются дополнительные параметры (см. раздел "Фильтры" на стр. 212), с помощью которых необходимо точно определить значение, которое будет передано в фильтр. Например, при выборе варианта **активный лист** потребуется указать название активного листа, ключ записи и поле ключа записи.
     - С помощью раскрывающегося списка **Если** можно выбрать, требуется ли создать отрицательное условие фильтра.

     Условие можно удалить с помощью кнопки .
   - С помощью кнопки **Добавить группу** добавляются группы условий. Оператор **И** можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

Группу условий можно удалить с помощью кнопки .

- С помощью кнопки **Добавить фильтр** в условия добавляются существующие ресурсы фильтров, которые выбираются в раскрывающемся списке **Выберите фильтр**. В ресурс вложенного фильтра можно перейти с помощью кнопки .

  Вложенный фильтр можно удалить с помощью кнопки .

Фильтр добавлен.

Перейдите к следующему шагу мастера установки.

Шаг 5. Агрегация событий

Это необязательный шаг мастера установки. В закладке мастера установки **Агрегация событий** можно выбрать или создать ресурс правила агрегации (на стр. 194), в параметрах которого будут определены условия для объединения однотипных событий. В коллектор можно добавить более одного правила агрегации.

► *Чтобы добавить в набор ресурсов коллектора существующее правило агрегации,*

Нажмите на кнопку **Добавить правило агрегации** и в раскрывающемся меню **Правило агрегации** выберите требуемый ресурс.

► *Чтобы добавить в набор ресурсов коллектора новое правило агрегации:*

1. Нажмите на кнопку **Добавить правило агрегации** и в раскрывающемся меню **Правило агрегации** выберите пункт **Создать**.
2. В поле **Название** введите название для создаваемого ресурса фильтра. Название должно содержать от 1 до 128 символов Юникода.
3. В поле **Предел событий** укажите количество событий, которое должно быть получено для того, чтобы сработало правило агрегации и события были объединены. Значение по умолчанию: 100.
4. В поле **Время ожидания событий** укажите, в течение которого получаются события для объединения. По истечении этого срока правило агрегирования срабатывает и создается новое событие. Значение по умолчанию: 60.
5. В разделе **Группирующие поля** с помощью кнопки **Добавить поле** выберите поля, по которым будут определяться однотипные события. Выбранные события можно удалять с помощью кнопок со значком крестика.
6. В разделе **Уникальные поля** с помощью кнопки **Добавить поле** можно выбрать поля, наличие которых выведет событие из процесса агрегации даже при наличии полей, указанных в разделе **Группирующие поля**. Выбранные события можно удалять с помощью кнопок со значком крестика.
7. В разделе **Поля суммы** с помощью кнопки **Добавить поле** можно выбрать поля, значения которых будут просуммированы в процессе агрегации. Выбранные события можно удалять с помощью кнопок со значком крестика.
8. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

   Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Правило агрегации добавлено. Его можно удалить с помощью кнопки .

Перейдите к следующему шагу мастера установки.

Шаг 6. Обогащение событий

Это необязательный шаг мастера установки. В закладке мастера установки **Обогащение событий** можно указать, какими данными и из каких источников следует дополнить обрабатываемые коллектором события. События можно обогащать данными, полученными с помощью LDAP (см. раздел "Подключение по протоколу LDAP" на стр. 102), или же посредством правил обогащения (см. раздел "Правила обогащения" на стр. 194).

Обогащение с помощью LDAP

► *Чтобы включить обогащение с помощью LDAP:*

1. Нажмите **Добавить сопоставление с учетными записями LDAP**.

   Откроется блок параметров обогащения с помощью LDAP.

2. В блоке параметров **Сопоставление с учетными записями LDAP** с помощью кнопки **Добавить домен** укажите домен учетных записей. Доменов можно указать несколько.

3. В таблице **Обогащение полей KUMA** задайте правила сопоставления запросов KUMA с ответами LDAP:

   - В столбце **Поле KUMA** укажите поле события KUMA (см. раздел "Модель данных нормализованного события" на стр. 471), данные из которого следует отправить в LDAP.
   - В столбце **LDAP-атрибут** укажите тип отправляемых в LDAP данных.
   - В столбце **Поле для записи данных** укажите, в какое поле события KUMA следует поместить данные, полученные из LDAP.

   С помощью кнопки **Добавить строку** в таблицу можно добавить строку, а с помощью кнопки ✕ – удалить. С помощью кнопки **Применить сопоставление по умолчанию** можно заполнить таблицу сопоставления стандартными значениями.

В блок ресурсов для коллектора добавлены правила обогащения события данными, полученными из LDAP (см. раздел "Подключение по протоколу LDAP" на стр. 102).

При добавлении в существующий коллектор обогащения с помощью LDAP или изменении параметров обогащения требуется остановить и запустить сервис снова (см. раздел "Перезапуск сервиса" на стр. 231).

Обогащение с помощью правил обогащения

Правил обогащения может быть несколько. Их можно добавить с помощью кнопки **Добавить обогащение** или удалить с помощью кнопки ✕. Можно использовать существующие ресурсы правил обогащения или же создать правила непосредственно в мастере установки.

► *Чтобы добавить в набор ресурсов существующее правило обогащения:*

1. Нажмите **Добавить обогащение**.

   Откроется блок параметров правила реагирования.

2. В раскрывающемся списке **Правило обогащения** выберите нужный ресурс.

Правило обогащения добавлено в набор ресурсов для коллектора.

► *Чтобы создать в наборе ресурсов новое правило обогащения:*

1. Нажмите **Добавить обогащение**.

   Откроется блок параметров правила реагирования.
2. В раскрывающемся списке **Правило обогащения** выберите **Создать**.
3. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к ним параметры:
   - константа (см. раздел "Обогащение, тип константа" на стр. 195)
   - словарь (см. раздел "Обогащение, тип словарь" на стр. 196)
   - событие (см. раздел "Обогащение, тип событие (для ресурса обогащения)" на стр. 196)
   - шаблон (см. раздел "Обогащение, тип шаблон" на стр. 197)
   - dns (см. раздел "Обогащение, тип dns" на стр. 196)
   - cybertrace (см. раздел "Обогащение, тип cybertrace" на стр. 195)
   - часовой пояс (см. раздел "Обогащение, тип часовой пояс" на стр. 197)
   - геоданные (см. раздел "Обогащение, тип геоданные" на стр. 198)
4. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию логирование выключено.
5. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом правила обогащения. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

   Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

В набор ресурсов для коллектора добавлено новое правило обогащения.

Перейдите к следующему шагу мастера установки.

Шаг 7. Маршрутизация

Это необязательный шаг мастера установки. В закладке мастера установки **Маршрутизация** можно выбрать или создать ресурсы точек назначения (см. раздел "Точки назначения" на стр. 199), в параметрах которых будут определено, куда следует перенаправлять обработанные коллектором события. Обычно события от коллектора перенаправляются в две точки: в коррелятор (на стр. 23) для анализа и поиска угроз; в хранилище (на стр. 24) для хранения, а также чтобы обработанные события можно было просматривать позднее. При необходимости события можно отправлять в другие места. Точек назначения может быть несколько.

► *Чтобы добавить в набор ресурсов коллектора существующую точку назначения:*

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:
   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.
   - Выберите **Другое**, если хотите отправлять события в другие места.

К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях программы.

Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. В раскрывающемся списке **Точка назначения** выберите нужную точку назначения.

   Название окна меняется на **Изменить точку назначения**, параметры выбранного ресурса отображаются в окне. Ресурс можно открыть для редактирования в новой вкладке браузера с помощью кнопки .

3. Нажмите **Сохранить**.

Выбранная точка назначения отображается в закладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

► *Чтобы добавить в набор ресурсов коллектора новую точку назначения:*

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:
   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.
   - Выберите **Другое**, если хотите отправлять события в другие места.

   К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях программы.

   Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.

2. Укажите параметры в закладке **Основные параметры**:
   - В раскрывающемся списке **Точка назначения** выберите **Создать**.
   - Введите в поле **Название** уникальное имя для точки назначения. Название должно содержать от 1 до 128 символов Юникода.
   - С помощью переключателя **Выключено**, выберите, будут ли события отправляться в эту точку назначения. По умолчанию отправка событий включена.
   - Выберите **Тип** точки назначения:
     - Выберите **storage**, если хотите настроить отправку обработанных событий в хранилище.
     - Выберите **correlator**, если хотите настроить отправку обработанных событий в коррелятор.
     - Выберите **nats**, **tcp**, **http**, **kafka** или **file**, если хотите настроить отправку событий в другие места.
   - Укажите **URL**, куда следует отправлять события, в формате hostname:<порт API>.

     Для всех типов, кроме **nats**, **file** и **diode** с помощью кнопки **URL** можно указать несколько адресов отправки, если в вашу лицензию KUMA включен модуль High Level Availability.

     Если в качестве типа точки назначения выбраны **storage** или **correlator**, поле **URL** можно заполнить автоматически с помощью раскрывающегося списка **Копировать URL сервиса**, в

котором отображаются активные сервисы (см. раздел "Сервисы KUMA" на стр. 229) выбранного типа.

- Для типов **nats** и **kafka** в поле **Топик** укажите, в какой топик должны записываться данные. Топик должен содержать от 1 до 255 символов Юникода.

3. При необходимости укажите параметры в закладке **Дополнительные параметры**. Доступные параметры зависят от выбранного типа точки назначения (на стр. 199):

   - **Сжатие** – раскрывающийся список, в котором можно включить сжатие Snappy. По умолчанию сжатие **Выключено**.
   - **Прокси-сервер** – раскрывающийся список для выбора ресурса прокси-сервера (см. раздел "Прокси-серверы" на стр. 226).
   - **Размер буфера** – поле, в котором можно указать размер буфера (в байтах) для ресурса точки назначения. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.
   - **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.
   - **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
   - **Идентификатор хранилища** – идентификатор хранилища NATS.
   - **Режим TLS** – раскрывающийся список, в котором можно указать условия использование шифрования TLS:
     - **Выключено** (по умолчанию) – не использовать шифрование TLS.
     - **Включено** – использовать шифрование, но без верификации.
     - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы (см. раздел "Изменение корневого сертификата" на стр. 46) и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

     При использовании TLS невозможно указать IP-адрес в качестве URL.
   - **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:
     - **Любой**
     - **Сначала первый**
     - **По очереди**
   - **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.
   - **Путь** – путь к файлу, если выбран тип точки назначения **file**.
   - **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.
   - **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.

- Вы можете установить проверки работоспособности, используя поля **Путь проверки работоспособности** и **Ожидание проверки работоспособности**. Вы также можете отключить проверку работоспособности, установив флажок **Проверка работоспособности отключена**.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.
- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.
- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

4. Нажмите **Сохранить**.

Созданная точка назначения отображается в закладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Перейдите к следующему шагу мастера установки.

Шаг 8. Проверка параметров

Это обязательный и заключительный шаг мастера установки. На этом шаге в KUMA создается набор ресурсов для сервиса (см. раздел "Наборы ресурсов для сервисов" на стр. 235) и на основе этого набора автоматически создаются сервисы (см. раздел "Сервисы KUMA" на стр. 229):

- Набор ресурсов для коллектора отображается в разделе **Ресурсы → Коллекторы**. Его можно использовать для создания новых сервисов коллектора. При изменении этого набора ресурсов все сервисы, которые работают на его основе, будут использовать новые параметры, если сервисы перезапустить (см. раздел "Перезапуск сервиса" на стр. 231): для этого можно использовать кнопки **Сохранить и перезапустить сервисы** и **Сохранить и обновить параметры сервисов**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы (см. раздел "Операции с ресурсами" на стр. 129).
- Сервисы отображаются в разделе **Ресурсы → Активные сервисы**. Созданные с помощью мастера установки сервисы выполняют функции внутри программы KUMA – для связи с внешними частями сетевой инфраструктуры необходимо установить аналогичные внешние сервисы на предназначенных для них серверах и устройствах. Например, внешний сервис коллектора следует установить на сервере, предназначенном для получения событий; внешние сервисы хранилища – на серверах с развернутой службой ClickHouse; внешние сервисы агентов – на тех устройствах Windows, где требуется получать и откуда необходимо пересылать события Windows.

► *Чтобы завершить мастер установки:*

1. Нажмите **Сохранить и создать сервис**.

   В закладке мастера установки **Проверка параметров** отображается таблица сервисов, созданных на основе набора ресурсов, выбранных в мастере установки. В нижней части окна отображаются примеры команд, с помощью которых необходимо установить внешние аналоги этих сервисов на предназначенные для них серверы и устройства.

   Например:

/opt/kaspersky/kuma/kuma collector --core https://kuma-example:<порт, используемый для связи с Ядром KUMA> --id <идентификатор сервиса> --api.port <порт, используемый для связи с сервисом> --install

Порт для связи с Ядром KUMA, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Также следует убедиться в сетевой связности системы KUMA и при необходимости открыть используемые ее компонентами порты (см. раздел "Настройка сетевого доступа" на стр. 41).

2. Закройте мастер, нажав **Сохранить коллектор**.

Сервис коллектора создан в KUMA. Теперь аналогичный сервис необходимо установить на сервере (см. раздел "Установка коллектора в сетевой инфраструктуре KUMA" на стр. 250), предназначенном для получения событий.

Если в коллекторы был выбран коннектор типа wmi или wec, потребуется также установить (см. раздел "Установка агента KUMA на устройствах Windows" на стр. 267) автоматически (см. раздел "Автоматически созданные агенты" на стр. 269) созданные агенты (см. раздел "Об агентах" на стр. 29) KUMA.

Установка коллектора в сетевой инфраструктуре KUMA

Коллектор (на стр. 20) состоит из двух частей (см. раздел "Сервисы KUMA" на стр. 229): одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры (см. раздел "Установка KUMA в производственной среде" на стр. 39), предназначенной для получения событий. В сетевой инфраструктуре устанавливается вторая часть коллектора.

► *Чтобы установить коллектор:*

1. Войдите на сервер, на котором вы хотите установить сервис.
2. Выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma collector --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA (см. раздел "Получение идентификатора сервиса" на стр. 231)> --api.port <порт, используемый для связи с устанавливаемым компонентом> --install
```

Пример: `sudo /opt/kaspersky/kuma/kuma collector --core https://kuma.example.com:7210 --id XXXX --api.port YYYY --install`

Команду, с помощью которой можно установить коллектор на сервере, можно скопировать на последнем шаге мастера установщика. В ней автоматически указывается адрес и порт сервера Ядра KUMA, идентификатор устанавливаемого коллектора, а также порт, который этот коллектор использует для связи. Перед установкой необходимо убедиться в сетевой связности компонентов KUMA.

При развертывании нескольких сервисов KUMA на одном хосте в процессе установки необходимо указать уникальные порты (см. раздел "Настройка сетевого доступа" на стр. 41) для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

Коллектор установлен. С его помощью можно получать и передавать на обработку данные из источника события.

Проверка правильности установки коллектора

► *Проверить готовность коллектора к получению событий можно следующим образом:*

1. В веб-интерфейсе KUMA откройте раздел **Ресурсы** → **Активные сервисы**.
2. Убедитесь, что у установленного вами коллектора зеленый статус.

Если коллектор установлен правильно и вы уверены, что из источника событий приходят данные, то при поиске связанных с ним событий (см. раздел "Поиск связанных событий" на стр. 234) в таблице должны отображаться события.

► *Чтобы проверить наличие ошибок нормализации с помощью раздела **События** веб-интерфейса KUMA:*

1. Убедитесь, что запущен сервис коллектора.
2. Убедитесь, что источник событий передает события в KUMA.
3. Убедитесь, что в разделе **Ресурсы** веб-интерфейса KUMA в раскрывающемся списке **Хранить исходное событие** ресурса **Нормализатор** выбрано значение **При возникновении ошибок**.
4. В разделе **События** в KUMA выполните поиск событий со следующими параметрами:
   - `ServiceID = <идентификатор коллектора, который требуется проверить (см. раздел "Получение идентификатора сервиса" на стр. 231)>`
   - `Raw != ""`

   Если при этом поиске будут обнаружены какие-либо события, это означает, что есть ошибки нормализации, и их необходимо исследовать.

► *Чтобы проверить наличие ошибок нормализации с помощью панели мониторинга Grafana™:*

1. Убедитесь, что запущен сервис коллектора.
2. Убедитесь, что источник событий передает события в KUMA.
3. Откройте раздел Метрики и перейдите по ссылке KUMA Collectors.
4. Проверьте, отображаются ли ошибки в разделе Errors (Ошибки) виджета Normalization (Нормализация).

   Если в результате обнаружены ошибки нормализации, их необходимо исследовать.

В коллекторах типа WEC (см. раздел "Тип wec" на стр. 191) и WMI (см. раздел "Тип wmi" на стр. 190) необходимо убедиться, что для подключения к агенту используется уникальный порт. Этот порт

указывается в разделе **Транспорт** (см. раздел "**Шаг 2. Транспорт**" на стр. 238) мастера установки коллектора.

Создание коррелятора

Коррелятор (на стр. 23) состоит из двух частей (см. раздел "Сервисы KUMA" на стр. 229): одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для обработки событий.

Действия в веб-интерфейсе KUMA

Создание коррелятора в веб-интерфейсе KUMA производится с помощью мастера установки, в процессе выполнения которого необходимые ресурсы (см. раздел "Ресурсы KUMA" на стр. 128) объединяются в набор ресурсов для коррелятора (см. раздел "Наборы ресурсов для сервисов" на стр. 235), а по завершении мастера на основе этого набора ресурсов автоматически создается и сам сервис.

► *Чтобы создать коррелятор в веб-интерфейсе KUMA,*

запустите мастер установки коррелятора:

- В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Добавить коррелятор**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Корреляторы** нажмите **Добавить коррелятор**.

В результате выполнения шагов мастера в веб-интерфейсе KUMA создается сервис коррелятора.

В набор ресурсов для коррелятора объединяются следующие ресурсы:

- правила корреляции (на стр. 134);
- правила обогащения (на стр. 194) (при необходимости);
- правила реагирования (на стр. 217) (при необходимости);
- точки назначения (на стр. 199) (как правило, одна: задается отправка событий в хранилище).

Эти ресурсы можно подготовить заранее, а можно создать в процессе выполнения мастера установки.

Действия на сервере коррелятора KUMA

При установке коррелятора на сервер (см. раздел "Установка коррелятора в сетевой инфраструктуре KUMA" на стр. 262), предназначенный для обработки событий, на сервере требуется в запустить команду, которая отображается на последнем шаге мастера установки. При установке необходимо указать идентификатор (см. раздел "Получение идентификатора сервиса" на стр. 231), автоматически присвоенный сервису в веб-интерфейсе KUMA, а также используемый для связи порт.

Проверка установки

После создания коррелятора рекомендуется убедиться (см. раздел "Проверка правильности установки коррелятора" на стр. 263) в правильности его работы.

kaspersky

В этом разделе

Запуск мастера установки коррелятора 253
Установка коррелятора в сетевой инфраструктуре KUMA 262
Проверка правильности установки коррелятора 263

Запуск мастера установки коррелятора

Коррелятор (на стр. 23) состоит из двух частей (см. раздел "Сервисы KUMA" на стр. 229): одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры, предназначенном для обработки событий. В мастере установки создается первая часть коррелятора.

► *Чтобы запустить мастер установки коррелятора:*

- В веб-интерфейсе KUMA в разделе **Ресурсы** нажмите **Добавить коррелятор**.
- В веб-интерфейсе KUMA в разделе **Ресурсы** → **Коррелляторы** нажмите **Добавить коррелятор**.

Следуйте указаниям мастера.

Шаги мастера, кроме первого и последнего, можно выполнять в произвольном порядке. Переключаться между шагами можно с помощью кнопок **Вперед** и **Назад**, а также нажимая на названия шагов в левой части окна.

По завершении мастера в веб-интерфейсе KUMA в разделе **Ресурсы** → **Коррелляторы** создается набор ресурсов для коррелятора (см. раздел "Наборы ресурсов для сервисов" на стр. 235), а в разделе **Ресурсы** → **Активные сервисы** добавляется сервис коррелятора (см. раздел "Сервисы KUMA" на стр. 229).

В этом разделе

Шаг 1. Общие параметры коррелятора 253
Шаг 2. Глобальные переменные 254
Шаг 3. Корреляция 255
Шаг 4. Обогащение 255
Шаг 5. Реагирование 256
Шаг 6. Маршрутизация 258
Шаг 7. Проверка параметров 261

Шаг 1. Общие параметры коррелятора

Это обязательный шаг мастера установки. На этом шаге указывается основные параметры коррелятора: название и тенант, которому он будет принадлежать.

► *Чтобы задать основные параметры коррелятора:*

- В поле **Название** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.
- В раскрывающемся списке **Тенант** выберите тенант (см. раздел "О тенантах" на стр. 25), которому будет принадлежать коррелятор. От выбора тенанта зависит, какие ресурсы будут доступны при его создании.

  Если вы с какого-либо последующего шага мастера установки вернетесь в это окно и выберите другого тенанта, вам потребуется вручную изменить все ресурсы, которые вы успели добавить в сервис. В сервис можно добавлять только ресурсы из выбранного и общего тенантов.

- В поле **Рабочие процессы** при необходимости укажите количество процессов, которые может одновременно запускать сервис. По умолчанию количество рабочих процессов соответствует количеству vCPU сервера, на котором установлен сервис.
- При необходимости с помощью раскрывающегося списка **Отладка** включите логирование операций сервиса (см. раздел "Журналы KUMA" на стр. 408).
- В поле **Описание** можно добавить описание сервиса: до 256 символов Юникода.

Основные параметры коррелятора заданы. Перейдите к следующему шагу мастера установки.

Шаг 2. Глобальные переменные

Если для покрытия каких-то сценариев обеспечения безопасности недостаточно отслеживания значений в полях событий, активных листах или словарях, вы можете воспользоваться глобальными и локальными переменными (см. раздел "Переменные в корреляторах" на стр. 144). С их помощью можно выполнять различные действия над поступающими в корреляторы значениями, реализуя сложную логику выявления угроз. Переменным можно присвоить какую-либо функцию, а затем обращаться к ним из правил корреляции, как к обычным полям событий, получая в ответ результат срабатывания функции.

► *Чтобы добавить глобальную переменную в коррелятор,*

Нажмите на кнопку **Добавить переменную** и укажите следующие параметры:

- В окне **Переменная** введите название переменной.

  Требования к наименованию переменных (см. раздел "Требования к наименованию переменных" на стр. 157)

- В окне **Значение** введите функцию переменной.

  Описание функций переменных (см. раздел "Функции переменных" на стр. 146).

Глобальная переменная добавлена. К ней можно обращаться из правил корреляции (см. раздел "Шаг 3. Корреляция" на стр. 255), добавляя перед названием переменной символ $. Переменных может быть несколько. Добавленные переменные можно изменить или удалить с помощью значка ✕.

Перейдите к следующему шагу мастера установки.

Шаг 3. Корреляция

Это необязательный, но рекомендуемый шаг мастера установки. В закладке мастера установки **Корреляция** следует выбрать или создать ресурсы правил корреляции (см. раздел "Правила корреляции" на стр. 134). В этих ресурсах задаются последовательности событий, указывающих на происшествия, связанные с безопасностью: при обнаружении таких последовательностей коррелятор (на стр. 23) создает корреляционное событие и алерт (см. раздел "Об алертах" на стр. 27).

Если вы добавили в коррелятор глобальные переменные (см. раздел "Шаг 2. Глобальные переменные" на стр. 254), все добавленные правила корреляции могут к ним обращаться.

Добавленные в набор ресурсов для коррелятора правила корреляции отображаются в таблице со следующими столбцами:

- **Правила корреляции** – название ресурса правила корреляции.
- **Тип** – тип правила корреляции: **standard**, **simple**, **operational**. Таблицу можно отфильтровать по значениям этого столбца, нажав на его заголовок и выбрав нужные значения.
- **Действия** – перечень действий, которые совершит коррелятор при срабатывании правила корреляции. Действия указываются в параметрах правила корреляции. Таблицу можно отфильтровать по значениям этого столбца, нажав на его заголовок и выбрав нужные значения.

С помощью поля **Поиск** можно искать правила корреляции. Добавленные правила корреляции можно убрать из набора ресурсов, выбрав нужные правила и нажав **Удалить**.

При выборе правила корреляции открывается окно с его параметрами: параметры ресурса можно изменить и сохранить с помощью кнопки **Сохранить**. При нажатии в этом окне на кнопку **Удалить**, правило корреляции отвязывается от набора ресурсов.

► *Чтобы привязать к набору ресурсов для коррелятора существующие правила корреляции:*

1. Нажмите **Привязать**.

   Откроется окно выбора ресурсов.

2. Выберите нужные правила корреляции и нажмите **ОК**.

Правила корреляции привязаны к набору ресурсов для коррелятора и отображаются в таблице правил.

► *Чтобы создать в наборе ресурсов для коррелятора новое правило корреляции:*

1. Нажмите **Добавить**.

   Откроется окно создания правила корреляции.

2. Укажите параметры правила корреляции (см. раздел "Правила корреляции" на стр. 134) и нажмите **Сохранить**.

Правило корреляции создано и привязано к набору ресурсов для коррелятора. Оно отображается в таблице правил корреляции, а также в списке ресурсов в разделе **Ресурсы → Правила корреляции**.

Перейдите к следующему шагу мастера установки.

Шаг 4. Обогащение

Это необязательный шаг мастера установки. В закладке мастера установки **Обогащение** можно выбрать или создать ресурс правил обогащения (см. раздел "Правила обогащения" на стр. 194) с указанием, какими данными и из каких источников следует дополнить создаваемые коррелятором корреляционные события.

Правил обогащения может быть несколько. Их можно добавить с помощью кнопки **Добавить** или удалить с помощью кнопки ✕.

► *Чтобы добавить в набор ресурсов существующее правило обогащения:*

1. Нажмите **Добавить**.

   Откроется блок параметров правила обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите нужный ресурс.

Правило обогащения добавлено в набор ресурсов для коррелятора.

► *Чтобы создать в наборе ресурсов новое правило обогащения:*

1. Нажмите **Добавить**.

   Откроется блок параметров правила обогащения.

2. В раскрывающемся списке **Правило обогащения** выберите **Создать**.
3. В раскрывающемся списке **Тип источника данных** выберите, откуда будут поступать данные для обогащения, и заполните относящиеся к ним параметры:
   - константа (см. раздел "Обогащение, тип константа" на стр. 195)
   - словарь (см. раздел "Обогащение, тип словарь" на стр. 196)
   - событие (см. раздел "Обогащение, тип событие (для ресурса обогащения)" на стр. 196)
   - шаблон (см. раздел "Обогащение, тип шаблон" на стр. 197)
   - dns (см. раздел "Обогащение, тип dns" на стр. 196)
   - cybertrace (см. раздел "Обогащение, тип cybertrace" на стр. 195)
   - часовой пояс (см. раздел "Обогащение, тип часовой пояс" на стр. 197)
4. С помощью раскрывающегося списка **Отладка** укажите, следует ли включить логирование операций сервиса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию логирование выключено.
5. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом правила обогащения. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

   Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

В набор ресурсов для коррелятора добавлено новое правило обогащения.

Перейдите к следующему шагу мастера установки.

Шаг 5. Реагирование

Это необязательный шаг мастера установки. В закладке мастера установки **Реагирование** можно выбрать или создать ресурс правил реагирования (см. раздел "Правила реагирования" на стр. 217) с указанием, какие действия требуется выполнить при срабатывании правил корреляции (см. раздел "Правила корреляции" на стр. 134). Правил реагирования может быть несколько. Их можно добавить с помощью кнопки **Добавить** или удалить с помощью кнопки ✕.

► *Чтобы добавить в набор ресурсов существующее правило реагирования:*

1. Нажмите **Добавить**.

   Откроется окно с параметрами правила реагирования.

2. В раскрывающемся списке **Правило реагирования** выберите нужный ресурс.

Правило реагирования добавлено в набор ресурсов для коррелятора.

► *Чтобы создать в наборе ресурсов новое правило реагирования:*

1. Нажмите **Добавить**.

   Откроется окно с параметрами правила реагирования.

2. В раскрывающемся списке **Правило реагирования** выберите **Создать**.
3. В раскрывающемся списке **Тип** выберите тип правила реагирования и заполните относящиеся к ним параметры:

   - **ksctasks** – правила реагирования для автоматического запуска задач на активах Kaspersky Security Center. Например, вы можете настроить автоматический запуск антивирусной проверки или обновление базы данных.

     Автоматический запуск задач выполняется при интеграции KUMA с Kaspersky Security Center (см. раздел "Интеграция с Kaspersky Security Center" на стр. 73). Задачи запускаются только на активах, импортированных из Kaspersky Security Center.

     Параметры реагирования типа ksctasks (см. раздел "Реагирование ksctasks" на стр. 258)

   - **script** – правила реагирования для автоматического запуска скрипта. Например, вы можете создать скрипт с командами, которые требуется выполнить на сервере KUMA при обнаружении выбранных событий.

     Файл скрипта хранится на сервере, где установлен сервис коррелятора (см. раздел "Установка коррелятора в сетевой инфраструктуре KUMA" на стр. 262), использующий ресурс реагирования: /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора (см. раздел "Получение идентификатора сервиса" на стр. 231)>/scripts.

     Пользователю `kuma` этого сервера требуются права на запуск скрипта.

     Параметры реагирования типа script (см. раздел "Реагирование script" на стр. 258)

   - **kata/edr** – правила реагирования для автоматического создания правил запрета, запуска сетевой изоляции или запуска программы на активах Kaspersky Endpoint Detection and Response и Kaspersky Security Center.

     Автоматические действия по реагированию выполняются при интеграции KUMA с Kaspersky Endpoint Detection and Response (см. раздел "Интеграция с Kaspersky Endpoint Detection and Response" на стр. 80).

- В поле **Рабочие процессы** укажите количество процессов, которые сервис может запускать одновременно.

  По умолчанию количество рабочих процессов соответствует количеству виртуальных процессоров сервера, на котором установлен сервис.

  Поле не обязательно для заполнения.

1. В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться ресурсом правила реагирования. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

В набор ресурсов для коррелятора добавлено новое правило реагирования.

Перейдите к следующему шагу мастера установки.

Реагирование ksctasks

- **Задача Kaspersky Security Center** (обязательно) – название задачи Kaspersky Security Center, которую требуется запустить. Задачи должны быть созданы заранее, и их названия должны начинаться со слова "`KUMA `". Например, "`KUMA antivirus check`".
- **Поле события** (обязательно) – определяет поле события для актива, для которого нужно запустить задачу Kaspersky Security Center. Возможные значения:
  - SourceAssetID
  - DestinationAssetID
  - DeviceAssetID

Для отправки запросов в Kaspersky Security Center необходимо убедиться, что Kaspersky Security Center доступен по протоколу UDP.

Реагирование script

- **Время ожидания** – количество секунд, которое выждет система, прежде чем запустить скрипт.
- **Название скрипта** (обязательно) – имя файла скрипта.

  Если ресурс реагирования прикреплен к сервису коррелятора, однако в папке /opt/kaspersky/kuma/correlator/<Идентификатор коррелятора>/scripts файл скрипта отсутствует, коррелятор не будет работать.
- **Аргументы скрипта** – параметры или значения полей событий, которые необходимо передать скрипту.

  Если в скрипте производятся какие-либо действия с файлами, к ним следует указывать абсолютный путь.

  Параметры можно обрамлять кавычками (").

  Имена полей событий передаются в формате `{{.EventField}}`, где `EventField` – это имя поля события, значение которого должно быть передано в скрипт.

  Пример: `-n "\"usr\": {{.SourceUserName}}"`

Шаг 6. Маршрутизация

Это необязательный шаг мастера установки. В закладке мастера установки **Маршрутизация** можно выбрать или создать ресурсы точек назначения (см. раздел "Точки назначения" на стр. 199), в параметрах которых будут определено, куда следует перенаправлять созданные коррелятором события. Обычно события от коррелятора перенаправляются в хранилище (на стр. 24) для хранения и для возможности

просматривать их позднее. При необходимости события можно отправлять в другие места. Точек назначения может быть несколько.

► *Чтобы добавить в набор ресурсов коррелятора существующую точку назначения:*

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:
   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.
   - Выберите **Другое**, если хотите отправлять события в другие места.

     К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях программы.

   Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.
2. В раскрывающемся списке **Точка назначения** выберите нужную точку назначения.

   Название окна меняется на **Изменить точку назначения**, параметры выбранного ресурса отображаются в окне. Ресурс можно открыть для редактирования в новой вкладке браузера с помощью кнопки  .
3. Нажмите **Сохранить**.

Выбранная точка назначения отображается в закладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

► *Чтобы добавить в набор ресурсов коррелятора новую точку назначения:*

1. В раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, которую вы хотите добавить:
   - Выберите **Хранилище**, если хотите настроить отправку обработанных событий в хранилище.
   - Выберите **Коррелятор**, если хотите настроить отправку обработанных событий в коррелятор.
   - Выберите **Другое**, если хотите отправлять события в другие места.

     К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях программы.

   Открывается окно **Добавить точку назначения**, где можно указать параметры пересылки событий.
2. Укажите параметры в закладке **Основные параметры**:
   - В раскрывающемся списке **Точка назначения** выберите **Создать**.
   - Введите в поле **Название** уникальное имя для точки назначения. Название должно содержать от 1 до 128 символов Юникода.
   - С помощью переключателя **Выключено**, выберите, будут ли события отправляться в эту точку назначения. По умолчанию отправка событий включена.
   - Выберите **Тип** точки назначения:
     - Выберите **storage**, если хотите настроить отправку обработанных событий в хранилище.

- Выберите **correlator**, если хотите настроить отправку обработанных событий в коррелятор.
- Выберите **nats**, **tcp**, **http**, **kafka** или **file**, если хотите настроить отправку событий в другие места.

- Укажите **URL**, куда следует отправлять события, в формате hostname:<порт API>.

  Для всех типов, кроме **nats** и **file** с помощью кнопки **URL** можно указать несколько адресов отправки, если в вашу лицензию KUMA включен модуль High Level Availability.

  Если в качестве типа точки назначения выбраны **storage** или **correlator**, поле **URL** можно заполнить автоматически с помощью раскрывающегося списка **Копировать URL сервиса**, в котором отображаются активные сервисы (см. раздел "Сервисы KUMA" на стр. 229) выбранного типа.

- Для типов **nats** и **kafka** в поле **Топик** укажите, в какой топик должны записываться данные. Топик должен содержать от 1 до 255 символов Юникода.

3. При необходимости укажите параметры в закладке **Дополнительные параметры**. Доступные параметры зависят от выбранного типа точки назначения (на стр. 199):

   - **Сжатие** – раскрывающийся список, в котором можно включить сжатие Snappy. По умолчанию сжатие **Выключено**.
   - **Прокси-сервер** – раскрывающийся список для выбора ресурса прокси-сервера (см. раздел "Прокси-серверы" на стр. 226).
   - **Размер буфера** – поле, в котором можно указать размер буфера (в байтах) для ресурса точки назначения. Значение по умолчанию: 1 МБ; максимальное: 64 МБ.
   - **Время ожидания** – поле, в котором можно указать время ожидания (в секундах) ответа другого сервиса или компонента. Значение по умолчанию: `30`.
   - **Размер дискового буфера** – поле, в котором можно указать размер дискового буфера в байтах. По умолчанию размер равен 10 ГБ.
   - **Идентификатор хранилища** – идентификатор хранилища NATS.
   - **Режим TLS** – раскрывающийся список, в котором можно указать условия использование шифрования TLS:
     - **Выключено** (по умолчанию) – не использовать шифрование TLS.
     - **Включено** – использовать шифрование, но без верификации.
     - **С верификацией** – использовать шифрование с верификацией сертификата, подписанного корневым сертификатом KUMA. Корневой сертификат и ключ KUMA создаются автоматически при установке программы (см. раздел "Изменение корневого сертификата" на стр. 46) и располагаются на сервере Ядра KUMA в папке /opt/kaspersky/kuma/core/certificates/.

     При использовании TLS невозможно указать IP-адрес в качестве URL.
   - **Политика выбора URL** – раскрывающийся список, в котором можно выбрать способ определения, на какой URL следует отправлять события, если URL было указано несколько:
     - **Любой**
     - **Сначала первый**
     - **По очереди**
   - **Разделитель** – этот раскрывающийся список используется для указания символа, определяющего границу между событиями. По умолчанию используется `\n`.

- **Путь** – путь к файлу, если выбран тип точки назначения **file**.
- **Интервал очистки буфера** – это поле используется для установки времени (в секундах) между отправкой данных в точку назначения. Значение по умолчанию: `100`.
- **Рабочие процессы** – это поле используется для установки количества служб, обрабатывающих очередь. Значение по умолчанию равно количеству vCPU сервера, на котором установлено Ядро KUMA.
- Вы можете установить проверки работоспособности, используя поля **Путь проверки работоспособности** и **Ожидание проверки работоспособности**. Вы также можете отключить проверку работоспособности, установив флажок **Проверка работоспособности отключена**.
- **Отладка** – раскрывающийся список, в котором можно указать, будет ли включено логирование ресурса (см. раздел "Журналы KUMA" на стр. 408). По умолчанию указывается значение **Выключено**.
- С помощью раскрывающегося списка **Дисковый буфер** можно включить или выключить использование дискового буфера. По умолчанию дисковый буфер отключен.
- В разделе **Фильтр** можно задать условия определения событий, которые будут обрабатываться этим ресурсом. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

  Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

4. Нажмите **Сохранить**.

Созданная точка назначения отображается в закладке мастера установки. Точку назначения можно удалить из набора ресурсов, выбрав ее и в открывшемся окне нажав **Удалить**.

Перейдите к следующему шагу мастера установки.

Шаг 7. Проверка параметров

Это обязательный и заключительный шаг мастера установки. На этом шаге в KUMA создается набор ресурсов для сервиса (см. раздел "Наборы ресурсов для сервисов" на стр. 235) и на основе этого набора автоматически создаются сервисы (см. раздел "Сервисы KUMA" на стр. 229):

- Набор ресурсов для коллектора отображается в разделе **Ресурсы → Коррелляторы**. Его можно использовать для создания новых сервисов коррелятора. При изменении этого набора ресурсов все сервисы, которые работают на его основе, будут использовать новые параметры, если сервисы перезапустить (см. раздел "Перезапуск сервиса" на стр. 231): для этого можно использовать кнопки **Сохранить и перезапустить сервисы** и **Сохранить и обновить параметры сервисов**.

  Набор ресурсов можно изменять, копировать, переносить из папки в папку, удалять, импортировать и экспортировать, как другие ресурсы (см. раздел "Операции с ресурсами" на стр. 129).
- Сервисы отображаются в разделе **Ресурсы → Активные сервисы**. Созданные с помощью мастера установки сервисы выполняют функции внутри программы KUMA – для связи с внешними частями сетевой инфраструктуры необходимо установить аналогичные внешние сервисы на предназначенных для них серверах и устройствах. Например, внешний сервис коррелятора следует установить на сервере, предназначенном для обработки событий; внешние сервисы хранилища – на серверах с развернутой службой ClickHouse; внешние сервисы агентов – на тех устройствах Windows, где требуется получать и откуда необходимо пересылать события Windows.

► *Чтобы завершить мастер установки:*

1. Нажмите **Сохранить и создать сервис**.

В закладке мастера установки **Проверка параметров** отображается таблица сервисов, созданных на основе набора ресурсов, выбранных в мастере установки. В нижней части окна отображаются примеры команд, с помощью которых необходимо установить внешние аналоги этих сервисов на предназначенные для них серверы и устройства.

Например:

/opt/kaspersky/kuma/kuma correlator --core https://kuma-example:<порт, используемый для связи с Ядром KUMA> --id <идентификатор сервиса> --api.port <порт, используемый для связи с сервисом> --install

Порт для связи с Ядром KUMA, идентификатор сервиса и порт для связи с сервисом добавляются в команду автоматически. Также следует убедиться в сетевой связности системы KUMA и при необходимости открыть используемые ее компонентами порты (см. раздел "Настройка сетевого доступа" на стр. 41).

2. Закройте мастер, нажав **Сохранить**.

Сервис коррелятора создан в KUMA. Теперь аналогичный сервис необходимо установить на сервере (см. раздел "Установка коррелятора в сетевой инфраструктуре KUMA" на стр. 262), предназначенном для обработки событий.

Установка коррелятора в сетевой инфраструктуре KUMA

Коррелятор (на стр. 23) состоит из двух частей (см. раздел "Сервисы KUMA" на стр. 229): одна часть создается внутри веб-интерфейса KUMA, а другая устанавливается на сервере сетевой инфраструктуры (см. раздел "Установка KUMA в производственной среде" на стр. 39), предназначенном для обработки событий. В сетевой инфраструктуре устанавливается вторая часть коррелятора.

► *Чтобы установить коррелятор:*

1. Войдите на сервер, на котором вы хотите установить сервис.
2. Выполните следующую команду:

```
sudo /opt/kaspersky/kuma/kuma correlator --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA (см. раздел "Получение идентификатора сервиса" на стр. 231)> --api.port <порт, используемый для связи с устанавливаемым компонентом> --install
```

Пример: `sudo /opt/kaspersky/kuma/kuma correlator --core https://kuma.example.com:7210 --id XXXX --api.port YYYY --install`

> Команду, с помощью которой можно установить коррелятор на сервере, можно скопировать на последнем шаге мастера установщика. В ней автоматически указывается адрес и порт сервера Ядра KUMA, идентификатор устанавливаемого коррелятора, а также порт, который этот коррелятор использует для связи. Перед установкой необходимо убедиться в сетевой связности компонентов KUMA.
> При развертывании нескольких сервисов KUMA на одном хосте в процессе установки необходимо указать уникальные порты (см. раздел "Настройка сетевого доступа" на стр. 41) для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

Коррелятор установлен. С его помощью можно анализировать события на предмет угроз.

Проверка правильности установки коррелятора

► *Проверить готовность коррелятора к получению событий можно следующим образом:*

1. В веб-интерфейсе KUMA откройте раздел **Ресурсы** → **Активные сервисы**.
2. Убедитесь, что у установленного вами коррелятора зеленый статус.

Если в коррелятор поступают события, удовлетворяющие условиям фильтра правил корреляции, на закладке событий будут отображаться события (см. раздел "Поиск связанных событий" на стр. 234) с параметрами `DeviceVendor=Kaspersky` и `DeviceProduct=KUMA`. Название сработавшего правила корреляции будет отображаться как название этих событий корреляции.

Если события корреляции не найдены

Можно создать более простую версию правила корреляции, чтобы найти возможные ошибки. Используйте правило корреляции типа **simple** (см. раздел "**Правила корреляции типа simple**" на стр. 139) и одно действие **Отправить событие на дальнейшую обработку**. Рекомендуется создать фильтр для поиска событий, которые KUMA получает регулярно.

При обновлении, добавлении или удалении правила корреляции требуется перезапустить (см. раздел "Перезапуск сервиса" на стр. 231) коррелятор.

Когда вы закончите тестирование правил корреляции, необходимо удалить все тестовые и временные правила корреляции из KUMA и перезапустить (см. раздел "Перезапуск сервиса" на стр. 231) коррелятор.

Создание агента

Агент KUMA (см. раздел "Об агентах" на стр. 29) состоит из двух частей (см. раздел "Сервисы KUMA" на стр. 229): одна часть создается внутри веб-интерфейса KUMA, а вторая устанавливается на сервере или устройстве сетевой инфраструктуры.

Создание агента производится в несколько этапов:

a. **Создание набора ресурсов агента в веб-интерфейсе KUMA (см. раздел "Создание набора ресурсов для агента" на стр. 264)**
b. **Создание сервиса агента в веб-интерфейсе KUMA (на стр. 266)**
c. **Установка серверной части агента на устройстве, с которого требуется передавать сообщения (см. раздел "Установка агента в сетевой инфраструктуре KUMA" на стр. 266)**

Агент KUMA для устройств Windows может быть создан автоматически (см. раздел "Автоматически созданные агенты" на стр. 269) при создании коллектора с типом транспорта wmi или wec (см. раздел "Шаг 2. Транспорт" на стр. 238). Набор ресурсов и сервис таких агентов создаются в мастере установки

коллектора, однако их все равно требуется установить на устройстве (см. раздел "Установка агента в сетевой инфраструктуре KUMA" на стр. 266), с которого требуется передать сообщение.

В этом разделе

Создание набора ресурсов для агента 264
Создание сервиса агента в веб-интерфейсе KUMA 266
Установка агента в сетевой инфраструктуре KUMA 266
Автоматически созданные агенты 269
Обновление агентов 269

Создание набора ресурсов для агента

Сервис агента в веб-интерфейсе KUMA создается на основе набора ресурсов (см. раздел "Наборы ресурсов для сервисов" на стр. 235) для агента, в котором объединяются коннекторы (на стр. 169) и точки назначения (на стр. 199).

► *Чтобы создать набор ресурсов для агента в веб-интерфейсе KUMA:*

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Агенты** нажмите **Добавить агент**.

   Откроется окно создания агента с активной закладкой **Общие параметры**.
2. Заполните параметры в закладке **Общие параметры**:
   - В поле **Название агента** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.
   - В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать хранилище.
   - При необходимости установите флажок **Отладка**, чтобы включить логирование операций сервиса (см. раздел "Журналы KUMA" на стр. 408).
   - В поле **Описание** можно добавить описание сервиса: до 256 символов Юникода.
3. Создайте подключение для агента с помощью кнопки + и переключитесь на добавленную закладку **Подключение <номер>**.

   Закладки можно удалять с помощью кнопки ×.
4. В блоке параметров **Коннектор** добавьте ресурс коннектора (см. раздел "Коннекторы" на стр. 169):
   - Если хотите выбрать существующий ресурс, выберите его в раскрывающемся списке.
   - Если хотите создать новый ресурс, выберите в раскрывающемся списке **Создать** и укажите его параметры:
     - В поле **Название** укажите имя коннектора. Название должно содержать от 1 до 128 символов Юникода.
     - В раскрывающемся списке **Тип** выберите тип коннектора и укажите его параметры в закладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа коннектора:
       - tcp (см. раздел "Тип tcp" на стр. 172)

- udp (см. раздел "Тип udp" на стр. 173)
- nats (см. раздел "Тип nats" на стр. 174)
- kafka (см. раздел "Тип kafka" на стр. 176)
- http (см. раздел "Тип http" на стр. 178)
- file (см. раздел "Тип file" на стр. 185)
- ftp (см. раздел "Тип ftp" на стр. 188)
- nfs (см. раздел "Тип nfs" на стр. 189)
- wmi (см. раздел "Тип wmi" на стр. 190)
- wec (см. раздел "Тип wec" на стр. 191)
- snmp (см. раздел "Тип snmp" на стр. 192)

Типом агента считается тип использованного в нем коннектора. Исключением являются агенты с точкой назначения типа diode: такие агенты считаются diode-агентами (см. раздел "Передача в KUMA событий из изолированных сегментов сети" на стр. 366). При использовании типа коннектора **tcp** или **upd** на этапе нормализации (см. раздел "Шаг 3. Парсинг событий" на стр. 239) в поле событий DeviceAddress, если она пустая, будут записаны IP-адреса устройств, с которых были получены события.

- В поле **Описание** можно добавить описание ресурса: до 256 символов Юникода.

Ресурс коннектора добавлен в выбранное подключение набора ресурсов агента. Созданный ресурс доступен только в этом наборе ресурсов и не отображается в разделе веб-интерфейса **Ресурсы** → **Коннекторы**.

5. В блоке параметров **Точки назначения** добавьте ресурсы точек назначения (см. раздел "Точки назначения" на стр. 199).
   - Если хотите выбрать существующий ресурс, выберите его в раскрывающемся списке.
   - Если хотите создать новый ресурс, выберите в раскрывающемся списке **Создать** и укажите его параметры:
     - В поле **Название** укажите имя точки назначения. Название должно содержать от 1 до 128 символов Юникода.
     - В раскрывающемся списке **Тип** выберите тип точки назначения и укажите ее параметры в закладках **Основные параметры** и **Дополнительные параметры**. Набор доступных параметров зависит от выбранного типа точки назначения:
       - **nats** (см. раздел "**Тип nats**" на стр. 200) – используется для коммуникации через NATS.
       - **tcp** (см. раздел "**Тип tcp**" на стр. 201) – используется для связи по протоколу TCP.
       - **http** (см. раздел "**Тип http**" на стр. 203) – используется для связи по протоколу HTTP.
       - **diode** (см. раздел "**Тип diode**" на стр. 204) – используется для передачи событий с помощью диода данных (см. раздел "Передача в KUMA событий из изолированных сегментов сети" на стр. 366).
       - **kafka** (см. раздел "**Тип kafka**" на стр. 206) – используется для коммуникаций с помощью kafka.
       - **file** (см. раздел "**Тип file**" на стр. 208) – используется для записи в файл.

- **storage** (см. раздел "**Тип storage**" на стр. 209) – используется для передачи данных в хранилище.
- **correlator** (см. раздел "**Тип correlator**" на стр. 210) – используется для передачи данных в коррелятор.

- В поле **Описание** можно добавить описание ресурса: до 256 символов Юникода.

  Дополнительные параметры точки назначения агента (например, сжатие и режим TLS) должны совпадать с дополнительными параметрами точки назначения коллектора, с которым вы хотите связать агент.

  Точек назначения может быть несколько. Их можно добавить с помощью кнопки **Добавить точку назначения** и удалить с помощью кнопки ✕.

6. Повторите шаги 3–5 для каждого подключения агента, которое вы хотите создать.
7. Нажмите **Сохранить**.

Набор ресурсов для агента создан и отображается в разделе **Ресурсы** → **Агенты**. Теперь можно создать сервис агента в KUMA (см. раздел "Создание сервиса агента в веб-интерфейсе KUMA" на стр. 266).

Создание сервиса агента в веб-интерфейсе KUMA

Когда набор ресурсов для агента создан (см. раздел "Создание набора ресурсов для агента" на стр. 264), можно перейти к созданию сервиса агента в KUMA.

► *Чтобы создать сервис агента в веб-интерфейсе KUMA:*

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** нажмите **Добавить сервис**.
2. В открывшемся окне **Выберите сервис** выберите только что созданный набор ресурсов для агента и нажмите **Создать сервис**.

Сервис агента создан в веб-интерфейсе KUMA и отображается в разделе **Ресурсы** → **Активные сервисы**. Теперь сервисы агента необходимо установить на каждом устройстве (см. раздел "Установка агента в сетевой инфраструктуре KUMA" на стр. 266), с которого вы хотите передавать данные в коллектор. При установке используется идентификатор сервиса (см. раздел "Получение идентификатора сервиса" на стр. 231).

Установка агента в сетевой инфраструктуре KUMA

Когда сервис агента создан в KUMA (см. раздел "Создание сервиса агента в веб-интерфейсе KUMA" на стр. 266), можно перейти к установке агента на устройствах сетевой инфраструктуры, с которых вы хотите передавать данные в коллектор.

Перед установкой убедитесь в сетевой связности системы и откройте используемые компонентами порты.

kaspersky

В этом разделе

Установка агента KUMA на устройствах Linux 267
Установка агента KUMA на устройствах Windows 267

Установка агента KUMA на устройствах Linux

► *Чтобы установить агент KUMA на устройство Linux:*

1. Войдите на сервер, на котором вы хотите установить сервис.
2. Выполните следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma agent --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA (см. раздел "Получение идентификатора сервиса" на стр. 231)> --wd <путь к директории, где будут размещаться файлы устанавливаемого агента. Если не указывать этот флаг, файлы будут храниться в директории, где расположен файл kuma>
   ```

   Пример: `sudo /opt/kaspersky/kuma/kuma agent --core https://kuma.example.com:7210 --id XXXX --wd /opt/kaspersky/kuma/agent/XXXX`

Агент KUMA установлен на устройство Linux. Агент пересылает данные в KUMA: можно настроить коллектор (на стр. 20) для их приема.

Установка агента KUMA на устройствах Windows

Перед установкой агента KUMA на устройстве Windows администратору сервера необходимо создать на устройстве Windows учетную запись с правами EventLogReaders и Log on as a service. Эту же учетную запись необходимо использовать для запуска агента.

► *Чтобы установить агент KUMA на устройство Windows:*

1. Скопируйте файл kuma.exe в папку на устройстве Windows. Для установки рекомендуется использовать папку `C:\Users\<имя пользователя>\Desktop\KUMA`.

   Файл kuma.exe находится внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.
2. Запустите командную строку на устройстве Windows с правами администратора и найдите папку с файлом kuma.exe.
3. Выполните следующую команду:

   ```
   kuma agent --core https://<полное доменное имя сервера ядра KUMA>:<порт, используемый сервером ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса агента, созданного в KUMA (см. раздел "Получение идентификатора
   ```

сервиса" на стр. 231)> --user <имя пользователя, под которым будет работать агент, включая домен> --install

Пример: kuma agent --core https://kuma.example.com:7210 --id XXXXX --user domain\username --install

Справочная информация об установщике доступна по команде kuma help agent.

4. Введите пароль для пользователя, под которым будет работать агент.

Создана папка C:\ProgramData\Kaspersky Lab\KUMA\agent\<Идентификатор Агента>, в нее установлен сервис агента KUMA. Агент пересылает события Windows в KUMA: можно настроить коллектор (на стр. 20) для их приема.

Когда сервис агента установлен, он запускается автоматически. Сервис также настроен на перезапуск в случае сбоев. Агент можно перезапустить из веб-интерфейса KUMA, но только когда сервис активен. В противном случае сервис требуется перезапустить вручную на машине Windows.

Удаление агента KUMA с устройств Windows (см. раздел "Удаление агента KUMA с устройств Windows" на стр. 268)

При настройке сервисов можно проверить конфигурацию на наличие ошибок до установки, запустив агент с помощью команды kuma agent --core https://<полное доменное имя сервера ядра KUMA>:<порт, используемый сервером ядра KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса агента, созданного в KUMA (см. раздел "Получение идентификатора сервиса" на стр. 231)> --user <имя пользователя, под которым будет работать агент, включая домен>.

Удаление агента KUMA с устройств Windows

► *Чтобы удалить агент KUMA с устройства Windows:*

1. Запустите командную строку на компьютере Windows с правами администратора и найдите папку с файлом kuma.exe.
2. Выполните любую из команд ниже:
   - kuma.exe agent --cfg <путь к файлу конфигурации агента> --uninstall
   - kuma.exe agent --id <идентификатор сервиса агента, созданного в KUMA (см. раздел "Получение идентификатора сервиса" на стр. 231)> --uninstall

Указанный агент KUMA удален с устройства Windows. События Windows больше не отправляются в KUMA.

kaspersky

Автоматически созданные агенты

При создании коллектора (см. раздел "Запуск мастера установки коллектора" на стр. 236) с коннекторами типа wec и wmi (см. раздел "Коннекторы" на стр. 169) автоматически создаются агенты для приема событий Windows.

Автоматически созданные агенты имеют ряд особенностей:

- Автоматически созданные агенты могут иметь только одно подключение.
- Автоматически созданные агенты отображаются в разделе **Ресурсы** → **Агенты**, в конце их названия указаны слова `auto created`. Агенты можно просмотреть или удалить.
- Параметры автоматически созданных агентов указываются автоматически на основе параметров коллектора из разделов **Подключение источников** и **Транспорт**. Изменить параметры можно только в коллекторе, для которого был создан агент.
- В качестве описания автоматически созданного агента используется описание коллектора в разделе **Подключение источников**.
- Отладка автоматически созданного агента включается и выключается в разделе коллектора **Подключение источников**.
- При удалении коллектора с автоматически созданным агентом вам будет предложено удалить коллектор вместе с агентом или удалить только коллектор. При удалении только коллектора агент станет доступен для редактирования.
- При удалении автоматически созданных агентов тип коллектора меняется на **http**, а из поля **URL** коллектора удаляется адрес подключения.

В интерфейсе KUMA автоматически созданные агенты появляются одновременно с созданием коллектора, однако их все равно требуется установить на устройстве (см. раздел "Установка агента в сетевой инфраструктуре KUMA" на стр. 266), с которого требуется передать сообщение.

Обновление агентов

При обновлении версий KUMA требуется обновить и установленные на удаленных машинах агенты WMI и WEC.

► *Чтобы обновить агент:*

1. Установите на удаленной машине новый агент (см. раздел "Установка агента KUMA на устройствах Windows" на стр. 267).

   Агент обновлен, но данные от него не поступают из-за недействительного сертификата.

2. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Активные сервисы** сбросьте сертификат (см. раздел "Перезапуск сервиса" на стр. 231) обновляемого агента.
3. На удаленной машине с установленным агентом запустите службу "KUMA Windows Agent <идентификатор сервиса (см. раздел "Получение идентификатора сервиса" на стр. 231)>".

   Подробнее о службах Windows смотрите в документации вашей версии Windows.

Агент и его сертификаты обновлены.

kaspersky

Создание хранилища

Хранилище (на стр. 24) состоит из двух частей (см. раздел "Сервисы KUMA" на стр. 229): одна часть создается внутри веб-интерфейса KUMA, а вторая устанавливается на серверах сетевой инфраструктуры, предназначенных для хранения событий. Серверная часть хранилища KUMA представляет собой собранные в кластер узлы ClickHouse.

Для каждого кластера ClickHouse требуется установить отдельное хранилище.

Перед созданием хранилища продумайте структуру кластера и разверните требуемую сетевую инфраструктуру. При выборе конфигурации кластера ClickHouse учитывайте требования вашей организации к хранению событий.
В качестве файловой системы рекомендуется использовать ext4 https://clickhouse.com/docs/en/operations/tips/#file-system.

Создание хранилища производится в несколько этапов:

a. **Создание набора ресурсов хранилища в веб-интерфейсе KUMA (см. раздел "Создание набора ресурсов для хранилища" на стр. 270)**
b. **Создание сервиса хранилища в веб-интерфейсе KUMA (на стр. 271)**
c. **Установка узлов хранилища в сетевой инфраструктуре KUMA (см. раздел "Установка хранилища в сетевой инфраструктуре KUMA" на стр. 271)**

При создании узлов кластера хранилища убедитесь в сетевой связности системы и откройте используемые компонентами порты.

В этом разделе

Создание набора ресурсов для хранилища 270
Создание сервиса хранилища в веб-интерфейсе KUMA 271
Установка хранилища в сетевой инфраструктуре KUMA 271

Создание набора ресурсов для хранилища

Сервис хранилища в веб-интерфейсе KUMA создается на основе набора ресурсов для хранилища.

► *Чтобы создать набор ресурсов для хранилища в веб-интерфейсе KUMA:*

1. В веб-интерфейсе KUMA в разделе **Ресурсы** → **Хранилища** нажмите **Добавить хранилище**.

   Откроется окно создания хранилища.

2. В поле **Название хранилища** введите уникальное имя создаваемого сервиса. Название должно содержать от 1 до 128 символов Юникода.

3. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать хранилище.
4. В поле **Описание** можно добавить описание сервиса: до 256 символов Юникода.
5. В поле **Срок хранения по умолчанию, дней** укажите, в течение какого времени вы хотите хранить события в кластере.
6. В поле **Срок хранения событий аудита, дней** укажите, в течение какого времени вы хотите хранить события аудита. Минимальное значение и значение по умолчанию: `365`.
7. При необходимости добавьте в хранилище пространства с помощью кнопки **Добавить пространство**. Пространств может быть несколько. Пространства можно удалить с помощью кнопки **Удалить пространство**. После создания сервиса пространства можно будет просматривать и удалять в окне **Разделы** (см. раздел "**Окно Разделы**" на стр. 232).

   Доступные параметры:

   - В поле **Название** укажите название пространства: от 1 до 128 символов Юникода.
   - В поле **Срок хранения, дней** укажите количество дней, в течение которых события будут храниться в кластере.
   - В разделе **Фильтр** можно задать условия определения событий, которые будут помещаться в это пространство. В раскрывающемся списке можно выбрать существующий ресурс фильтра или выбрать **Создать**, чтобы создать новый фильтр.

     Создание фильтра в ресурсах (см. раздел "Создание фильтра в ресурсах" на стр. 216)

Набор ресурсов для хранилища создан и отображается в разделе **Ресурсы → Хранилища**. Теперь можно создать сервис хранилища (см. раздел "Создание сервиса хранилища в веб-интерфейсе KUMA" на стр. 271).

Создание сервиса хранилища в веб-интерфейсе KUMA

Когда набор ресурсов для агента хранилища (см. раздел "Создание набора ресурсов для хранилища" на стр. 270), можно перейти к созданию сервиса агента в KUMA.

► *Чтобы создать сервис хранилища в веб-интерфейсе KUMA:*

1. В веб-интерфейсе KUMA в разделе **Ресурсы → Активные сервисы** нажмите **Добавить сервис**.
2. В открывшемся окне **Выберите сервис** выберите только что созданный набор ресурсов для хранилища и нажмите **Создать сервис**.

Сервис хранилища создан в веб-интерфейсе KUMA и отображается в разделе **Ресурсы → Активные сервисы**. Теперь сервисы хранилища необходимо установить на каждом узле кластера ClickHouse (см. раздел "Установка хранилища в сетевой инфраструктуре KUMA" на стр. 271), используя идентификатор сервиса (см. раздел "Получение идентификатора сервиса" на стр. 231).

kaspersky

Установка хранилища в сетевой инфраструктуре KUMA

► *Чтобы создать хранилище:*

1. Войдите на сервер, на котором вы хотите установить сервис.
2. Выполните следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma storage --core https://<FQDN сервера Ядра KUMA>:<порт, используемый Ядром KUMA для внутренних коммуникаций (по умолчанию используется порт 7210)> --id <идентификатор сервиса, скопированный из веб-интерфейса KUMA (см. раздел "Получение идентификатора сервиса" на стр. 231)> --install
   ```

   Пример: `sudo /opt/kaspersky/kuma/kuma storage --core https://kuma.example.com:7210 --id XXXXX --install`

   > При развертывании нескольких сервисов KUMA на одном хосте в процессе установки необходимо указать уникальные порты (см. раздел "Настройка сетевого доступа" на стр. 41) для каждого компонента с помощью параметра `--api.port <порт>`. По умолчанию используется значение `--api.port 7221`.

3. Повторите шаги 1–2 для каждого узла хранилища (см. раздел "Подготовка файла инвентаря" на стр. 44).

Хранилище установлено.

kaspersky

Аналитика

KUMA предоставляет обширную аналитику по данным, доступным программе из следующих источников:

- События в хранилище
- Алерты
- Активы
- Учетные записи, импортированные из Active Directory
- Сведения из коллекторов о количестве обработанных событий
- Метрики

Вы можете настроить и получать аналитику в разделах **Панель мониторинга**, **Отчеты**, **Состояние источников** веб-интерфейса KUMA. Для построения аналитики используются только данные из тенантов (см. раздел "О тенантах" на стр. 25), к которым у пользователя есть доступ.

Отображаемый формат даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

В этом разделе

Панель мониторинга 273
Отчеты 278
Состояние источников 285
Виджеты 288

Панель мониторинга

В KUMA можно настроить **Панель мониторинга** для отображения самой свежей информации (*аналитики*) о процессах KUMA. Аналитика создается с помощью *виджетов* (см. раздел "*Виджеты*" на стр. 288), специализированных инструментов, которые могут отображать определенные типы информации. Если виджет отображает данные о событиях (см. раздел "Фильтрация и поиск событий" на стр. 341), алертах (см. раздел "Фильтрация алертов" на стр. 330) или инцидентах (см. раздел "О таблице инцидентов" на стр. 307), при нажатии на его заголовок открывается соответствующий раздел веб-интерфейса KUMA с активным фильтром и/или поисковым запросом, с помощью которых отображаются данные из виджета.

Коллекции виджетов называются *макетами*. Администраторы и аналитики (см. раздел "Роли пользователей" на стр. 57) могут создавать (см. раздел "Создание макета панели мониторинга" на стр. 274), редактировать (см. раздел "Редактирование макета панели мониторинга" на стр. 276) и удалять (см. раздел "Удаление макета панели мониторинга" на стр. 276) макеты. Также макет можно назначить макетом по умолчанию (см. раздел "Выбор макета панели мониторинга в качестве макета по умолчанию" на стр. 275), чтобы он отображался при открытии раздела **Панель мониторинга**.

kaspersky

Информация в разделе **Панель мониторинга** регулярно обновляется в соответствии с настройками макета, но вы можете принудительно обновить данные с помощью кнопки  в верхней части окна. Время последнего обновления отображается рядом с заголовком окна.

Данные, отображаемые на панели мониторинга, зависят от доступных вам тенантов.

Для удобства презентации данных аналитики вы можете включить режим ТВ (см. раздел "Включение и отключение режима ТВ" на стр. 278). Это позволяет скрыть левую панель с разделами интерфейса KUMA и перейти в полноэкранный режим просмотра панели мониторинга в FullHD разрешении. В режиме ТВ вы также можете настроить показ слайд-шоу для выбранных виджетов.

В этом разделе

Создание макета панели мониторинга 274

Выбор макета панели мониторинга 275

Выбор макета панели мониторинга в качестве макета по умолчанию 275

Редактирование макета панели мониторинга 276

Удаление макета панели мониторинга 276

Преднастроенные виджеты 276

Включение и отключение режима ТВ 278

Создание макета панели мониторинга

► *Чтобы создать макет:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.
2. Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и выберите **Создать макет**.

   Откроется окно **Новый макет**.
3. В раскрывающемся списке **Тенанты** выберите тенантов (см. раздел "О тенантах" на стр. 25), которым будет принадлежать создаваемый макет.
4. В раскрывающемся списке **Период** выберите период времени, по которому требуется аналитика:
   - **1 час**
   - **1 день** (это значение выбрано по умолчанию)
   - **7 дней**
   - **30 дней**
   - **В течение периода** – получать аналитику за выбранный период времени. Период времени устанавливается с помощью календаря, который отображается при выборе этого параметра.

     Верхняя граница периода не включается в определяемый с ее помощью отрезок времени. Это означает, что, например, для получения аналитики за сутки следует настроить период День1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

5. В раскрывающемся списке **Обновлять каждые** выберите частоту обновления данных в виджетах макета:
   - **1 минута**
   - **5 минут**
   - **15 минут**
   - **1 час** (это значение выбрано по умолчанию)
   - **24 часа**
6. В раскрывающемся списке **Добавить виджет** выберите требуемый виджет (см. раздел "Виджеты" на стр. 288) и настройте его параметры.

   В макет можно добавить более одного виджета.

   Виджеты также можно перетаскивать по окну и изменять их размер с помощью кнопки , которая появляется при наведении указателя мыши на виджет.

   Добавленные в макет виджеты можно редактировать или удалять, нажав на значок , а затем выбрав требуемое действие: **Изменить** или **Удалить**.
   - Добавление виджетов (см. раздел "Добавление виджета" на стр. 299)
   - Редактирование виджетов (см. раздел "Редактирование виджетов" на стр. 300)
7. В поле **Название макета** введите уникальное имя макета. Должно содержать от 1 до 128 символов Юникода.
8. Нажмите **Сохранить**.

Новый макет создан и отображается в разделе **Панель мониторинга** веб-интерфейса KUMA.

Выбор макета панели мониторинга

► *Чтобы выбрать макет:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.
2. Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и выберите нужный макет.

Выбранный макет отображается в разделе **Панель мониторинга** веб-интерфейса KUMA.

Выбор макета панели мониторинга в качестве макета по умолчанию

► *Чтобы выбрать макет, который будет отображаться на панели мониторинга по умолчанию:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.
2. Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и наведите указатель мыши на требуемый макет.
3. Нажмите на значок .

Выбранный макет теперь является макетом по умолчанию.

Редактирование макета панели мониторинга

► *Чтобы изменить макет:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.
2. Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и наведите указатель мыши на требуемый макет.
3. Нажмите на значок  .
4. Откроется окно **Настройка макета**.
5. Внесите необходимые изменения. Параметры, доступные для изменения, аналогичны параметрам, доступным при создании макета (см. раздел "Создание макета панели мониторинга" на стр. 274).
6. Нажмите **Сохранить**.

Макет изменен и отображается в разделе **Панель мониторинга** веб-интерфейса KUMA.

Если макет был удален или присвоен другому тенанту, пока вы вносили в него изменения, при нажатии на кнопку **Сохранить** отобразится ошибка. Макет сохранен не будет. Перезагрузите страницу веб-браузера, чтобы в раскрывающемся списке в правом верхнем углу просмотреть перечень доступных макетов.

Удаление макета панели мониторинга

► *Чтобы удалить макет:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.
2. Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и наведите указатель мыши на требуемый макет.
3. Нажмите на значок  и подтвердите действие.

Макет удален.

Преднастроенные виджеты

KUMA поставляется с набором преднастроенных макетов с виджетами (см. раздел "Виджеты" на стр. 288):

- Макет Alerts Overview (Обзор алертов):
  - Active Alerts (Активные алерты)
  - Unassigned Alerts (Неназначенные алерты)
  - Alerts distribution (Распределение алертов)

  - Alerts by Assignee (Алерты по исполнителю)
  - Alerts by Status (Алерты по статусу)
  - Alerts count by rule (Количество алертов по правилу)
  - Alerts by Priority (Алерты по уровню важности)
  - Affected Assets (Затронутые активы)
  - Affected Assets Categories (Затронутые категории активов)
  - Affected Users (Затронутые пользователи)
  - Latest Alerts (Последние алерты)
  - Top Log Sources by Alerts count (Топ источников событий по количеству алертов)
  - Top Log Sources by convention rate (Топ источников событий по условному рейтингу)
  - Alerts by tenant (Алерты по тенантам)
- Макет Incidents Overview (Обзор инцидентов):
  - Active incidents (Активные инциденты)
  - Unassigned Incidents (Неназначенные инциденты)
  - Incidents distribution (Распределение инцидентов)
  - Incidents by assignee (Инциденты по исполнителю)
  - Incidents by Status (Инциденты по статусам)
  - Incidents by Priority (Инциденты по уровню важности)
  - Incidents by Tenant (Инциденты по тенантам)
  - Affected Assets in Incidents (Активы в инцидентах)
  - Affected Assets Categories in Incidents (Категории активов в инцидентах)
  - Affected Users in Incidents (Пользователи в инцидентах)
  - Latest Incidents (Последние инциденты)
- Макет Network Overview (Обзор сетевой активности):
  - Top internal IP by Netflow Traffic Volume (BytesIn) (Топ внутренних IP-адресов по полученному netflow-трафику)
  - Top external IP by Netflow Traffic Volume (BytesIn) (Топ внешних IP-адресов по полученному netflow-трафику)
  - Netflow top hosts for remote control (ports 3389, 22, 135) (Топ хостов, на которые были обращения на порты 3389, 22, 135 для удаленного управления)
  - Netflow total bytes by internal ports (Топ внутренних портов по приему netflow-трафика)
  - Top Log Sources by Events count (Топ источников событий)
  - Top Events categories (Топ категорий событий)
  - Assets count (Количество активов)
  - Users count (Количество пользователей)

kaspersky

Включение и отключение режима ТВ

Мы рекомендуем для отображения аналитики в режиме ТВ создать отдельного пользователя (см. раздел "Создание пользователя" на стр. 69) с минимально необходимым набором.

► *Чтобы включить режим ТВ:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.
2. В правом верхнем углу нажмите на кнопку .

   Откроется окно **Параметры**.
3. Переведите переключатель **Режим ТВ** в положение **Включено**.
4. Если вы хотите настроить показ виджетов в режиме слайд-шоу, выполните следующие действия:
   a. Переведите переключатель **Слайд-шоу** в положение **Включено**.
   b. В поле **Время ожидания** укажите, через сколько секунд должно происходить переключение виджетов.
   c. В раскрывающемся списке **Очередь** выберите виджеты для просмотра.
   d. Если требуется, измените порядок показа виджетов, перетаскивая их с помощью кнопки .
5. Нажмите на кнопку **Сохранить**.

Режим ТВ будет включен. Чтобы вернуться к работе с веб-интерфейсом KUMA, нужно отключить режим ТВ.

► *Чтобы отключить режим ТВ:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Панель мониторинга**.
2. В правом верхнем углу нажмите на кнопку .

   Откроется окно **Параметры**.
3. Переведите переключатель **Режим ТВ** в положение **Выключено**.
4. Нажмите на кнопку **Сохранить**.

Режим ТВ будет отключен. В левой части экрана отобразится панель с разделами веб-интерфейса KUMA.

Отчеты

В KUMA можно настроить регулярное формирование отчетов о процессах программы.

Отчеты формируются с помощью *шаблонов отчетов* (см. раздел "*Шаблон отчета*" на стр. 279), которые созданы и хранятся в закладке **Шаблоны** раздела **Отчеты**.

Сформированные отчеты (на стр. 283) хранятся в закладке **Сформированные отчеты** раздела **Отчеты**.

kaspersky

В этом разделе

Шаблон отчета 279
Сформированные отчеты 283

Шаблон отчета

Шаблоны отчетов используются для указания аналитических данных, которые следует включать в отчет, а также для настройки частоты (см. раздел "Настройка расписания отчетов" на стр. 281) создания отчетов. Администраторы и аналитики (см. раздел "Роли пользователей" на стр. 57) могут создавать (см. раздел "Создание шаблона отчета" на стр. 280), редактировать (см. раздел "Изменение шаблона отчета" на стр. 281) и удалять (см. раздел "Удаление шаблона отчета" на стр. 283) шаблоны отчетов. Отчеты, созданные с использованием шаблонов отчетов, отображаются на закладке **Сформированные отчеты**.

Шаблоны отчетов доступны на закладке **Шаблоны** раздела **Отчеты**, где отображается таблица существующих шаблонов. В таблице есть следующие столбцы:

- **Название** – имя шаблона отчетов.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.

  Вы также можете искать шаблоны отчетов, используя поле **Поиск**, которое открывается по нажатию на заголовок столбца **Название**.

- **Период** – период времени, за который извлекается аналитика отчета.
- **Расписание** – периодичность, с которой отчеты должны формироваться по созданным шаблонам. Если расписание отчета не настроено, отображается значение `выключено`.
- **Создал** – имя пользователя, создавшего шаблон отчета.
- **Последнее обновление** – дата последнего обновления шаблона отчета.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.

- **Последний отчет** – дата и время формирования последнего отчета по шаблону отчета.
- **Отправить по электронной почте** – в этом столбце отображается метка напротив шаблонов отчетов, для которых настроено уведомление пользователей по почте о сформированных отчетах.
- **Тенант** – название тенанта, которому принадлежит шаблон отчета.

Вы можете нажать имя шаблона отчета, чтобы открыть раскрывающийся список с доступными командами:

- **Создать отчет** – используйте эту команду, чтобы немедленно сформировать отчет. Созданные отчеты отображаются на закладке **Сформированные отчеты**.
- **Изменить расписание** – используйте эту команду, чтобы настроить расписание для формирования отчетов и определить пользователей, которые должны получать уведомления по электронной почте о сформированных отчетах.
- **Изменить шаблон отчета** – используйте эту команду, чтобы настроить виджеты и период времени, за который должна быть извлечена аналитика.

- **Дублировать шаблон отчета** – используйте эту команду, чтобы создать копию существующего шаблона отчета.
- **Удалить шаблон отчета** – используйте эту команду, чтобы удалить шаблон отчета.

В этом разделе

Создание шаблона отчета 280
Настройка расписания отчетов 281
Изменение шаблона отчета 281
Копирование шаблона отчета 282
Удаление шаблона отчета 283

Создание шаблона отчета

► *Чтобы создать шаблон отчета:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.
2. Нажмите на кнопку **Новый шаблон**.

   Откроется окно **Новый шаблон отчета**.
3. В раскрывающемся списке **Тенанты** выберите тенантов (см. раздел "О тенантах" на стр. 25), которым будет принадлежать создаваемый макет.
4. В раскрывающемся списке **Период** выберите период времени, по которому требуется аналитика:
   - **Сегодня** (это значение выбрано по умолчанию)
   - **На этой неделе**
   - **В этом месяце**
   - **В течение периода** – получать аналитику за выбранный период времени.

     Верхняя граница периода не включается в определяемый с ее помощью отрезок времени. Это означает, что, например, для получения аналитики за сутки следует настроить период День1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.
   - **Другой** – получать аналитику за последние N дней/недель/месяцев/лет.
5. В поле **Срок хранения** укажите, на протяжении какого времени следует хранить сформированные по этому шаблону отчеты.
6. В поле **Название шаблона** введите уникальное название шаблона отчета. Должно содержать от 1 до 128 символов Юникода.
7. В раскрывающемся списке **Добавить виджет** выберите требуемый виджет (см. раздел "Виджеты" на стр. 288) и настройте его параметры.

   В шаблон отчета можно добавить более одного виджета.

   Виджеты также можно перетаскивать по окну и изменять их размер с помощью кнопки  , которая появляется при наведении указателя мыши на виджет.

Добавленные в макет виджеты можно редактировать или удалять, наведя на них указатель мыши, нажав появившийся значок , а затем выбрав требуемое действие: **Изменить** или **Удалить**.

- Добавление виджетов (см. раздел "Добавление виджета" на стр. 299)
- Редактирование виджетов (см. раздел "Редактирование виджетов" на стр. 300)

8. При необходимости можно поменять логотип шаблона отчетов с помощью кнопки **Изменить логотип**.

   Если нажать кнопку **Изменить логотип**, открывается окно загрузки, в котором можно указать файл изображения для логотипа. Изображение должно быть файлом .jpg, .png или .gif размером не более 3 МБ.

   Добавленный логотип будет отображаться в отчете вместо логотипа KUMA.

9. Нажмите **Сохранить**.

Новый шаблон отчета создан и отображается в закладке **Отчеты** → **Шаблоны** веб-интерфейса KUMA. Вы можете сформировать этот отчет вручную. Если вы хотите, чтобы отчеты создавались автоматически, требуется настроить расписание.

Настройка расписания отчетов

► *Чтобы настроить расписания отчетов:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.
2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Изменить расписание**.

   Откроется окно **Параметры отчета**.

3. Если вы хотите, чтобы отчет формировался регулярно:
   a. Включите переключатель **Расписание**.

      В группе настроек **Повторять каждый** задайте периодичность создания отчетов.

   b. В поле **Время** укажите время, когда должен быть сформирован отчет. Вы можете ввести значение вручную или с помощью значка часов.
4. В раскрывающемся списке **Отправить** можно выбрать пользователей, которым следует отправлять по электронной почте ссылки на сформированные отчеты.

   > Чтобы сформированные отчеты можно было отправлять по электронной почте, следует настроить SMTP-соединение (см. раздел "Подключение к SMTP-серверу" на стр. 407).

5. Нажмите **Сохранить**.

Расписание отчетов настроено.

Изменение шаблона отчета

► *Чтобы изменить шаблон отчета:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.

2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Изменить шаблон отчета**.

   Откроется окно **Изменить шаблон отчета**.

   > Это окно также можно открыть на закладке **Отчеты** → **Сформированные отчеты**, нажав имя существующего отчета и выбрав в раскрывающемся списке **Изменить шаблон отчета**.

3. Внесите необходимые изменения:
   - Измените тенантов, которым принадлежит шаблон отчета.
   - Обновите период времени, за который вам требуется аналитика.
   - Добавьте виджеты (см. раздел "Добавление виджета" на стр. 299)
   - Измените расположение виджетов, перетаскивая их.
   - Измените размер виджетов с помощью кнопки , которая появляется при наведении указателя мыши на виджет.
   - Отредактируйте виджеты (см. раздел "Редактирование виджетов" на стр. 300)
   - Удалите виджеты, наведя на них указатель мыши, а затем нажав на появившийся значок и выбрав **Удалить**.
   - В поле справа от раскрывающегося списка **Добавить виджет** введите уникальное имя шаблона отчета. Должно содержать от 1 до 128 символов Юникода.
   - Измените логотип отчета с помощью кнопки **Изменить логотип**.
   - Измените срок хранения отчетов, сформированных по этому шаблону.
4. Нажмите **Сохранить**.

Шаблон отчета изменен и отображается в закладке **Отчеты** → **Шаблоны** веб-интерфейса KUMA.

Копирование шаблона отчета

► *Чтобы создать копию шаблона отчета:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.
2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Дублировать шаблон отчета**.

   Откроется окно **Новый шаблон отчета**. Название виджета изменено на `<Шаблон отчета> - копия`.
3. Внесите необходимые изменения:
   - Измените тенантов, которым принадлежит шаблон отчета.
   - Обновите период времени, за который вам требуется аналитика.
   - Добавьте виджеты (см. раздел "Добавление виджета" на стр. 299)
   - Измените расположение виджетов, перетаскивая их.

- Измените размер виджетов с помощью кнопки , которая появляется при наведении указателя мыши на виджет.
- Отредактируйте виджеты (см. раздел "Редактирование виджетов" на стр. 300)
- Удалите виджеты, наведя на них указатель мыши, а затем нажав на появившийся значок и выбрав **Удалить**.
- В поле справа от раскрывающегося списка **Добавить виджет** введите уникальное имя шаблона отчета. Должно содержать от 1 до 128 символов Юникода.
- Измените логотип отчета с помощью кнопки **Изменить логотип**.

4. Нажмите **Сохранить**.

Шаблон отчета создан и отображается в закладке **Отчеты** → **Шаблоны** веб-интерфейс KUMA.

Удаление шаблона отчета

► *Чтобы удалить шаблон отчета:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.
2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Удалить шаблон отчета**.

   Откроется окно подтверждения.
3. Если вы хотите удалить только шаблон отчета, нажмите кнопку **Удалить**.
4. Если вы хотите удалить шаблон отчета и все отчеты, сформированные с помощью этого шаблона, нажмите **Удалить с отчетами**.

Шаблон отчета удален.

Сформированные отчеты

Все отчеты формируются с помощью шаблонов отчетов (см. раздел "Шаблон отчета" на стр. 279). Сформированные отчеты доступны на закладке **Сформированные отчеты** в разделе **Отчеты** и отображаются в таблице со следующими столбцами:

- **Название** – имя шаблона отчетов.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.
- **Период** – период времени, за который была извлечена аналитика отчета.
- **Последний отчет** – дата и время создания отчета.

  Вы можете отсортировать таблицу по этому столбцу, нажав заголовок и выбрав **По возрастанию** или **По убыванию**.
- **Тенант** – название тенанта, которому принадлежит отчет.

Вы можете нажать на название отчета, чтобы открыть раскрывающийся список с доступными командами:

- **Открыть отчет** – используйте эту команду, чтобы открыть окно данными отчета.
- **Сохранить как HTML** – используйте эту команду, чтобы сохранить отчет в виде HTML-файла.

- **Создать отчет** – используйте эту команду, чтобы немедленно сформировать отчет. Обновите окно браузера, чтобы увидеть вновь созданный отчет в таблице.
- **Изменить шаблон отчета** – используйте эту команду, чтобы настроить виджеты и период времени (см. раздел "Изменение шаблона отчета" на стр. 281), за который должна быть извлечена аналитика.
- **Удалить отчет** – используйте эту команду, чтобы удалить отчет.

В этом разделе

Просмотр отчетов 284

Создание отчетов 284

Сохранение отчетов в формате HTML 285

Удаление отчетов 285

Просмотр отчетов

► *Чтобы просмотреть отчет:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице отчета нажмите имя сформированного отчета и в раскрывающемся списке выберите **Открыть отчет**.

   Откроется новая закладка браузера с виджетами, отображающими аналитику отчетов. Если виджет отображает данные о событиях (см. раздел "Фильтрация и поиск событий" на стр. 341), алертах (см. раздел "Фильтрация алертов" на стр. 330) или инцидентах (см. раздел "О таблице инцидентов" на стр. 307), при нажатии на его заголовок открывается соответствующий раздел веб-интерфейса KUMA с активным фильтром и/или поисковым запросом, с помощью которых отображаются данные из виджета.
3. Отчет можно сохранить в html-файл с помощью кнопки **Сохранить как HTML**.

Создание отчетов

Вы можете создать отчет вручную или настроить расписание, чтобы отчеты создавались автоматически.

► *Чтобы создать отчет вручную:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Шаблоны**.
2. В таблице шаблонов отчета нажмите имя шаблона отчета и в раскрывающемся списке выберите **Создать отчет**.

   > Отчет также можно создать на закладке **Отчеты** → **Сформированные отчеты**, нажав имя существующего отчета и выбрав в раскрывающемся списке **Создать отчет**.

   Отчет создается и помещается на закладку **Отчеты** → **Сформированные отчеты**.

► *Чтобы создавать отчеты автоматически,*

настройте расписание отчетов (см. раздел "Настройка расписания отчетов" на стр. 281).

Сохранение отчетов в формате HTML

► *Чтобы сохранить отчет в формате HTML:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице отчета нажмите имя сформированного отчета и в раскрывающемся списке выберите **Сохранить как HTML**.

Отчет сохраняется в виде HTML-файла используя настройки вашего браузера.

Удаление отчетов

► *Чтобы удалить отчет:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Отчеты** → **Сформированные отчеты**.
2. В таблице отчета нажмите имя сформированного отчета и в раскрывающемся списке выберите **Удалить отчет**.

   Откроется окно подтверждения.
3. Нажмите **ОК**.

Состояние источников

В KUMA можно контролировать состояние источников, из которых поступают данные в коллекторы (см. раздел "Коллектор" на стр. 20). На одном сервере может быть несколько источников событий (см. раздел "О событиях" на стр. 25), а данные из нескольких источников могут поступать в один коллектор. Источники событий идентифицируются по следующим полям событий (см. раздел "Модель данных нормализованного события" на стр. 471) (данные в этих полях регистрозависимые):

- DeviceProduct
- DeviceAddress или DeviceHostName

Списки источников формируются в коллекторах, объединяются в Ядре KUMA и отображаются в веб-интерфейсе программы в разделе **Состояние источников** в закладке **Список источников событий** (на стр. 286). Данные обновляются ежеминутно.

Данные о частоте и количестве поступающих событий являются важным показателем состояния наблюдаемой системы. Вы можете настроить политики мониторинга, чтобы изменения отслеживались автоматически и при достижении индикаторами определенных граничных значений автоматически создавались уведомления. Политики мониторинга отображаются в веб-интерфейсе KUMA в разделе **Состояние источников** в закладке **Политики мониторинга** (на стр. 287).

При срабатывании политик мониторинга создаются события мониторинга с данными об источнике событий.

kaspersky

В этом разделе

Список источников событий 286
Политики мониторинга 287

Список источников событий

Источники событий отображаются в таблице в разделе **Состояние источников → Список источников событий**. На одной странице отображается до 250 источников. Таблицу можно сортировать, нажимая на заголовок столбца нужного параметра. Источники событий можно искать с помощью поля **Поиск**. При нажатии на источник событий открывается график поступления данных.

При необходимости вы можете настроить период обновления данных в таблице. Доступные периоды обновления: **1 минута**, **5 минут**, **15 минут**, **1 час**. По умолчанию указано значение: **Не обновлять**. Настройка периода обновления может потребоваться для отслеживания изменений в списке источников.

Доступны следующие столбцы:

- **Статус** – статус источника:
  - зеленый – события поступают в пределах присвоенной политики мониторинга;
  - красный – частота или количество поступающих событий выходит за границы, определенные в политике мониторинга;
  - серый – источнику событий не присвоена политика мониторинга.

  Таблицу можно фильтровать по этому параметру.
- **Название** – название источника события. Название формируется автоматически из следующих полей событий:
  - DeviceProduct;
  - DeviceAddress и/или DeviceHostname;
  - DeviceProcessName;
  - Tenant.

  Вы можете изменить название источника событий.
- **Имя хоста или IP-адрес** – название хоста или IP-адрес, откуда поступают события.
- **Политика мониторинга** – название политики мониторинга, назначенной источнику событий.
- **Поток** – частота, с которой из источника поступают события.
- **Нижний порог** – нижняя граница допустимого количества поступающих событий, указанная в политике мониторинга.
- **Верхний порог** – верхняя граница допустимого количества поступающих событий, указанная в политике мониторинга.
- **Тенант** – тенант, к которому относятся события, поступающие из источника.

Если выбрать источники событий, становятся доступны следующие кнопки:

- **Сохранить в CSV** – с помощью этой кнопки можно выгрузить данные выбранных источников событий в файл с названием event-source-list.csv в кодировке UTF-8.
- **Включить политику** и **Выключить политику** – с помощью этих кнопок для источников событий можно включить или выключить политику мониторинга. При включении требуется выбрать политику в раскрывающемся списке. При выключении требуется указать, на какой период необходимо отключить политику: временно или навсегда.

  В редких случаях из-за наложения внутренних процессов KUMA через несколько секунд после выключения политики ее статус может снова измениться с серого на зеленый. В таких случаях необходимо повторно выключить политику мониторинга.

- **Удалить источник событий** – с помощью этой кнопки источники событий можно удалить из таблицы. Статистика по этому источнику также будет удалена. Если данные из источника продолжают поступать в коллектор, источник событий снова появится в таблице, при этом его старая статистика учитываться не будет.

Политики мониторинга

Политики мониторинга источников событий отображаются в таблице в разделе **Состояние источников** → **Политики мониторинга**. Таблицу можно сортировать, нажимая на заголовок столбца нужного параметра. При нажатии на политику открывается область данных с ее параметрами, которые можно изменить.

Доступны следующие столбцы:

- **Название** – название политики мониторинга.
- **Нижний порог** – нижняя граница допустимого количества поступающих событий, указанная в политике мониторинга.
- **Верхний порог** – верхняя граница допустимого количества поступающих событий, указанная в политике мониторинга.
- **Интервал** – период, который учитывается политикой мониторинга.
- **Тип** – тип политики мониторинга:
  - **byCount** – политикой мониторинга отслеживается количество поступающих событий.
  - **byEPS** – политикой мониторинга отслеживается частота поступающих событий.
- **Тенант** – тенант, к которому относится политика мониторинга.

► *Чтобы добавить политику мониторинга:*

1. В веб-интерфейсе KUMA в разделе **Состояние источников** → **Политики мониторинга** нажмите **Добавить политику** и в открывшемся окне укажите параметры:
   - В поле **Название политики** введите уникальное имя создаваемой политики. Название должно содержать от 1 до 128 символов Юникода.
   - В раскрывающемся списке **Тенант** выберите тенант (см. раздел "О тенантах" на стр. 25), которому будет принадлежать политика. От выбора тенанта зависит, для каких источников событий можно будет включить политику мониторинга.
   - В раскрывающемся списке **Тип политики** выберите, как будут отслеживаться поступающие события: по частоте или по количеству.

- В поле **Нижний порог** и **Верхний порог** определите, выход за какие границы будет считаться отклонением от нормы, при котором будет политика мониторинга будет срабатывать, создавая алерт и рассылая уведомления.
- В поле **Период подсчета** укажите, за какой период в политике мониторинга должны учитываться данные из источника мониторинга. Максимальное значение: 14 дней.
- При необходимости укажите с помощью кнопки **Адрес электронной почты** электронные адреса, на которые следует отправить уведомления о срабатывании политики мониторинга KUMA.

  Для рассылки уведомлений необходимо настроить подключение к SMTP-серверу (на стр. 407).

2. Нажмите **Добавить**.

Политика мониторинга добавлена.

► *Чтобы удалить политику мониторинга,*

Выберите нужную политику, нажмите **Удалить политику** и подтвердите действие.

Невозможно удалить предустановленные политики мониторинга, а также политики, назначенные источникам данных.

Виджеты

Виджеты в KUMA используются для получения аналитики для панели мониторинга (см. раздел "Панель мониторинга" на стр. 273) и отчетов (см. раздел "Отчеты" на стр. 278).

При нажатии на заголовки или легенду виджетов о событиях (см. раздел "Фильтрация и поиск событий" на стр. 341), алертах (см. раздел "Фильтрация алертов" на стр. 330) или инцидентах (см. раздел "О таблице инцидентов" на стр. 307) открывается соответствующий раздел веб-интерфейса KUMA с данными из виджета, полученными с помощью фильтров раздела и/или поисковым запросом. Подробнее см. ниже. Этот функционал недоступен в режиме создания и редактирования макетов.

Если в виджете настроено деление периода, по которому строится аналитика, на отрезки, то значения или графики будут отображаться парами: аналитика за текущий отрезок периода (пользовательский цвет) и аналитика за предыдущий отрезок периода (серый цвет).

Виджеты организованы в группы, каждая из которых связана с типом аналитики, которую она предоставляет. В KUMA доступны следующие группы виджетов и виджеты:

- **События** (см. раздел "**Настраиваемая аналитика по событиям**" на стр. 293) – виджет для создания аналитики на основе событий.

  При нажатии на заголовок этого виджета можно перейти в раздел **События** веб-интерфейса KUMA. При этом для запроса событий из виджета применяется SQL-запрос (см. раздел "Фильтрация и поиск событий" на стр. 341), указанный в виджете. Запрос указывается без группировки (за исключением табличных графиков), но с учетом условий, указанных в параметре WHERE. Параметр LIMIT в запросе принимается равным 250.
- **Активные листы** (см. раздел "**Настраиваемая аналитика по активным листам**" на стр. 297) – виджет для создания аналитики на основе активных листов корреляторов.

При нажатии на заголовок этого виджета можно перейти в раздел активного листа, по которому строится аналитика виджета.

- Алерты – группа для аналитики об алертах. При нажатии на заголовок или легенду виджетов этой группы можно перейти в раздел **Алерты** веб-интерфейса KUMA для подробного просмотра данных из виджета.

  В группу входят следующие виджеты:

  - **Активные алерты** – количество незакрытых алертов.
  - **Активные алерты по тенантам** – количество незакрытых алертов, сгруппированных по тенантам.
  - **Алерты по тенантам** – количество алертов всех статусов, сгруппированных по тенантам.
  - **Неназначенные алерты** – количество алертов со статусом **Новый**.
  - **Алерты по исполнителю** – количество назначенных алертов, сгруппированных по исполнителю.
  - **Алерты по статусу** – количество алертов, сгруппированных по статусу.
  - **Алерты по уровню важности** – количество незакрытых алертов, сгруппированных по уровню важности.
  - **Алерты по правилу корреляции** – количество незакрытых алертов, сгруппированных по правилам корреляции. Для этого виджета недоступны подробные сведения по нажатию на заголовок виджета.
  - **Последние алерты** – таблица, содержащая последние 10 незакрытых алертов.
  - **Распределение алертов** – количество алертов, созданных в течение указанного в виджете периода.

- Активы – группа для аналитики об активах из обработанных событий. В эту группу входят следующие виджеты:

  - **Затронутые активы** – таблица связанных с алертами активов, в которой указан уровень важности актива и количество незакрытых алертов, с которыми он связан.
  - **Категории затронутых активов** – категории активов, привязанных к незакрытым алертам.
  - **Количество активов** – количество активов, добавленных в KUMA.
  - **Активы в инцидентах по тенантам** – количество активов в незакрытых инцидентах, сгруппированных по тенантам.
  - **Активы в алертах по тенантам** – количество активов в незакрытых алертах, сгруппированных по тенантам.

- Инциденты – группа для аналитики об инцидентах. При нажатии на заголовок или легенду виджетов этой группы можно перейти в раздел **Инциденты** веб-интерфейса KUMA для подробного просмотра данных из виджета.

  В группу входят следующие виджеты:

  - **Активные инциденты** – количество незакрытых инцидентов.
  - **Неназначенные инциденты** – количество инцидентов со статусом **Открыт**.
  - **Распределение инцидентов** – количество инцидентов, созданных в течение указанного в виджете периода.

- **Инциденты по исполнителю** – количество инцидентов со статусом **Назначен**, сгруппированных по пользователям KUMA.
- **Инциденты по статусам** – количество инцидентов, сгруппированных по статусам.
- **Инциденты по уровню важности** – количество незакрытых инцидентов, сгруппированных по уровню важности. Доступные типы диаграмм: круговая, столбчатая.
- **Активные инциденты по тенантам** – количество незакрытых инцидентов, сгруппированных по тенантам, доступным пользователю.
- **Все инциденты** – количество инцидентов всех статусов.
- **Все инциденты по тенантам** – количество инцидентов всех статусов, сгруппированных по тенантам.
- **Активы в инцидентах** – количество активов в незакрытых инцидентах. Для этого виджета недоступны подробные сведения по нажатию на заголовок виджета.
- **Категории активов в инцидентах** – категории активов, которые затронуты незакрытыми инцидентами. Доступные типы диаграмм: круговая, столбчатая. Для этого виджета недоступны подробные сведения по нажатию на заголовок виджета.
- **Пользователи в инцидентах** – пользователи, затронутые в инцидентах. Доступные типы диаграмм: таблица, круговая, столбчатая. Для этого виджета недоступны подробные сведения по нажатию на заголовок виджета.
- **Последние инциденты** – последние 10 незакрытых инцидентов.

- Источники событий – группа для аналитики об источниках событий. В группу входят следующие виджеты:
  - **Топ источников событий по количеству алертов** – количество незакрытых алертов, сгруппированных по источникам событий.
  - **Топ источников событий по условному рейтингу** – количество событий, для которых существует незакрытый алерт, сгруппированных по источникам событий.

    В связи с оптимизациями хранения событий в алертах в ряде случаев количество алертов созданных источниками может быть искажено. Для получения точной статистики рекомендуется в правиле корреляции указать поле события Device Product в качестве уникального, а также включить хранение всех базовых событий в корреляционном событии. Правила корреляции с такими настройками являются более ресурсоемкими.

- Пользователи – группа для аналитики о пользователях из обработанных событий. В группу входят следующие виджеты:
  - **Пользователи в алертах** – количество пользователей, связанных с незакрытыми алертами.
  - **Количество пользователей AD** – количество учетных записей в Active Directory, полученных по LDAP в течение указанного в виджете периода.

kaspersky

В этом разделе

Стандартные виджеты 291
Настраиваемая аналитика по событиям 293
Настраиваемая аналитика по активным листам 297
Добавление виджета 299
Редактирование виджетов 300

Стандартные виджеты

В этом разделе описываются параметры всех виджетов, кроме виджета События (см. раздел "Настраиваемая аналитика по событиям" на стр. 293) и Активные листы (см. раздел "Настраиваемая аналитика по активным листам" на стр. 297).

Доступные параметры виджетов зависят от выбранного типа виджета. Тип виджета определяется по значку:

-  – круговая диаграмма
-  – счетчик
-  – таблица
-  и  – столбчатая диаграмма

Параметры круговых диаграмм, счетчиков и таблиц

Параметры круговых диаграмм, счетчиков и таблиц располагается на одной закладке. Набор параметров зависит от выбранного виджета:

- **Название** – поле для названия виджета. Должно содержать от 1 до 128 символов Юникода.
- **Описание** – поле для описания виджета. Вы можете добавить до 4000 символов Юникода, описывающих виджет.
- **Тенант** – раскрывающийся список для выбора тенанта, по данным которого будет отображаться аналитика. По умолчанию используется параметр **Как на макете**.
- **Период** – раскрывающийся список для настройки периода времени, за который должна отображаться аналитика. Доступные варианты:
  - **Как на макете** – когда выбран этот параметр, значение периода времени виджета отражает период, который был настроен для макета. Этот вариант выбран по умолчанию.
  - **1 час** – получить аналитику за предыдущий час.
  - **1 день** – получить аналитику за предыдущий день.
  - **7 дней** – получить аналитику за предыдущие 7 дней.
  - **30 дней** – получить аналитику за предыдущие 30 дней.
  - **В течение периода** – получать аналитику за выбранный период времени. Период времени устанавливается с помощью календаря, который отображается при выборе этого параметра.

> Верхняя граница периода не включается в определяемый с ее помощью отрезок времени. Это означает, что, например, для получения аналитики за сутки следует настроить период День1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.

- **Хранилище** – раскрывающийся список для выбора хранилища, события которого будут использоваться для создания аналитики.
- **Цвет** – раскрывающийся список для выбора цвета отображения информации:
  - **по умолчанию** – использовать цвет шрифта, который используется в вашем браузере по умолчанию;
  - **зеленый**;
  - **красный**;
  - **синий**;
  - **желтый**.
- **Горизонтальный** – включите этот переключатель, если хотите использовать горизонтальную гистограмму вместо вертикальной. По умолчанию этот переключатель выключен.
- **Легенда** – выключите этот переключатель, если не хотите, чтобы в виджете отображалась легенда для аналитики. По умолчанию этот переключатель включен.
- **Пустые значения в легенде** – включите этот переключатель, если хотите, чтобы в легенде для аналитики отображались параметры с нулевыми значениями. По умолчанию этот переключатель выключен.
- **Десятичные знаки** – это поле используется, чтобы указать степень округления значений. Значение по умолчанию: **Авто**.

Параметры столбчатых диаграмм

Параметры столбчатых диаграмм располагаются в двух закладках. Набор параметров зависит от выбранного виджета:

- – закладка предназначена для настройки масштаба графика. Доступные параметры:
  - Поля **Минимальное значение Y** и **Максимальное значение Y** используются для определения масштаба оси Y. Поле **Десятичные знаки** слева используется для установки параметра округления для значений оси Y.
  - Поля **Минимальное значение X** и **Максимальное значение X** используются для определения масштаба оси X. Поле **Десятичные знаки** справа используется для установки параметра округления для значений оси X.

  > На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

- – закладка предназначена для настройки отображения аналитики виджета.
  - **Название** – поле для названия виджета. Должно содержать от 1 до 128 символов Юникода.
  - **Описание** – поле для описания виджета. Вы можете добавить до 512 символов Юникода, описывающих виджет.

- **Тенант** – раскрывающийся список для выбора тенанта, по данным которого будет отображаться аналитика.
- **Период** – раскрывающийся список для настройки периода времени, за который должна отображаться аналитика. Доступные варианты:
  - **Как на макете** – когда выбран этот параметр, значение периода времени виджета отражает период, который был настроен для макета. Этот вариант выбран по умолчанию.
  - **1 час** – получить аналитику за предыдущий час.
  - **1 день** – получить аналитику за предыдущий день.
  - **7 дней** – получить аналитику за предыдущие 7 дней.
  - **30 дней** – получить аналитику за предыдущие 30 дней.
  - **В течение периода** – получать аналитику за выбранный период времени. Период времени устанавливается с помощью календаря, который отображается при выборе этого параметра.
- **Хранилище** – раскрывающийся список для выбора хранилища, события которого будут использоваться для создания аналитики.
- **Цвет** – раскрывающийся список для выбора цвета отображения информации:
  - **по умолчанию** – использовать цвет шрифта, который используется в вашем браузере по умолчанию.
  - **зеленый**
  - **красный**
  - **синий**
  - **желтый**
- **Горизонтальный** – включите этот переключатель, если хотите использовать горизонтальную гистограмму вместо вертикальной. По умолчанию этот переключатель выключен.
- **Легенда** – выключите этот переключатель, если не хотите, чтобы в виджете отображалась легенда для аналитики. По умолчанию этот переключатель включен.
- **Пустые значения в легенде** – включите этот переключатель, если хотите, чтобы в легенде для аналитики отображались параметры с нулевыми значениями. По умолчанию этот переключатель выключен.
- **Десятичные знаки** – это поле используется, чтобы указать степень округления значений. Значение по умолчанию: **Авто**.

Настраиваемая аналитика по событиям

Вы можете использовать виджет **События** для получения необходимой аналитики на основе SQL-запросов по событиям. В зависимости от выбранного значения типа графика доступны две или три закладки параметров:

-  – эта закладка используется для определения типа виджета и построения поиска для аналитики.

- – закладка предназначена для настройки масштаба графика. Эта закладка доступна только для типов графиков (см. ниже) **Столбчатая диаграмма**, **Линейная диаграмма**, **Календарная диаграмма**.
- – закладка предназначена для настройки отображения аналитики виджета.

Следующие параметры доступны для закладки :

- **График** – этот раскрывающийся список используется для выбора типа графика виджета. Доступные варианты:
  - **Круговая диаграмма**
  - **Столбчатая диаграмма**
  - **Счетчик**
  - **Линейная диаграмма**
  - **Таблица**
  - **Календарная диаграмма**
- **Тенант** – раскрывающийся список для выбора тенанта, по данным которого будет отображаться аналитика. По умолчанию используется параметр **Как на макете**.
- **Период** – раскрывающийся список для настройки периода времени, за который должна отображаться аналитика. Доступные варианты:
  - **Как на макете** – когда выбран этот параметр, значение периода времени виджета отражает период, который был настроен для макета. Этот вариант выбран по умолчанию.
  - **1 час** – получить аналитику за предыдущий час.
  - **1 день** – получить аналитику за предыдущий день.
  - **7 дней** – получить аналитику за предыдущие 7 дней.
  - **30 дней** – получить аналитику за предыдущие 30 дней.
  - **В течение периода** – получать аналитику за выбранный период времени. Период времени устанавливается с помощью календаря, который отображается при выборе этого параметра.

    Верхняя граница периода не включается в определяемый с ее помощью отрезок времени. Это означает, что, например, для получения аналитики за сутки следует настроить период День1, 00:00:00 – День 2, 00:00:00, а не День 1, 00:00:00 – День 1, 23:59:59.
- **Показывать данные за предыдущий период** – переключатель, с помощью которого в виджете можно включить отображение данных сразу за два периода: за текущий и за предыдущий. Это может быть полезно для оценки динамики изменений.
- **Хранилище** – хранилище, в котором должен выполняться поиск.
- Поле SQL-запроса – в этом можно ввести поисковый запрос, аналогичный фильтрации событий с использованием синтаксиса SQL.

  Для виджетов **События** с помощью кнопки можно открыть конструктор запросов, аналогичный параметрам конструктора фильтра событий:

  Описание параметров конструктора запросов (см. раздел "Пользовательский виджет - конструктор запросов" на стр. 296)

Пример условий поиска в конструкторе запросов (см. раздел "Пользовательский виджет - пример" на стр. 297)

Следующие параметры доступны для закладки  :

- Поля **Минимальное значение Y** и **Максимальное значение Y** используются для определения масштаба оси Y. Поле **Десятичные знаки** слева используется для установки параметра округления для значений оси Y.
- Поля **Минимальное значение X** и **Максимальное значение X** используются для определения масштаба оси X. Поле **Десятичные знаки** справа используется для установки параметра округления для значений оси X.

  На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

- Поля **Толщина линии** и **Размер указателя** отображаются для типа графика **Линейная диаграмма** и используются для настройки отображения графика.

Следующие параметры доступны для закладки  :

- **Название** – поле для названия виджета. Должно содержать от 1 до 128 символов Юникода.
- **Описание** – поле для описания виджета. Вы можете добавить до 512 символов Юникода, описывающих виджет.
- **Цвет** – раскрывающийся список для выбора цвета отображения информации:
  - **по умолчанию** – использовать цвет шрифта, который используется в вашем браузере по умолчанию;
  - **зеленый**;
  - **красный**;
  - **синий**;
  - **желтый**.
- **Горизонтальный** – включите этот переключатель, если хотите использовать горизонтальную гистограмму вместо вертикальной. По умолчанию этот переключатель выключен.
- **Легенда** – выключите этот переключатель, если не хотите, чтобы в виджете отображалась легенда для аналитики. По умолчанию этот переключатель включен.
- **Пустые значения в легенде** – включите этот переключатель, если хотите, чтобы в легенде для аналитики отображались параметры с нулевыми значениями. По умолчанию этот переключатель выключен.
- **Десятичные знаки** – поле для ввода количества десятичных знаков, до которых отображаемое значение должно быть округлено. Значение по умолчанию: **авто**.
- **Длительность отрезков периода** (доступно для типов графика **Календарная диаграмма**) – раскрывающийся список для выбора длительности отрезков, на которые требуется делить период.

Пользовательский виджет - конструктор запросов

- **SELECT** – используйте эти поля для определения полей событий, которые необходимо извлечь для аналитики. Количество доступных полей зависит от выбранного типа графика виджета (см. выше).

  В левом выпадающем списке вы можете выбрать поля событий из необходимых для аналитики.

  Среднее поле показывает, для чего выбранное поле используется в виджете: **metric** (метрики) или **value** (значение).

  > При выборе типа виджета **Таблица** значения в средних полях становятся доступны для редактирования и отображаются в виде названий столбцов. В качестве значений доступны только символы ANSII-ASCII.

  В правом раскрывающемся списке вы можете выбрать, как должны обрабатываться значения поля события типа **metric** (метрики) для виджета:

  - **count** – выберите этот вариант для подсчета событий. Эта опция доступна только для поля события ID.
  - **max** – выберите этот параметр, чтобы отобразить максимальное значение поля события из выборки событий.
  - **min** – выберите этот параметр, чтобы отображать минимальное значение поля события из выборки событий.
  - **avg** – выберите эту опцию, чтобы отображать среднее значение поля события из выборки событий.
  - **sum** – выберите этот параметр, чтобы отобразить сумму значений полей событий из выборки событий.
- **SOURCE** – этот раскрывающийся список используется для выбора типа источника данных. Для выбора доступна только опция **events** (события).
- **WHERE** – эта группа настроек используется для создания условий поиска:

  В левом раскрывающемся списке вы можете выбрать поле события, которое хотите использовать в качестве фильтра.

  В среднем выпадающем списке вы можете выбрать нужного оператора. Доступные операторы различаются в зависимости от типа значения выбранного поля события.

  Справа вы можете выбрать или ввести значение поля события. В зависимости от выбранного типа значения поля события может потребоваться ввести значение вручную, выбрать его в раскрывающемся списке или выбрать в календаре.

  Вы можете добавить условия поиска с помощью кнопки **Добавить условие** или удалить их с помощью кнопки со значком крестика.

  Вы также можете добавить группы условий, используя кнопку **Добавить группу**. По умолчанию группы условий добавляются с оператором **AND**, однако если на него нажать, оператор можно поменять. Доступные значения: **AND**, **OR**, **NOT**. Группы условий удаляются с помощью кнопки **Удалить группу**.
- **GROUP BY** – этот раскрывающийся список используется для выбора полей событий, по которым осуществляется группировка событий. Этот параметр недоступен для типа графиков **Счетчик**.

- **ORDER BY** – этот раскрывающийся список используется для определения способа сортировки информации из результатов поиска в виджете. Этот параметр недоступен для типов графиков **Календарная диаграмма** и **Счетчик**.

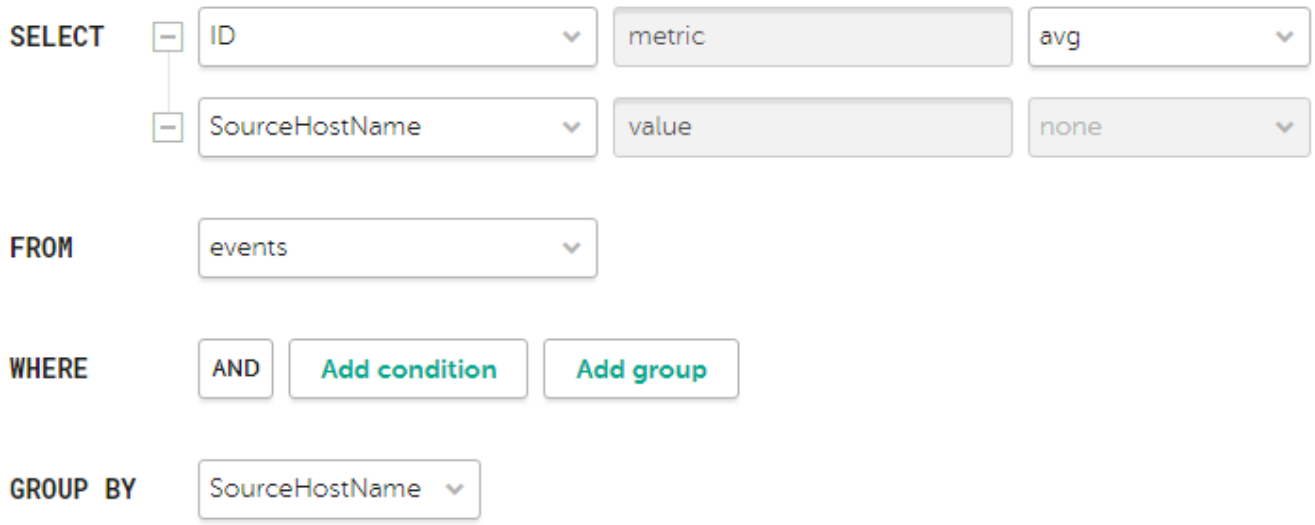
  В левом раскрывающемся списке вы можете выбрать значение, метрику или поле события, которое будет использоваться для сортировки.

  В правом раскрывающемся списке можно выбрать порядок сортировки: **ASC** – для сортировки по возрастанию, **DESC** – для сортировки по убыванию.

  Для графиков типа **Таблица** можно добавить условия сортировки с помощью кнопки **Добавить столбец**.

- **LIMIT** – это поле используется для установки максимального количества точек данных для виджета. Этот параметр недоступен для типов графиков **Календарная диаграмма** и **Счетчик**.

Пользовательский виджет - пример



Настраиваемая аналитика по активным листам

Вы можете использовать виджеты **Активные листы** для получения необходимой аналитики на основе SQL-запросов активным листам (см. раздел "Активные листы" на стр. 224). В зависимости от выбранного значения типа графика доступны две или три закладки параметров:

- – эта закладка используется для определения типа виджета и построения поиска для аналитики.
- – закладка предназначена для настройки масштаба графика. Эта закладка доступна только для типов графиков (см. ниже) **Столбчатая диаграмма**.
- – закладка предназначена для настройки отображения аналитики виджета.

Следующие параметры доступны для закладки  :

- **График** – этот раскрывающийся список используется для выбора типа графика виджета. Доступные варианты:
  - **Круговая диаграмма**
  - **Столбчатая диаграмма**
  - **Счетчик**
  - **Таблица**
- **Тенант** – раскрывающийся список для выбора тенанта, по данным которого будет отображаться аналитика. По умолчанию используется параметр **Как на макете**.
- **Коррелятор** – название сервиса коррелятор, по активному листу которого требуется аналитика.
- **Активный лист** – название активного листа, в котором должен выполняться поиск.

  Один и тот же ресурс активного листа может быть использован разными сервисами корреляторов, однако при этом для каждого коррелятора создается своя сущность активного листа. Таким образом, содержимое активных листов, используемых разными корреляторами, различается, даже если идентификатор и название активных листов одинаковые.

- Поле SQL-запроса – в этом можно ввести поисковый запрос, аналогичный поиску событий (см. раздел "Создание SQL-запроса вручную" на стр. 345) с использованием синтаксиса SQL.

  В отличие от поиска по событиям, в поисковых запросах по активным листам параметру **FROM** должно соответствовать значение `` `records` ``.

  Для запросов доступны служебные поля `_key` (поле с ключами записей активного листа) и `_count` (сколько раз эта запись была добавлена в активный лист), а также пользовательские поля.

  Примеры:

  - `SELECT count(_key) AS metric, Status AS value FROM `records` GROUP BY value ORDER BY metric DESC LIMIT 250` – Запрос для круговой диаграммы, который возвращает количество ключей активного листа (агрегация `count` по полю `_key`) и все варианты значений пользовательского поля `Status`. В виджете отображается круговая диаграмма с общим количеством записей активного листа, пропорционально разделенным на количество вариантов значений поля `Status`.
  - `SELECT Name, Status, _count AS Number FROM `records` WHERE Description ILIKE '%ftp%' ORDER BY Name DESC LIMIT 250` – Запрос для таблицы, которая возвращает значения пользовательских полей `Name` и `Status`, а также служебного поля `_count` у тех записей активного листа, в которых значения пользовательского поля `Description` соответствует запросу `ILIKE '%ftp%'`. В виджете отображается таблица со столбцами Status, Name и Number.

Следующие параметры доступны для закладки  :

- Поля **Минимальное значение Y** и **Максимальное значение Y** используются для определения масштаба оси Y. Поле **Десятичные знаки** слева используется для установки параметра округления для значений оси Y.

- Поля **Минимальное значение X** и **Максимальное значение X** используются для определения масштаба оси X. Поле **Десятичные знаки** справа используется для установки параметра округления для значений оси X.

  > На осях графиков могут отображаться отрицательные значения. Это связано с масштабированием графиков на виджете и может быть исправлено выставлением нуля в качестве минимальных значений графиков вместо **Авто**.

Следующие параметры доступны для закладки :

- **Название** – поле для названия виджета. Должно содержать от 1 до 128 символов Юникода.
- **Описание** – поле для описания виджета. Вы можете добавить до 512 символов Юникода, описывающих виджет.
- **Цвет** – раскрывающийся список для выбора цвета отображения информации:
  - **по умолчанию** – использовать цвет шрифта, который используется в вашем браузере по умолчанию.
  - **зеленый**
  - **красный**
  - **синий**
  - **желтый**
- **Горизонтальный** – включите этот переключатель, если хотите использовать горизонтальную гистограмму вместо вертикальной. По умолчанию этот переключатель выключен.
- **Легенда** – выключите этот переключатель, если не хотите, чтобы в виджете отображалась легенда для аналитики. По умолчанию этот переключатель включен.
- **Пустые значения в легенде** – включите этот переключатель, если хотите, чтобы в легенде для аналитики отображались параметры с нулевыми значениями. По умолчанию этот переключатель выключен.
- **Десятичные знаки** – поле для ввода количества десятичных знаков, до которых отображаемое значение должно быть округлено. Значение по умолчанию: **авто**.

kaspersky

Добавление виджета

► *Чтобы добавить виджет:*

1. В раскрывающемся списке **Добавить виджет** выберите требуемый виджет.

   Откроется окно с параметрами виджета. С помощью кнопки **Предварительный просмотр** можно увидеть, как будет выглядеть настраиваемый виджет на макете.

2. Настройте параметры виджета и нажмите **Добавить**.

Редактирование виджетов

► *Чтобы отредактировать виджет:*

1. Наведите указатель мыши на нужный виджет и нажмите на появляющийся значок  .
2. В раскрывающемся списке выберите значение **Изменить**.

   Откроется окно с параметрами виджета. С помощью кнопки **Предварительный просмотр** можно увидеть, как будет выглядеть настраиваемый виджет на макете.

3. Измените параметры виджета и нажмите **Сохранить**.

kaspersky

Работа с тенантами

Доступ к тенантам (см. раздел "О тенантах" на стр. 25) регулируется в настройках пользователей. *Главный администратор* (см. раздел "*Роли пользователей*" на стр. 57) имеет доступ к данным всех тенантов. Только пользователь с этой ролью может создавать и выключать тенанты.

Тенанты отображаются в таблице раздела веб-интерфейса KUMA **Параметры** → **Тенанты**. Нажимая на столбцы, таблицу можно отсортировать.

Доступные столбцы:

- **Название** – название тенанта. Таблицу можно фильтровать по этому столбцу.
- **Ограничение EPS** – размер квоты EPS (частота обработки событий в секунду), выделенной тенанту из общей квоты EPS, которая определяется лицензией.
- **Описание** – описание тенанта.
- **Выключено** – отметка о том, является ли тенант неактивным.

  По умолчанию неактивные тенанты в таблице не отображаются. Вы можете их просмотреть, установив флажок **Показать выключенных**.
- **Создан** – дата создания тенанта.

► *Чтобы создать тенант:*

1. В разделе веб-интерфейса KUMA **Параметры** → **Тенанты** нажмите **Добавить**.

   Откроется окно **Добавить тенант**.
2. В поле **Название** укажите название тенанта. Название должно содержать от 1 до 128 символов Юникода.
3. В поле **Ограничение EPS** укажите квоту EPS для тенанта. Сумма EPS всех тенантов не может превышать EPS лицензии.
4. При необходимости добавьте **Описание** тенанта. Описание должно содержать не более 256 символов Юникода.
5. Нажмите **Сохранить**.

Тенант добавлен и отображается в таблице тенантов.

► *Чтобы выключить или включить тенант:*

1. В разделе веб-интерфейса KUMA **Параметры** → **Тенанты** выберите нужный тенант.

   Если тенант выключен и не отображается в таблице, установите флажок **Показать выключенных**.
2. Нажмите **Выключить** или **Включить**.

При выключении тенанта принадлежащие ему сервисы автоматически останавливаются, прием и обработка событий прекращается, EPS тенанта более не учитывается в общем количестве EPS лицензии.

При включении тенанта его сервисы требуется запустить вручную.

kaspersky

В этом разделе

Выбор тенанта 302
Правила принадлежности к тенантам 302

Выбор тенанта

Если вы имеете доступ к нескольким тенантам (см. раздел "О тенантах" на стр. 25), в KUMA можно выбрать, данные каких тенантов будут отображаться в веб-интерфейсе KUMA.

► *Чтобы выбрать тенант для отображения данных:*

1. В веб-интерфейсе KUMA нажмите **Выбрано тенантов**.

   Откроется область выбора тенантов.

2. Установите флажки напротив тенантов, данные которых вы хотите видеть в разделах веб-интерфейса KUMA.
3. Требуется выбрать как минимум один тенант. Тенанты можно искать с помощью поля **Поиск**.
4. Закройте область выбора тенантов, нажав **Выбрано тенантов**.

В разделах веб-интерфейса KUMA отображаются только данные и аналитика, относящаяся к выбранным тенантам.

От выбранных для отображения данных тенантов зависит, какие тенанты можно будет указать при создании ресурсов, сервисов, макетов, шаблонов отчетов, виджетов, инцидентов, активов и других параметров KUMA, где можно выбрать тенант.

Правила принадлежности к тенантам

Правила наследования тенанта

Важно отслеживать, к какому тенанту принадлежат создаваемые в KUMA объекты: от этого зависит, кто к ним будет иметь доступ и взаимодействие с какими объектами можно настроить. Правила определения тенанта:

- Тенант объекта (например, сервиса или ресурса) определяется пользователем при его создании.

  После создания объекта выбранный для него тенант невозможно изменить. Ресурсы (см. раздел "Ресурсы KUMA" на стр. 128), однако, можно экспортировать, а затем импортировать (см. раздел "Экспорт и импорт ресурсов" на стр. 132) в другой тенант.

- Тенант алерта и корреляционного события наследуется от создавшего их коррелятора.

  Название тенанта указывается в поле события (см. раздел "Модель данных нормализованного события" на стр. 471) `TenantId`.

- Если события разных тенантов, обрабатываемых одним коррелятором, не смешиваются, создаваемые им корреляционные события наследуют тенант события.
- Тенант инцидента наследуется от алерта.

kaspersky

Примеры мультитенантных взаимодействий

Мультитенантность в KUMA дает возможность централизованно расследовать алерты и инциденты, возникающие в разных тенантах. Ниже приведены сценарии, по которым можно проследить, к каким тенантам принадлежат создаваемые объекты.

При корреляции событий от разных тенантов в общем потоке **не следует** группировать события по тенанту: то есть не нужно в правилах корреляции (см. раздел "Шаг 3. Корреляция" на стр. 255) в поле **Группирующие поля** указывать поле события `TenantId`. Группировка событий по тенанту необходима, только если нужно не смешивать события от разных тенантов.
Сервисы (см. раздел "Сервисы KUMA" на стр. 229), которые должны быть размещены на мощностях главного тенанта, разворачиваются только пользователями с ролью главный администратор.

- Корреляция событий в рамках одного тенанта, коррелятор выделен для этого тенанта и развернут на его стороне (на стр. 303)
- Корреляция событий в рамках одного тенанта, коррелятор выделен для этого тенанта и развернут на стороне главного тенанта (см. раздел "Кросс-тенанты - сценарий 2" на стр. 303)
- Централизованная корреляция событий, поступающих от разных тенантов (см. раздел "Кросс-тенанты - сценарий 3" на стр. 304)
- Тенант коррелирует свои события, но в главном тенанте дополнительно осуществляется централизованная корреляция событий (см. раздел "Кросс-тенанты - сценарий 4" на стр. 305)
- Один коррелятор для двух тенантов (см. раздел "Кросс-тенанты - сценарий 5" на стр. 306)

► *Условие:*

Коллектор и коррелятор принадлежат тенанту 2 (tenantID=2)

► *Сценарий:*

1. Коллектор тенанта 2 получает и отправляет события в коррелятор тенанта 2.
2. При срабатывании корреляционных правил в коррелляторе создаются корреляционные события с идентификатором тенанта tenantID=2.
3. Коррелятор отправляет корреляционные события в раздел хранилища для тенанта 2.
4. Создается алерт, привязанный к тенанту с идентификатором tenantID=2.
5. К алерту привязываются события, из-за которых он был создан.

Инцидент создается (см. раздел "Создание инцидента" на стр. 312) пользователем вручную. Тенант инцидента определяется тенантом пользователя (см. раздел "Выбор тенанта" на стр. 302). Алерт привязывается к инциденту вручную (см. раздел "Обработка инцидентов" на стр. 314) или автоматически (см. раздел "Автоматическая привязка алертов к инцидентам" на стр. 315).

Кросс-тенанты - сценарий 2

► *Условие:*

- Коллектор развернут на тенанте 2 и принадлежат ему (tenantID=2).

- Коррелятор развернут на стороне главного тенанта.

  Принадлежность коррелятора определяется главным администратором в зависимости того, кто будет расследовать инциденты тенанта 2: сотрудники главного тенанта или тенанта 2. Принадлежность алерта и инцидента зависит от принадлежности коррелятора.

► *Сценарий 1. Коррелятор принадлежит тенанту 2 (tenantID=2):*

1. Коллектор тенанта 2 получает и отправляет события в коррелятор.
2. При срабатывании корреляционных правил в корреляторе создаются корреляционные события с идентификатором тенанта tenantID=2.
3. Коррелятор отправляет корреляционные события в раздел хранилища тенанта 2.
4. Создается алерт, привязанный к тенанту с идентификатором tenantID=2.
5. К алерту привязываются события, из-за которых он был создан.

► *Результат 1:*

- Созданный алерт и привязанные к нему события доступны сотрудникам тенанта 2.

► *Сценарий 2. Коррелятор принадлежит главному тенанту (tenantID=1):*

1. Коллектор тенанта 2 получает и отправляет события в коррелятор.
2. При срабатывании корреляционных правил в корреляторе создаются корреляционные события с идентификатором тенанта tenantID=1.
3. Коррелятор отправляет корреляционные события в раздел хранилища главного тенанта.
4. Создается алерт, привязанный к тенанту с идентификатором tenantID=1.
5. К алерту привязываются события, из-за которых он был создан.

► *Результат 2:*

- Алерт и привязанные к нему события недоступны сотрудникам тенанта 2.
- Алерт и привязанные к нему события доступны сотрудникам главного тенанта.

Кросс-тенанты - сценарий 3

► *Условие:*

- Развернуто два коллектора: на тенанте 2 и тенанте 3. Оба коллектора отправляют события в один коррелятор.
- Коррелятор принадлежит главному тенанту. Правило корреляции ожидает события от обоих тенантов.

► *Сценарий:*

1. Коллектор тенанта 2 получает и отправляет события в коррелятор главного тенанта.
2. Коллектор тенанта 3 получает и отправляет события в коррелятор главного тенанта.

3. При срабатывании корреляционного правила в коррелляторе создаются корреляционные события с идентификатором тенанта tenantID=1.
4. Коррелятор отправляет корреляционные события в раздел хранилища главного тенанта.
5. Создается алерт, привязанный к главному тенанту с идентификатором tenantID=1.
6. К алерту привязываются события, из-за которых он был создан.

► *Результат:*

- Алерт и привязанные к нему события недоступны сотрудникам тенанта 2.
- Алерт и привязанные к нему события недоступны сотрудникам тенанта 3.
- Алерт и привязанные к нему события доступны сотрудникам главного тенанта.

Кросс-тенанты - сценарий 4

► *Условие:*

- Развернуто два коллектора: на главном тенанте и тенанте 2.
- Развернуто два коррелятора:
  - Коррелятор 1 принадлежит главному тенанту и принимает события с коллектора главного тенанта и коррелятора 2.
  - Коррелятор 2 принадлежит тенанту 2 и принимает события с коллектора тенанта 2.

► *Сценарий:*

1. Коллектор тенанта 2 получает и отправляет события в коррелятор 2.
2. При срабатывании корреляционного правила в коррелляторе тенанта 2 создаются корреляционные события с идентификатором тенанта tenantID=2.
   - Коррелятор 2 отправляет корреляционные события в раздел хранилища тенанта 2.
   - Создается алерт 1, привязанный к тенанту с идентификатором tenantID=2.
   - К алерту привязываются события, из-за которых он был создан.
   - Корреляционные события от коррелятора тенанта 2 отправляются в коррелятор 1.
3. Коллектор главного тенанта получает и отправляет события в коррелятор 1.
4. В коррелляторе 1 обрабатываются события обоих тенантов. При срабатывании корреляционного правила создаются корреляционные события с идентификатором тенанта tenantID=1.
   - Коррелятор 1 отправляет корреляционные события в раздел хранилища главного тенанта.
   - Создается алерт 2, привязанный к тенанту с идентификатором tenantID=1.
   - К алерту привязываются события, из-за которых он был создан.

► *Результат:*

- Алерт 2 и привязанные к нему события недоступны сотрудникам тенанта 2.
- Алерт 2 и привязанные к нему события доступны сотрудникам главного тенанта.

kaspersky

Кросс-тенанты - сценарий 5

Если вы не хотите, чтобы при корреляции события от разных тенантов смешивались, в правилах корреляции (см. раздел "Шаг 3. Корреляция" на стр. 255) в поле **Группирующие поля** следует указывать поле события `TenantId`. В таком случае алерт наследует тенант от коррелятора.

► *Условие:*

- Развернуто два коллектора: на тенанте 2 и тенанте 3.
- Развернут один коррелятор, принадлежащий главному тенанту (tenantID=1). Он принимает события от обоих тенантов, но обрабатывает их независимо друг от друга.

► *Сценарий:*

1. Коллектор тенанта 2 получает и отправляет события в коррелятор.
2. Коллектор тенанта 3 получает и отправляет события в коррелятор.
3. При срабатывании корреляционного правила в коррелляторе создаются корреляционные события с идентификатором тенанта tenantID=1.
   - Коррелятор отправляет корреляционные события в раздел хранилища главного тенанта.
   - Создается алерт, привязанный к главному тенанту с идентификатором tenantID=1.
   - К алерту привязываются события, из-за которых он был создан.

► *Результат:*

- Алерты, созданные на основе событий от тенанта 2 и 3, недоступны сотрудникам тенантов 2 и 3.
- Алерты и привязанные к ним события доступны сотрудникам главного тенанта.

kaspersky

Работа с инцидентами

В разделе **Инциденты** веб-интерфейса (см. раздел "Об инцидентах" на стр. 28) KUMA можно создавать (см. раздел "Создание инцидента" на стр. 312), просматривать (см. раздел "Просмотр информации об инциденте" на стр. 310) и обрабатывать (см. раздел "Обработка инцидентов" на стр. 314) инциденты. При необходимости вы также можете фильтровать инциденты. При нажатии на название инцидента открывается окно со сведениями о нем.

Отображаемый формат даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

См. также:

Об инцидентах 28

В этом разделе:

О таблице инцидентов 307
Сохранение и выбор конфигураций фильтра инцидентов 309
Удаление конфигураций фильтра инцидентов 310
Просмотр информации об инциденте 310
Создание инцидента 312
Обработка инцидентов 314
Изменение инцидентов 315
Автоматическая привязка алертов к инцидентам 315
Категории и типы инцидентов 316
Экспорт инцидентов в НКЦКИ 317

О таблице инцидентов

В основной части раздела **Инциденты** отображается таблица с информацией о зарегистрированных инцидентах. При необходимости вы можете изменить набор столбцов и порядок их отображения в таблице.

Как настроить таблицу инцидентов (см. раздел "Параметры отображения для таблицы инцидентов" на стр. 309)

Доступные столбцы таблицы инцидентов:

- **Название** – название инцидента.
- **Длительность инцидента** – время, на протяжении которого происходил инцидент (время между первым и последним событием, относящимся к инциденту).

- **Назначен** – имя сотрудника службы безопасности, которому инцидент передан для расследования или реагирования.
- **Создано** – дата и время создания инцидента. С помощью этого столбца инциденты можно фильтровать по времени их создания.
  - Доступны преднастроенные периоды: **Сегодня**, **Вчера**, **На этой неделе**, **На прошлой неделе**.
  - При необходимости можно задать произвольный период с помощью календаря, который открывается при выборе пунктов **До даты**, **После даты**, **В течение периода**.
- **Тенант** – название тенанта, которому принадлежит инцидент.
- **Статус** – текущее состояние инцидента:
  - **Открыт** – новый, еще не обработанный инцидент.
  - **Назначен** – инцидент обработан и передан сотруднику службы безопасности для расследования или реагирования.
  - **Закрыт** – инцидент закрыт, угроза безопасности устранена.
- **Количество алертов** – количество алертов, входящих в инцидент. Учитываются только алерты тех тенантов, к которым у вас есть доступ.
- **Уровень важности** – степень значимости потенциальной угрозы безопасности: **Критический**  , **Высокий**  , **Средний**  , **Низкий** .
- **Категории затронутых активов** – категории активов с наибольшим уровнем важности, относящихся к алерту. Отображается не более трех категорий.
- **Изменен** – дата и время последнего изменения, сделанного в инциденте.
- **Первое событие** и **Последнее событие** – дата и время первого и последнего события в инциденте.
- **Категория инцидента** и **Тип инцидента** – категория и тип угрозы (см. раздел "Категории и типы инцидентов" на стр. 316), присвоенные инциденту.
- **Экспорт в НКЦКИ** – статус экспорта данных об инциденте в НКЦКИ:
  - **Не экспортировался** – данные не передавались в НКЦКИ.
  - **Ошибка экспорта** – попытка передать данные в НКЦКИ завершилась ошибкой, данные не переданы.
  - **Экспортирован** – данные об инциденте успешно переданы в НКЦКИ.
- **Ветвь** – данные о том, в каком узле был создан инцидент. По умолчанию отображаются инциденты вашего узла. Этот столбец отображается только при включенном режиме иерархии (см. раздел "Работа в режиме иерархии" на стр. 320).

В поле **Поиск** можно ввести регулярное выражение для поиска инцидентов по связанным с ними активами, пользователям, тенантам или корреляционным правилам. Параметры, по которым производится поиск:

- Активы: название, FQDN, IP-адрес.
- Учетные записи Active Directory: атрибуты displayName, SAMAccountName, UserPrincipalName.
- Корреляционные правила: название.
- Пользователи KUMA, которым назначены алерты: имя, логин, адрес электронной почты.
- Тенанты: название.

При фильтрации инцидентов по какому-либо параметру соответствующий столбец в таблице инцидентов подсвечивается желтым цветом.

Параметры отображения для таблицы инцидентов

1. В правом верхнем углу таблицы инцидентов нажмите на значок .

   Откроется окно настройки таблицы.

2. Установите флажки напротив тех параметров, которые требуется отображать в таблице.

   Когда вы устанавливаете флажок, таблица событий обновляется и добавляется новый столбец. При снятии флажка столбец исчезает.

   С помощью поля **Поиск** можно искать параметры таблицы.

   При нажатии на кнопку **По умолчанию** для отображения выбираются следующие столбцы:

   - **Название**.
   - **Длительность инцидента**.
   - **Назначен**.
   - **Создано**.
   - **Тенант**.
   - **Статус**.
   - **Количество алертов**.
   - **Уровень важности**.
   - **Категории затронутых активов**.

3. При необходимости измените порядок отображения столбцов, перетащив заголовки столбцов.
4. Чтобы отсортировать инциденты по определенному параметру, нажмите на заголовок нужного столбцы и в раскрывающемся списке выберите один из вариантов: **По возрастанию** или **По убыванию**.
5. Чтобы отфильтровать инциденты по определенному параметру, нажмите на заголовок нужного столбца и в раскрывающемся списке выберите требуемые фильтры. Набор фильтров, доступный в раскрывающемся списке, зависит от выбранного столбца.
6. Чтобы снять фильтры, нажмите на заголовок нужного столбца и выберите **Очистить фильтр**.

Сохранение и выбор конфигураций фильтра инцидентов

В KUMA можно сохранять изменения настроек таблицы инцидентов в виде фильтров. Конфигурации фильтров сохраняются на сервере Ядра KUMA и доступны всем пользователям KUMA того тенанта, для которого они были созданы.

► *Чтобы сохранить текущие настройки фильтра:*

1. В разделе KUMA **Инциденты** откройте раскрывающийся список **Выбрать фильтр**.

2. Выберите **Сохранить текущий фильтр**.

   Откроется окно для ввода названия нового фильтра и выбора тенанта, которому он будет принадлежать.

3. Введите название конфигурации фильтра. Название должно быть уникальным для фильтров алертов, фильтров инцидентов и фильтров событий.
4. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать фильтр, и нажмите **Сохранить**.

Конфигурация фильтра сохранена.

► *Чтобы выбрать ранее сохраненную конфигурацию фильтра:*

1. В разделе KUMA **Инциденты** откройте раскрывающийся список **Выбрать фильтр**.
2. Выберите нужную конфигурацию.

Конфигурация фильтра активна.

Вы можете выбрать фильтр, который будет использоваться по умолчанию, поставив в раскрывающемся списке **Фильтры** звездочку левее названия требуемой конфигурации фильтра.

► *Чтобы сбросить текущие настройки фильтра,*

откройте раскрывающийся список **Фильтры** и выберите **Очистить фильтр**.

Удаление конфигураций фильтра инцидентов

► *Чтобы удалить ранее сохраненную конфигурацию фильтра:*

1. В разделе KUMA **Инциденты** откройте раскрывающийся список **Фильтры**.
2. Нажмите значок  рядом с фильтром, который требуется удалить.
3. Нажмите **ОК**.

Конфигурация фильтра удалена для всех пользователей KUMA.

Просмотр информации об инциденте

► *Чтобы просмотреть информацию об инциденте:*

1. В окне веб-интерфейса программы выберите раздел **Инциденты**.
2. Выберите инцидент, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об инциденте.

Некоторые параметры инцидентов доступны для редактирования.

В верхней части окна информации об инциденте расположена панель инструментов и указано имя пользователя, которому назначен инцидент. В этом окне вы можете обработать инцидент: назначить его пользователю, объединить его с другим инцидентом или закрыть.

Раздел **Описание** содержит следующие данные:

- **Создан** – дата и время создания инцидента.
- **Название** – название инцидента.

  Название инцидента можно изменить, введя в поле новое название и нажав **Сохранить**. Название должно содержать от 1 до 128 символов Юникода.
- **Тенант** – название тенанта, которому принадлежит инцидент.

  Тенанта можно изменить, выбрав необходимый тенант в раскрывающемся списке и нажав **Сохранить**.
- **Статус** – текущее состояние инцидента:
  - **Открыт** – новый, еще не обработанный инцидент.
  - **Назначен** – инцидент обработан и передан сотруднику службы безопасности для расследования или реагирования.
  - **Закрыт** – инцидент закрыт, угроза безопасности устранена.
- **Уровень важности** – значимость угрозы, которую представляет инцидент. Возможные значения:
  - **Критический**.
  - **Высокий**.
  - **Средний**.
  - **Низкий**.

  Уровень важности можно изменить, выбрав нужное значение раскрывающемся списке и нажав **Сохранить**.
- **Категории затронутых активов** – категории, к которым принадлежат связанные с инцидентом активы.
- **Появление первого события** и **Появление последнего события** – дата и время первого и последнего события в инциденте.
- **Тип инцидента** и **Категория инцидента** – тип и категория угрозы, присвоенная инциденту. Значения можно изменить, выбрав в раскрывающемся списке нужное и нажав **Сохранить**.
- **Экспорт в НКЦКИ** – сведения о том, экспортировался ли этот инцидент в НКЦКИ.
- **Описание** – описание инцидента.

  Описание можно изменить, введя в поле новый текст и нажав **Сохранить**. Описание должно содержать не более 256 символов Юникода.
- **Связанные тенанты** – тенанты, относящиеся к связанным с инцидентом алертам, активам и пользователям.
- **Доступные тенанты** – тенанты, алерты которых можно привязывать к инциденту автоматически (см. раздел "Автоматическая привязка алертов к инцидентам" на стр. 315).

  Список доступных тенантов можно изменить, установив в раскрывающемся списке флажки напротив нужных тенантов и нажав **Сохранить**.

Раздел **Связанные алерты** содержит таблицу алертов, относящихся к инциденту. При нажатии на название алерта открывается окно с подробными данными об этом алерте (см. раздел "Просмотр информации об алерте" на стр. 333).

Разделы **Связанные активы** и **Связанные пользователи** содержат таблицы с данными об активах и пользователях, относящихся к инциденту. Эта информация поступает из алертов, связанных с инцидентом.

Таблицы в разделах **Связанные алерты**, **Связанные активы** и **Связанные пользователи** можно дополнить данными, нажав в нужном разделе на кнопку **Привязать** и выбрав в открывшемся окне объект, который следует привязать к инциденту. При необходимости вы можете отвязать объекты от инцидента. Для этого вам требуется выбрать необходимые объекты, нажать **Отвязать** в разделе, к которому они относятся, и сохранить изменения. Если объекты добавлены в инцидент автоматически, их нельзя отвязать, пока не отвязан алерт, в котором они упоминаются.

Раздел **Журнал изменений** содержит записи об изменениях, которые вы и пользователи вносили в инцидент. Изменения регистрируются автоматически, при этом есть возможность вручную добавлять комментарии.

Создание инцидента

► *Чтобы создать инцидент:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Инциденты**.
2. Нажмите **Создать инцидент**.

   Откроется окно создания инцидента.
3. Заполните обязательные параметры инцидента:
   - В поле **Название** введите название инцидента. Название должно содержать от 1 до 128 символов Юникода.
   - В раскрывающемся списке **Тенант** выберите тенант, которому принадлежит создаваемый инцидент.
4. При необходимости укажите другие параметры инцидента:
   - В раскрывающемся списке **Уровень важности** выберите степень угрозы, которую представляет инцидент. Доступные значения: **Низкий**, **Средний**, **Высокий**, **Критический**.
   - В полях **Появление первого события** и **Появление последнего события** укажите временной диапазон, в котором были получены события, относящиеся к инциденту.
   - В раскрывающихся списках **Категория инцидента** и **Тип инцидента** выберите категорию и тип инцидента (см. раздел "Категории и типы инцидентов" на стр. 316). Доступные типы инцидента зависят от выбранной категории.
   - Добавьте **Описание** инцидента. Описание должно содержать не более 256 символов Юникода.
   - В раскрывающемся списке **Доступные тенанты** выберите тенанты, алерты которых можно будет привязывать к инциденту автоматически (см. раздел "Автоматическая привязка алертов к инцидентам" на стр. 315).
   - В разделе **Связанные алерты** добавьте алерты, относящиеся к инциденту.

     Привязка алертов к инцидентам (см. раздел "Привязка алертов к инцидентам" на стр. 313)
   - В разделе **Связанные активы** добавьте активы, относящиеся к инциденту.

Привязка активов к инцидентам (см. раздел "Привязка активов к инцидентам" на стр. 313)

- В разделе **Связанные пользователи** добавьте пользователей, относящихся к инциденту.

  Привязка пользователей к инцидентам (см. раздел "Привязка пользователей к инцидентам" на стр. 314)

- Добавьте **Комментарий** к инциденту.

5. Нажмите **Сохранить**.

Инцидент создан.

Привязка активов к инцидентам

► *Чтобы привязать актив к инциденту:*

1. В разделе **Связанные активы** окна инцидента (см. раздел "Просмотр информации об инциденте" на стр. 310) нажмите **Привязать**.

   Откроется окно со списком активов.

2. Выберите нужные активы.

   Активы можно искать с помощью поля **Поиск**.

3. Нажмите **Привязать**.

Активы связаны с инцидентом и отображаются в разделе **Связанные активы**.

► *Чтобы отвязать активы от инцидента:*

1. Выберите нужные активы в разделе **Связанные активы** и нажмите на кнопку **Отвязать**.
2. Нажмите **Сохранить**.

Активы отвязаны от инцидента.

Привязка алертов к инцидентам

► *Чтобы привязать алерт к инциденту:*

1. В разделе **Связанные алерты** окна инцидента (см. раздел "Просмотр информации об инциденте" на стр. 310) нажмите **Привязать**.

   Откроется окно со списком непривязанных к инцидентам алертов.

2. Выберите требуемые алерты.

   Алерты можно искать по пользователям, активам, тенантам и корреляционным правилам с помощью регулярных выражений PCRE.

3. Нажмите **Привязать**.

Алерты связаны с инцидентом и отображаются в разделе **Связанные алерты**.

► *Чтобы отвязать алерты от инцидента:*

1. Выберите нужные алерты в разделе **Связанные алерты** и нажмите на кнопку **Отвязать**.

2. Нажмите **Сохранить**.

Алерты отвязаны от инцидента. Также алерт можно отвязать от инцидента в окне алерта (см. раздел "Просмотр информации об алерте" на стр. 333) с помощью кнопки **Отвязать**.

Привязка пользователей к инцидентам

► *Чтобы привязать пользователя к инциденту:*

1. В разделе **Связанные пользователи** окна инцидента (см. раздел "Просмотр информации об инциденте" на стр. 310) нажмите **Привязать**.

   Откроется окно со списком пользователей.

2. Выберите нужных пользователей.

   Пользователей можно искать с помощью поля **Поиск**.

3. Нажмите **Привязать**.

Пользователи связаны с инцидентом и отображаются в разделе **Связанные пользователи**.

► *Чтобы отвязать пользователей от инцидента:*

1. Выберите нужных пользователей в разделе **Связанные пользователи** и нажмите на кнопку **Отвязать**.
2. Нажмите **Сохранить**.

Пользователи отвязаны от инцидента.

Обработка инцидентов

Вы можете назначить инцидент пользователю, объединить инциденты или закрыть инцидент.

► *Чтобы обработать инцидент:*

1. Выберите необходимые инциденты одним из следующих способов:
   - В разделе **Инциденты** веб-интерфейса KUMA нажмите на инцидент, который нужно обработать.

     Откроется окно инцидента (см. раздел "Просмотр информации об инциденте" на стр. 310), в его верхней части расположена панель инструментов.
   - В разделе **Инциденты** веб-интерфейса KUMA установите флажок рядом с требуемыми инцидентами.

     В нижней части окна отобразится панель инструментов.
2. В раскрывающемся списке **Назначить** выберите пользователя, которому вы хотите назначить инцидент.

   Вы можете назначить инцидент себе, выбрав **Мне**.

   Инциденту будет присвоен статус **Назначен**, а в раскрывающемся списке **Назначить** отобразится имя выбранного пользователя.

3. При необходимости измените параметры инцидента (см. раздел "Изменение инцидентов" на стр. 315).
4. После расследования закройте инцидент:
   a. Нажмите **Закрыть**.

      Откроется окно подтверждения.

   b. Укажите причину закрытия инцидента:

      - **одобрен**. Это означает, что были приняты необходимые меры по устранению угрозы безопасности.
      - **не одобрен**. Это означает, что инцидент был ложным, а полученные события не указывают на угрозу безопасности.

   c. Нажмите **Закрыть**.

   Инциденту будет присвоен статус **Закрыт**. Инциденты с таким статусом невозможно редактировать, и они отображаются в таблице инцидентов, только если при фильтрации таблицы в раскрывающемся списке **Статус** установлен флажок **Закрыт**. Изменить статус закрытого инцидента или назначить его другому пользователю невозможно, однако его можно объединить с другим инцидентом.
5. При необходимости объедините выбранные инциденты с другим инцидентом:
   a. Нажмите **Объединить** и в открывшемся окне выберите инцидент, в который следует поместить все данные из выбранных инцидентов.
   b. Подтвердите выбор, нажав **Объединить**.

   Инциденты будут объединены.

Инцидент обработан.

Изменение инцидентов

► *Чтобы изменить параметры инцидента:*

1. В разделе **Инциденты** веб-интерфейса KUMA нажмите на инцидент, параметры которого нужно изменить.

   Откроется окно инцидента (см. раздел "Просмотр информации об инциденте" на стр. 310).
2. Измените нужные параметры. Для редактирования доступны все параметры инцидента, которые можно задать при его создании (см. раздел "Создание инцидента" на стр. 312).
3. Нажмите **Сохранить**.

Инцидент будет изменен.

Автоматическая привязка алертов к инцидентам

В KUMA можно настроить автоматическую привязку создаваемых алертов к уже существующим инцидентам, если у алертов и инцидентов есть пересечения по относящимся к ним активам или пользователям. Если настройка включена, то при создании алерта программа выполняет поиск инцидентов за указанный период, к которым относятся активы или пользователи из алерта. Кроме того, программа

проверяет, чтобы созданный алерт относился к тенантам, указанным в инцидентах в качестве параметра **Доступные тенанты** (см. раздел "**Просмотр информации об инциденте**" на стр. 310). Если удовлетворяющий условиям инцидент найден, программа связывает созданный алерт и найденный инцидент.

► *Чтобы настроить автоматическую привязку алертов к инцидентам:*

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Инциденты** → **Автоматическая привязка алертов к инцидентам**.
2. Установите флажок **Включить** в блоках параметров **Привязка при пересечении по активам** и/или **Привязка при пересечении по пользователям**, в зависимости от того, какие связи необходимо искать между инцидентами и алертами.
3. Задайте **Срок давности создания инцидента** для параметров, по которым необходимо искать связи. Создаваемые алерты будут сравниваться с инцидентами не старше указанного срока.

Автоматическая привязка алертов к инцидентам настроена.

► *Чтобы выключить автоматическую привязку алертов к инцидентам,*

в разделе веб-интерфейса KUMA **Параметры** → **Инциденты** → **Автоматическая привязка алертов к инцидентам** установите флажок **Выключено**.

Категории и типы инцидентов

Для удобства работы вы можете присваивать категории и типы (см. раздел "Обработка инцидентов" на стр. 314). Если инциденту присвоена категория НКЦКИ, его можно экспортировать в НКЦКИ.

Категории и типы инцидентов, которые можно экспортировать в НКЦКИ (см. раздел "Доступные категории и типы инцидентов" на стр. 116)

Категории инцидентов можно просмотреть или изменить в разделе **Параметры** → **Инциденты** → **Типы инцидентов**, где они отображаются в виде таблицы. При нажатии на заголовки столбцов можно менять параметры сортировки таблицы. Таблица содержит следующие столбцы:

- **Категория инцидента** – общий признак инцидента или компьютерной атаки. Таблицу можно фильтровать по значениям этого столбца.
- **Тип инцидента** – класс инцидента или компьютерной атаки.
- **Категория для НКЦКИ** – соответствие типа инцидента номенклатуре НКЦКИ. Невозможно экспортировать в НКЦКИ инциденты, которым присвоены пользовательские типы и категории. Таблицу можно фильтровать по значениям этого столбца.
- **Уязвимость** – указывает ли тип инцидента на уязвимость.
- **Создан** – дата создания типа инцидента.
- **Изменен** – дата изменения типа инцидента.

► *Чтобы добавить тип инцидента:*

1. В разделе веб-интерфейса KUMA **Параметры** → **Инциденты** → **Типы инцидентов** нажмите **Добавить**.

   Откроется окно создания типа инцидента.

2. Заполните поля **Тип** и **Категория**.
3. Если создаваемый тип инцидента соответствует номенклатуре НКЦКИ, установите флажок **Категория для НКЦКИ**.
4. Если тип инцидента указывает на уязвимость, установите флажок **Уязвимость**.
5. Нажмите **Сохранить**.

Тип инцидента создан.

Экспорт инцидентов в НКЦКИ

Инциденты, созданные в KUMA можно экспортировать в НКЦКИ. Перед экспортом инцидентов требуется настроить интеграцию с НКЦКИ (см. раздел "Интеграция с НКЦКИ" на стр. 114). Инцидент можно экспортировать только один раз. Экспорт инцидентов в НКЦКИ доступен пользователя с включенным флажком **Может взаимодействовать с НКЦКИ** в параметрах пользователя (см. раздел "Создание пользователя" на стр. 69).

Экспорт инцидентов в НКЦКИ доступен, только если лицензия программы включает модуль GosSOPKA.

► *Чтобы экспортировать инцидент в НКЦКИ:*

1. В разделе **Инциденты** веб-интерфейса KUMA выберите инцидент, который вы хотите экспортировать, одним из указанных ниже способов:
   - Установите флажок рядом с нужным инцидентом.
   - Откройте нужный инцидент (см. раздел "Просмотр информации об инциденте" на стр. 310).
2. Нажмите **Экспортировать в НКЦКИ**.

   Откроется окно с параметрами экспорта.
3. Укажите параметры в закладке **Основные** окна **Экспорт в НКЦКИ**:
   - **Категория инцидента** и **Тип инцидента** – укажите тип и категорию (см. раздел "Категории и типы инцидентов" на стр. 316) инцидента. В НКЦКИ можно экспортировать только инциденты определенных категорий и типов.

     Категории и типы инцидентов, которые можно экспортировать в НКЦКИ (см. раздел "Доступные категории и типы инцидентов" на стр. 116)
   - **TLP** (обязательно) – присвойте инциденту маркер протокола Traffic Light, определяющий характер сведений об инциденте. По умолчанию используется значение **RED**. Доступные значения:
     - **WHITE** – раскрытие не ограничено;
     - **GREEN** – раскрытие только для сообщества;
     - **AMBER** – раскрытие только для организаций;
     - **RED** – раскрытие только для круга лиц.

- **Название информационной системы** (обязательно) – укажите название информационного ресурса, в котором произошел инцидент. В поле можно ввести до 500 000 символов.
- **Категория КИИ системы** (обязательно) – укажите категорию критичной информационной структуры (КИИ) вашей организации. Если у вашей организации нет категории КИИ, выберите пункт **Информационный ресурс не является объектом КИИ**.
- **Сфера деятельности компании** (обязательно) – укажите сферу деятельности вашей организации. По умолчанию используется значение, указанное в параметрах интеграции с НКЦКИ (см. раздел "Интеграция с НКЦКИ" на стр. 114).

  Доступные сферы деятельности компании (см. раздел "Сферы деятельности компании" на стр. 116)
- **Местоположение** (обязательно) – выберите в раскрывающемся списке местоположение вашей организации.
- **Затронутая система имеет подключение к интернету** – установите этот флажок, если активы, относящиеся к инциденту, имеют подключение к интернету. Кроме того, дополнительно после завершения экспорта в личном кабинете ГосСОПКА в карточке уведомления укажите технические сведения о компьютерном инциденте, компьютерной атаке или уязвимости. По умолчанию этот флажок снят.
- **Сведения о продукте** (обязательно) – эта таблица становится доступна, если в качестве категории инцидента вы выбрали пункт **Уведомление о наличии уязвимости**.

  С помощью кнопки **Добавить элемент** можно добавить в таблицу строку. В столбце **Название** требуется указать название программы (например, `MS Office`), а в столбце **Версия** – версию программы (например, `2.4`).
- Идентификатор уязвимости – при необходимости укажите идентификатор обнаруженной уязвимости. Например, `CVE-2020-1231`.

  Это поле становится доступно, если в качестве категории инцидента вы выбрали пункт **Уведомление о наличии уязвимости**.
- Наименование и версия уязвимого продукта – при необходимости укажите наименование и версию уязвимого продукта. Например, `Операционные системы Microsoft и их компоненты`.

  Это поле становится доступно, если в качестве категории инцидента вы выбрали пункт **Уведомление о наличии уязвимости**.

4. При необходимости укажите параметры в закладке **Дополнительно** окна **Экспорт в НКЦКИ**.

   Набор параметров в закладке зависит от выбранных категории и типа инцидента:

   - **Средство обнаружения инцидента** – укажите название продукта, с помощью которого был зарегистрирован инцидент. Например, `KUMA 1.5`.
   - **Требуется привлечение сил ГосСОПКА** – установите этот флажок, если вам требуется помощью сотрудников ГосСОПКА.
   - **Время завершения инцидента** – оставьте это поле пустым. Дату и время восстановления штатного режима работы контролируемого информационного ресурса (объекта КИИ) после компьютерного инцидента, окончания компьютерной атаки или устранения уязвимости можно будет указать в вашем личном кабинете ГосСОПКА.

Если указать время завершения инцидента, данные об этом инциденте невозможно будет экспортировать в НКЦКИ.

- **Влияние на доступность** – оцените степень последствий инцидента для доступности системы:
  - Высокое
  - Низкое
  - Отсутствует
- **Влияние на целостность** – оцените степень последствий инцидента для целостности системы:
  - Высокое
  - Низкое
  - Отсутствует
- **Влияние на конфиденциальность** – оцените степень последствий инцидента для конфиденциальности информации:
  - Высокое
  - Низкое
  - Отсутствует
- **Иные последствия** – укажите иные значимые последствия инцидента.
- **Город** – укажите город, в котором находится ваша организация.

5. Нажмите **Экспорт**.
6. Подтвердите экспорт.

Сведения об инциденте переданы в НКЦКИ, параметр инцидента **Экспорт в НКЦКИ** меняется на **Успешно экспортирован**. Если в экспортированный инцидент требуется внести изменения, это следует делать в вашем личном кабинете ГосСОПКА.

kaspersky

Работа в режиме иерархии

KUMA, развернутые в разных организациях, могут быть объединены в иерархическую структуру. Взаимодействие родительских и дочерних KUMA (или *узлов*) предоставляет следующие возможности:

- Родительские узлы KUMA получают от дочерних узлов KUMA данные о других потомках. Это позволяет родительскому узлу видеть свою ветвь иерархического дерева.
- Родительские узлы KUMA получают от потомков данные об инцидентах (см. раздел "Об инцидентах" на стр. 28) и, если дочерний узел включил соответствующие настройки (см. раздел "Включение и выключение режима иерархии" на стр. 329), данные о связанных с инцидентами алертах (см. раздел "Об алертах" на стр. 27) и событиях (см. раздел "О событиях" на стр. 25).
- Дочерние узлы KUMA располагают данными только о своем родительском узле KUMA.

Родительский и дочерний узлы взаимодействуют через API. Для аутентификации используются самоподписанные сертификаты, которыми администраторы родительской и дочерней организаций должны обменяться при подключении узлов друг к другу.

Один родительский узел может иметь более одного дочернего узла. Дочерний узел может быть подключен только к одному родительскому узлу. Родительский узел не может быть дочерним узлом своих потомков.

Пользователи с ролью главный администратор (см. раздел "Роли пользователей" на стр. 57) могут настроить режим иерархии в веб-интерфейсе KUMA в разделе **Параметры** → **Иерархия**:

- На закладке **Профиль узла** можно настроить профиль вашего узла, создать сертификат, а также включить и выключить режим иерархии.
- На закладке **Структура** можно просматривать доступную вам ветвь иерархического дерева, изменять подключенные узлы или отключать их.
- На обеих закладках можно подключать узлы – родительский и дочерние.

Инциденты дочерних узлов могут просматривать пользователи всех ролей в веб-интерфейсе KUMA в разделе **Инциденты** (см. раздел "**Работа с инцидентами**" на стр. 307). В инцидентах можно получить сведения о связанных с ними алертах, событиях, активах и пользователях.

В этом разделе

Первое включение режима иерархии 320
Создание сертификата узла 321
Соединение узлов в иерархическую структуру 322
Просмотр своей ветви иерархии и доступных узлов 326
Изменение профиля узла 327
Просмотр инцидентов от узлов-потомков 328
Включение и выключение режима иерархии 329

kaspersky

Первое включение режима иерархии

При первом включении режима иерархии необходимо заполнить профиль своего узла.

► *Чтобы заполнить профиль своего узла:*

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Иерархия** → **Профиль узла**.
2. В поле **Название организации** укажите название своей организации (1–128 символов). Это название будет использоваться в качестве названия вашего узла в иерархии.

   Для изменения названия организации потребуется пересоздать сертификат вашего узла и заменить его на узлах, к которым вы подключены.
3. В поле **FQDN** укажите FQDN своего узла.
4. При необходимости в раскрывающемся списке **Прокси-сервер** выберите ресурс прокси-сервера (см. раздел "Прокси-серверы" на стр. 226), который требуется использовать для обращения к другим узлам. Прокси-сервер можно создать с помощью кнопки . Выбранный прокси-сервер можно изменить, нажав на кнопку .

   В URL прокси-сервера можно указывать учетные данные только с использованием следующих символов: буквы латинского алфавита, цифры, специальные символы ("-", ".", "_", ":", "~", "!", "$", "&", "\", "(", ")", "*", "+", ",", ";", "=", "%", "@"). URL в ресурсе прокси-сервера указывается с помощью ресурса секрета (см. раздел "Секреты" на стр. 226): он выбирается в раскрывающемся списке **Брать URL из секрета**.
5. Нажмите **Создать сертификат**.

Профиль вашего узла KUMA заполнен и режим иерархии включен. При включении режима иерархии автоматически создается сертификат (см. раздел "Создание сертификата узла" на стр. 321), используемый для аутентификации вашего узла. С помощью значка вы можете скачать сертификат, чтобы затем передать его по защищенному каналу связи другим узлам для создания соединения.

Создание сертификата узла

Для аутентификации узлов иерархии используются самоподписанные *сертификаты узлов*. Сертификат содержит название организации и ее FQDN.

Сертификат создается при включении режима иерархии, но вы можете пересоздать сертификат. Сертификат необходимо пересоздать при изменении названия узла или его FQDN.

► *Чтобы создать сертификат узла:*

1. Откройте раздел веб-интерфейс KUMA **Параметры** → **Иерархия** → **Профиль узла**.

   Откроется окно с параметрами вашего узла в иерархии.
2. Нажмите на кнопку **Создать сертификат**.

   Откроется окно создания сертификата.
3. В поле **FQDN** укажите FQDN своего узла.

4. В поле **Название организации** укажите название своей организации (1–128 символов). Это название будет использоваться в качестве названия вашего узла в иерархии.
5. Закройте окно, нажав **Сохранить**.

Сертификат узла создан. Его можно скачать, нажав на значок  , и передать по защищенному каналу связи другим узлам для создания соединения.

Соединение узлов в иерархическую структуру

Перед соединением узлов следует убедиться, что на них включен режим иерархии, настроены профили узлов и созданы сертификаты узлов. Родительский и дочерний узлы должны обменяться своими сертификатами по защищенным каналам связи.

Соединение узлов иерархии состоит из следующих шагов:

- Дочерний узел подключается к родительскому узлу.
- Родительский узел подключает дочерний узел.

Перед соединением узлов убедитесь, что системное время на машинах синхронизируется с NTP-сервером. См. подробнее для Oracle Linux (см. раздел "Подготовка целевой машины" на стр. 43) и для Astra Linux Special Edition https://wiki.astralinux.ru/pages/viewpage.action?pageId=27361687.

Когда соединение установлено, родительский узел каждые 5 минут запрашивает у дочерних узлов имеющиеся у них сведения об иерархии, выстраивая таким образом структуру доступной для себя ветви иерархического дерева. Эти данные отображаются в разделе веб-интерфейса KUMA **Параметры** → **Иерархия** → **Структура** после обновления веб-страницы.

Сведения об иерархической структуре можно принудительно обновить в помощью кнопки **Обновить структуру**. Для отображения обновленных данных необходимо обновить страницу веб-браузера.

В этом разделе

Подключение к родительскому узлу 322
Подключение дочернего узла 323
Отключение от узла 323
Изменение узла 324
Ошибки при подключении узлов 325

kaspersky

Подключение к родительскому узлу

► *Чтобы подключиться к родительскому узлу:*

1. Откройте раздел веб-интерфейс KUMA **Параметры** → **Иерархия** и нажмите на кнопку **Подключиться к родительскому узлу**.

   Откроется окно **Подключение к родительскому узлу**.

2. Загрузите в KUMA сертификат (см. раздел "Создание сертификата узла" на стр. 321) родительского узла с помощью кнопки **Загрузить сертификат**.

   В окне отобразится описание сертификата с указанием выпустившей его организации и ее FQDN.

3. При необходимости в поле **Порт** укажите порт для доступа к родительскому узлу.

4. Нажмите **Сохранить**.

Вы подключились к родительскому узлу. Он теперь может добавить ваш узел в качестве дочернего, чтобы получать данные о ваших дочерних узлах и просматривать ваши инциденты.

Подключение дочернего узла

Если вы подключили родительский узел (см. раздел "Подключение к родительскому узлу" на стр. 322), вы сможете добавить дочерние узлы только после того, как ваш родительский узел добавит вас в качестве дочернего узла. Перед подключением дочернего узла убедитесь, что он добавил ваш узел в качестве родительского.

► *Чтобы подключить дочерний узел:*

1. Откройте раздел веб-интерфейс KUMA **Параметры** → **Иерархия** и нажмите на кнопку **Подключить дочерний узел**.

   Откроется окно **Подключение дочернего узла**.

2. Загрузите в KUMA сертификат дочернего узла с помощью кнопки **Загрузить сертификат**.

   В окне отобразится описание сертификата с указанием выпустившей его организации и ее FQDN.

3. При необходимости в поле **Порт** укажите порт для доступа к дочернему узлу.

4. Нажмите **Сохранить**.

Дочерний узел добавлен и отображается на закладке **Параметры** → **Иерархия** → **Структура**. На этой же закладке отображаются потомки дочернего узла. Вы можете просматривать инциденты своих дочерних узлов и их потомков.

kaspersky

Отключение от узла

Вы можете отключиться от родительского или дочернего узла. Невозможно отключиться от узлов, которые являются потомками ваших дочерних узлов.

► *Чтобы отключиться от узла:*

1. Откройте раздел веб-интерфейс KUMA **Параметры** → **Иерархия** и перейдите на закладку **Структура**.

   Отобразится иерархическая структура.

2. Выберите узел, от которого вы хотите отключиться.

   В правой части окна отобразится область деталей со сведениями об узле.

3. Нажмите **Отключить**.

Вы отключились от узла. Если вы отключились от родительского узла, он больше не получает данные о ваших дочерних узлах и инцидентах. Если вы отключились от дочернего узла, вы больше не получаете данные о его дочерних узлах и его инцидентах.

Изменение узла

Если название и/или FQDN узла изменились, этот узел должен перевыпустить сертификат, после чего необходимо повторить процедуру соединения узлов. Устаревшие узлы необходимо отключить.

Порт подключения к узлам можно изменить в области деталей узла, не перевыпуская сертификат.

► *Чтобы изменить параметры подключения к узлу:*

1. Откройте в веб-интерфейсе KUMA в разделе **Параметры** → **Иерархия** закладку **Структура** и выберите требуемый узел.

   В правой части окна отобразится область деталей узла.

2. В поле **Порт** укажите требуемый порт.
3. Измените настройки почтовых оповещений о появлении инцидентов на дочернем узле:
   - Если требуется выключить оповещения, снимите флажок **Отслеживание инцидентов**.
   - Если требуется включить оповещения, установите флажок **Отслеживание инцидентов** и добавьте с помощью поля ввода требуемые адреса электронной почты.

     Для отправки почтовых уведомлений требуется настроить подключение к SMTP-серверу (на стр. 407).
4. Нажмите **Сохранить**

Параметры подключения к узлу изменены.

kaspersky

Ошибки при подключении узлов

Ошибки, возникающие при подключении узлов, в веб-интерфейсе KUMA могут отображаться не полностью. Полный ответ сервера можно просмотреть в консоли разработчика используемого вами браузера.

В таблице ниже перечислены ошибки, которые могут возникнуть при соединении узлов KUMA в иерархию, а также рекомендации по их устранению.

Ошибки, возникающие при установлении подключения к узлу, отображаются во всплывающих окнах в нижней части экрана. Ошибки в уже подключенных узлах можно просмотреть в разделе веб-интерфейса KUMA **Параметры** → **Иерархия** → **Структура**: текст ошибки отображается, если навести указатель мыши на значок красного треугольника рядом с узлом, в работе с которым произошла ошибка.

Сообщение об ошибке	Возможная причина возникновения ошибки	Рекомендация по устранению
`failed to exchange settings with child: <Post-запрос на адрес дочернего узла>: connect: connection refused`	Отказано в соединении. Произошла попытка добавить дочерний узел, который не добавил сертификат родительского узла.	• Подключить сначала на дочернем узле родительский узел, затем на родительском узле добавить дочерний. • Проверить включена ли иерархия на дочернем узле.
`Невозможно добавить свой узел KUMA в качестве родительского или дочернего узла`	Из узлов KUMA невозможно выстроить циклическую структуру.	Удостоверьтесь, что иерархическая структура, которую вы хотите выстроить, является древовидной.
`corrupted certificate`	Некорректный сертификат.	Необходимо проверить файл сертификата.
`failed to exchange settings with child: <Post-запрос на адрес дочернего узла>: context deadline exceeded`	Соединение не было установлено из-за превышения времени ожидания отклика.	Проверить включена ли машина дочернего узла.
`failed to exchange settings with child: <Post-запрос на адрес дочернего узла>: x509: certificate has expired or is not yet valid`	Отказано в соединении из-за недействительного сертификата.	• Убедиться в актуальности сертификата дочернего узла. • Убедиться, что системное время узлов синхронизируется с NTP-сервером.

failed to exchange settings with child: <Post-запрос на адрес дочернего узла>: certificate signed by unknown authority (possibly because of "x509: invalid signature: parent certificate cannot sign this kind of certificate" while trying to verify candidate authority certificate "<название узла>"	Отказано в соединении из-за недействительного сертификата.	Убедиться в актуальности сертификата родительского узла.
failed to exchange settings with child: <Post-запрос на адрес дочернего узла>: dial tcp: lookup <адрес дочернего узла> on <IP-адрес дочернего узла>: no such host	В сертификате дочернего узла несуществующий FQDN.	Убедиться в актуальности сертификата дочернего узла.
Already exists	Такой узел уже существует в структуре.	Проверьте иерархическую структуру, которую вы хотите построить.
Родительский узел уже указан в качестве дочернего узла		Не подключать родительский узел, который является дочерним узлом в этой иерархии.
Failed to query branch {"branchID":"<идентификатор ветки>","branchName":"<название узла>","branchFQDN":"<FQDN узла>","error":"Get \"<URL дочернего узла>/children\": remote error: tls: bad certificate"}	Дочерний узел удалил родителя.	Необходимо, чтобы дочерний узел подключил родительский узел.
error: <Post-запрос на адрес дочернего узла>: read tcp <IP-адреса узлов>: read: connection reset by peer	В настройках подключения узлов указаны неверные порты.	Убедиться, что в настройках узла указан верный порт и используется действительный сертификат.
"error":"Get \"<URL дочернего узла>/children\": proxyconnect tcp: x509: certificate signed by unknown authority"	Осуществляется подключение к узлу с некорректными настройками прокси-сервера.	Убедиться в корректности настроек прокси-сервера.

kaspersky

Просмотр своей ветви иерархии и доступных узлов

В веб-интерфейсе KUMA в разделе **Параметры** → **Иерархия** на закладке **Структура** можно просмотреть вашу ветвь иерархического дерева от родительского узла до всех потомков дочерних узлов. Ваш узел в иерархии подсвечен зеленым.

При нажатии на узел ветви в правой части окна открывается область деталей узла, в которой можно выполнить следующие действия:

- Изменить порт подключения к родительскому или дочернему узлу.
- Отключить родительский или дочерний узел.
- Изменить настройки почтовых уведомлений об инцидентах для дочерних узлов и их потомков.

Изменение профиля узла

Вы можете изменить параметры профиля своего узла.

► *Чтобы изменить параметры вашего узла:*

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Иерархия** → **Профиль узла**.
2. При необходимости в раскрывающемся списке **Прокси-сервер** выберите ресурс прокси-сервера (см. раздел "Прокси-серверы" на стр. 226), который требуется использовать для обращения к другим узлам. Прокси-сервер можно создать с помощью кнопки  . Выбранный прокси-сервер можно изменить, нажав на кнопку  .

   В URL прокси-сервера можно указывать учетные данные только с использованием следующих символов: буквы латинского алфавита, цифры, специальные символы ("-", ".", "_", ":", "~", "!", "$", "&", "\", "(", ")", "*", "+", ",", ";", "=", "%", "@"). URL в ресурсе прокси-сервера указывается с помощью ресурса секрета (см. раздел "Секреты" на стр. 226): он выбирается в раскрывающемся списке **Брать URL из секрета**.
3. При необходимости в поле **Порт** укажите порт, используемый для доступа к вашему узлу. Убедитесь, что доступ к порту не закрыт.
4. При необходимости в поле **Время ожидания** укажите, сколько секунд необходимо ожидать ответа узлов при попытке соединения. Значение по умолчанию – 60.
5. При необходимости установите или снимите флажки **Не включать события в инциденты, отправляемые в родительский узел** и **Не включать алерты в инциденты, отправляемые в родительский узел**. По умолчанию эти флажки сняты.
6. Нажмите **Сохранить**.

Параметры вашего узла изменены.

Если вы хотите изменить FQDN или название своего узла, пересоздайте сертификат узла (см. раздел "Создание сертификата узла" на стр. 321).

kaspersky

Просмотр инцидентов от узлов-потомков

Если режим иерархии включен (см. раздел "Включение и выключение режима иерархии" на стр. 329), вы можете просмотреть инциденты, созданные на дочерних узлах и их потомках, в разделе **Инциденты**. В таблице инцидентов отображается столбец **Ветвь**, с помощью которого можно фильтровать инциденты по узлам, в которых они были созданы. По умолчанию в таблице инцидентов отображаются инциденты, созданные на вашем узле.

► *Чтобы выбрать узлы, инциденты которых вы хотите просмотреть:*

1. Откройте в веб-интерфейсе KUMA раздел **Инциденты**.
2. Нажмите на заголовок столбца **Ветвь** и в открывшемся окне нажмите на значок  .

   В правой части окна отобразится область деталей с иерархической структурой организаций. С помощью кнопки можно раскрыть или скрыть все ветви структуры, а также выбрать все узлы KUMA.
3. Выберите требуемые узлы и нажмите **Сохранить**.

В таблице инцидентов отображаются инциденты, созданные на выбранных вами узлах.

При нажатии на инцидент открывается окно с подробными данными об инциденте (см. раздел "Просмотр информации об инциденте" на стр. 310). Данные доступны только для чтения, инцидент с другого узла невозможно изменить или обработать.

Особенности просмотра данных об инциденте, созданном на другом узле:

- Раздел окна инцидента **Связанные алерты** содержит сведения, только если на дочернем узле настроена передача в родительский узел данных об относящихся к инцидентам алертах.

  При нажатии на название относящегося к инциденту алерта открывается окно с подробными данными об этом алерте (см. раздел "Просмотр информации об алерте" на стр. 333). Эти данные также доступны только для чтения, алерт другого узла невозможно изменить или обработать.
- Раздел **Связанные события** в окне алерта, относящегося к инциденту другого узла, содержит сведения, только если на дочернем узле настроена передача в родительский узел данных об относящихся к инцидентам событиях.

  В этом случае с помощью кнопки **Найти в событиях** можно открывать таблицу событий (см. раздел "Детализированный анализ" на стр. 336) и искать нужные события (см. раздел "Ограничение сложности запросов в режиме детализированного анализа" на стр. 348). При этом вы не можете выбрать хранилище, а на SQL-запросы налагаются ограничения поиска событий в режиме детализированного анализа. В этом режиме действует обогащение данных (например, с помощью Kaspersky Threat Intelligence Portal (см. раздел "Интеграция с Kaspersky Threat Intelligence Portal" на стр. 87), Kaspersky CyberTrace (см. раздел "Интеграция с Kaspersky CyberTrace" на стр. 81) или Active Directory (см. раздел "Интеграция с Active Directory" на стр. 102)). На родительских узлах недоступны результаты обогащения данными Kaspersky Threat Intelligence Portal, сделанные на дочерних узлах.

См. также:

Об инцидентах 28
Об алертах 27
О событиях 25

Включение и выключение режима иерархии

► *Чтобы включить или выключить режим иерархии:*

1. Откройте в веб-интерфейсе KUMA раздел **Параметры** → **Иерархия** → **Профиль узла**.
2. Включите или выключите режим иерархии:
   - Если вы хотите включить режим иерархии, снимите флажок **Выключено**.
   - Если вы хотите выключить режим иерархии, установите флажок **Выключено**.
3. Нажмите **Сохранить**.

Режим иерархии включен или выключен.

kaspersky

Работа с алертами

В разделе **Алерты** веб-интерфейса KUMA можно просматривать (см. раздел "Просмотр информации об алерте" на стр. 333) и обрабатывать алерты (см. раздел "Обработка алертов" на стр. 335), зарегистрированные программой. Алерты можно фильтровать (см. раздел "Фильтрация алертов" на стр. 330). По нажатию на название алерта открывается окно со сведениями о нем.

Отображаемый формат даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

Переполнение алертов

Каждый алерт и привязанные к нему события не могут превышать размер 16 МБ. Когда этот предел достигнут:

- Новые события не смогут быть привязаны к алерту.
- В столбце **Обнаружен** у алерта отображается тег **Переполнен**. Такой же тег отображается в разделе **Информация об алерте** окна сведений об алерте.

Алерты, у которых есть предупреждения о переполнении, следует обрабатывать как можно скорее.

В этом разделе

Фильтрация алертов 330
Просмотр информации об алерте 333
Обработка алертов 335
Детализированный анализ 336
Срок хранения алертов 337
Правила сегментации алертов 338
Уведомления об алертах 339

Фильтрация алертов

В KUMA в разделе **Алерты** можно делать выборки алертов с помощью инструментов фильтрации (см. раздел "Настройка таблицы алертов" на стр. 331) и сортировки.

Конфигурацию фильтра можно сохранить (см. раздел "Сохранение и выбор конфигураций фильтра алертов" на стр. 332). Существующие конфигурации фильтров можно удалить (см. раздел "Удаление конфигураций фильтра алертов" на стр. 332).

kaspersky

В этом разделе

Настройка таблицы алертов 331
Сохранение и выбор конфигураций фильтра алертов 332
Удаление конфигураций фильтра алертов 332

Настройка таблицы алертов

В основной части раздела **Алерты** отображается таблица с информацией о зарегистрированных алертах. Нажав на заголовки столбцов можно открыть раскрывающиеся списки с инструментами для фильтрации алертов и настройки таблицы алертов:

- Уровень важности () – степень значимости потенциальной угрозы безопасности: критическая  , высокая  , средняя  , низкая .
- **Название** – имя алерта.

  Если рядом с названием алерта отображается тег **Переполнен**, это означает, что размер алерта достиг или приближается к пределу и должен быть обработан как можно скорее.

- **Статус** – текущее состояние алерта:
  - **Новый** – новый, еще не обработанный алерт.
  - **Назначен** – алерт обработан и передан сотруднику службы безопасности для расследования или реагирования.
  - **Закрыт** – алерт закрыт. Алерт был ложный или угроза безопасности устранена.
  - **Эскалирован** – на основе этого алерта был создан инцидент (см. раздел "Об инцидентах" на стр. 28).
- **Назначен** – имя сотрудника службы безопасности, которому алерт передан для расследования или реагирования.
- **Инцидент** – название инцидента, к которому привязан алерт.
- **Первое появление** – дата и время создания первого корреляционного события в последовательности событий, приведшего к созданию алерта.
- **Последнее появление** – дата и время создания последнего корреляционного события в последовательности событий, приведшего к созданию или обновлению алерта.
- **Категории** – категории активов с наибольшим уровнем важности, относящихся к алерту. Отображается не более трех категорий.
- **Тенант** – название тенанта, которому принадлежит алерт.

В поле **Поиск** можно ввести регулярное выражение для поиска алертов по связанным с ними активам, пользователям, тенантам или корреляционным правилам. Параметры, по которым производится поиск:

- Активы: название, FQDN, IP-адрес.
- Учетные записи Active Directory: атрибуты displayName, SAMAccountName, UserPrincipalName.

- Корреляционные правила: название.
- Пользователи KUMA, которым назначены алерты: имя, логин, адрес электронной почты.
- Тенанты: название.

При фильтрации алертов по какому-либо параметру соответствующий заголовок таблицы алертов подсвечивается желтым цветом.

Сохранение и выбор конфигураций фильтра алертов

В KUMA можно сохранять изменения настроек таблицы алертов в виде фильтров. Конфигурации фильтров сохраняются на сервере Ядра KUMA и доступны всем пользователям KUMA того тенанта, для которого они были созданы.

► *Чтобы сохранить текущие настройки фильтра:*

1. В разделе KUMA **Алерты** откройте раскрывающийся список **Фильтры**.
2. Выберите **Сохранить текущий фильтр**.

   Появится поле для ввода названия нового фильтра и выбора тенанта, которому он будет принадлежать.
3. Введите название для конфигурации фильтра. Название должно быть уникальным для фильтров алертов, фильтров инцидентов и фильтров событий.
4. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать фильтр, и нажмите **Сохранить**.

Конфигурация фильтра сохранена.

► *Чтобы выбрать ранее сохраненную конфигурацию фильтра:*

1. В разделе KUMA **Алерты** откройте раскрывающийся список **Фильтры**.
2. Выберите нужную конфигурацию.

Конфигурация фильтра активна.

> Вы можете выбрать фильтр, который будет использоваться по умолчанию, поставив в раскрывающемся списке **Фильтры** звездочку левее названия требуемой конфигурации фильтра.

► *Чтобы сбросить текущие настройки фильтра,*

Откройте раскрывающийся список **Фильтры** и выберите **Очистить фильтры**.

Удаление конфигураций фильтра алертов

► *Чтобы удалить ранее сохраненную конфигурацию фильтра:*

1. В разделе KUMA **Алерты** откройте раскрывающийся список **Фильтры**.

2. Нажмите значок  на фильтре, который требуется удалить.
3. Нажмите **ОК**.

Конфигурация фильтра удалена для всех пользователей KUMA.

Просмотр информации об алерте

► *Чтобы просмотреть информацию об алерте:*

1. В окне веб-интерфейса программы выберите раздел **Алерты**.

   Отобразится таблица алертов.

2. Нажмите на имя алерта, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией об алерте.

В верхней части окна с информацией об алерте расположена панель инструментов, а также указаны уровень важности алерта и имя пользователя, которому назначен этот алерт. В этом окне можно обработать алерт (см. раздел "Обработка алертов" на стр. 335): изменить его уровень важности, назначить его пользователю, закрыть, создать на его основе инцидент.

Раздел Информация об алерте

Этот раздел позволяет просмотреть основную информацию об алерте. Он содержит следующие данные:

- **Уровень важности правила корреляции** – уровень важности правила корреляции, в результате срабатывания которого создан алерт.
- **Наивысшая важность категории активов** – самый высокий уровень важности категории активов из тех, которые принадлежат связанным с этим алертом активам. Если с алертом связано несколько активов, отображается наибольшее значение.
- **Привязан к инциденту** – если алерт привязан к инциденту,то отображаются название и статус алерта.
- **Первое появление** – дата и время создания первого корреляционного события (см. раздел "О событиях" на стр. 25) в последовательности событий, приведшего к созданию алерта.
- **Последнее появление** – дата и время создания последнего корреляционного события в последовательности событий, приведшего к созданию или обновлению алерта.
- **Идентификатор алерта** – уникальный идентификатор алерта в KUMA.
- **Тенант** – название тенанта (см. раздел "О тенантах" на стр. 25), которому принадлежит алерт.
- **Правило корреляции** – название правила корреляции (на стр. 134), в результате срабатывания которого создан алерт. Название правила представлено в виде ссылки, по которой можно перейти к настройкам этого правила корреляции.
- **Переполнен** – тег, означающий, что размер алерта достиг или приближается к пределу объема в 16 МБ и алерт необходимо обработать как можно скорее. Новые события не добавляются к переполненным алертам, но по ссылке **Смотреть все возможные связанные события** можно отфильтровать все события, которые могли быть связаны с алертом при отсутствии переполнения.

Раздел Связанные события

Этот раздел содержит таблицу событий, относящихся к алерту. Если нажать значок › рядом с правилом корреляции, отобразятся базовые события из этого правила корреляции. События можно сортировать по уровню важности и времени.

При выборе события в таблице открывается область деталей, содержащая информацию о выбранном событии. В области деталей также отображает кнопка **Подробные сведения**, при нажатии на которую открывается окно, содержащее информацию о корреляционном событии (см. раздел "Открытие окна корреляционного события" на стр. 357).

Ссылки **Найти в событиях** под корреляционными событиями и кнопка **Найти в событиях** справа от заголовка раздела используются для детализированного анализа (см. раздел "Детализированный анализ" на стр. 336).

С помощью кнопки **Скачать события** вы можете скачать информацию о связанных событиях в виде файла в формате CSV (в кодировке UTF-8). В файле доступны столбцы, заполненные хотя бы в одном связанном событии.

Некоторые редакторы CSV-файлов воспринимают значение разделителя (например, \n) в экспортируемом из КУМА CSV-файла как перенос строки, а не как разделитель. Может быть нарушено разделение файла на строки. Если вы столкнулись с подобным, то может потребоваться дополнительное редактирование CSV-файла, полученного из КУМА.

Раздел Связанные активы

Этот раздел содержит таблицу хостов (см. раздел "Управление активами" на стр. 376), относящихся к алерту. Информация о хостах поступает из событий, связанных с алертом. С помощью поля **Поиск по IP или FQDN** можно искать нужные хосты. Активы можно сортировать по столбцам **Количество** и **Актив**.

В этом разделе также отображаются активы, связанные с алертом. При нажатии на название актива открывается окно **Информация об активе**.

С помощью кнопки **Скачать активы** вы можете скачать информацию о связанных активах в виде файла в формате CSV (в кодировке UTF-8). В файле доступны столбцы: **Количество**, **Название**, **IP-адрес**, **Полное доменное имя**, **Категории**.

Раздел Связанные пользователи

Этот раздел содержит таблицу пользователей, относящихся к алерту. Информация о пользователях поступает из событий, связанных с алертом. С помощью поля **Поиск пользователей** можно искать нужных пользователей. Пользователей можно сортировать по столбцам **Количество**, **Пользователь**, **User principal name** (Основное имя пользователя) и **Адрес электронной почты**.

С помощью кнопки **Скачать пользователей** вы можете скачать информацию о связанных пользователях в виде файла в формате CSV (в кодировке UTF-8). В файле доступны столбцы: **Количество**, **Пользователь**, **User principal name**, **Адрес электронной почты**, **Домен**.

Раздел Журнал изменений

Этот раздел содержит записи об изменениях, которые пользователи внесли в алерт. Изменения регистрируются автоматически, при этом есть возможность вручную добавлять комментарии. Комментарии можно сортировать по столбцу **Время**.

При необходимости в поле **Комментарий** вы можете внести комментарий к алерту и нажать **Добавить**, чтобы сохранить его.

Обработка алертов

Вы можете изменить уровень важности алерта, назначить алерт пользователю, закрыть алерт или создать на основе алерта инцидент.

► *Чтобы обработать алерт:*

1. Выберите необходимые алерты одним из следующих способов:
   - В разделе **Алерты** веб-интерфейса KUMA нажмите на алерт, сведения о котором вы хотите просмотреть.

     Открывается окно алерта, в верхней его части расположена панель инструментов.
   - В разделе **Алерты** веб-интерфейса KUMA установите флажок рядом с требуемым алертом. Можно выбрать более одного алерта.

     > Алерты со статусом **Закрыт** не могут быть выбраны для обработки.

     В нижней части окна отображается панель инструментов.
2. Измените уровень важности алерта с помощью раскрывающегося списка **Уровень важности**:
   - **Низкий**
   - **Средний**
   - **Высокий**
   - **Критический**

   Уровень важности алерта принимает выбранное значение.
3. Назначьте алерт пользователю с помощью раскрывающегося списка **Назначить**.

   > Вы можете назначить алерт себе, выбрав **Мне**.

   Статус алерта меняется на **Назначен**, а в раскрывающемся списке **Назначить** отображается имя выбранного пользователя.
4. Создайте на основе алерта инцидент:
   a. Нажмите **Создать инцидент**.

      Откроется окно создания инцидента. В качестве названия инцидента используется название алерта.

   b. Измените нужны параметры инцидента и нажмите **Сохранить**.

   Инцидент создан, статус алерта меняется на **Эскалирован**. Алерт можно отвязать от инцидента, выбрав его и нажав **Отвязать**.
5. Закройте алерт:
   a. Нажмите **Закрыть алерт**.

Откроется окно подтверждения.

b. Укажите причину закрытия алерта:

- **Отработан**. Это означает, что были приняты необходимые меры по устранению угрозы безопасности.
- **Неверные данные**. Это означает, что алерт был ложным, а полученные события не указывают на угрозу безопасности.
- **Неверное правило корреляции**. Это означает, что алерт был ложным, а полученные события не указывают на угрозу безопасности. Возможно, требуется коррекция правила корреляции.

c. Нажмите **ОК**.

Статус алерта меняется на **Закрыт**. Алерты с таким статусом не обновляются новыми событиями корреляции и отображаются в таблице алертов, только если в раскрывающемся списке **Статус** установлен флажок **Закрыт**. Изменить статус закрытого алерта или назначить его другому пользователю невозможно.

Детализированный анализ

Детализированный анализ используется, когда вам нужно получить дополнительную информацию об угрозе, из-за которой был создан алерт: реальна ли угроза, откуда она исходит, на какие элементы сетевой среды она влияет, как следует бороться с угрозой. Анализ событий, связанных с корреляционными событиями, которые в свою очередь породили алерт, может помочь вам определить курс действий.

В KUMA режим детализированного анализа включается, когда вы нажимаете ссылку **Найти в событиях** в окне алерта (см. раздел "Просмотр информации об алерте" на стр. 333) или в окне корреляционного события (см. раздел "Открытие окна корреляционного события" на стр. 357). В режиме детализированного анализа отображается таблица событий с фильтрами, автоматически настроенными на поиск событий из алерта или корреляционного события. Фильтры также соответствуют времени продолжительности алерта или времени регистрации события корреляции. Вы можете изменить эти фильтры (см. раздел "Фильтрация и поиск событий" на стр. 341), чтобы найти другие события и узнать больше о процессах, связанных с угрозой.

В режиме детализированного анализа становится доступным дополнительный раскрывающийся список  :

- **Все события** – просмотр всех событий.
- **События алерта** (выбрано по умолчанию) – просмотр только событий, связанных с алертом.

  При фильтрации событий, связанным с алертом, действуют ограничения на сложность (см. раздел "Создание SQL-запроса вручную" на стр. 345) поисковых SQL-запросов.

Вы можете вручную привязать событие к алертам. К алерту можно привязать только не привязанные к нему события.

В режиме детализированного анализа можно создавать и сохранять конфигурации фильтров событий (см. раздел "Фильтрация и поиск событий" на стр. 341). При использовании этого фильтра в обычном режиме просмотра событий будут отображены все события, соответствующие критериям фильтра, независимо от того, привязаны ли они к алерту, выбранному для детализированного анализа.

► *Чтобы привязать базовое событие к алерту:*

1. В разделе **Алерты** веб-интерфейса KUMA нажмите алерт, к которому вы хотите привязать событие.

   Откроется окно алерта.

2. В разделе **Связанные события** нажмите кнопку **Найти в событиях**.

   Откроется таблица событий с включенными фильтрами даты и времени, соответствующим дате и времени регистрации привязанных к алерту событий, а в столбцах отображаются параметры, используемые правилом корреляции для создания алерта. В таблице событий также отображается столбец **Привязка к алерту**, в котором отмечаются события, привязанные к алерту.

3. В раскрывающемся списке  выберите значение **Все события**.

4. Измените фильтры, чтобы найти событие, которое требуется привязать к алерту.

5. Выберите нужное событие и нажмите кнопку **Привязать к алерту** в нижней части области деталей события.

Событие будет привязано к алерту. Вы можете отвязать это событие от алерта, нажав в области деталей **Отвязать от алерта**.

Когда событие привязывается или отвязывается от алерта, в его окне в разделе **Журнал изменений** добавляется запись об этом действии. Вы можете перейти по ссылке в этой записи и в открывшейся области деталей события или отвязать его, или привязать к алерту с помощью кнопок **Привязать к алерту** и **Отвязать от алерта**.

Срок хранения алертов

По умолчанию алерты хранятся в KUMA в течение года, но этот срок можно изменить, исправив параметры запуска программы в файле /usr/lib/systemd/system/kuma-core.service на сервере Ядра KUMA.

► *Чтобы изменить срок хранения алертов:*

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.
2. В файле /usr/lib/systemd/system/kuma-core.service измените следующую строку, подставив нужное количество дней:

   ```
   ExecStart=/opt/kaspersky/kuma/kuma core --alerts.retention <количество дней, в течение которых требуется хранить алерты> --external :7220 --internal :7210 --mongo mongodb://localhost:27017
   ```

3. Перезапустите KUMA, выполнив последовательно следующие команды:

   a. `systemctl daemon-reload`

   b. `systemctl restart kuma-core`

Срок хранения алертов изменен.

kaspersky

Правила сегментации алертов

В KUMA можно настроить *правила сегментации алертов*, то есть создание отдельных алертов по определенным условиям. Это может оказаться полезным, когда коррелятор (на стр. 23) группирует однотипные корреляционные события (см. раздел "О событиях" на стр. 25) в один общий алерт, однако вы хотите, чтобы на основе некоторых из этих событий, отличающихся чем-то важным от других, создавались отдельные алерты.

Правила сегментации создаются отдельно для каждого тенанта (см. раздел "О тенантах" на стр. 25). Они отображаются в разделе **Параметры** → **Алерты** → **Правила сегментации** веб-интерфейса KUMA в таблице со следующими столбцами:

- **Тенант** – название тенанта, которому принадлежат правила сегментации.
- **Обновлено** – дата и время последнего обновления правил сегментации.
- **Выключено** – в этом столбце отображается метка, если правила сегментации выключены.

► *Чтобы создать правило сегментации алерта:*

1. Откройте раздел **Параметры** → **Алерты** → **Правила сегментации** веб-интерфейса KUMA.
2. Выберите тенант, для которого вы хотите создать правило сегментации:
   - Если у тенанта уже есть правила сегментации, выберите его в таблице.
   - Если у тенанта нет правил сегментации, нажмите **Добавить тенант** и в раскрывающемся списке **Тенант** выберите нужный тенант.
3. В блоке параметров **Правила сегментации** нажмите **Добавить** и укажите параметры правила сегментации:
   - **Название** (обязательно) – в этом поле укажите название правила сегментации.
   - **Правило корреляции** (обязательно) – в этом раскрывающемся списке выберите правило корреляции, события которого вы хотите выделить в отдельный алерт.
   - **Селектор** (обязательно) – в этом блоке параметров требуется задать условие, при котором правило сегментации будет срабатывать. Условия формулируются аналогично фильтрам.
4. Нажмите **Сохранить**.

Правило сегментации алертов создано. События, подходящие под эти правила, будут объединены в отдельный алерт с названием правила сегментации.

► *Чтобы выключить правила сегментации:*

1. Откройте раздел **Параметры** → **Алерты** веб-интерфейса KUMA и выберите тенант, правила сегментации которого вы хотите выключить.
2. Установите флажок **Выключено**.
3. Нажмите **Сохранить**.

Правила сегментации алертов выбранного тенанта выключены.

Уведомления об алертах

При создании и назначении алертов по электронной почте рассылаются стандартные уведомления (см. раздел "Уведомления KUMA" на стр. 410) KUMA. Вы можете настроить рассылку уведомлений о создании алерта на основе пользовательского шаблона (см. раздел "Шаблоны уведомлений" на стр. 220) электронной почты.

► *Чтобы настроить рассылку уведомлений о создании алерта на основе пользовательского шаблона:*

1. Откройте раздел **Параметры** → **Алерты** → **Правила уведомлений** веб-интерфейса KUMA.
2. Выберите тенант, для которого вы хотите создать правило уведомления:
   - Если у тенанта уже есть правила уведомлений, выберите его в таблице.
   - Если у тенанта нет правил уведомлений, нажмите **Добавить тенант** и в раскрывающемся списке **Тенант** выберите нужный тенант.
3. В блоке параметров **Правила уведомлений** нажмите **Добавить** и укажите параметры правила уведомлений:
   - **Название** (обязательно) – в этом поле укажите название правила уведомления.
   - **Адреса получателей** (обязательно) – в этом блоке параметров с помощью кнопки **Адрес электронной почты** можно добавить адреса электронной почты, на которые необходимо отправлять уведомления о создании алертов. Адреса добавляются по одному.

     Кириллические домены не поддерживаются. Например, уведомление по адресу `login@домен.рф` отправлено не будет.

   - **Правила корреляции** (обязательно) – в этом блоке параметров необходимо выбрать одно или несколько правил корреляции, при срабатывании которых будут отправляться уведомления.

     В окне в виде древовидной структуры отображаются правила корреляции из общего и выбранного пользователем тенанта. Для выбора правила необходимо установить флажок рядом с ним. Можно установить флажок рядом с папкой: в таком случае будут выбраны все правила корреляции в этой папке и ее подпапках.
   - **Шаблон** (обязательно) – в этом блоке параметров необходимо выбрать шаблон электронной почты (см. раздел "Шаблоны уведомлений" на стр. 220), по которому будут создаваться рассылаемые уведомления. Для выбора шаблона нажмите на значок  , в открывшемся окне выберите требуемый шаблон и нажмите **Сохранить**.

Шаблон можно создать, нажав на значок плюса, или отредактировать выбранный шаблон, нажав на значок карандаша.

- **Выключено** – установив этот флажок вы можете выключить правило уведомления.

4. Нажмите **Сохранить**.

Правило уведомления создано. Когда по выбранным правилам корреляции будет создаваться алерт, на указанные адреса электронной почты будут отправляться уведомления, созданные на основе пользовательских шаблонов электронной почты. Стандартные уведомления KUMA о том же событии на указанные адреса отправлены не будут.

► *Чтобы выключить правила уведомлений для тенанта:*

1. Откройте раздел **Параметры** → **Алерты** → **Правила уведомлений** веб-интерфейса KUMA и выберите тенант, правила уведомлений которого вы хотите выключить.
2. Установите флажок **Выключено**.
3. Нажмите **Сохранить**.

Правила уведомлений выбранного тенанта выключены.

kaspersky

Работа с событиями

В разделе **События** веб-интерфейса KUMA вы можете просматривать полученные программой события, чтобы расследовать угрозы безопасности или создавать правила корреляции (на стр. 134). В таблице событий отображаются данные, полученные после выполнения SQL-запроса (см. раздел "Фильтрация и поиск событий" на стр. 341).

События можно отправлять в коррелятор для ретроспективной проверки (см. раздел "Ретроспективная проверка" на стр. 359).

Отображаемый формат даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

См. также:

О событиях 25

Архитектура программы 19

Модель данных нормализованного события 471

В этом разделе:

Фильтрация и поиск событий 341

Просмотр информации о событии 353

Экспорт событий 353

Выбор хранилища 354

Получение статистики по событиям в таблице 355

Настройка таблицы событий 355

Обновление таблицы событий 356

Открытие окна корреляционного события 357

Фильтрация и поиск событий

По умолчанию в разделе **События** веб-интерфейса KUMA данные не отображаются. Для просмотра событий в поле поиска нужно задать SQL-запрос и нажать на кнопку  . SQL-запрос можно ввести вручную (см. раздел "Создание SQL-запроса вручную" на стр. 345) или сформировать с помощью конструктора запросов (см. раздел "Формирование SQL-запроса с помощью конструктора" на стр. 343).

В SQL-запросах поддерживается агрегирование и группировка данных (см. раздел "Создание SQL-запроса вручную" на стр. 345).

Вы можете добавить условия фильтрации в уже сформированный SQL-запрос в окне просмотра статистики (см. раздел "Получение статистики по событиям в таблице" на стр. 355), таблицы событий и области деталей событий (см. раздел "Просмотр информации о событии" на стр. 353):

- Изменение запроса из окна статистики (см. раздел "Изменение параметров фильтра в окне статистики" на стр. 352)
- Изменение запроса из таблицы событий (см. раздел "Изменение фильтра в таблице событий" на стр. 352)
- Изменение запроса из области деталей события (см. раздел "Изменение фильтра в области деталей события" на стр. 352)

После изменения запроса все параметры запроса, включая добавленные условия фильтрации, переносятся в конструктор и строку поиска.
Параметры запроса, введенного вручную в строке поиска, при переключении на конструктор не переносятся в конструктор: вам требуется создать запрос заново. При этом запрос, созданный в конструкторе, не перезаписывает запрос, введенный в строке поиска, пока вы не нажмете на кнопку **Применить** в окне конструктора.

В поле ввода SQL-запроса можно включить отображение непечатаемых символов (см. раздел "Редактирование своей учетной записи" на стр. 71).

События можно также фильтровать по временному периоду (см. раздел "Фильтрация событий по периоду" на стр. 349). Результаты поиска можно автоматически обновлять (см. раздел "Обновление таблицы событий" на стр. 356).

Конфигурацию фильтра можно сохранить (см. раздел "Сохранение и выбор конфигураций фильтра событий" на стр. 350). Существующие конфигурации фильтров можно удалить (см. раздел "Удаление конфигураций фильтра событий" на стр. 350).

Функции фильтрации доступны пользователям всех ролей (см. раздел "Роли пользователей" на стр. 57).

Подробнее об SQL см. в справке ClickHouse https://clickhouse.com/docs/ru/sql-reference/. Также см. использование операторов в KUMA (см. раздел "Создание SQL-запроса вручную" на стр. 345) и поддерживаемые функции (см. раздел "Поддерживаемые функции ClickHouse" на стр. 351).

kaspersky

См. также:

О событиях 25
Хранилище 24
Формирование SQL-запроса с помощью конструктора 343
Создание SQL-запроса вручную 345
Ограничение сложности запросов в режиме детализированного анализа 348
Фильтрация событий по периоду 349
Сохранение и выбор конфигураций фильтра событий 350
Удаление конфигураций фильтра событий 350
Поддерживаемые функции ClickHouse 351
Изменение параметров фильтра в окне статистики 352
Изменение фильтра в области деталей события 352
Изменение фильтра в таблице событий 352

Формирование SQL-запроса с помощью конструктора

В KUMA вы можете сформировать SQL-запрос для фильтрации событий с помощью конструктора запросов.

► *Чтобы сформировать SQL-запрос с помощью конструктора:*

1. В разделе **События** веб-интерфейса KUMA нажмите на кнопку  .

   Откроется окно конструктора запросов.

2. Сформулируйте поисковый запрос, указав данные в следующих блоках параметров:

   - **SELECT** – поля событий, которые следует возвращать. По умолчанию выбрано значение *, означающее, что необходимо возвращать все доступные поля события. Для оптимизации поиска в раскрывающемся списке вы можете выбрать определенные поля, тогда данные из других полей загружаться не будут.

     Выбрав поле события, вы можете в поле справа от раскрывающегося списка указать псевдоним для столбца выводимых данных, а в крайнем правом раскрывающемся списке можно выбрать операцию, которую следует произвести над данными: **count**, **max**, **min**, **avg**, **sum**.

     Если вы используете в запросе функции агрегации, настройка отображения таблицы событий (см. раздел "Настройка таблицы событий" на стр. 355), сортировка событий по возрастанию и убыванию, получение статистики (см. раздел "Получение статистики по событиям в таблице" на стр. 355), а также ретроспективная проверка (на стр. 359) недоступны.

     В режиме детализированного анализа (см. раздел "Детализированный анализ" на стр. 336) при фильтрации по событиям, связанным с алертами, невозможно производить операции над данными полей событий и присваивать названия столбцам выводимых данных.

- **FROM** – источник данных. Выберите значение **events**.
- **WHERE** – условия фильтрации событий.

  Условия и группы условий можно добавить с помощью кнопок **Добавить условие** и **Добавить группу**. По умолчанию в группе условий выбрано значение оператора **AND**, однако если на него нажать, оператор можно изменить. Доступные значения: **AND**, **OR**, **NOT**. Структуру условий и групп условий можно менять, перетаскивая выражения с помощью мыши за значок .

  Добавление условий фильтра:

  a. В раскрывающемся списке слева выберите поле события, которое вы хотите использовать для фильтрации.

  b. В среднем раскрывающемся списке выберите нужный оператор. Доступные операторы зависят от типа значения выбранного поля события.

  c. Введите значение условия. В зависимости от выбранного типа поля вам потребуется ввести значение вручную, выбрать его в раскрывающемся списке или выбрать в календаре.

  Условия фильтра можно удалить с помощью кнопки . Группы условий удаляются с помощью кнопки **Удалить группу**.
- **GROUP BY** – поля событий или псевдонимы, по которым следует группировать возвращаемые данные.

  Если вы используете в запросе группировку данных, настройка отображения таблицы событий (см. раздел "Настройка таблицы событий" на стр. 355), сортировка событий по возрастанию и убыванию, получение статистики (см. раздел "Получение статистики по событиям в таблице" на стр. 355), а также ретроспективная проверка (на стр. 359) недоступны.

  > В режиме детализированного анализа при фильтрации по событиям, связанным с алертами, невозможно группировать возвращаемые данные.
- **ORDER BY** – столбцы, по которым следует сортировать возвращаемые данные. В раскрывающемся списке справа можно выбрать порядок: **DESC** – по убыванию, **ASC** – по возрастанию.
- **LIMIT** – количество отображаемых в таблице строк.

  Значение по умолчанию – 250.

  Если при фильтрации событий (см. раздел "Фильтрация событий по периоду" на стр. 349) по пользовательскому периоду количество строк в результатах поиска превышает заданное значение, вы можете отобразить в таблице дополнительные строки, нажав на кнопку **Показать больше записей**. Кнопка не отображается при фильтрации событий по стандартному периоду.

3. Нажмите на кнопку **Применить**.

   Текущий SQL-запрос будет перезаписан. В поле поиска отобразится сформированный SQL-запрос.

   Если вы хотите сбросить настройки конструктора, нажмите на кнопку **Запрос по умолчанию**.

   Если вы хотите закрыть конструктор, не перезаписывая существующий запрос, нажмите на кнопку .

4. Для отображения данных в таблице нажмите на кнопку .

В таблице отобразятся результаты поиска по сформированному SQL-запросу.

kaspersky

При переходе в другой раздел веб-интерфейса сформированный в конструкторе запрос не сохраняется. Если вы повторно вернетесь в раздел **События**, в конструкторе будет отображаться запрос по умолчанию.
Подробнее об SQL см. в справке ClickHouse https://clickhouse.com/docs/ru/sql-reference/. Также см. использование операторов в KUMA (см. раздел "Создание SQL-запроса вручную" на стр. 345) и поддерживаемые функции (см. раздел "Поддерживаемые функции ClickHouse" на стр. 351).

См. также:

Создание SQL-запроса вручную 345
О событиях 25
Хранилище 24

Создание SQL-запроса вручную

С помощью строки поиска вы можете вручную создавать SQL-запросы любой сложности для фильтрации событий (см. раздел "Фильтрация и поиск событий" на стр. 341).

► *Чтобы сформировать SQL-запрос вручную:*

1. Перейдите в раздел **События** веб-интерфейса KUMA.

   Откроется форма с полем ввода.

2. Введите SQL-запрос в поле ввода.

3. Нажмите на кнопку  .

Отобразится таблица событий, соответствующих условиям вашего запроса. При необходимости вы можете отфильтровать события по периоду (см. раздел "Фильтрация событий по периоду" на стр. 349).

Поддерживаемые функции и операторы

- `SELECT` – поля событий, которые следует возвращать.

  Для `SELECT` в программе поддержаны следующие функции и операторы:

  - Функции агрегации: `count, avg, max, min, sum`.
  - Арифметические операторы: `+, -, *, /, <, >, =, !=, >=, <=`.

    Вы можете комбинировать эти функции и операторы.

    Если вы используете в запросе функции агрегации, настройка отображения таблицы событий (см. раздел "Настройка таблицы событий" на стр. 355), сортировка событий по возрастанию и убыванию, получение статистики (см. раздел "Получение статистики по событиям в таблице" на стр. 355), а также ретроспективная проверка (на стр. 359) недоступны.

- `FROM` – источник данных.

При создании запроса в качестве источника данных вам нужно указать значение events.

- `WHERE` – условия фильтрации событий.
  - `AND, OR, NOT, =, !=, >, >=, <, <=`
  - `IN`
  - `BETWEEN`
  - `LIKE`
  - `ILIKE`
  - `inSubnet`
  - `match` (в запросах используется синтаксис регулярных выражений re2 https://github.com/google/re2/wiki/Syntax)
- `GROUP BY` – поля событий или псевдонимы, по которым следует группировать возвращаемые данные.

  Если вы используете в запросе группировку данных, настройка отображения таблицы событий (см. раздел "Настройка таблицы событий" на стр. 355), сортировка событий по возрастанию и убыванию, получение статистики (см. раздел "Получение статистики по событиям в таблице" на стр. 355), а также ретроспективная проверка (на стр. 359) недоступны.
- `ORDER BY` – столбцы, по которым следует сортировать возвращаемые данные.

  Возможные значения:
  - `DESC` – по убыванию.
  - `ASC` – по возрастанию.
- `OFFSET` – пропуск указанного количества строк перед выводом результатов запроса.
- `LIMIT` – количество отображаемых в таблице строк.

  Значение по умолчанию – 250.

  Если при фильтрации событий (см. раздел "Фильтрация событий по периоду" на стр. 349) по пользовательскому периоду количество строк в результатах поиска превышает заданное значение, вы можете отобразить в таблице дополнительные строки, нажав на кнопку **Показать больше записей**. Кнопка не отображается при фильтрации событий по стандартному периоду.

Примеры запросов:

- `SELECT * FROM `events` WHERE Type IN ('Base', 'Audit') ORDER BY Timestamp DESC LIMIT 250`

Все события таблицы events с типом **Base** и **Audit**, отсортированные по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- `SELECT * FROM `events` WHERE BytesIn BETWEEN 1000 AND 2000 ORDER BY Timestamp ASC LIMIT 250`

Все события таблицы events, для которых в поле **BytesIn** значение полученного трафика находится в диапазоне от 1000 до 2000 байт, отсортированные по столбцу **Timestamp** в порядке возрастания. Количество отображаемых в таблице строк – 250.

- `SELECT * FROM `events` WHERE Message LIKE '%ssh:%' ORDER BY Timestamp DESC LIMIT 250`

Все события таблицы events, которые в поле **Message** содержат данные, соответствующие заданному шаблону `%ssh:%` в нижнем регистре, и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- `SELECT * FROM `events` WHERE inSubnet(DeviceAddress, '00.0.0.0/00') ORDER BY Timestamp DESC LIMIT 250`

Все события таблицы events для хостов, которые входят в подсеть 00.0.0.0/00, отсортированные по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- `SELECT * FROM `events` WHERE match(Message, 'ssh.*') ORDER BY Timestamp DESC LIMIT 250`

Все события таблицы events, которые в поле **Message** содержат текст, соответствующий шаблону `ssh.*`, и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

- `SELECT max(BytesOut) / 1024 FROM `events``

Максимальный размер исходящего трафика (КБ) за выбранный период времени.

- `SELECT count(ID) AS "Count", SourcePort AS "Port" FROM `events` GROUP BY SourcePort ORDER BY Port ASC LIMIT 250`

Количество событий и номер порта. События сгруппированы по номеру порта и отсортированы по столбцу **Port** в порядке возрастания. Количество отображаемых в таблице строк – 250.
Столбцу **ID** в таблице событий присвоено имя Count, столбцу **SourcePort** присвоено имя Port.

Если вы хотите указать в запросе специальный символ, вам требуется экранировать его, поместив перед ним обратную косую черту (\).

Пример:

```
SELECT * FROM `events` WHERE match(Message, 'ssh:\'connection.*') ORDER BY Timestamp DESC LIMIT 250
```

Все события таблицы events, которые в поле **Message** содержат текст, соответствующий шаблону `ssh: 'connection'`, и отсортированы по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

При создании нормализатора (см. раздел "Нормализаторы" на стр. 158) для событий вы можете выбрать, сохранять ли значения полей исходного события. Данные сохраняются в поле события **Extra**. Поиск событий по этому полю осуществляется с помощью оператора LIKE.

Пример:

```
SELECT * FROM `events` WHERE DeviceAddress = '00.00.00.000' AND Extra
LIKE '%"app":"example"%' ORDER BY Timestamp DESC LIMIT 250
```

Все события таблицы events для хостов с IP-адресом 00.00.00.000, на которых запущен процесс example, отсортированные по столбцу **Timestamp** в порядке убывания. Количество отображаемых в таблице строк – 250.

При переключении на конструктор параметры запроса, введенного вручную в строке поиска, не переносятся в конструктор: вам требуется создать запрос заново. При этом запрос, созданный в конструкторе, не перезаписывает запрос, введенный в строке поиска, пока вы не нажмете на кнопку **Применить** в окне конструктора.
Подробнее об SQL см. в справке ClickHouse https://clickhouse.com/docs/ru/sql-reference/. Также см. поддерживаемые функции ClickHouse (на стр. 351).

См. также:

Формирование SQL-запроса с помощью конструктора 343
Ограничение сложности запросов в режиме детализированного анализа 348
О событиях 25
Хранилище 24

Ограничение сложности запросов в режиме детализированного анализа

При детализированном анализе (см. раздел "Детализированный анализ" на стр. 336) сложность SQL-запросов для фильтрации событий ограничена, если при расследовании алерта в раскрывающемся списке выбран пункт **События алерта**. В этом случае для фильтрации событий доступны только перечисленные ниже функции и операторы.

При выборе в раскрывающемся списке пункта **Все события** эти ограничения не действуют.

- `SELECT`
  - В качестве символа подстановки используется `*`.
- `WHERE`
  - `AND`, `OR`, `NOT`, `=`, `!=`, `>`, `>=`, `<`, `<=`
  - `IN`
  - `BETWEEN`

- `LIKE`
- `inSubnet`

Примеры:

- `WHERE Type IN ('Base', 'Correlated')`
- `WHERE BytesIn BETWEEN 1000 AND 2000`
- `WHERE Message LIKE '%ssh:%'`
- `WHERE inSubnet(DeviceAddress, '10.0.0.1/24')`

- `ORDER BY`

  Сортировка возможна по столбцам.

- `OFFSET`

  Пропуск указанного количества строк перед выводом результатов запроса.

- `LIMIT`

  Значение по умолчанию – 250.

  Если при фильтрации событий (см. раздел "Фильтрация событий по периоду" на стр. 349) по пользовательскому периоду количество строк в результатах поиска превышает заданное значение, вы можете отобразить в таблице дополнительные строки, нажав на кнопку **Показать больше записей**. Кнопка не отображается при фильтрации событий по стандартному периоду.

В режиме детализированного анализа при фильтрации по событиям, связанным с алертами, невозможно группировать возвращаемые данные. В режиме детализированного анализа при фильтрации по событиям, связанным с алертами, невозможно производить операции над данными полей событий и присваивать названия столбцам выводимых данных.

Фильтрация событий по периоду

В KUMA вы можете настроить отображение событий, относящихся к определенному временному периоду.

► *Чтобы отфильтровать события по периоду:*

1. В разделе **События** веб-интерфейса KUMA в верхней части окна откройте раскрывающийся список **Период**.
2. Если вы хотите выполнить фильтрацию по стандартному периоду, выберите один из следующих вариантов:
   - **5 минут**
   - **15 минут**
   - **1 час**
   - **24 часа**
   - **В течение периода**

     При выборе этого варианта в открывшемся календаре выберите дату начала и окончания периода и нажмите **Применить фильтр**. Формат даты и времени зависит от настроек вашей операционной системы. При необходимости вы также можете изменить значения даты вручную.

3. Нажмите на кнопку .

   Если установлен фильтр по периоду, отобразятся только события, зарегистрированные в течение указанного интервала времени. Период отобразится в верхней части окна.

Вы также можете настроить отображение событий с помощью гистограммы событий, которая отображается при нажатии на кнопку в верхней части раздела **События**. События отобразятся, если нажать на нужный ряд данных или выделить требуемый период времени и нажать на кнопку **Показать события**.

Сохранение и выбор конфигураций фильтра событий

В KUMA вы можете сохранять конфигурации фильтров для использования в будущем или другими пользователями. При сохранении фильтра вы сохраняете настроенные параметры сразу всех активных фильтров: фильтр по периоду, конструктору запросов и параметры таблицы событий. Поисковые запросы сохраняются на сервере Ядра KUMA и доступны всем пользователям KUMA выбранного тенанта.

► *Чтобы сохранить текущие настройки фильтра, запроса и периода:*

1. В разделе **События** веб-интерфейса KUMA нажмите на значок рядом с выражением фильтра и выберите **Сохранить текущий фильтр**.
2. В открывшемся окне в поле **Название** введите название конфигурации фильтра. Название должно содержать до 128 символов Юникода.
3. В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать создаваемый фильтр.
4. Нажмите **Сохранить**.

Конфигурация фильтра сохранена.

► *Чтобы выбрать ранее сохраненную конфигурацию фильтра:*

в разделе **События** веб-интерфейса KUMA нажмите на значок рядом с выражением фильтра и выберите нужный фильтр.

Выбранная конфигурация активна: в поле поиска отображается поисковый запрос, в верхней части окна настроенные параметры периода и частоты обновления результатов поиска. Для отправки поискового запроса нажмите на кнопку .

Если нажать на значок рядом с названием конфигурации фильтра, она станет использоваться в качестве конфигурации по умолчанию.

Удаление конфигураций фильтра событий

► *Чтобы удалить ранее сохраненную конфигурацию фильтра:*

1. В разделе **События** веб-интерфейса KUMA нажмите на значок рядом с поисковым запросом фильтра и нажмите значок рядом с конфигурацией, которую требуется удалить.
2. Нажмите **ОК**.

Конфигурация фильтра удалена для всех пользователей KUMA.

kaspersky

Поддерживаемые функции ClickHouse

В KUMA поддерживаются следующие функции ClickHouse:

- Арифметические функции.
- Массивы – все функции, кроме:
  - has;
  - range;
  - функций, в которых обязательны к использованию функции высшего порядка (стрелочные лямбда-выражения (->)).
- Функции сравнения: все операторы, кроме == и less.
- Логические функции: только функция not.
- Функции преобразования типов.
- Функции для работы с датами и временем: все функции, кроме date_add и date_sub.
- Функции для работы со строками.
- Функции поиска в строках – все функции, кроме:
  - position;
  - multiSearchAllPositions, multiSearchAllPositionsUTF8, multiSearchFirstPosition, multiSearchFirstIndex, multiSearchAny;
  - like и ilike;
- Условные функции: только обычный оператор if (тернарный оператор и оператор miltif не поддерживаются).
- Математические функции.
- Функции округления.
- Функции разбиения и слияния строк и массивов.
- Битовые функции.
- Функции для работы с UUID.
- Функции для работы с URL.
- Функции для работы с IP-адресами.
- Функции для работы с Nullable-аргументами.
- Функции для работы с географическими координатами.

Функции поиска и замены в строках, а также функции из остальных разделов не поддерживаются.

Подробнее об SQL см. в справке ClickHouse https://clickhouse.com/docs/ru/sql-reference/.

Изменение параметров фильтра в окне статистики

► *Чтобы изменить параметры фильтрации из окна **Статистика**:*

1. Откройте область деталей **Статистика** одним из следующих способов:
   - В правом верхнем углу таблицы событий в раскрывающемся списке  выберите **Статистика**.
   - В таблице событий нажмите на любое значение и в открывшемся контекстном меню выберите **Статистика**.

   В правой части окна откроется область деталей **Статистика**.
2. Откройте раскрывающийся список необходимого параметра и наведите курсор мыши на требуемое значение.
3. С помощью значков плюса и минуса измените параметры фильтрации, выполнив одно из следующих действий:
   - Если вы хотите включить в выборку событий только события с выбранным значением, нажмите +.
   - Если вы хотите исключить из выборки событий все события с выбранным значением, нажмите −.

В результате параметры фильтрации и таблица событий будут обновлены, а в верхней части экрана отобразится измененный поисковый запрос.

Изменение фильтра в области деталей события

► *Чтобы изменить параметры фильтрации в области деталей события:*

1. В разделе **События** веб-интерфейса KUMA нажмите на нужное событие.

   В правой части окна откроется область деталей **Информация о событии**.
2. Измените параметры фильтрации, используя значки плюса или минуса рядом с необходимыми параметрами:
   - Если вы хотите включить в выборку событий только события с выбранным значением, нажмите +.
   - Если вы хотите исключить из выборки событий все события с выбранным значением, нажмите −.

В результате параметры фильтрации и таблица событий будут обновлены, а в верхней части экрана отобразится измененный поисковый запрос.

Изменение фильтра в таблице событий

► *Чтобы изменить параметры фильтрации из таблицы событий:*

1. В разделе **События** веб-интерфейса KUMA нажмите на любое значение параметра события в таблице событий.
2. В открывшемся меню выберите один из следующих вариантов:

- Если вы хотите оставить в таблице только события с выбранным значением, выберите **Искать события с этим значением**.
- Если вы хотите исключить из таблицы все события с выбранным значением, выберите **Искать события без этого значения**.

В результате параметры фильтрации и таблица событий обновляются, а в верхней части экрана отображается измененный поисковый запрос.

Просмотр информации о событии

► *Чтобы просмотреть информацию о событии:*

1. В окне веб-интерфейса программы выберите раздел **События**.
2. Выполните поиск событий с помощью конструктора запросов (см. раздел "Формирование SQL-запроса с помощью конструктора" на стр. 343) или введя запрос в строке поиска (см. раздел "Создание SQL-запроса вручную" на стр. 345).

   Отобразится таблица событий.
3. Выберите событие, информацию о котором вы хотите просмотреть.

   Откроется окно с информацией о событии.

В правой части окна отображается область деталей **Информация о событии** со списком параметров события и их значений. В этой области деталей можно:

- Включить выбранное поле в поиск или исключить его из поиска, нажав на + и − рядом со значением параметра.
- По хешу файла в поле **FileHash** раскрывается список, в котором вы можете выбрать одно из следующих действий:
  - Показать информацию из Threat Lookup.

    Доступно при интеграции с Kaspersky Threat Intelligence Portal (см. раздел "Интеграция с Kaspersky Threat Intelligence Portal" на стр. 87).
  - Добавить в Internal TI CyberTrace.
  - Доступно при интеграции с Kaspersky CyberTrace (см. раздел "Интеграция с Kaspersky CyberTrace" на стр. 81).
- По ссылке с именем коллектора в поле **Service** вы можете просмотреть параметры сервиса, зарегистрировавшего событие.

  Вы также можете привязать событие к алерту, если программа находится в режиме детализированного анализа (см. раздел "Детализированный анализ" на стр. 336), и открыть окно **Информация о корреляционном событии** (см. раздел "**Открытие окна корреляционного события**" на стр. 357), если выбранное событие является корреляционным.

Экспорт событий

Из KUMA можно экспортировать информацию о событиях в TSV-файл. Выборка событий, которые будут экспортированы в TSV-файл, зависит от настроек фильтра (см. раздел "Фильтрация и поиск событий" на

стр. 341). Информация экспортируется из столбцов, которые в данный момент отображаются в таблице событий (см. раздел "Настройка таблицы событий" на стр. 355), при этом столбцы в файле наполняются доступными данными, даже если в таблице событий в веб-интерфейсе KUMA они были пустыми из-за особенностей SQL-запроса.

► *Чтобы экспортировать информацию о событиях:*

1. В разделе **События** веб-интерфейса KUMA откройте раскрывающийся список  и выберите **Экспортировать в формат TSV**.

   Новая задача экспорта TSV-файла создается в разделе **Диспетчер задач**.

2. Найдите созданную вами задачу в разделе **Диспетчер задач**.

   Когда файл будет готов к загрузке, в строке задачи в столбце **Статус** отобразится значок  .

3. Нажмите на название типа задачи и в раскрывающемся списке выберите **Загрузить**.

   TSV-файл с информацией о событиях будет загружен с использованием настроек вашего браузера. Имя файла по умолчанию: event-export-<date>_<time>.tsv.

Файл сохраняется в соответствии с настройками вашего веб-браузера.

Выбор хранилища

События, которые отображаются в веб-интерфейсе KUMA в разделе **События**, получены из хранилища (см. раздел "Хранилище" на стр. 24) (то есть кластера ClickHouse). В зависимости от потребностей вашей компании у вас может быть более одного хранилища, однако для получения событий необходимо указывать, события из какого именно хранилища вам требуются.

► *Чтобы выбрать хранилище, из которого вы хотите получать события,*

В разделе **События** веб-интерфейса KUMA откройте раскрывающийся список  и выберите нужный кластер хранилища.

В таблице событий отображаются события из указанного хранилища. Имя выбранного хранилища отображается в раскрывающемся списке  .

В раскрывающемся списке  отображаются только кластеры тенантов (см. раздел "О тенантах" на стр. 25), доступных пользователю, а также кластер главного тенанта.

См. также:

Хранилище 24

kaspersky

Получение статистики по событиям в таблице

Вы можете получить статистику по текущей выборке событий, отображаемой в таблице событий. Выборка событий зависит от параметров фильтрации (см. раздел "Фильтрация и поиск событий" на стр. 341).

► *Чтобы получить статистику:*

в правом верхнем углу таблицы событий в раскрывающемся списке  выберите **Статистика** или в таблице событий нажмите на любое значение и в открывшемся контекстном меню выберите **Статистика**.

Появится область деталей **Статистика** со списком параметров текущей выборки событий. Числа возле каждого параметра указывают количество событий в выборке, для которых задан этот параметр. Если параметр раскрыть, отображается его пять наиболее частотных значений. С помощью поля **Поиск** можно найти нужные параметры.

В окне **Статистика** можно менять фильтр событий.

При использовании для фильтрации событий SQL-запросов с группировкой и агрегацией данных статистика недоступна.

Настройка таблицы событий

В разделе **События** отображаются ответы на SQL-запросы (см. раздел "Фильтрация и поиск событий" на стр. 341) пользователя, представленные в виде таблицы. Таблицу можно обновлять (см. раздел "Обновление таблицы событий" на стр. 356).

Столбцы таблицы событий, отображаемые по умолчанию:

- **Тенант**.
- **Timestamp**.
- **Name**.
- **DeviceProduct**.
- **DeviceVendor**.
- **DestinationAddress**.
- **DestinationUserName**.

В KUMA можно настроить отображаемый набор полей событий и порядок их отображения. Выбранную конфигурацию можно сохранить (см. раздел "Сохранение и выбор конфигураций фильтра событий" на стр. 350).

При использовании для фильтрации событий (см. раздел "Создание SQL-запроса вручную" на стр. 345) SQL-запросов с группировкой и агрегацией данных статистика недоступна, а состав и порядок столбцов зависит от SQL-запроса.

► *Чтобы настроить поля, отображаемые в таблице событий:*

1. В правом верхнем углу таблицы событий нажмите значок .

   Откроется окно для выбора полей событий, которые требуется отображать в таблице событий.

2. Установите флажки напротив полей, которые требуется отображать в таблице. С помощью поля **Поиск** можно найти нужные поля.

   Вы можете отобразить в таблице любое поле события из модели данных событий KUMA. Параметры **Timestamp** (Время) и **Name** (Название) всегда отображаются в таблице. С помощью кнопки **По умолчанию** можно вернуть исходные настройки отображения таблицы событий.

   Когда вы устанавливаете флажок, таблица событий обновляется и добавляется новый столбец. При снятии флажка столбец исчезает.

   > Столбец можно удалить из таблицы событий, если нажать на его заголовок и в раскрывающемся списке выбрать **Скрыть столбец**.

3. При необходимости измените порядок отображения столбцов, перетаскивая заголовки столбцов в таблице событий.

4. Если вы хотите сортировать события по определенному столбцу, нажмите на его заголовок и в раскрывающемся списке выберите один из вариантов: **По возрастанию** или **По убыванию**.

Выбранные поля событий отобразятся в таблице раздела **События** в качестве столбцов в указанном вами порядке.

Обновление таблицы событий

Таблицу событий можно обновлять, перегружая страницу веб-браузера. Можно также настроить автоматическое обновление таблицы событий, установив частоту обновления. По умолчанию автоматическое обновление отключено.

► *Чтобы включить автоматическое обновление,*

Выберите частоту обновления в раскрывающемся списке :

- **5 секунд**
- **15 секунд**
- **30 секунд**
- **1 минута**
- **5 минут**
- **15 минут**

Таблица событий обновляется автоматически.

► *Чтобы выключить автоматические обновление,*

Выберите **Не обновлять** в раскрывающемся списке .

kaspersky

Открытие окна корреляционного события

Вы можете просматривать подробные сведения о корреляционном событии в окне **Информация о корреляционном событии**.

► *Чтобы открыть окно корреляционного события:*

1. В разделе **События** веб-интерфейса KUMA нажмите на корреляционное событие.

   Вы можете использовать фильтры для поиска событий корреляции, присвоив значение `correlated` параметру `Type`.

   Откроется область деталей выбранного события. Если выбранное событие является корреляционным, в нижней части области деталей будет отображаться кнопка **Подробные сведения**.

2. Нажмите на кнопку **Подробные сведения**.

Откроется окно корреляционного события. Название события отображается в левом верхнем углу окна.

В разделе **Информация о корреляционном событии** окна корреляционного события отображаются следующие данные:

- **Уровень важности корреляционного события** – важность корреляционного события.
- **Правило корреляции** – название правила корреляции (на стр. 134), которое породило корреляционное событие. Название правила представлено в виде ссылки, по которой можно перейти к настройкам этого правила корреляции.
- Уровень важности правила корреляции – важность правила корреляции, вызвавшего корреляционное событие.
- **Идентификатор правила корреляции** – идентификатор правила корреляции, которое породило корреляционное событие.
- **Тенант** – название тенанта, которому принадлежит корреляционное событие.

Раздел **Связанные события** окна корреляционного события содержит таблицу событий, относящихся к корреляционному событию. Это базовые события, в результате обработки которых было создано корреляционное событие. При выборе события в правой части окна веб-интерфейса открывается область деталей.

Ссылка **Найти в событиях** справа от заголовка раздела используется для детализированного анализа (см. раздел "Детализированный анализ" на стр. 336).

Раздел **Связанные активы** окна корреляционного события содержит таблицу узлов, относящихся к корреляционному событию. Эта информация поступает из базовых событий, связанных с корреляционным событием. При нажатии на название актива открывается окно **Информация об активе**.

Раздел **Связанные пользователи** окна корреляционного события содержит таблицу пользователей, относящихся к корреляционному событию. Эта информация поступает из базовых событий, связанных с корреляционным событием.

kaspersky

См. также:

Об алертах 27

Коррелятор 23

Детализированный анализ 336

kaspersky

Ретроспективная проверка

Вы можете использовать функцию *Ретроспективная проверка* для "воспроизведения" событий в KUMA путем передачи выборки событий в коррелятор (на стр. 23) для их обработки определенными правилами корреляции (см. раздел "Правила корреляции" на стр. 134). Можно указать, чтобы во время ретроспективной проверки событий создавались алерты (см. раздел "Об алертах" на стр. 27). Ретроспективная проверка может быть полезна при отладке ресурсов правил корреляции или анализе исторических данных.

При ретроспективной проверке события не обогащаются данными из CyberTrace (см. раздел "Интеграция с Kaspersky CyberTrace" на стр. 81) и Kaspersky Threat Intelligence Portal (см. раздел "Интеграция с Kaspersky Threat Intelligence Portal" на стр. 87).

Активные листы (на стр. 224) при ретроспективной проверке обновляются.

Ретроспективную проверку невозможно проводить на выборках событий, полученных с помощью SQL-запросов с группировкой данных, агрегацией данных и с арифметическими выражениями.

► *Чтобы включить ретроспективную проверку:*

1. В разделе **События** веб-интерфейса KUMA получите необходимую выборку событий:
   - Выберите хранилище.
   - Настройте поисковое выражение с помощью конструктора или поискового запроса.
   - Задайте необходимый временной период.
2. В раскрывающемся списке  выберите **Ретроспективная проверка**.

   Откроется окно ретроспективной проверки.
3. В раскрывающемся списке **Коррелятор** выберите сервис коррелятора, в который будут загружены выбранные события.
4. В раскрывающемся списке **Правила корреляции** выберите правила корреляции, с помощью которых необходимо обработать выбранные события.
5. Если вы хотите, чтобы в процессе обработки событий срабатывали правила реагирования, включите переключатель **Выполнить правила реагирования**.
6. Если вы хотите, чтобы в процессе обработки событий создавались алерты, включите переключатель Создать алерты. Если вы хотите, чтобы при обработке событий создавались алерты, включите переключатель **Создать алерты**.
7. Нажмите на кнопку **Создать задачу**.

В разделе **Диспетчер задач** создана задача ретроспективной проверки.

► *Чтобы просмотреть результаты проверки,*

В разделе **Диспетчер задач** веб-интерфейса KUMA нажмите на созданную вами задачу и в раскрывающемся списке выберите **Перейти к событиям**.

Открывается новая вкладка браузера с таблицей событий, обработанных в ходе ретроспективной проверки, а также агрегированными и корреляционными событиями, созданные во время обработки.

В зависимости от настроек вашего браузера может потребоваться ваше подтверждение на открытие новой вкладки с результатами ретроспективной проверки. Подробнее см. в документации вашего браузера.

kaspersky

Работа с геоданными

В KUMA можно загрузить список соответствий IP-адресов или диапазонов IP-адресов географическим данным, чтобы затем использовать эту информацию при обогащении (см. раздел "Правила обогащения" на стр. 194) событий.

В этом разделе

Формат геоданных 361

Конвертация геоданных из MaxMind и IP2Location 362

Импорт и экспорт геоданных 363

Сопоставление геоданных по умолчанию 364

Формат геоданных

Геоданные можно загрузить в KUMA в виде CSV-файла в кодировке UTF-8. В качестве разделителя используется запятая. В первой строке файла указаны заголовки полей: `Network,Country,Region,City,Latitude,Longitude`.

Таблица 6. Описание CSV-файла

Имя заголовка поля в CSV	Описание поля	Пример
`Network`	IP-адрес в одном из следующих форматов: • единичный IP-адрес; • диапазон IP-адресов; • IP-адрес в формате CIDR. Допускается перемешивание ipv4- и ipv6-адресов. Обязательное поле.	• `192.168.2.24` • `192.168.2.25-192.168.2.35` • `131.10.55.70/8` • `2001:DB8::0/120`
`Country`	Принятое в вашей организации обозначение страны. Например, ее название или код. Обязательное поле.	• `Russia` • `RU`

`Region`	Принятое в вашей организации обозначение области. Например, ее название или код.	• `Sverdlovsk Oblast` • `RU-SVE`
`City`	Принятое в вашей организации обозначение города. Например, его название или код.	• `Yekaterinburg` • `65701000001`
`Latitude`	Широта описываемой точки в десятичном формате. Поле может быть пустым – в этом случае при импорте в KUMA будет использовано значение 0.	`56.835556`
`Longitude`	Долгота описываемой точки в десятичном формате. Поле может быть пустым – в этом случае при импорте в KUMA будет использовано значение 0.	`60.612778`

Конвертация геоданных из MaxMind и IP2Location

В KUMA можно использовать геоданные, полученные из MaxMind https://dev.maxmind.com/geoip/docs/databases/city-and-country?lang=en#csv-databases и IP2Location https://www.ip2location.com/database/ip2location, однако перед этим их требуется конвертировать в поддерживаемый KUMA формат (см. раздел "Формат геоданных" на стр. 361). Конвертацию можно произвести помощью приведенного ниже скрипта.

Скачать скрипт converter.zip

Для запуска скрипта требуется Python 2.7 или выше.

Команда запуска скрипта:

```
python converter.py --type <тип обрабатываемых геоданных: "maxmind" или
"ip2location"> --out <директория, в которую будет помещен CSV-файл с
```

```
геоданными в формате KUMA> --input <путь к ZIP-архиву с геоданными из
MaxMind или IP2location>
```

При запуске скрипта с флагом `--help` отображается справка по доступным параметрам запуска скрипта:
`python converter.py --help`

Команда для конвертации файла с российской базой диапазонов IP-адресов из ZIP-архива MaxMind:

```
python converter.py --type maxmind --lang ru --input MaxMind.zip --out
geoip_maxmind_ru.csv
```

Без указания параметра `--lang` скрипт по умолчанию получает информацию из файла GeoLite2-City-Locations-en.csv из ZIP-архива.

Отсутствие параметра `--lang` для MaxMind равнозначно команде:

```
python converter.py --type maxmind --input MaxMind.zip --out
geoip_maxmind.csv
```

Команда для конвертации файла из ZIP-архива IP2Location:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-
DB11.CSV.ZIP --out geoip_ip2location.csv
```

Команда для конвертации файла из нескольких ZIP-архивов IP2Location:

```
python converter.py --type ip2location --input IP2LOCATION-LITE-
DB11.CSV.ZIP IP2LOCATION-LITE-DB11.IPV6.CSV.ZIP --out
geoip_ip2location_ipv4_ipv6.csv
```

Параметр `--lang` для IP2Location не используется.

Импорт и экспорт геоданных

При необходимости в KUMA вы можете вручную импортировать и экспортировать геоданные. Геоданные импортируются и экспортируются в файле формате CSV. При успешном импорте геоданных ранее добавленные данные перезаписываются и в KUMA создается событие аудита (см. раздел "Поля событий аудита" на стр. 502).

► *Чтобы импортировать геоданные в KUMA:*

1. Подготовьте CSV-файл (см. раздел "Формат геоданных" на стр. 361) с геоданными.

   Геоданные, полученные из MaxMind и IP2Location, требуется конвертировать (см. раздел "Конвертация геоданных из MaxMind и IP2Location" на стр. 362) в поддерживаемый KUMA формат.

2. В веб-интерфейсе KUMA откройте раздел **Параметры** → **Общие**.

3. В блоке параметров **Геоданные** нажмите на кнопку **Импортировать из файла** и выберите CSV-файл с геоданными.

   Дождитесь окончания импорта геоданных. При обновлении страницы загрузка данных прерывается.

Геоданные загружены в KUMA.

► *Чтобы экспортировать геоданные из KUMA,*

1. В веб-интерфейсе KUMA откройте раздел **Параметры** → **Общие**.
2. В блоке параметров **Геоданные** нажмите на кнопку **Экспортировать**.

Геоданные будут скачаны в виде CSV-файла (в кодировке UTF-8) с названием geoip.csv в соответствии с настройками вашего браузера.

Данные экспортируются в том же формате, в каком они были загружены, за исключением диапазонов IP-адресов. Если в KUMA в импортированном файле диапазон адресов указан в формате `1.0.0.0/24`, то в файле экспорта диапазон отобразится в формате `1.0.0.0-1.0.0.255`.

kaspersky

Сопоставление геоданных по умолчанию

Если при настройке правила обогащения (на стр. 194) геоданными в качестве источника IP-адреса выбрать поля события `SourceAddress`, `DestinationAddress` и `DeviceAddress`, становится доступна кнопка **Применить сопоставление по умолчанию**. С ее помощью можно добавить преднастроенные пары соответствий атрибутов геоданных (см. раздел "Формат геоданных" на стр. 361) и полей события (см. раздел "Модель данных нормализованного события" на стр. 471), описанные ниже.

Соответствия по умолчанию для поля события SourceAddress

Атрибут геоданных	Поле события
Страна	`SourceCountry`
Регион	`SourceRegion`
Город	`SourceCity`
Широта	`SourceLatitude`
Долгота	`SourceLongitude`

Соответствия по умолчанию для поля события DestinationAddress

Атрибут геоданных	Поле события
Страна	`DestinationCountry`
Регион	`DestinationRegion`
Город	`DestinationCity`
Широта	`DestinationLatitude`
Долгота	`DestinationLongitude`

Соответствия по умолчанию для поля события DeviceAddress

Атрибут геоданных	Поле события
Страна	`DeviceCountry`
Регион	`DeviceRegion`
Город	`DeviceCity`
Широта	`DeviceLatitude`
Долгота	`DeviceLongitude`

kaspersky

Передача в KUMA событий из изолированных сегментов сети

Схема передачи данных

С помощью диодов данных можно передавать события из изолированных сегментов сети в KUMA. Передача данных организована следующим образом:

1. Установленный на изолированном сервере агент KUMA с точкой назначения (см. раздел "Тип diode" на стр. 204) **diode** принимает события и сначала копит их во временной директории, а затем перемещает в директорию, из которой их заберет диод данных.

   Во временной директории события копятся до переполнении буфера точки назначения или в течение 10 секунд после последней записи на диск. Затем события записываются в файл, в качестве названия которого используется хеш-сумма (SHA-256) содержимого файла. Этот файл перемещается в директорию, обрабатываемую диодом данных.

2. Диод данных перемещает файлы из директории изолированного сервера в директорию внешнего сервера.

3. Установленный на внешнем сервере коллектор KUMA с коннектором (см. раздел "Тип diode" на стр. 187) **diode** считывает и обрабатывает события из файлов той директории, в которой размещает файлы диод данных.

   После считывания из файла всех событий он автоматически удаляется. Перед считыванием событий происходит верификация содержимого файлов по хеш-сумме в названии файла. Если содержимое не проходит верификацию, файл удаляется.

В указанной выше схеме компоненты KUMA отвечают за перемещение событий в определенную директорию внутри изолированного сегмента и за прием событий из определенной директории во внешнем сегменте сети. Перемещение файлов с событиями из директории изолированного сегмента сети в директорию внешнего сегменте сети осуществляет диод данных.

Для каждого источника данных внутри изолированного сегмента сети необходимо создать свой агент и коллектор KUMA, а также настроить диод данных на работу с отдельными директориями.

Настройка компонентов KUMA

Настройка компонентов KUMA для передачи данных из изолированных сегментов сети состоит из следующих этапов:

1. Создание сервиса коллектора во внешнем сегменте сети.

   На этом этапе необходимо создать и установить коллектор (см. раздел "Создание коллектора" на стр. 235) для получения и обработки файлов, которые диод данных будет перемещать из изолированного сегмента сети. Создать коллектор и все требуемые для него ресурсы можно с помощью мастера установки коллектора.

   На шаге **Транспорт** (см. раздел "**Шаг 2. Транспорт**" на стр. 238) требуется выбрать или создать коннектор типа **diode** (см. раздел "**Тип diode**" на стр. 187). В коннекторе необходимо указать директорию, в которую диод данных будет перемещать файлы из изолированного сегмента сети.

   Пользователь kuma, под которым работает коллектор, должен иметь права на чтение, запись и удаление в директории, в которую диод данных перемещает данные из изолированного сегмента сети.

2. Создание набора ресурсов агента KUMA.

На этом этапе необходимо создать набор ресурсов агента (см. раздел "Создание набора ресурсов для агента" на стр. 264) KUMA, который будет в изолированном сегменте сети получать события и подготавливать их для передачи диоду данных. Набор ресурсов diode-агента имеет следующие особенности:

- Ресурс точки назначения в агенте должен иметь тип **diode** (см. раздел "**Тип diode**" на стр. 204). В этом ресурсе необходимо указать директорию, из которой диод данных будет перемещать файлы во внешний сегмент сети.
- Для diode-агента невозможно выбрать коннекторы типа **sql** или **netflow**.

3. Скачивание конфигурационного файла агента в виде JSON-файла.

   a. Набор ресурсов агента с точкой назначения типа diode необходимо скачать в виде JSON-файла (см. раздел "Конфигурационный файл diode-агента" на стр. 368).

   b. Если в наборе ресурсов агента использовались ресурсы секретов, конфигурационный файл необходимо вручную дополнить данными секретов.

4. Установка сервиса агента KUMA в изолированном сегменте сети.

   На этом этапе необходимо установить агент в изолированном сегменте сети на основе конфигурационного файла агента, созданного на предыдущем этапе. Установка возможна на устройствах Linux (см. раздел "Установка Linux-агента в изолированном сегменте сети" на стр. 374) и Windows (см. раздел "Установка Windows-агента в изолированном сегменте сети" на стр. 374).

Настройка диода данных

Диод данных необходимо настроить следующим образом:

- Данные необходимо передавать атомарно из директории изолированного сервера (куда их помещает агент KUMA) в директорию внешнего сервера (где их считывает коллектор KUMA).
- Переданные файлы необходимо удалять с изолированного сервера.

Сведения о настройке диода данных можно получить в документации используемого в вашей организации диода данных.

Особенности работы

При работе с изолированными сегментами сети не поддерживаются работа с SQL и NetFlow.

При использовании указанной выше схемы невозможно администрирование агента через веб-интерфейс KUMA, поскольку он располагается в изолированном сегменте сети. В списке активных сервисов KUMA такие агенты не отображаются.

kaspersky

В этом разделе:

Конфигурационный файл diode-агента 368
Описание полей секретов 373
Установка Linux-агента в изолированном сегменте сети 374
Установка Windows-агента в изолированном сегменте сети 374

См. также:

Об агентах 29
Коллектор 20
Наборы ресурсов для сервисов 235

Конфигурационный файл diode-агента

Созданный набор ресурсов агента с точкой назначения типа diode можно скачать в виде конфигурационного файла. Этот файл используется при установке агента в изолированном сегменте сети.

► *Чтобы скачать конфигурационный файл,*

В веб-интерфейсе KUMA в разделе **Ресурсы** → **Агенты** выберите нужный набор ресурсов агента с точкой назначения diode и нажмите **Скачать конфигурацию**.

Конфигурация параметров агента скачивается в виде JSON-файла в соответствии с параметрами вашего браузера. Ресурсы секретов, использованные в наборе ресурсов агента, скачиваются пустыми, их идентификаторы указаны в файле в разделе "secrets". Для использования файла конфигурации для установки агента в изолированном сегменте сети необходимо вручную дополнить файл конфигурации секретами (см. раздел "Описание полей секретов" на стр. 373) (например, указать URL и пароли, используемые в коннекторе агента для получения событий).

Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к файлу на сервере, где будет установлен агент. Чтение файла должно быть доступно пользователю, от имени которого будет запускаться diode-агент.

Ниже приводится пример конфигурационного файла diode-агента с коннектором типа kafka.

```
{
    "config": {
        "id": "<идентификатор набора ресурсов агента>",
        "name": "<название набора ресурсов агента>",
```

```
"proxyConfigs": [
  {
    "connector": {
      "id": "<идентификатор ресурса коннектора. В этом примере приводится коннектор типа kafka, но в diode-агенте можно использовать коннекторы и других типов. Если ресурс коннектора создан непосредственно в наборе ресурсов агента, значение идентификатора отсутствует.>",
      "name": "<название ресурса коннектора>",
      "kind": "kafka",
      "connections": [
        {
          "kind": "kafka",
          "urls": [
            "localhost:9093"
          ],
          "host": "",
          "port": "",
          "secretID": "<идентификатор ресурса секрета>",
          "clusterID": "",
          "tlsMode": "",
          "proxy": null,
          "rps": 0,
          "maxConns": 0,
          "urlPolicy": "",
          "version": "",
          "identityColumn": "",
          "identitySeed": "",
          "pollInterval": 0,
          "query": "",
          "stateID": "",
          "certificateSecretID": "",
          "authMode": "pfx",
          "secretTemplateKind": "",
          "certSecretTemplateKind": ""
```

```
                    }
                ],
                "topic": "<название топика kafka>",
                "groupID": "<идентификатор группы kafka>",
                "delimiter": "",
                "bufferSize": 0,
                "characterEncoding": "",
                "query": "",
                "pollInterval": 0,
                "workers": 0,
                "compression": "",
                "debug": false,
                "logs": [],
                "defaultSecretID": "",
                "snmpParameters": [
                    {
                        "name": "",
                        "oid": "",
                        "key": ""
                    }
                ],
                "remoteLogs": null,
                "defaultSecretTemplateKind": ""
            },
            "destinations": [
                {
                    "id": "<идентификатор ресурса точки назначения. Если ресурс точки назначения создан непосредственно в наборе ресурсов агента, значение идентификатора отсутствует.>",
                    "name": "<название ресурса точки назначения>",
                    "kind": "diode",
                    "connection": {
                        "kind": "file",
                        "urls": [
```

```
                "<путь к директории, в которую точка назначения должна помещать события для передачи из изолированного сегмента сети диодом данных>",
                "<путь к временной директории, в которую помещаются события для подготовки к передаче диодом данных>"
            ],
            "host": "",
            "port": "",
            "secretID": "",
            "clusterID": "",
            "tlsMode": "",
            "proxy": null,
            "rps": 0,
            "maxConns": 0,
            "urlPolicy": "",
            "version": "",
            "identityColumn": "",
            "identitySeed": "",
            "pollInterval": 0,
            "query": "",
            "stateID": "",
            "certificateSecretID": "",
            "authMode": "",
            "secretTemplateKind": "",
            "certSecretTemplateKind": ""
        },
        "topic": "",
        "bufferSize": 0,
        "flushInterval": 0,
        "diskBufferDisabled": false,
        "diskBufferSizeLimit": 0,
        "healthCheckPath": "",
        "healthCheckTimeout": 0,
        "healthCheckDisabled": false,
```

```
                    "timeout": 0,
                    "workers": 0,
                    "delimiter": "",
                    "debug": false,
                    "disabled": false,
                    "compression": "",
                    "filter": null,
                    "path": ""
                }
            ]
        }
    ],
    "workers": 0,
    "debug": false
},
"secrets": {
    "<идентификатор ресурса секрета>": {
        "pfx": "<зашифрованный pfx-ключ>",
        "pfxPassword": "<пароль к зашифрованному pfx-ключу. Вместо действительного пароля из KUMA экспортируется значение changeit. В файле конфигурации необходимо вручную указать содержимое секретов>"
    }
},
"tenantID": "<идентификатор тенанта>"
}
```

kaspersky

Описание полей секретов

Поля секрета

Название поля	Тип	Описание
`user`	строка	Имя пользователя.
`password`	строка	Пароль.
`token`	строка	Токен.
`urls`	массив строк	Список URL.
`publicKey`	строка	Публичный ключ (используется в PKI).
`privateKey`	строка	Приватный ключ (используется в PKI).
`pfx`	строка, содержащая base64-закодированное содержимое pfx	Содержимое pfx файла, закодированное в base64. На Linux получить base64-кодировку файла можно при помощи команды `base64 -w0 src > dst`.
`pfxPassword`	строка	Пароль от pfx.
`securityLevel`	строка	Используется в snmp3. Возможные значения: `NoAuthNoPriv`, `AuthNoPriv`, `AuthPriv`.
`community`	строка	Используется в snmp1.
`authProtocol`	строка	Используется в snmp3. Возможные значения: `MD5`, `SHA`, `SHA224`, `SHA256`, `SHA384`, `SHA512`.
`privacyProtocol`	строка	Используется в snmp3. Возможные значения: `DES`, `AES`.
`privacyPassword`	строка	Используется в snmp3.

`certificate`	строка, содержащая base64-закодированное содержимое pem	Содержимое pem файла, закодированное в base64. На Linux получить base64-кодировку файла можно при помощи команды `base64 -w0 src > dst`.

Установка Linux-агента в изолированном сегменте сети

► *Чтобы установить в изолированном сегменте сети агент KUMA на устройство Linux:*

1. Поместите на Linux-сервер в изолированном сегменте сети, который будет использоваться для получения агентом событий и с которого диод данных будет перемещать файлы во внешний сегмент сети, следующие файлы:
   - Конфигурационный файл агента (см. раздел "Конфигурационный файл diode-агента" на стр. 368).

     Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к конфигурационному файлу так, чтобы доступ на чтение файла был только у пользователя KUMA.

   - Исполняемый файл /opt/kaspersky/kuma/kuma (см. раздел "Команды для запуска и установки компонентов вручную" на стр. 462) (можно скопировать с сервера с установленными компонентами KUMA).
2. Выполните следующую команду:

   sudo ./kuma agent --cfg <путь к конфигурационному файлу агента> --wd <путь к директории, где будут размещаться файлы устанавливаемого агента. Если не указывать этот флаг, файлы будут храниться в директории, где расположен файл kuma>

Сервис агента установлен и запущен на сервере в изолированном сегменте сети. Он получает события и передает их диоду данных для отправки во внешний сегмент сети.

Установка Windows-агента в изолированном сегменте сети

Перед установкой агента KUMA на устройстве Windows администратору сервера необходимо создать на устройстве Windows учетную запись с правами EventLogReaders и Log on as a service. Эту же учетную запись необходимо использовать для запуска агента.

► *Чтобы установить в изолированном сегменте сети агент KUMA на устройство Windows:*

1. Поместите на Window-сервер в изолированном сегменте сети, который будет использоваться для получения агентом событий и с которого диод данных будет перемещать файлы во внешний сегмент сети, следующие файлы:
   - Конфигурационный файл агента (см. раздел "Конфигурационный файл diode-агента" на стр. 368).

     Необходимо при помощи списка контроля доступа (ACL) настроить права доступа к конфигурационному файлу так, чтобы доступ на чтение файла был только у пользователя, под которым будет работать агент.

   - Исполняемый файл kuma.exe. Файл можно найти внутри установщика в директории /kuma-ansible-installer/roles/kuma/files/.

   Рекомендуется использовать папку `C:\Users\<имя пользователя>\Desktop\KUMA`.
2. Запустите командную строку на устройстве Windows с правами администратора и найдите папку с файлом kuma.exe.
3. Выполните следующую команду:

   ```
   kuma.exe agent --cfg <путь к конфигурационному файлу агента> --user <имя пользователя, под которым будет работать агент, включая домен> --install
   ```

   Справочная информация об установщике доступна по команде `kuma.exe help agent`.
4. Введите пароль для пользователя, под которым будет работать агент.

Создана папка `C:\ProgramData\Kaspersky Lab\KUMA\agent\<Идентификатор Агента>`, в нее установлен сервис агента KUMA. Агент перемещает события в папку для обработки диодом данных.

При установке агента конфигурационный файл агента и файл kuma.exe перемещаются в рабочую директорию C:\ProgramData\Kaspersky Lab\KUMA\agent\<идентификатор агента, указанный в конфигурационном файле>.

Когда сервис агента установлен, он запускается автоматически. Сервис также настроен на перезапуск в случае сбоев.

Удаление агента KUMA с устройств Windows (см. раздел "Удаление агента KUMA с устройств Windows" на стр. 268)

При настройке сервисов можно проверить конфигурацию на наличие ошибок до установки, запустив агент с помощью команды `kuma.exe agent --cfg <путь к конфигурационному файлу агента>`.

kaspersky

Управление активами

Вы можете управлять активами KUMA: просматривать информацию об активах (см. раздел "Просмотр информации об активе" на стр. 379), добавлять (см. раздел "Добавление активов" на стр. 381), редактировать (см. раздел "Изменение параметров активов" на стр. 392) и удалять (см. раздел "Удаление активов" на стр. 394) активы.

См. также:

Об активах 28

Модель данных актива 491

В этом разделе:

Категории активов 376

Добавление категории активов 377

Настройка таблицы активов 378

Поиск активов 379

Просмотр информации об активе 379

Добавление активов 381

Назначение активу категории 390

Изменение параметров активов 392

Удаление активов 394

Обновление программ сторонних производителей и закрытие уязвимостей на активах Kaspersky Security Center 394

Перемещение активов в выбранную группу администрирования 396

Аудит активов 397

Категории активов

В KUMA активы распределены по категориям, имеющим древовидную структуру. Вы можете просмотреть дерево категорий в разделе **Активы → Все активы** веб-интерфейса KUMA. Если выбрать узел дерева, в правой части окна отображаются активы, относящиеся к соответствующей категории. Активы из подкатегорий выбранной категории не отображаются, если вы не укажете, что хотите отображать активы рекурсивно.

Категории активам можно присваивать вручную (см. раздел "Изменение параметров активов" на стр. 392) или автоматически. Автоматическая категоризация может быть реактивной, когда категории наполняются активами с помощью правил корреляции (см. раздел "Правила корреляции" на стр. 134), или активной,

когда категории присваиваются все активы, удовлетворяющие определенным условиям. Способ категоризации можно указать в параметрах категории при ее создании или изменении.

Если навести указатель мыши на категорию, справа от названия категории появится значок с многоточием. При нажатии на этот значок отобразится контекстное меню категорией, в котором можно выбрать следующие действия:

- **Показать активы** – просмотреть активы выбранной категории в правой части окна.
- **Отображать активы рекурсивно** – просмотреть активы из подкатегорий выбранной категории. Если вы хотите выйти из режима рекурсивного просмотра, выберите категорию для просмотра.
- **О категории** – просмотреть информации о выбранной категории в области деталей **Информация о категории**, которая отображается в правой части окна веб-интерфейса.
- **Начать категоризацию** – стартовать автоматическую привязку активов к выбранной категории. Доступно для категорий с активным способом категоризации.
- **Добавить подкатегорию** – добавление подкатегории (см. раздел "Добавление категории активов" на стр. 377) к выбранной категории.
- **Изменить категорию** – изменение выбранной категории.
- **Удалить категорию** – удаление выбранной категории. Удалять можно только категории без активов или подкатегорий. В противном случае опция **Удалить категорию** будет неактивна.
- **Сделать закладкой** – отображение выбранной категории на отдельной закладке. Отменить это действие можно, выбрав в контекстном меню нужной категории **Убрать из закладок**.

Добавление категории активов

► *Чтобы добавить категорию активов:*

1. Откройте раздел **Активы** веб-интерфейса KUMA.
2. Откройте окно создания категории:
   - Нажмите на кнопку **Добавить категорию**.
   - Если вы хотите создать подкатегорию, в контекстном меню родительской категории выберите **Добавить подкатегорию**.

   В правой части окна веб-интерфейса отобразится область деталей **Добавить категорию**.
3. Добавьте сведения о категории:
   - В поле **Название** введите название категории. Название должно содержать от 1 до 128 символов Юникода.
   - В поле **Родительская категория** укажите место категории в дереве категорий:
     a. Нажмите на кнопку  .

        Откроется окно **Выбор категорий**, в котором отображается дерево категорий. Если вы создаете новую категорию, а не подкатегорию, то в окне может отображаться несколько деревьев категорий активов: по одному для каждого доступного вам тенанта. Выбор тенанта в этом окне невозможно отменить.

     b. Выберите родительскую категорию для создаваемой вами категории.

c. Нажмите **Сохранить**.

Выбранная категория отобразится в поле **Родительская категория**.

- В поле **Тенант** отображается тенант (см. раздел "О тенантах" на стр. 25), в структуре которого вы выбрали родительскую категорию. Тенанта категории невозможно изменить.
- Назначьте уровень важности категории в раскрывающемся списке **Уровень важности**.
- При необходимости в поле **Описание** добавьте примечание: до 256 символов Юникода.

4. В раскрывающемся списке **Способ категоризации** выберите, как категория будет пополняться активами. В зависимости от выбора может потребоваться указать дополнительные параметры:
   - **Вручную** – активы можно привязать к категории только вручную.
   - **Активно** – активы будут с определенной периодичностью привязываться к категории, если удовлетворяют заданному фильтру.

     Активная категория активов (см. раздел "Активная категория активов" на стр. 391)
   - **Реактивно** – категория будет наполняться активами с помощью правил корреляции (см. раздел "Правила корреляции" на стр. 134).
5. Нажмите **Сохранить**.

Новая категория добавлена в дерево категорий активов.

Настройка таблицы активов

В KUMA можно настроить содержимое и порядок отображения столбцов в таблице активов. Эти параметры хранятся локально на вашем компьютере.

► *Чтобы настроить параметры отображения таблицы активов:*

1. В правом верхнем углу таблицы активов нажмите значок  .
2. В раскрывшемся списке установите флажки напротив параметров, которые требуется отображать в таблице:
   - **Полное доменное имя**
   - **IP-адрес**
   - **Источник актива**
   - **Владелец**
   - **MAC-адрес**
   - **Создан**
   - **Последнее обновление**
   - **Тенант**

   Когда вы устанавливаете флажок, таблица активов обновляется и добавляется новый столбец. При снятии флажка столбец исчезает. Таблицу можно сортировать по некоторым столбцам.
3. Если требуется изменить порядок отображения столбцов, зажмите левую клавишу мыши на названии столбца и перетащите его в нужное место таблицы.

Параметры отображения таблицы активов настроены.

Поиск активов

В KUMA есть функция полнотекстового поиска по параметрам активов. Поиск выполняется по параметрам **Название**, **Полное доменное имя**, **IP-адрес**, **MAC-адрес** и **Владелец**.

► *Чтобы найти нужный актив,*

в разделе **Активы** веб-интерфейса KUMA введите поисковый запрос в поле **Поиск** и нажмите **ENTER** или значок  .

В таблице отобразятся все активы, названия которых соответствуют критериям поиска.

Просмотр информации об активе

► *Чтобы просмотреть информацию об активе:*

1. В веб-интерфейсе KUMA перейдите в раздел **Активы**.
2. Выберите категорию с требуемыми активами.

   Отобразится таблица активов.
3. Выберите актив.

В окне информации об активе может отображаться следующая информация:

- **Название** – имя актива.

  Активы, импортированные в KUMA, сохраняют имена, которые были заданы для них в источнике. Вы можете изменить эти имена в веб-интерфейсе KUMA.
- **Тенант** – название тенанта (см. раздел "О тенантах" на стр. 25), которому принадлежит актив.
- **Источник актива** – источник информации об активе. Источников может быть несколько (см. раздел "Добавление активов" на стр. 381): сведения можно добавить в веб-интерфейсе KUMA или с помощью API, а также импортировать из Kaspersky Security Center, KICS for Networks и отчетов MaxPatrol.

  Добавляя в KUMA сведения об одном и том же активе из нескольких источников, следует учитывать правила слияния данных об активах.
- **Создан** – дата и время добавления актива в KUMA.
- **Последнее обновление** – дата и время изменения информации об активе.
- **Владелец** – владелец актива, если он указан.
- **IP-адрес** – IP-адрес актива (если предоставлен).

Если в KUMA есть несколько активов с одинаковыми IP-адресами, актив, добавленный позже, возвращается во всех случаях поиска активов по IP-адресу. Если в сети вашей организации допустимо наличие активов с одинаковыми IP-адресами, разработайте и используйте дополнительные атрибуты для идентификации активов. Это может оказаться важным при корреляции.

- **Полное доменное имя** – полностью определенное имя домена актива, если указано.
- **MAC-адрес** – MAC-адрес актива (если предоставлен).
- **Операционная система** – операционная система актива.
- **Связанные алерты** – алерты (см. раздел "Об алертах" на стр. 27), с которыми связан актив (если есть).

  Для просмотра списка алертов, с которыми связан актив, можно перейти по ссылке **Найти в алертах**. Откроется закладка **Алерты** с поисковым выражением, позволяющим отфильтровать все активы с соответствующим идентификатором.
- **Категории** – категории (см. раздел "Категории активов" на стр. 376), к которым относится актив (если есть).
- **Информация о программном обеспечении** и **Информация об оборудовании** – если указаны параметры программного обеспечения и оборудования актива, они отображаются в этом разделе.
- Сведения об уязвимостях актива:
  - **Уязвимости Kaspersky Security Center** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из Kaspersky Security Center.

    Вы можете узнать больше об уязвимости, нажав на значок , открывающий портал Kaspersky Threats. Вы также можете обновить список уязвимостей, нажав на ссылку **Обновить** и запросив обновленную информацию из Kaspersky Security Center.
  - **Уязвимости KICS for Networks** – уязвимости актива, если есть. Эта информация доступна для активов, импортированных из KICS for Networks.
- Сведения об источниках актива:
  - **Последнее подключение к Kaspersky Security Center** – время последнего получения сведений об активе из Kaspersky Security Center. Эта информация доступна для активов, импортированных из Kaspersky Security Center.
  - **Идентификатор хоста** – идентификатор агента Kaspersky Security Center, от которого получены сведения об активе. Эта информация доступна для активов, импортированных из Kaspersky Security Center.
  - **IP-адрес сервера KICS for Networks** и **Идентификатор коннектора KICS for Networks** – данные об экземпляре KICS for Networks, из которого был импортирован актив.

По кнопке **Реагирование KSC** вы можете запустить на активе выполнение задачи Kaspersky Security Center.

Доступно при интеграции с Kaspersky Security Center (см. раздел "Интеграция с Kaspersky Security Center" на стр. 73).

kaspersky

Добавление активов

Вы можете добавлять информацию об активах следующими способами:

- Вручную.

  Вы можете добавить актив в веб-интерфейсе KUMA или с помощью API (см. раздел "Импорт активов" на стр. 433).

- Импортировать активы.

  Вы можете импортировать активы из Kaspersky Security Center (см. раздел "Импорт информации об активах из Kaspersky Security Center" на стр. 384), KICS for Networks (см. раздел "Импорт информации об активах из KICS for Networks" на стр. 390) и отчетов MaxPatrol (см. раздел "Импорт информации об активах из MaxPatrol" на стр. 385).

При добавлении активы, уже существующие в KUMA, могут объединяться с добавляемыми активами. Для этого требуется отсутствие противоречия между идентификатором Kaspersky Security Center или KICS for Networks активов. Противоречие отсутствует, если одно из сравниваемых полей не заполнено или значения для полей полностью совпадают.

Если противоречие отсутствует, информация об активах обновляется при следующих условиях:

- Совпадает IP-адрес актива.
- Совпадает MAC-адрес актива.
- Совпадает полное доменное имя актива.
- Совпадает полное доменное имя и IP-адрес активов.

  Проверка производится по всему массиву значений IP-адресов. Если IP-адрес актива входит в состав полного доменного имени, значения считаются совпавшими.

- Совпадает полное доменное имя и MAC-адрес активов.

  Проверка производится по всему массиву значений MAC-адресов. При полном совпадении хотя бы одного значения массива с полным доменным именем значения считаются совпавшими.

- Совпадает IP-адрес и MAC-адрес активов.

  Проверка производится по всему массиву значений IP- и MAC-адресов. При полном совпадении хотя бы одного значения в массивах значения считаются совпавшими.

Для каждого поля проверка производится отдельно и завершается при первом совпадении.

Информация об активах может формироваться из разных источников. Если добавляемый актив и актив KUMA содержат данные, полученные из одного и того же источника, эти данные перезаписываются. Например, актив Kaspersky Security Center при импорте в KUMA получил полное доменное имя и информацию о программном обеспечении. При импорте актива из Kaspersky Security Center с аналогичным полным доменным именем эти данные будут перезаписаны при условии, что они указаны для добавляемого актива. Все поля, в которых могут обновляться данные, приведены в таблице *Обновляемые данные*.

Обновляемые данные

Название поля	Принцип обновления
Название	Выбирается согласно следующему приоритету: • Задано вручную. • Получено из Kaspersky Security Center. • Получено KICS for Networks.
Владелец	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано вручную.
IP-адрес	Данные объединяются. Если в массиве адресов есть одинаковые адреса, копия дублирующегося адреса удаляется.
Полное доменное имя	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS for Networks. • Задано вручную.
MAC-адрес	Данные объединяются. Если в массиве адресов есть одинаковые адреса, один из дублирующихся адресов удаляется.
Операционная система	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Получено KICS for Networks. • Задано вручную.
Уязвимости	Данные активов KUMA дополняются информацией из добавляемых активов. В информации об активе данные группируются по названию источника. Устранение уязвимостей для каждого источника осуществляется отдельно.
Информация о программном обеспечении	Данные из KICS for Networks записываются всегда (при наличии). Для других источников выбирается первое значение согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано вручную.
Информация об оборудовании	Выбирается первое значение из источников согласно следующему приоритету: • Получено из Kaspersky Security Center. • Задано через API.

Обновленные данные отображаются в информации об активе. Вы можете просмотреть информацию об активе в веб-интерфейсе KUMA (см. раздел "Управление активами" на стр. 376).

При добавлении новых активов эти данные могут быть перезаписаны. Если данные, из которых сформирована информация об активе, не обновляются из источников более 30 дней, актив удаляется. При следующем добавлении актива из тех же источников создается новый актив.

При редактировании в веб-интерфейсе KUMA активов, информация о которых получена из Kaspersky Security Center или KICS for Networks, вы можете изменить следующие данные актива:

- Название.
- Категория.

Если информация об активе добавлена вручную, при редактировании в веб-интерфейсе KUMA этих активов вы можете изменить следующие данные актива:

- Название.
- Название тенанта, которому принадлежит актив.
- IP-адрес.
- Полное доменное имя.
- MAC-адрес.
- Владелец.
- Категория.
- Операционная система.
- Информация об оборудовании.

Редактирование данных об активах через REST API недоступно. При импорте из REST API происходит обновление данных по правилам слияния информации об активах, приведенным выше.

В этом разделе

Добавление информации об активах в веб-интерфейсе KUMA 383
Импорт информации об активах из Kaspersky Security Center 384
Импорт информации об активах из MaxPatrol 385
Импорт информации об активах из KICS for Networks 390

Добавление информации об активах в веб-интерфейсе KUMA

► *Чтобы добавить актив в веб-интерфейсе KUMA:*

1. В разделе **Активы** веб-интерфейса KUMA нажмите на кнопку **Добавить актив**.

   В правой части окна откроется область деталей **Добавить актив**.
2. Введите параметры актива:
   - **Название актива** (обязательно).
   - **Тенант** (обязательно).
   - **IP-адрес** и/или **Полное доменное имя** (обязательно).
   - **MAC-адрес**.
   - **Владелец**.
3. При необходимости присвойте активу одну или несколько категорий:

   a. Нажмите кнопку  .

Откроется окно **Выбор категорий**.

b. Установите флажки рядом с категориями, которые следует присвоить активу. С помощью значков ⊞ и ⊟ вы можете разворачивать и сворачивать списки категорий.

c. Нажмите **Сохранить**.

Выбранные категории отобразятся в полях **Категории**.

4. При необходимости добавьте в раздел **Программное обеспечение** сведения об операционной системе актива.
5. При необходимости добавьте в раздел **Информация об оборудовании** сведения об оборудовании актива.
6. Нажмите на кнопку **Добавить**.

Актив создан и отображается в таблице активов в назначенной ему категории или в категории **Активы без категории**.

Импорт информации об активах из Kaspersky Security Center

В Kaspersky Security Center зарегистрированы все активы, которые находятся под защитой этой программы. Вы можете импортировать информацию об активах, защищаемых Kaspersky Security Center, в KUMA. Для этого вам требуется предварительно настроить интеграцию между программами (см. раздел "Интеграция с Kaspersky Security Center" на стр. 73).

В KUMA предусмотрены следующие типы импорта активов из KSC:

- Импорт информации обо всех активах всех серверов KSC.
- Импорт информации об активах выбранного сервера KSC.

► *Чтобы импортировать информацию обо всех активах всех серверов KSC:*

1. В веб-интерфейсе KUMA выберите раздел **Активы**.
2. Нажмите на кнопку **Импортировать активы**.

   Откроется окно **Импорт активов из Kaspersky Security Center**.
3. В раскрывающемся списке выберите тенант, для которого вы хотите выполнить импорт.

   В этом случае программа загружает информацию обо всех активах всех серверов KSC, для которых настроено подключение к выбранному тенанту.

   Если вы хотите импортировать информацию обо всех активах всех серверов KSC для всех тенантов, выберите **Все тенанты**.
4. Нажмите на кнопку **ОК**.

Информация об активах будет импортирована.

Чтобы импортировать информацию об активах одного сервера KSC:

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры** → **Kaspersky Security Center**.

   Откроется окно **Интеграция с Kaspersky Security Center по тенантам**.
2. Выберите тенант, для которого вы хотите импортировать активы.

   Окроется окно **Интеграция с Kaspersky Security Center**.

3. Нажмите на подключение для требуемого сервера Kaspersky Security Center.

   Откроется окно с параметрами этого подключения к Kaspersky Security Center.

4. Выполните одно из следующих действий:

   - Если вы хотите импортировать все активы, подключенные к выбранному серверу KSC, нажмите на кнопку **Импортировать активы**.
   - Если вы хотите импортировать только активы, которые подключены к подчиненному серверу или включены в одну из групп (например, группу Нераспределенные устройства), выполните следующие действия:

     a. Нажмите на кнопку **Загрузить иерархию**.

     b. Установите флажки рядом с именами подчиненных серверов или групп, из которых вы хотите импортировать информацию об активах.

     c. Установите флажок **Импортировать активы из новых групп**, если вы хотите импортировать активы из новых групп.

        Если ни один флажок не установлен, при импорте выгружается информация обо всех активах выбранного сервера KSC.

     d. Нажмите на кнопку **Сохранить**.

     e. Нажмите на кнопку **Импортировать активы**.

Информация об активах будет импортирована.

Импорт информации об активах из MaxPatrol

В KUMA можно импортировать сведения об активах из отчетов о результатах сканирования сетевых устройств с помощью MaxPatrol, системы контроля защищенности и соответствия стандартам. Импорт происходит через API (см. раздел "REST API" на стр. 413) с помощью утилиты maxpatrol-tool на сервере, где установлено Ядро KUMA (см. раздел "Ядро" на стр. 20). Импортированные активы отображаются в веб-интерфейсе KUMA в разделе **Активы**. При необходимости вы можете редактировать параметры активов (см. раздел "Изменение параметров активов" на стр. 392).

Утилита предоставляется по запросу (см. раздел "Обращение в службу технической поддержки" на стр. 412).

Импорт поддерживается из MaxPatrol 8.

► *Чтобы импортировать данные об активах из отчета MaxPatrol:*

1. Сформируйте в MaxPatrol отчет сканирования сетевых активов в формате **XML file** и скопируйте файл отчета на сервер Ядра KUMA. Подробнее о задачах на сканирование и форматах выходных файлов см. в документации MaxPatrol.

   Импорт данных из отчетов в формате **SIEM integration file** не поддерживается. Требуется выбрать формат **XML file**.

2. Создайте файл с токеном (см. раздел "Редактирование своей учетной записи" на стр. 71) для доступа к KUMA REST API. Для удобства рекомендуется разместить его в папке отчета MaxPatrol. Файл не должен содержать ничего, кроме токена.

   Требования к учетным записям, для которых генерируется API-токен:

   - Роль Администратора или Аналитика (см. раздел "Роли пользователей" на стр. 57).
   - Доступ к тенанту, в который будут импортированы активы.
   - Настроены права на использование API-запросов GET /users/whoami (см. раздел "Просмотр информации о предъявителе токена" на стр. 457) и POST /api/v1/assets/import (см. раздел "Импорт активов" на стр. 433).

     Мы рекомендуем для импорта активов из MaxPatrol создать отдельного пользователя (см. раздел "Создание пользователя" на стр. 69) с минимально необходимым набором прав на использование API-запросов.

3. Скопируйте утилиту maxpatrol-tool на сервер с Ядром KUMA и сделайте файл утилиты исполняемым с помощью команды `chmod +x <путь до файла maxpatrol-tool на сервере с Ядром KUMA>`.
4. Запустите утилиту maxpatrol-tool:

   ```
   ./maxpatrol-tool --kuma-rest <адрес и порт сервера KUMA REST API> --token <путь и имя файла с API-токеном> --tenant <название тенанта, куда будут помещены активы> <путь и имя файла с отчетом MaxPatrol>
   ```

   Пример: `./maxpatrol-tool --kuma-rest example.kuma.com:7223 --token token.txt --tenant Main example.xml`

Вы можете использовать дополнительные флаги и команды для импорта. Например, команду для отображения полного отчета о полученных активах `--verbose, -v`. Подробное описание доступных флагов и команд приведено в таблице Флаги и команды утилиты maxpatrol-tool. Также для просмотра информации о доступных флагах и командах вы можете использовать команду --help.

Информация об активах будет импортирована из отчета MaxPatrol в KUMA. В консоли отображаются сведения о количестве новых и обновленных активов.

Пример:

inserted 2 assets;

updated 1 assets;

errors occured: []

Поведение утилиты при импорте активов (см. раздел "Импорт активов" на стр. 433):

- Данные импортированных в KUMA через API активов перезаписываются, а сведения об их устраненных уязвимостях удаляются.
- Активы с недействительными данными пропускаются. Сведения об ошибках отображаются при использовании флага `--verbose`.
- Если в одном отчете MaxPatrol есть активы с одинаковыми IP-адресами и полными именами домена (FQDN), они объединяются. Сведения об их уязвимостях и программном обеспечении также объединяются в одном активе.

При загрузке активов из MaxPatrol активы с аналогичными IP-адресами и полными именами доменов (FQDN), ранее импортированные из Kaspersky Security Center, перезаписываются.

Чтобы этого избежать, вам требуется настроить фильтрацию активов по диапазону с помощью команды `--ignore <диапазоны IP-адресов> или -i <диапазоны IP-адресов>`. Активы, соответствующие условиям фильтрации, не загружаются. Описание команды вы можете просмотреть в таблице *Флаги и команды утилиты maxpatrol-tool*.

Флаги и команды утилиты maxpatrol-tool

Флаги и команды	Описание
`--kuma-rest <адрес и порт сервера KUMA REST API>, -a <адрес и порт сервера KUMA REST API>`	Адрес сервера с Ядром KUMA, куда будет производиться импорт активов, с указанием порта. Например, `example.kuma.com:7223`. По умолчанию для обращения по API используется порт 7223. При необходимости его можно изменить.
`--token <путь и имя файла с API-токеном>, -t <путь и имя файла с API-токеном>`	Путь и имя файла, содержащее токен для доступа к REST API (см. раздел "Редактирование своей учетной записи" на стр. 71). Файл должен содержать только токен. Учетной записи, для которой генерируется API-токен, должна быть присвоена роль Администратора или Аналитика.
`--tenant <название тенанта>, -T <название тенанта>`	Название тенанта KUMA (см. раздел "О тенантах" на стр. 25), в который будут импортированы активы из отчета MaxPatrol.
`--dns <диапазоны IP-адресов> или -d <диапазоны IP-адресов>`	Используется для обогащения IP-адресов FQDN из указанных диапазонов с помощью DNS, если для этих адресов FQDN не был указан. Пример: `--dns 0.0.0.0-9.255.255.255,11.0.0.0-255.255.255,10.0.0.2`
`--dns-server <IP-адрес DNS-сервера>, -s <IP-адрес DNS-сервера>`	Адрес DNS-сервера, к которому должна обращаться утилита для получения информации о FQDN. Пример: `--dns-server 8.8.8.8`
`--ignore <диапазоны IP-адресов> или -i <диапазоны IP-адресов>`	Диапазоны адресов активов, которые при импорте следует пропустить. Пример: `--ignore 8.8.0.0-8.8.255.255, 10.10.0.1`
`--verbose, -v`	Выведение полного отчета о полученных активах и ошибках, возникших в процессе импорта.

Флаги и команды	Описание

`--help`, `-h`
`help`
	Получение справочной информации об утилите или команде.
	Примеры:
	`./maxpatrol-tool help`
	`./maxpatrol-tool <команда> --help`

`version`	Получение информации о версии утилиты maxpatrol-tool.
`completion`	Создание скрипта автозавершения для указанной оболочки.

Примеры:

- `./maxpatrol-tool --kuma-rest example.kuma.com:7223 --token token.txt --tenant Main example.xml` – импорт активов в KUMA из отчета MaxPatrol example.xml.
- `./maxpatrol-tool help` – получение справки об утилите.

Возможные ошибки

Сообщение об ошибке	Описание
must provide path to xml file to import assets	Не указан путь к файлу отчета MaxPatrol.
incorrect IP address format	Некорректный формат IP-адреса. Может возникнуть при указании некорректных диапазонов IP.
no tenants match specified name	Для указанного названия тенанта не было найдено подходящих тенантов с помощью REST API.
unexpected number of tenants (%v) match specified name. Tenants are: %v	Из KUMA вернулось больше одного тенанта для указанного названия тенанта.
could not parse file due to error: %w	Ошибка чтения xml-файла с отчетом MaxPatrol.
error decoding token: %w	Ошибка чтения файла с API-токеном.
error when importing files to KUMA: %w	Ошибка передачи сведений об активах в KUMA.
skipped asset with no FQDN and IP address	У одного из активов в отчете не было FQDN и IP-адреса. Сведения об этом активе не были отправлены в KUMA.
skipped asset with invalid FQDN: %v	У одного из активов в отчете был некорректный FQDN. Сведения об этом активе не были отправлены в KUMA.
skipped asset with invalid IP address: %v	У одного из активов в отчете был некорректный IP-адрес. Сведения об этом активе не были отправлены в KUMA.
KUMA response: %v	При импорте сведений об активах произошла ошибка с указанным ответом.
unexpected status code %v	При импорте сведений об активах от KUMA был получен неожиданный код HTTP.

Импорт информации об активах из KICS for Networks

После создания интеграции с KICS for Networks задачи на получение данных об активах KICS for Networks создаются автоматически. Это происходит в следующих случаях:

- Сразу после создания новой интеграции.
- Сразу после изменения параметров существующей интеграции.
- Регулярно по расписанию каждые несколько часов. По умолчанию каждые 12 часов. Расписание можно изменить.

Задачи на обновление данных об учетных записях можно создать вручную.

► *Чтобы запустить задачу на обновление данных об активах KICS for Networks для тенанта:*

1. Откройте в веб-интерфейсе KUMA разделе **Параметры** → **Kaspersky Industrial CyberSecurity for Networks**.
2. Выберите требуемый тенант.

   Откроется окно **Интеграция с Kaspersky Industrial CyberSecurity for Networks**.
3. Нажмите на кнопку **Импортировать активы**.

В разделе **Диспетчер задач** веб-интерфейса KUMA добавлена задача (см. раздел "Просмотр таблицы задач" на стр. 405) на получение данных об учетных записях выбранного тенанта.

Назначение активу категории

► *Чтобы назначить категорию одному активу:*

1. В веб-интерфейсе KUMA перейдите в раздел **Активы**.
2. Выберите категорию с требуемыми активами.

   Отобразится таблица активов.
3. Выберите актив.
4. В открывшемся окне нажмите на кнопку **Изменить**.
5. В поле **Категории** нажмите на кнопку .
6. Выберите категорию.

   Если вы хотите перенести актив в раздел **Активы без категории**, вам требуется удалить существующие для актива категории, нажав на кнопку .
7. Нажмите на кнопку **Сохранить**.

Категория будет назначена.

► *Чтобы назначить категорию нескольким активам:*

1. В веб-интерфейсе KUMA перейдите в раздел **Активы**.

2. Выберите категорию с требуемыми активами.

   Отобразится таблица активов.

3. Установите флажки рядом с активами, для которых вы хотите изменить категорию.
4. Нажмите на кнопку **Привязать к категории**.
5. В открывшемся окне выберите категорию.
6. Нажмите на кнопку **Сохранить**.

Категория будет назначена.

Не назначайте активам категорию `Categorized assets`.

Активная категория активов

1. В раскрывающемся списке **Регулярность категоризации** укажите периодичность, в которой активы будут привязываться к категории. Можно выбрать значения от одного раза в час до одного раза в сутки.

   Категоризацию можно запустить принудительно, выбрав в контекстном меню категории **Начать категоризацию**.

2. В блоке параметров **Условия** укажите фильтр, которому должны соответствовать условия для привязывания к категории.

   Условия можно добавлять с помощью кнопок **Добавить условие**. Группы условий можно добавлять с помощью кнопок **Добавить группу**. Групповые операторы можно переключать между значениями **И**, **ИЛИ**, **НЕ**.

   Операнды и операторы фильтра категоризации (см. раздел "Операнды и операторы фильтра категоризации" на стр. 392)

3. С помощью кнопки **Проверить условия** убедитесь, что указанный фильтр верен: при нажатии на кнопку отображается окно **Активы, найденные по заданным условиям** с перечнем активов, удовлетворяющих условиям поиска.

kaspersky

Операнды и операторы фильтра категоризации

Операнд	Операторы	Комментарий
Номер сборки	>, >=, =, <=, <	
ОС	=, like	Оператор like обеспечивает регистронезависимый поиск.
IP-адрес	inSubnet, inRange	IP-адрес указывается в нотации CIDR (например: 192.168.0.0/24). При выборе оператора inRange допускается указывать только адреса из частных диапазонов IP-адресов (например: 10.0.0.0-10.255.255.255). Оба адреса должны быть из одного диапазона.
Полное доменной имя	=, like	Оператор like обеспечивает регистронезависимый поиск.
CVE	=, in	Оператор in позволяет указать массив значений.

Изменение параметров активов

В KUMA можно изменять параметры активов. У добавленных вручную активов можно изменять все параметры. У активов, импортированных из Kaspersky Security Center, можно изменить только название актива и его категорию.

► *Чтобы изменить параметры актива:*

1. В разделе **Активы** веб-интерфейса KUMA нажмите на актив, который вы хотите изменить.

   В правой части окна откроется область **Информация об активе**.

2. Нажмите на кнопку **Изменить**.

   Откроется окно **Изменить актив**.

3. Внесите необходимые изменения в доступные поля:

   - **Название актива** (обязательно. Это единственное поле, доступное для редактирования у активов, импортированных из Kaspersky Security Center или KICS for Networks.)
   - **IP-адрес** и/или **Полное доменное имя** (обязательно)
   - **MAC-адрес**
   - **Владелец**
   - **Информация о программном обеспечении**:
     - **Название ОС**
     - **Версия ОС**
   - **Информация об оборудовании**:

Параметры оборудования (см. раздел "Раздел Информация об оборудовании" на стр. 393)

4. Назначьте или измените активу категорию:

   a. Нажмите кнопку  .

      Откроется окно **Выбор категорий**.

   b. Установите флажки рядом с категориями, которые следует присвоить активу.

   c. Нажмите **Сохранить**.

   Выбранные категории отобразятся в полях **Категории**.

   Кроме того, можно выбрать актив и перетащить его в нужную категорию. Эта категория будет добавлена в список категорий актива.

   Не назначайте активам категорию `Categorized assets`.

5. Если требуется, разделе **Программное обеспечение** добавьте сведения об операционной системе актива.
6. Если требуется, в разделе **Информация об оборудовании** добавьте сведения об оборудовании актива.
7. Нажмите на кнопку **Сохранить**.

Параметры актива изменены.

Раздел Информация об оборудовании

В раздел **Информация об оборудовании** можно добавить сведения об оборудовании актива:

Доступные поля для описания CPU актива:

- **Название процессора**
- **Частота процессора**
- **Количество ядер процессора**

Активу можно добавить процессоры с помощью ссылки **Добавить процессор**.

Доступные поля для описания диска актива:

- **Свободных байт на диске**
- **Объем диска**

Активу можно добавить диски с помощью ссылки **Добавить диск**.

Доступные поля для описания RAM актива:

- **Частота оперативной памяти**
- **Общий объем ОЗУ**

Доступные поля для описания сетевой карты актива:

- **Название сетевой карты**
- **Производитель сетевой карты**
- **Версия драйвера сетевой карты**

Активу можно добавить сетевые карты с помощью ссылки **Добавить сетевую карту**.

Удаление активов

В KUMA есть возможность удалять активы.

► *Чтобы удалить актив:*

1. В разделе **Активы** веб-интерфейса KUMA нажмите на актив, которое вы хотите удалить.

   В правой части окна откроется область **Информация об активе**.
2. Нажмите на кнопку **Удалить**.

   Откроется окно подтверждения.
3. Нажмите **ОК**.

Актив удален.

Импортированные из Kaspersky Security Center активы удаляются автоматически, если информация о них не обновлялась в течение 30 дней. Обновление актива может не происходить как из-за отсутствия данных о нем в Kaspersky Security Center, так и из-за отключения KUMA от сервера Kaspersky Security Center. Если после удаления актива в KUMA сведения о нем снова поступают из Kaspersky Security Center, актив пересоздается с тем же идентификатором. Если пересоздать автоматически удаленный актив вручную, новый актив будет иметь идентификатор, отличный от идентификатора старого актива.

Обновление программ сторонних производителей и закрытие уязвимостей на активах Kaspersky Security Center

Вы можете обновлять программы сторонних производителей, в том числе программы Microsoft, установленные на активах Kaspersky Security Center, и закрывать уязвимости этих программ.

Предварительно вам нужно создать задачу *Установка требуемых обновлений и закрытие уязвимостей* на выбранном сервере Администрирования Kaspersky Security Center со следующими параметрами:

- Программа – Kaspersky Security Center.
- Тип задачи – *Установка требуемых обновлений и закрытие уязвимостей*.

- Устройства, которым будет назначена задача – вам требуется назначить задачу корневой группе администрирования.
- Правила для установки обновлений:
  - Устанавливать только утвержденные обновления.
  - Закрывать уязвимости с уровнем критичности, равным или выше (необязательный параметр).

    Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (*Средний*, *Высокий* или *Предельный*). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.
- Запуск по расписанию – расписание, в соответствии с которым выполняется задача.

О способах создания задачи см. подробнее в *справке Kaspersky Security Center*.

Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование.

Далее вам требуется установить обновления для программ сторонних производителей и закрыть уязвимости на активах в KUMA.

► *Чтобы установить обновления и закрыть уязвимости программ сторонних производителей на активе в KUMA:*

1. Откройте окно информации об активе одним из следующих способов:
   - В веб-интерфейсе KUMA выберите раздел **Активы** → выберите категорию с требуемыми активами → выберите актив.
   - В веб-интерфейсе KUMA выберите раздел **Алерты** → нажмите на ссылку с требуемым алертом → в разделе **Связанные активы** выберите актив.
   - В веб-интерфейсе KUMA выберите раздел **События** → выполните поиск и фильтрацию событий (см. раздел "Фильтрация и поиск событий" на стр. 341) → выберите требуемое событие → нажмите на ссылку в поле DeviceExternalID.
2. В окне информации об активе раскройте список **Уязвимости Kaspersky Security Center**.
3. Установите флажки рядом с программами, которые вы хотите обновить.
4. Нажмите на ссылку **Загрузить обновления**.
5. В открывшемся окне установите флажок рядом с идентификатором уязвимости, которую вы хотите закрыть.
6. Если в столбце **Лицензионное соглашение принято** для выбранного идентификатора отображается **Нет**, нажмите на кнопку **Принять обновления**.
7. Перейдите по ссылке в столбце **URL Лицензионного соглашения** и ознакомьтесь с текстом Лицензионного соглашения.
8. Если вы с ним согласны, в веб-интерфейсе KUMA нажмите на кнопку **Принять Лицензионные соглашения**.

   Напротив идентификатора уязвимости, для которого было принято Лицензионное соглашение, в столбце **Лицензионнные соглашения приняты** отобразится **Да**.

9. Повторите шаги 7–10 для каждого требуемого идентификатора уязвимости.
10. Нажмите на кнопку **ОК**.

Обновления будут загружены и установлены на активы, того сервера Администрирования, где была запущена задача, а также на активы всех подчиненные серверы Администрирования.

> Условия Лицензионного соглашения для обновления и закрытия уязвимостей требуется принять на каждом подчиненном сервере Администрирования отдельно.

Обновления устанавливаются на активы, на которых была обнаружена уязвимость.

Вы можете обновить список уязвимостей для актива в окне информации об активе, нажав на ссылку **Обновить**.

Перемещение активов в выбранную группу администрирования

Вы можете перемещать активы в выбранную группу администрирования Kaspersky Security Center. В этом случае на активы будут распространятся групповые политики и задачи. Подробнее о политиках и задачах Kaspersky Security Center см. *справку Kaspersky Security Center*.

Группы администрирования добавляются в KUMA при загрузке иерархии во время импорта активов из Kaspersky Security Center (см. раздел "Импорт информации об активах из Kaspersky Security Center" на стр. 384). Предварительно вам требуется настроить интеграцию KUMA с Kaspersky Security Center.

► *Чтобы переместить один актив в выбранную группу администрирования:*

1. Откройте окно информации об активе одним из следующих способов:
   - В веб-интерфейсе KUMA выберите раздел **Активы** → выберите категорию с требуемыми активами → выберите актив.
   - В веб-интерфейсе KUMA выберите раздел **Алерты** → нажмите на ссылку с требуемым алертом → в разделе **Связанные активы** выберите актив.
   - В веб-интерфейсе KUMA выберите раздел **События** → выполните поиск и фильтрацию событий (см. раздел "Фильтрация и поиск событий" на стр. 341) → выберите требуемое событие → нажмите на ссылку в поле DeviceExternalID.
2. В окне информации об активе нажмите на кнопку **Переместить в группу KSC**.
3. Нажмите на кнопку **Переместить в группу KSC**.
4. В открывшемся окне выберите группу.

   > Выбранная группа должна принадлежать тому же тенанту, которому принадлежит актив.

5. Нажмите на кнопку **Сохранить**.

Выбранный актив будет перемещен.

► *Чтобы переместить несколько активов в выбранную группу администрирования:*

1. В веб-интерфейсе KUMA выберите раздел **Активы**.
2. Выберите категорию с требуемыми активами.
3. Установите флажки рядом с активами, которые хотите переместить в группу.
4. Нажмите на кнопку **Переместить в группу KSC**.

   Кнопка активна, если все выбранные активы принадлежат одному серверу Администрирования.

5. В открывшемся окне выберите группу.
6. Нажмите на кнопку **Сохранить**.

Выбранные активы будут перемещены.

Вы можете посмотреть, к какой группе принадлежит актив, в информации об активе.

Аудит активов

В KUMA можно настроить (см. раздел "Настройка аудита активов" на стр. 398) создание событий аудита активов при следующих условиях:

- Актив добавлен в KUMA. Отслеживается создание актива вручную (см. раздел "Добавление информации об активах в веб-интерфейсе KUMA" на стр. 383), а также создание при импорте через REST API (см. раздел "Импорт активов" на стр. 433), импорте из Kaspersky Security Center (см. раздел "Импорт информации об активах из Kaspersky Security Center" на стр. 384) или KICS for Networks (см. раздел "Импорт информации об активах из KICS for Networks" на стр. 390).
- Параметры актива изменены. Отслеживается изменение значение следующих полей актива:
  - Name
  - IP address
  - Mac Address
  - FQDN
  - Operating system

  Изменения полей может происходить при обновлении актива во время импорта (см. раздел "Добавление активов" на стр. 381).
- Актив удален из KUMA. Отслеживается удаление активов вручную (см. раздел "Удаление активов" на стр. 394), а также автоматическое удаление активов, импортированных из Kaspersky Security Center и KICS for Networks (см. раздел "Особенности импорта информации об активах из KICS for Networks" на стр. 126), данные о которых перестали поступать.
- Сведения об уязвимости добавлены в актив. Отслеживается появление у активов новых данных об уязвимостях. Сведения об уязвимостях могут быть добавлены в актив, например, при импорте активов из Kaspersky Security Center или KICS for Networks.

- Уязвимость актива закрыта. Отслеживается удаление из актива сведений об уязвимости. Уязвимость считается закрытой, если данные о ней перестают поступать из всех источников, из которых ранее были получены сведения о ее появлении.
- Актив добавлен в категорию. Отслеживается присвоении активу категории активов (на стр. 376).
- Актив удален из категории. Отслеживается удаление актива из категории активов.

События аудита (см. раздел "Хранение и поиск событий аудита активов" на стр. 399) активов можно отправлять, например, на хранение или в коррелятоpы.

В этом разделе

Настройка аудита активов 398

Хранение и поиск событий аудита активов 399

Включение и выключение аудита активов 399

Настройка аудита активов

► *Чтобы настроить аудит активов:*

1. Откройте раздел **Параметры** → **Аудит активов** веб-интерфейса KUMA.
2. Выполните одно из действий с тенантом, для которого вы хотите настроить аудит активов:
   - Добавьте тенант с помощью кнопки **Добавить тенант**, если аудит активов для требуемого тенанта настраивается впервые.

     В открывшемся окне **Аудит активов** выберите имя для нового тенанта.
   - Выберите существующий тенант в таблице, если аудит активов для требуемого тенанта уже был настроен.

     В открывшемся окне **Аудит активов** имя тенанта уже задано и редактировать его нельзя.
   - Клонируйте настройки существующего тенанта, чтобы создать копию конфигурации условий для тенанта, для которого вы хотите настроить аудит активов впервые. Для этого установите флажок напротив тенанта, конфигурацию которого требуется копировать, и нажмите **Клонировать**. В открывшемся окне **Аудит активов** выберите имя тенанта, в котором будет использована конфигурация исходного тенанта.
3. Выберите для каждого условия создания событий аудита активов, куда будут отправляться создаваемые события:
   a. В блоке параметров нужного типа событий аудита активов в раскрывающемся списке **Добавить точку назначения** выберите тип точки назначения, куда следует отправлять создаваемые события:
      - Выберите **Хранилище**, если хотите, чтобы события отправлялись в хранилище.
      - Выберите **Коррелятор**, если хотите, чтобы события отправлялись в коррелятор.
      - Выберите **Другое**, если хотите выбрать иную точку назначения.

К этому типу относятся также сервисы коррелятора и хранилища, созданные в предыдущих версиях программы.

Откроется окно **Добавить точку назначения**, где вам требуется параметры пересылки событий.

b. В раскрывающемся списке **Точка назначения** выберите существующую точку назначения или выберите пункт **Создать**, если хотите создать новую точку назначения.

При создании новой точки назначения заполните параметры, как указано в описании ресурса точки назначения (см. раздел "Точки назначения" на стр. 199).

c. Нажмите **Сохранить**.

Точка назначения добавлена к условию создания событий аудита активов. Для каждого условия можно добавить несколько точек назначения. Вы также можете выключить уже настроенное условие создания событий аудита активов, для этого нажмите на флажок **Выключено** напротив требуемого условия.

4. Нажмите **Сохранить**.

Аудит активов настроен. События аудита активов будут создаваться для тех условий, для которых были добавлены точки назначения. Вы также можете выключить аудит активов для существующего тенанта. Для этого нажмите на требуемый тенант и установите флажок **Выключено** в верхней части открывшегося окна **Аудит активов**. Нажмите **Сохранить**.

Хранение и поиск событий аудита активов

События аудита активов считаются базовыми (см. раздел "Модель данных нормализованного события" на стр. 471) и не заменяют собой событий аудита (см. раздел "Поля событий аудита" на стр. 502). События аудита активов можно искать по следующим параметрам:

Поле события	Значение
DeviceVendor	`Kaspersky`
DeviceProduct	`KUMA`
DeviceCategory	`Audit assets`

Для событий аудита активов можно настроить пространство хранилища (см. раздел "Окно Разделы" на стр. 232) с особыми правилами хранения.

Включение и выключение аудита активов

Можно включить или выключить аудит активов для тенанта или для определенного условия в рамках одного тенанта.

► *Чтобы включить или выключить аудит активов для тенанта:*

1. Откройте раздел **Параметры** → **Аудит активов** веб-интерфейса KUMA и выберите тенант, для которого которого вы хотите включить или выключить аудит активов.

Откроется окно **Аудит активов**.

2. Установите или снимите в верхней части окна флажок **Выключено**.
3. Нажмите **Сохранить**.

► *Чтобы включить или выключить отдельное условие создания событий аудита активов:*

1. Откройте раздел **Параметры** → **Аудит активов** веб-интерфейса KUMA и выберите тенант, для которого которого вы хотите включить или выключить условие создания событий аудита активов.

   Откроется окно **Аудит активов**.
2. Установите или снимите напротив нужных условий флажок **Выключено**.
3. Нажмите **Сохранить**.

kaspersky

Управление KUMA

В этом разделе описываются общие параметры KUMA.

В этом разделе

Просмотр метрик KUMA 401
Работа с задачами KUMA 405
Подключение к SMTP-серверу 407
Онлайн-справка KUMA 408
Журналы KUMA 408
Резервное копирование KUMA 409
Уведомления KUMA 410

Просмотр метрик KUMA

Полная информация о рабочих характеристиках Ядра, коллекторов, корреляторов и хранилищ KUMA доступна в разделе **Метрики** веб-интерфейса KUMA. При выборе этого раздела открывается автоматически обновляемый портал Grafana, развернутый во время установки Ядра KUMA.

Логин и пароль Grafana по умолчанию: `admin` и `admin`.

Доступные показатели метрик

Показатели коллекторов:

- IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.
  - Processing EPS (Обрабатываемые события в секунду) – количество обрабатываемых событий в секунду.
  - Processing Latency (Время обработки события) – время, необходимое для обработки одного события (отображается медиана).
  - Output EPS (Вывод событий) – количество событий, отправляемых в точку назначения за секунду.
  - Output Latency (Задержка вывода) – время, необходимое для отправки пакета событий в пункт назначения и получения от него ответа (отображается медиана).
  - Output Errors (Ошибки вывода) – количество ошибок при отправке пакетов событий в пункт назначения в секунду. Сетевые ошибки и ошибки записи в дисковый буфер отображаются отдельно.
  - Output Event Loss (Потеря событий) – количество потерянных событий в секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер. События также

теряются, если место назначения ответило кодом ошибки (например, если запрос был недействительным).

- Normalization (Нормализация) – показатели, относящиеся к нормализаторам.
  - Raw & Normalized event size (Размер сырых и нормализованных событий) – размер необработанного события и размер нормализованного события (отображается медиана).
  - Errors (Ошибки) – количество ошибок нормализации в секунду.
- Filtration (Фильтрация) – показатели, относящиеся к фильтрам.
  - EPS (События, обрабатываемые в секунду) – количество событий, отклоняемых Коллектором за секунду. Коллектор отклоняет события только в том случае, если пользователь добавил ресурс фильтра в конфигурацию сервиса коллектора.
- Aggregation (Агрегация) – показатели, относящиеся к правилам агрегации.
  - EPS (События, обрабатываемые в секунду) – количество событий, полученных и созданных правилом агрегации за секунду. Этот показатель помогает определить эффективность правил агрегации.
  - Buckets (Контейнеры) – количество контейнеров в правиле агрегации.
- Enrichment (Обогащение) – показатели, относящиеся к правилам обогащения.
  - Cache RPS (Запросы к кешу в секунду) – количество запросов к локальному кешу в секунду.
  - Source RPS (Запросы к источнику в секунду) – количество запросов к источнику обогащения (например, к словарю).
  - Source Latency (Задержка источника) – время, необходимое для отправки запроса к источнику обогащения и получения от него ответа (отображается медиана).
  - Queue (Очередь) – размер очереди запросов на обогащение. Эта метрика помогает найти "узкие места" в правилах обогащения.
  - Errors (Ошибки) – количество ошибок запроса источника обогащения в секунду.

Показатели коррелляторов

- IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.
  - Processing EPS (Обрабатываемые события в секунду) – количество обрабатываемых событий в секунду.
  - Processing Latency (Время обработки события) – время, необходимое для обработки одного события (отображается медиана).
  - Output EPS (Вывод событий) – количество событий, отправляемых в точку назначения за секунду.
  - Output Latency (Задержка вывода) – время, необходимое для отправки пакета событий в пункт назначения и получения от него ответа (отображается медиана).
  - Output Errors (Ошибки вывода) – количество ошибок при отправке пакетов событий в пункт назначения в секунду. Сетевые ошибки и ошибки записи в дисковый буфер отображаются отдельно.
  - Output Event Loss (Потеря событий) – количество потерянных событий в секунду. События могут быть потеряны из-за сетевых ошибок или ошибок записи в дисковый буфер. События также теряются, если место назначения ответило кодом ошибки (например, если запрос был недействительным).

- Correlation (Корреляция) – показатели, относящиеся к правилам корреляции.
  - EPS (События, обрабатываемые в секунду) – количество корреляционных событий, создаваемых за секунду.
  - Buckets (Контейнеры) – количество контейнеров в правиле корреляции (только для правил корреляции стандартного типа).
- Active Lists (Активные листы) – показатели, относящиеся к активным листам.
  - RPS (Запросы в секунду) – количество запросов (и их тип) к активному листу в секунду.
  - Records (Записи) – количество записей в активном листе.
  - WAL Size (Размер журнала Write-Ahead-Log) – размер журнала упреждающей записи. Эта метрика помогает определить размер активного листа.

Показатели хранилища

- IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.
  - RPS (Запросы в секунду) – количество запросов к Хранилищу в секунду.
  - Latency (Задержка) – время проксирования одного запроса к узлу ClickHouse (отображается медиана).

Показатели Ядра

- IO (Ввод-вывод) – метрики, относящиеся к вводу и выводу сервиса.
  - RPS (Запросы в секунду) – количество запросов к Ядру в секунду.
  - Latency (Задержка) – время обработки одного запроса (отображается медиана).
  - Errors (Ошибки) – количество ошибок запросов в секунду.
- Notification Feed (Фид уведомлений) – показатели, относящиеся к активности пользователей.
  - Subscriptions (Подписки) – количество клиентов, подключенных к Ядру через SSE для получения сообщений сервера в реальном времени. Это число обычно коррелирует с количеством клиентов, использующих веб-интерфейс KUMA.
  - Errors (Ошибки) – количество ошибок отправки сообщений в секунду.
- Schedulers (Планировщики) – показатели, относящиеся к задачам Ядра.
  - Active (Активные) – количество повторяющихся активных системных задач. Задачи, созданные пользователем, игнорируются.
  - Latency (Задержка) – время обработки одного запроса (отображается медиана).
  - Position (Позиция) – позиция (отметка времени) задачи создания алерта. Следующее сканирование ClickHouse на предмет корреляционных событий начнется с этой позиции.
  - Errors (Ошибки) – количество ошибок задач в секунду.

Метрики, общие для всех сервисов

- Process (Процесс) – общие метрики процесса.
  - CPU (ЦП) – загрузка ЦП.
  - Memory (Память) – использование RAM (RSS).
  - DISK IOPS (Операции чтения/записи диска) – количество операций чтения / записи на диск в секунду.

  - DISK BPS (Считанные/записанные байты диска) – количество байтов, считываемых / записываемых на диск в секунду.
  - Network BPS (Байты, принятые/переданные по сети) – количество байтов, полученных / отправленных в секунду.
  - Network Packet Loss (Потеря пакетов) – количество сетевых пакетов, потерянных в секунду.
  - GC Latency (Задержка сборщика мусора) – время цикла сборщика мусора GO (Garbage Collector), отображается медиана.
  - Goroutines (Гоурутины) – количество активных гоурутин. Это число отличается от количества потоков.
- OS (ОС) – показатели, относящиеся к операционной системе.
  - Load (Нагрузка) – средняя нагрузка.
  - CPU (ЦП) – загрузка ЦП.
  - Memory (Память) – использование RAM (RSS).
  - Disk (Диск) – использование дискового пространства.

Срок хранения метрик

По умолчанию данные о работе KUMA хранятся 3 месяца. Этот срок можно изменить.

► *Чтобы изменить срок хранения метрик KUMA:*

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.
2. В файле /etc/systemd/system/multi-user.target.wants/kuma-victoria-metrics.service в параметре ExecStart измените флаг `--retentionPeriod=<срок хранения метрик в месяцах>`, подставив нужный срок. Например, `--retentionPeriod=4` означает, что метрики будут храниться 4 месяца.
3. Перезапустите KUMA, выполнив последовательно следующие команды:
   a. systemctl daemon-reload
   b. systemctl restart kuma-victoria-metrics

Срок хранения метрик изменен.

kaspersky

Работа с задачами KUMA

При работе в веб-интерфейсе программы вы можете выполнять различные операции с помощью задач. Например, вы можете выполнить импорт активов или экспортировать информацию о событиях KUMA в TSV-файл.

В этом разделе

Просмотр таблицы задач 405

Настройка отображения таблицы задач 406

Просмотр результата выполнения задачи 406

Повторный запуск задачи 407

Просмотр таблицы задач

Таблица задач содержит список созданных задач и находится в разделе **Диспетчер задач** окна веб-интерфейса программы. Вы можете просматривать задачи, созданные вами (текущим пользователем).

Пользователь с ролью главного администратора может просматривать задачи всех пользователей.

В таблице задач содержится следующая информация:

- **Статус** – статус задачи. Задаче может быть присвоен один из следующих статусов:
  - *Мигает зеленая точка* – задача активна.
  - **Завершено** – задача выполнена.
  - **Отмена** – задача отменена пользователем.
  - **Ошибка** – задача не была завершена из-за ошибки. Сообщение об ошибке отображается при наведении курсора мыши на значок восклицательного знака.
- **Задача** – тип задачи. В программе доступны следующие типы задач:
  - **Экспорт событий** – экспорт событий KUMA.
  - **Threat Lookup** – запрос данных с портала Kaspersky Threat Intelligence Portal.
  - **Ретроспективная проверка** – задание на воспроизведение событий.
  - **Импорт активов KSC** – импорт данных об активах с серверов Kaspersky Security Center.
  - **Импорт учетных записей** – импорт данных о пользователях из Active Directory.
  - **Импорт активов KICS for Networks** – импорт данных об активах из KICS for Networks.
- **Создал** – пользователь, создавший задачу. Если задача создана автоматически, в столбце указано **Задача по расписанию**.

  Этот столбец отображается только для пользователей с ролями главный администратор и администратор (см. раздел "Роли пользователей" на стр. 57).
- **Создана** – время создания задачи.

- **Последнее обновление** – время обновления задачи.
- **Тенант** – название тенанта, в котором была запущена задача.

Отображаемый формат даты:

- Английская локализация: ГГГГ-ММ-ДД.
- Русская локализация: ДД.ММ.ГГГГ.

Настройка отображения таблицы задач

Вы можете настроить отображение столбцов, а также порядок их следования в таблице задач.

► *Чтобы настроить отображение и порядок следования столбцов в таблице задач:*

1. В веб-интерфейсе KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. В заголовочной части таблицы нажмите на кнопку .
3. В отобразившемся окне выполните следующие действия:
   - Если вы хотите включить отображение столбца в таблице, установите флажок рядом с названием того параметра, который должен отображаться в таблице.
   - Если вы не хотите, чтобы параметр отображался в таблице, снимите флажок.

   Должен быть установлен хотя бы один флажок.
4. Если вы хотите сбросить настройки, нажмите на ссылку **По умолчанию**.
5. Если вы хотите изменить порядок отображения столбцов в таблице, наведите курсор мыши на название столбца, зажмите левую клавишу мыши и перетащите столбец в нужное место.

Отображение столбцов в таблице задач будет настроено.

Просмотр результата выполнения задачи

► *Чтобы просмотреть результат выполнения задачи:*

1. В веб-интерфейсе KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. Нажмите на ссылку с типом задачи в столбце **Задача**.

   Отобразится список доступных для этого типа задач операций.

3. Выберите **Показать результат**.

Откроется окно с результатом выполнения задачи.

Повторный запуск задачи

► *Чтобы перезапустить задачу:*

1. В веб-интерфейсе KUMA выберите раздел **Диспетчер задач**.

   Отобразится таблица задач.

2. Нажмите на ссылку с типом задачи в столбце **Задача**.

   Отобразится список доступных для этого типа задач операций.

3. Выберите **Перезапустить**.

Задача будет запущена повторно.

Подключение к SMTP-серверу

В KUMA можно настроить отправку уведомлений (см. раздел "Уведомления KUMA" на стр. 410) по электронной почте с помощью SMTP-сервера. Пользователи (см. раздел "Управление пользователями" на стр. 69) будут получать уведомления, если в настройках их профиля установлен флажок **Получать уведомления по почте**.

Для обработки уведомлений KUMA можно добавить только один SMTP-сервер. Управление подключением к SMTP-серверу осуществляется в разделе веб-интерфейса KUMA **Параметры → Общие → Параметры подключения к SMTP-серверу**.

► *Чтобы настроить подключение к SMTP-серверу:*

1. Откройте веб-интерфейс KUMA и выберите раздел **Параметры → Общие**.
2. В блоке параметров **Параметры подключения к SMTP-серверу** измените необходимые параметры:
   - **Выключено** – установите этот флажок, если хотите отключить подключение к SMTP-серверу.
   - **Адрес сервера** (обязательно) – адрес SMTP-сервера в одном из следующих форматов: hostname, IPv4, IPv6.
   - **Порт** (обязательно) – порт подключения к почтовому серверу. Значение должно быть целым числом от 1 до 65 535.
   - **От кого** (обязательно) – адрес электронной почты отправителя сообщения. Например, `kuma@company.com`.
   - **Псевдоним сервера Ядра KUMA** – отличное от FQDN название сервера Ядра KUMA, которое используется в вашей сети.
   - При необходимости в раскрывающемся списке **Секрет** выберите ресурс секрета (см. раздел "Секреты" на стр. 226) типа **credentials**, в котором записаны учетные данные для подключения к SMTP-серверу.

     Добавить секрет (см. раздел "Добавление секрета" на стр. 177)
   - Выберите периодичность уведомлений в раскрывающемся списке **Регулярность уведомлений мониторинга**.
   - Включите переключатель **Выключить уведомления мониторинга**, если не хотите получать уведомления о состоянии источников событий. По умолчанию переключатель выключен.

3. Нажмите **Сохранить**.

Соединение с SMTP-сервером настроено, пользователи могут получать сообщения электронной почты (см. раздел "Уведомления KUMA" на стр. 410) от KUMA.

Онлайн-справка KUMA

Онлайн-справка доступна на сайте "Лаборатории Касперского".

Онлайн-справка предоставляет информацию по следующим темам:

- Подготовка к установке и установка KUMA.
- Настройка и использование KUMA.

► *Чтобы открыть онлайн-справку для KUMA,*

войдите в веб-интерфейс KUMA, в левом нижнем углу окна нажмите имя учетной записи пользователя и в открывшемся меню нажмите на кнопку **Справка**.

Журналы KUMA

Некоторые сервисы и ресурсы KUMA могут регистрировать информацию, связанную с их работой. Эта функция включается с помощью флажка или выпадающего списка **Отладка** в параметрах сервиса или ресурса.

Журналы хранятся на машине, на которой установлен требуемый сервис или сервис, использующий требуемый ресурс:

- Журналы на машинах Linux можно просмотреть с помощью команды `journalctl` в консоли Linux.

  Примеры:

  - `journalctl -u kuma-collector * kuma-correlator * -f` – вернет последние журналы из коллекторов и коррелляторов, установленных на сервере, где была выполнена команда.
  - `journalctl -u kuma-collector-<идентификатор сервиса>` – вернет последние журналы определенного корректора, установленного на сервере, где была выполнена команда.
- Журналы на машинах Windows можно просмотреть в файле %PROGRAMDATA%\Kaspersky Lab\KUMA\<идентификатор агента>\agent.log. Работа агентов на машинах Windows журналируется всегда, если им присвоены права logon as a service (см. раздел "Установка агента KUMA на устройствах Windows" на стр. 267), однако при установленном флажке **Отладка** данные указываются более подробно.

Сервисы, где доступно ведение журнала:

- Коррелляторы
- Коллекторы
- Агенты

Ресурсы, где доступно ведение журнала:

- Коннекторы
- Правила обогащения
- Точки назначения

Резервное копирование KUMA

KUMA позволяет выполнять резервное копирование базы данных Ядра KUMA и сертификатов. Резервное копирование осуществляется с помощью исполняемого файла (см. раздел "Команды для запуска и установки компонентов вручную" на стр. 462) /opt/kaspersky/kuma/kuma.

Восстановление данных из резервной копии доступно только при сохранении версии KUMA.

► *Чтобы выполнить резервное копирование:*

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.
2. Выполните следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma tools backup --dst <путь к директории для резервной копии> --certificates
   ```

   Флаг `--certificates` не является обязательным и используется для резервного копирования сертификатов.

Резервная копия создана.

► *Чтобы восстановить данные из резервной копии:*

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.
2. Остановите Ядро KUMA, выполнив следующую команду:

   ```
   sudo systemctl stop kuma-core
   ```

3. Выполните следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma tools restore --src <путь к директории с резервной копией> --certificates
   ```

   Флаг `--certificates` не является обязательным и используется для восстановления сертификатов.

4. Запустите KUMA, выполнив следую команду:

   ```
   sudo systemctl start kuma-core
   ```

5. Пересоздайте сервисы, используя восстановленные наборы ресурсов для сервисов.

Данные восстановлены из резервной копии.

Что делать при сбоях в работе KUMA после восстановления данных из резервной копии (см. раздел "Сбои в работе KUMA после восстановления из резервной копии" на стр. 410)

Резервное копирование коллекторов не требуется, за исключением коллекторов с SQL-подключением. При восстановлении таких коллекторов следует вернуть к исходному начальное значение идентификатора.

Сбои в работе KUMA после восстановления из резервной копии

Если после восстановления данных не включается Ядро KUMA, необходимо повторить восстановление, обнулив при этом базу данных kuma в MongoDB®.

► *Чтобы восстановить данные KUMA с обнулением базы данных MongoDB:*

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.
2. Остановите Ядро KUMA, выполнив следующую команду:

   ```
   sudo systemctl stop kuma-core
   ```
3. Войдите в MongoDB, выполнив следующие команды:
   a. `cd /opt/kaspersky/kuma/mongodb/bin/`
   b. `./mongo`
4. Обнулите базу данных MongoDB, выполнив следующие команды:
   a. `use kuma`
   b. `db.dropDatabase()`
5. Выйдите из базы данных MongoDB, нажав **CTRL+C**.
6. Восстановите данные из резервной копии, выполнив следующую команду:

   ```
   sudo /opt/kaspersky/kuma/kuma tools restore --src <путь к директории с резервной копией> --certificates
   ```

   Флаг `--certificates` не является обязательным и используется для восстановления сертификатов.
7. Запустите KUMA, выполнив следую команду:

   ```
   sudo systemctl start kuma-core
   ```
8. Пересоздайте сервисы, используя восстановленные наборы ресурсов для сервисов.

Данные восстановлены из резервной копии.

Уведомления KUMA

Стандартные уведомления

В KUMA можно настроить отправку уведомлений по электронной почте с помощью SMTP-сервера. Для этого необходимо настроить подключение к SMTP-серверу (на стр. 407), а также установить флажок **Получать уведомления по почте** для пользователей (см. раздел "Управление пользователями" на стр. 69), которым должны приходить уведомления.

KUMA автоматически уведомляет пользователей о следующих событиях:

- создан отчет (см. раздел "Отчеты" на стр. 278) (уведомление получают пользователи, перечисленные в шаблоне отчета (см. раздел "Настройка расписания отчетов" на стр. 281));
- создан алерт (см. раздел "Просмотр информации об алерте" на стр. 333) (уведомление получают все пользователи);
- алерт назначен пользователю (уведомление получает пользователь, которому был назначен алерт);
- выполнена задача (см. раздел "Просмотр таблицы задач" на стр. 405) (уведомление получают пользователи, создавшие задачу).

Пользовательские уведомления

Вместо стандартных уведомлений KUMA о создании алертов можно рассылать уведомления на основании пользовательских шаблонов. Настройка пользовательских уведомлений взамен стандартных происходит по шагам:

- Создание ресурса шаблона электронной почты (см. раздел "Шаблоны уведомлений" на стр. 220).
- Создание правила уведомления (см. раздел "Уведомления об алертах" на стр. 339), в котором указываются правила корреляции и адреса электронной почты.

Когда по выбранным правилам корреляции будет создаваться алерт, на указанные адреса электронной почты будут отправляться уведомления, созданные на основе пользовательских шаблонов электронной почты. Стандартные уведомления KUMA о том же событии на указанные адреса отправлены не будут.

kaspersky

Обращение в службу технической поддержки

Если вам не удается найти решение своей проблемы в документации к программе, обратитесь к специалисту по технической поддержке в "Лабораторию Касперского".

Лаборатория Касперского предоставляет поддержку этой программы в течение ее жизненного цикла (см. страницу жизненного цикла программ (https://support.kaspersky.com/corporate/lifecycle)).

kaspersky

REST API

В KUMA можно обращаться из сторонних решений с помощью API. KUMA REST API работает через HTTP и представляет набор методов запрос/ответ.

Запросы REST API необходимо отправлять по следующему адресу:

https://<FQDN Ядра KUMA>/api/<Версия API><запрос>

Пример:

https://kuma.example.com:7223/api/v1

По умолчанию для запросов используется порт 7223. При необходимости порт можно изменить.

► *Чтобы изменить порт, используемый для запросов REST API:*

в файле /etc/systemd/system/multi-user.target.wants/kuma-core.service в строке `ExecStart=/opt/kaspersky/kuma/kuma core --external :7220 --internal :7210 --mongo mongodb://localhost:27017` добавьте флаг `--rest <требуемый номер порта для запросов REST API>`.

1. Войдите в ОС сервера, на котором установлено Ядро KUMA.
2. В файле /etc/systemd/system/multi-user.target.wants/kuma-core.service измените следующую строку, подставив нужный порт:

   ```
   ExecStart=/opt/kaspersky/kuma/kuma core --external :7220 --internal :7210 --mongo mongodb://localhost:27017 --rest <требуемый номер порта для запросов REST API>
   ```

3. Перезапустите KUMA, выполнив последовательно следующие команды:
   a. `systemctl daemon-reload`
   b. `systemctl restart kuma-core`

Для запросов REST API используется новый порт.

Убедитесь, что порт доступен и не закрыт межсетевым экраном.

Заголовок для аутентификации: Authorization: Bearer <токен>

Формат данных по умолчанию: JSON

Формат даты и времени: RFC 3339

Интенсивность запросов: не ограничена

kaspersky

В этом разделе

Создание токена 414
Настройка прав доступа к API 414
Авторизация API-запросов 415
Стандартная ошибка 415
Операции 416

Создание токена

► *Чтобы сгенерировать токен для пользователя:*

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Пользователи**.

   В правой части раздела **Параметры** отобразится таблица **Пользователи**.

2. Выберите нужного пользователя и в открывшейся справа области деталей нажмите на кнопку **Сгенерировать токен**.

   Откроется окно **Новый токен**.

3. Если требуется, установите срок действия токена:

   a. Установите флажок **Без окончания срока действия**.

   b. В поле **Срок действия** с помощью календаря укажите дату и время истечения срока действия создаваемого токена.

4. Нажмите на кнопку **Сгенерировать токен**.

   При нажатии на эту кнопку в области деталей пользователя отображается поле с автоматически созданным токеном. При закрытии окна токен больше не отображается, и, если вы его не скопировали, потребуется сгенерировать новый токен.

5. Нажмите **Сохранить**.

Токен сгенерирован и может быть использован для API-запросов. Таким же образом можно сгенерировать токен в профиле своей учетной записи (см. раздел "Редактирование своей учетной записи" на стр. 71).

Настройка прав доступа к API

В KUMA для каждого пользователя можно настроить операции (на стр. 416), которые можно выполнять от лица этого пользователя. Права можно настроить только для пользователей, созданных в KUMA.

► *Чтобы настроить доступные операции для пользователя:*

1. Откройте раздел веб-интерфейса KUMA **Параметры** → **Пользователи**.

   В правой части раздела **Параметры** отобразится таблица **Пользователи**.

2. Выберите нужного пользователя и в открывшейся справа области деталей нажмите на кнопку **Права доступа через API**.

   Откроется окно со списком доступных операций. По умолчанию пользователю доступны все API-запросы.

3. Установите или снимите флажок напротив требуемой операции.
4. Нажмите **Сохранить**.

Доступные операции для пользователя настроены.

Доступные операции можно аналогичным образом настроить в профиле своей учетной записи (см. раздел "Редактирование своей учетной записи" на стр. 71).

Авторизация API-запросов

Каждый запрос REST API должен включать авторизацию с помощью токена (см. раздел "Создание токена" на стр. 414). Пользователь, с помощью чьего токена выполняется API-запрос, должен иметь права на выполнение (см. раздел "Настройка прав доступа к API" на стр. 414) такого типа запросов.

К каждому запросу должен прилагаться следующий заголовок:

```
Authorization: Bearer <token>
```

Возможные ошибки:

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Некорректный заголовок	invalid authorization header	Example: <пример>
403	Токен не существует или пользователь-владелец выключен	access denied	

Стандартная ошибка

Возвращаемые KUMA ошибки имеют следующий формат:

```
type Error struct {
    Message    string      `json:"message"`
    Details    interface{} `json:"details"`
}
```

kaspersky

Операции

Описание доступных запросов и ответов.

В этом разделе

Просмотр списка активных листов на коррелляторе 417
Импорт записей в активный лист 419
Поиск алертов 422
Закрытие алертов 428
Поиск активов 429
Импорт активов 433
Удаление активов 437
Поиск событий 439
Просмотр информации о кластере 442
Поиск ресурсов 444
Загрузка файла с ресурсами 446
Просмотр содержимого файла с ресурсами 447
Импорт ресурсов 448
Экспорт ресурсов 450
Скачивание файла с ресурсами 451
Поиск сервисов 452
Поиск тенантов 455
Просмотр информации о предъявителе токена 457
Обновление словаря в сервисах 458
Получение словаря 461

kaspersky

Просмотр списка активных листов на коррелляторе

GET /api/v1/activeLists

Целевой коррелятор должен быть запущен.

Доступ: администратор, аналитик.

Параметры запроса

Имя	Тип данных	Обязательный	Описание	Пример значения
correlatorID	string	Да	Идентификатор сервиса коррелятора	00000000-0000-0000-0000-000000000000

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []ActiveListInfo


type ActiveListInfo struct {
    ID      string `json:"id"`
    Name    string `json:"name"`
    Dir     string `json:"dir"`
    Records uint64 `json:"records"`
    WALSize uint64 `json:"walSize"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Не указан идентификатор сервиса коррелятора	query parameter required	correlatorID
403	Пользователь не имеет необходимой роли в тенанте коррелятора	access denied	
404	Сервис с указанным идентификатором (correlatorID) не найден	service not found	
406	Сервис с указанным идентификатором (correlatorID) не является коррелятором	service is not correlator	
406	Коррелятор не выполнил первый старт	service not paired	
406	Тенант коррелятора отключен	tenant disabled	
50x	Не удалось обратиться к API коррелятора	correlator API request failed	вариативное
500	Не удалось декодировать тело ответа, полученное от коррелятора	correlator response decode failed	вариативное
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Импорт записей в активный лист

POST /api/v1/activeLists/import

Целевой коррелятор должен быть запущен.

Доступ: администратор, аналитик.

Параметры запроса

Имя	Тип данных	Обязательный	Описание	Пример значения
correlatorID	string	Да	Идентификатор сервиса коррелятора	00000000-0000-0000-0000-000000000000
activeListID	string	Если не указан activeListName	Идентификатор активного листа	00000000-0000-0000-0000-000000000000
activeListName	string	Если не указан activeListID	Имя активного листа	Attackers
format	string	Да	Формат импортируемых записей	csv, tsv, internal
keyField	string	Только для форматов csv и tsv	Имя поля в заголовке csv или tsv файла, которое будет использовано в качестве ключевого поля записи активного листа. Значения этого поля должны быть уникальными	ip
clear	bool	Нет	Очистить активный лист перед выполнением импорта. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются. Пример: /api/v1/activeLists/import?clear	

Тело запроса

Формат	Содержимое
csv	Первая строка – заголовок, где перечислены поля, разделенные запятой. Остальные строки – значения, соответствующие полям в заголовке, разделенные запятой. Количество полей на каждой строке должно быть одинаковым.
tsv	Первая строка – заголовок, где перечислены поля, разделенные TAB. Остальные строки – значения, соответствующие полям в заголовке, разделенные TAB. Количество полей на каждой строке должно быть одинаковым.
internal	Каждая строка содержит один индивидуальный объект JSON. Данные в internal формате можно получить путем экспорта содержимого активного листа из коррелятора в WEB-консоли KUMA.

Ответ

HTTP-код: 204

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Не указан идентификатор сервиса коррелятора	query parameter required	correlatorID
400	Не указан ни параметр activeListID, ни параметр activeListName	one of query parameters required	activeListID, activeListName
400	Не указан параметр format	query parameter required	format
400	Параметр format имеет неверное значение	invalid query parameter value	format
400	Параметр keyField не задан	query parameter required	keyField
400	Тело запроса имеет нулевую длину	request body required	
400	CSV или TSV файл не содержит поле, указанное в параметре keyField	correlator API request failed	line 1: header does not contain column <name>
400	Ошибка парсинга тела запроса	correlator API request failed	line <number>: <message>
403	Пользователь не имеет необходимой роли в тенанте коррелятора	access denied	

404	Сервис с указанным идентификатором (correlatorID) не найден	service not found	
404	Активный лист не найден	active list not found	
406	Сервис с указанным идентификатором (correlatorID) не является коррелятором	service is not correlator	
406	Коррелятор не выполнил первый старт	service not paired	
406	Тенант коррелятора отключен	tenant disabled	
406	Поиск активного листа выполнялся по имени (activeListName) и было найдено более одного активного листа	more than one matching active lists found	
50x	Не удалось обратиться к API коррелятора	correlator API request failed	вариативное
500	Не удалось декодировать тело ответа, полученное от коррелятора	correlator response decode failed	вариативное
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Поиск алертов

GET /api/v1/alerts

Доступ: администратор, аналитик, оператор.

Параметры запроса

Имя	Тип данных	Обязательный	Описание	Пример значения
page	number	Нет	Номер страницы. Начинается с 1. Размер страницы - 250 записей. Если параметр не указан, то используется значение по умолчанию - 1.	1
id	string	Нет	Идентификатор алерта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
tenantID	string	Нет	Идентификатор тенанта алерта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0000-000000000000
name	string	Нет	Имя алерта. Регистронезависимое регулярное выражение (PCRE).	alert ^My alert$
timestampField	string	Нет	Имя поля алерта, по которому выполняется сортировка (DESC) и поиск по периоду (from - to). По умолчанию lastSeen.	lastSeen, firstSeen
from	string	Нет	Нижняя границы периода в формате RFC3339. <timestampField> >= <from>	2021-09-06T00:00:00Z (UTC) 2021-09-06T00:00:00.000Z (UTC, с указанием миллисекунд) 2021-09-06T00:00:00Z+00:00 (MSK)

to	string	Нет	Верхняя периода в формате RFC3339. <timestampField> <= <to>	2021-09-06T00:00:00Z (UTC) 2021-09-06T00:00:00.000Z (UTC, с указанием миллисекунд) 2021-09-06T00:00:00Z+00:00 (MSK)
status	string	Нет	Статус алерта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	new, assigned, escalated, closed
withEvents	bool	Нет	Включить в ответ нормализованные события KUMA, связанные с найденными алертами. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются. Пример: /api/v1/alerts?withEvents	
withAffected	bool	Нет	Включить в ответ информацию об активах и аккаунтах, связанных с найденными алертами. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются. Пример: /api/v1/alerts?withAffected	

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Alert


type Alert struct {
    ID                string            `json:"id"`
    TenantID          string            `json:"tenantID"`
    TenantName        string            `json:"tenantName"`
    Name              string            `json:"name"`
    CorrelationRuleID string            `json:"correlationRuleID"`
    Priority          string            `json:"priority"`
    Status            string            `json:"status"`
    FirstSeen         string            `json:"firstSeen"`
    LastSeen          string            `json:"lastSeen"`
    Assignee          string            `json:"assignee"`
    ClosingReason     string            `json:"closingReason"`
    Overflow          bool              `json:"overflow"`
    Events            []NormalizedEvent `json:"events"`
    AffectedAssets    []AffectedAsset   `json:"affectedAssets"`
    AffectedAccounts  []AffectedAccount `json:"affectedAccounts"`
}


type NormalizedEvent map[string]interface{}


type AffectedAsset struct {
    ID               string          `json:"id"`
    TenantID         string          `json:"tenantID"`
    TenantName       string          `json:"tenantName"`
    Name             string          `json:"name"`
    FQDN             string          `json:"fqdn"`
```

```
    IPAddresses      []string        `json:"ipAddresses"`
    MACAddresses     []string        `json:"macAddresses"`
    Owner            string          `json:"owner"`
    OS               *OS             `json:"os"`
    Software         []Software      `json:"software"`
    Vulnerabilities  []Vulnerability `json:"vulnerabilities"`
    KSC              *KSCFields      `json:"ksc"`
    Created          string          `json:"created"`
    Updated          string          `json:"updated"`
}

type OS struct {
    Name    string `json:"name"`
    Version uint64 `json:"version"`
}

type Software struct {
    Name    string `json:"name"`
    Version string `json:"version"`
    Vendor  string `json:"vendor"`
}

type Vulnerability struct {
    KasperskyID           string   `json:"kasperskyID"`
    ProductName           string   `json:"productName"`
    DescriptionURL        string   `json:"descriptionURL"`
    RecommendedMajorPatch string   `json:"recommendedMajorPatch"`
    RecommendedMinorPatch string   `json:"recommendedMinorPatch"`
    SeverityStr           string   `json:"severityStr"`
    Severity              uint64   `json:"severity"`
    CVE                   []string `json:"cve"`
```

```
    ExploitExists          bool      `json:"exploitExists"`
    MalwareExists          bool      `json:"malwareExists"`
}

type AffectedAccount struct {
    Name              string `json:"displayName"`
    CN                string `json:"cn"`
    DN                string `json:"dn"`
    UPN               string `json:"upn"`
    SAMAccountName    string `json:"sAMAccountName"`
    Company           string `json:"company"`
    Department        string `json:"department"`
    Created           string `json:"created"`
    Updated           string `json:"updated"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Неверное значение параметра page	invalid query parameter value	page
400	Неверное значение параметра status	invalid status	<status>
400	Неверное значение параметра timestampField	invalid timestamp field	
400	Неверное значение параметра from	cannot parse from	вариативное
400	Неверное значение параметра to	cannot parse to	вариативное
400	Значение параметра from больше значения параметра to	from cannot be greater than to	
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Закрытие алертов

POST /api/v1/alerts/close

Целевой коррелятор должен быть запущен.

Доступ: администратор, аналитик, оператор.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательный	Описание	Пример значения
id	string	Да	Идентификатор алерта	00000000-0000-0000-0000-000000000000
reason	string	Да	Причина закрытия алерта	responded, incorrect data, incorrect correlation rule

Ответ

HTTP-код: 204

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Не указан идентификатор алерта (id)	id required	
400	Не указана причина закрытия алерта (reason)	reason required	
400	Неверное значение параметра reason	invalid reason	
403	Пользователь не имеет необходимой роли в тенанте алерта	access denied	
404	Алерт не найден	alert not found	
406	Тенант алерта отключен	tenant disabled	
406	Алерт уже закрыт	alert already closed	
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Поиск активов

GET /api/v1/assets

Доступ: администратор, аналитик, оператор.

Параметры запроса

Имя	Тип данных	Обязательный	Описание	Пример значения
page	number	Нет	Номер страницы. Начинается с 1. Размер страницы - 250 записей. Если параметр не указан, то используется значение по умолчанию - 1.	1
id	string	Нет	Идентификатор актива. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
tenantID	string	Нет	Идентификатор тенанта актива. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0000-000000000000
name	string	Нет	Название актива. Регистронезависимое регулярное выражение (PCRE).	asset ^My asset$
fqdn	string	Нет	FQDN актива. Регистронезависимое регулярное выражение (PCRE).	^com$
ip	string	Нет	IP-адрес актива. Регистронезависимое регулярное выражение (PCRE).	10.10 ^192.168.1.2$

mac	string	Нет	MAC-адрес актива. Регистронезависимое регулярное выражение (PCRE).	^00:0a:95:9d:68:16$

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Asset


type Asset struct {
    ID                  string          `json:"id"`
    TenantID            string          `json:"tenantID"`
    TenantName          string          `json:"tenantName"`
    Name                string          `json:"name"`
    FQDN                string          `json:"fqdn"`
    IPAddresses         []string        `json:"ipAddresses"`
    MACAddresses        []string        `json:"macAddresses"`
    Owner               string          `json:"owner"`
    OS                  *OS             `json:"os"`
    Software            []Software      `json:"software"`
    Vulnerabilities     []Vulnerability `json:"vulnerabilities"`
    KSC                 *KSCFields      `json:"ksc"`
    Created             string          `json:"created"`
    Updated             string          `json:"updated"`
}


type KSCFields struct {
    NAgentID          string `json:"nAgentID"`
    KSCInstanceID     string `json:"kscInstanceID"`
    KSCMasterHostname string `json:"kscMasterHostname"`
    LastVisible       string `json:"lastVisible"`
}
```

```
type OS struct {
    Name    string `json:"name"`
    Version uint64 `json:"version"`
}

type Software struct {
    Name    string `json:"name"`
    Version string `json:"version"`
    Vendor  string `json:"vendor"`
}

type Vulnerability struct {
    KasperskyID           string   `json:"kasperskyID"`
    ProductName           string   `json:"productName"`
    DescriptionURL        string   `json:"descriptionURL"`
    RecommendedMajorPatch string   `json:"recommendedMajorPatch"`
    RecommendedMinorPatch string   `json:"recommendedMinorPatch"`
    SeverityStr           string   `json:"severityStr"`
    Severity              uint64   `json:"severity"`
    CVE                   []string `json:"cve"`
    ExploitExists         bool     `json:"exploitExists"`
    MalwareExists         bool     `json:"malwareExists"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Неверное значение параметра page	invalid query parameter value	page
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Импорт активов

Особенности идентификации, создания и обновления активов

Активы импортируются в соответствии с правилами слияния данных об активах (см. раздел "Добавление активов" на стр. 381).

POST /api/v1/assets/import

Массовое создание или обновление активов.

Доступ: администратор, аналитик.

Тело запроса

Формат: JSON

```
type Request struct {
    TenantID string  `json:"tenantID"`
   Assets   []Asset `json:"assets"`
}

type Asset struct {
    Name            string          `json:"name"`
    FQDN            string          `json:"fqdn"`
    IPAddresses     []string        `json:"ipAddresses"`
    MACAddresses    []string        `json:"macAddresses"`
    Owner           string          `json:"owner"`
    OS              *OS             `json:"os"`
    Software        []Software      `json:"software"`
    Vulnerabilities []Vulnerability `json:"vulnerabilities"`
}

type OS struct {
    Name    string `json:"name"`
    Version uint64 `json:"version"`
}

type Software struct {
```

```
    Name    string `json:"name"`
    Version string `json:"version"`
    Vendor  string `json:"vendor"`
}


type Vulnerability struct {
    KasperskyID           string   `json:"kasperskyID"`
    ProductName           string   `json:"productName"`
    DescriptionURL        string   `json:"descriptionURL"`
    RecommendedMajorPatch string   `json:"recommendedMajorPatch"`
    RecommendedMinorPatch string   `json:"recommendedMinorPatch"`
    SeverityStr           string   `json:"severityStr"`
    Severity              uint64   `json:"severity"`
    CVE                   []string `json:"cve"`
    ExploitExists         bool     `json:"exploitExists"`
    MalwareExists         bool     `json:"malwareExists"`
}
```

Обязательные поля Request

Имя	Тип данных	Обязательный	Описание	Пример значения
tenantID	string	Да	Идентификатор тенанта	00000000-0000-0000-0000-000000000000
assets	[]Asset	Да	Массив импортируемых активов	

Обязательные поля Asset

Имя	Тип данных	Обязательный	Описание	Пример значения
fqdn	string	Если не указан ipAddresses	FQDN актива. Рекомендуется указывать именно FQDN, а не просто имя хоста. Приоритетный признак для идентификации актива.	my-asset-1.example.com my-asset-1
ipAddresses	[]string	Если не указан fqdn	Массив IP-адресов актива. IPv4 или IPv6. Первый элемент массива используется как второстепенный признак для идентификации актива.	["192.168.1.1", "192.168.2.2"] ["2001:0db8:85a3:0000:0000:8a2e:0370:7334"]

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
    InsertedIDs  map[int64]interface{} `json:"insertedIDs"`
    UpdatedCount uint64                `json:"updatedCount"`
    Errors       []ImportError         `json:"errors"`
}

type ImportError struct {
    Index   uint64 `json:"index"`
    Message string `json:"message"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Не указан идентификатор тенанта (tenantID)	tenantID required	
400	Попытка импорта активов в shared тенант	import into shared tenant not allowed	
400	В теле запроса не указан ни один актив	at least one asset required	
400	Не указано ни одно из обязательных полей	one of fields required	asset[<index>]: fqdn, ipAddresses
400	Неверный FQDN	invalid value	asset[<index>].fqdn
400	Неверный IP address	invalid value	asset[<index>].ipAddresses[<index>]
400	Дублируется IP адрес	duplicated value	asset[<index>].ipAddresses
400	Неверный MAC адрес	invalid value	asset[<index>].macAddresses[<index>]
400	Дублируется MAC адрес	duplicated value	asset[<index>].macAddresses
403	Пользователь не имеет необходимой роли в указанном тенанте	access denied	
404	Указанный тенант не найден	tenant not found	
406	Указанный тенант отключен	tenant disabled	
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Удаление активов

POST /api/v1/assets/delete

Доступ: администратор, аналитик.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательный	Описание	Пример значения
tenantID	string	Да	Идентификатор тенанта	00000000-0000-0000-0000-000000000000
ids	[]string	Если не указаны ни fqdns, ни ipAddresses	Список идентификаторов активов	["00000000-0000-0000-0000-000000000000"]
fqdns	[]string	Если не указаны ни ids, ни ipAddresses	Массив FQDN активов	["my-asset-1.example.com", "my-asset-1"]
ipAddresses	[]string	Если не указаны ни ids, ни fqdns	Массив основных IP адресов активов (первый элемент массива ipAddresses в запросе на импорт)	["192.168.1.1", "2001:0db8:85a3:0000:0000:8a2e:0370:7334"]

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
    DeletedCount uint64 `json:"deletedCount"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Не указан идентификатор тенанта (tenantID)	tenantID required	
400	Попытка удаления актива из общего тенанта	delete from shared tenant not allowed	
400	Не указано ни одно из обязательных полей	one of fields required	ids, fqdns, ipAddresses
400	Указан неверный FQDN	invalid value	fqdns[<index>]
400	Указан неверный IP адрес	invalid value	ipAddresses[<index>]
403	Пользователь не имеет необходимой роли в указанном тенанте	access denied	
404	Указанный тенант не найден	tenant not found	
406	Указанный тенант отключен	tenant disabled	
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Поиск событий

POST /api/v1/events

Доступ: администратор, аналитик, оператор.

Тело запроса

Формат: JSON

Request

Имя	Тип данных	Обязательный	Описание	Пример значения
period	Period	Да	Период поиска	
sql	string	Да	SQL запрос	SELECT * FROM events WHERE Type = 3 ORDER BY Timestamp DESC LIMIT 1000 SELECT sum(BytesOut) as TotalBytesSent, SourceAddress FROM events WHERE DeviceVendor = 'netflow' GROUP BY SourceAddress LIMIT 1000 SELECT count(Timestamp) as TotalEvents FROM events LIMIT 1
clusterID	string	Нет, если кластер единственный	Идентификатор Storage кластера. Можно найти запросив список сервисов с kind = storage. Идентификатор кластера будет в поле resourceID.	00000000-0000-0000-0000-000000000000
rawTimestamps	bool	Нет	Отображать timestamp'ы в исходном виде - Milliseconds since EPOCH. По умолчанию false.	true или false

emptyFields	bool	Нет	Отображать пустые поля нормализованных событий. По умолчанию false.	true или false

Period

Имя	Тип данных	Обязательный	Описание	Пример значения
from	string	Да	Нижняя граница периода в формате RFC3339. Timestamp >= <from>	2021-09-06T00:00:00Z (UTC) 2021-09-06T00:00:00.000Z (UTC, с указанием миллисекунд) 2021-09-06T00:00:00Z+00:00 (MSK)
to	string	Да	Верхняя граница периода в формате RFC3339. Timestamp <= <to>	2021-09-06T00:00:00Z (UTC) 2021-09-06T00:00:00.000Z (UTC, с указанием миллисекунд) 2021-09-06T00:00:00Z+00:00 (MSK)

Ответ

HTTP-код: 200

Формат: JSON

Результат выполнения SQL-запроса

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Нижняя граница диапазона не указана	period.from required	
400	Нижняя граница диапазона указана в неподдерживаемом формате	cannot parse period.from	вариативное
400	Нижняя граница диапазона равна нулю	period.from cannot be 0	
400	Верхняя граница диапазона не указана	period.to required	
400	Верхняя граница диапазона указана в неподдерживаемом формате	cannot parse period.to	вариативное
400	Верхняя граница диапазона равна нулю	period.to cannot be 0	
400	Нижняя граница диапазона больше верхней	period.from cannot be greater than period.to	
400	Неверный SQL запрос	invalid sql	вариативное
400	В SQL запросе фигурирует неверная таблица	the only valid table is `events`	
400	В SQL запросе отсутствует LIMIT	sql: LIMIT required	
400	LIMIT в SQL запросе превышает максимальный (1000)	sql: maximum LIMIT is 1000	
404	Storage cluster не найден	cluster not found	
406	Параметр clusterID не был указан и в KUMA зарегистрировано множество кластеров	multiple clusters found, please provide clusterID	
500	Нет доступных нод кластера	no nodes available	
50x	Любые другие внутренние ошибки	event search failed	вариативное

kaspersky

Просмотр информации о кластере

GET /api/v1/events/clusters

Доступ: администратор, аналитик, оператор.

Кластеры Main тенанта доступны всем пользователям.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	Пример значения
page	number	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1
id	string	Нет	Идентификатор кластера. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ	00000000-0000-0000-0000-000000000000
tenantID	string	Нет	Идентификатор тенанта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0000-000000000000
name	string	Нет	Имя кластера. Регистронезависимое регулярное выражение (PCRE).	cluster ^My cluster$

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Cluster


type Cluster struct {
    ID         string `json:"id"`
    Name       string `json:"name"`
    TenantID   string `json:"tenantID"`
    TenantName string `json:"tenantName"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Неверное значение параметра page	invalid query parameter value	page
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Поиск ресурсов

GET /api/v1/resources

Доступ: администратор, аналитик, оператор.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	Пример значения
page	number	Нет	Номер страницы. Начинается с 1. Размер страницы – 250 записей. Если параметр не указан, то используется значение по умолчанию – 1.	1
id	string	Нет	Идентификатор ресурса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
tenantID	string	Нет	Идентификатор тенанта ресурса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0000-000000000000
name	string	Нет	Имя ресурса. Регистронезависимое регулярное выражение (PCRE).	resource ^My resource$
kind	string	Нет	Тип ресурса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ	collector, correlator, storage, activeList, aggregationRule, connector, correlationRule, dictionary, enrichmentRule, destination, filter, normalizer, responseRule, search, agent, proxy, secret

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Resource


type Resource struct {
    ID          string `json:"id"`
    Kind        string `json:"kind"`
    Name        string `json:"name"`
    Description string `json:"description"`
    TenantID    string `json:"tenantID"`
    TenantName  string `json:"tenantName"`
    UserID      string `json:"userID"`
    UserName    string `json:"userName"`
    Created     string `json:"created"`
    Updated     string `json:"updated"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Неверное значение параметра page	invalid query parameter value	page
400	Неверное значение параметр kind	invalid kind	<kind>
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Загрузка файла с ресурсами

POST /api/v1/resources/upload

Доступ: администратор, аналитик.

Тело запроса

Зашифрованное содержимое файла с ресурсами в бинарном формате.

Ответ

HTTP-код: 200

Формат: JSON

Идентификатор файла. Следует указать его в теле запросов на просмотр содержимого файла и на импорт ресурсов.

```
type Response struct {
    ID string `json:"id"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Размер файла превышает максимально допустимый (64 МБ)	maximum file size is 64 MB	
403	Пользователь не имеет необходимых ролей ни в одном из тенантов	access denied	
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Просмотр содержимого файла с ресурсами

POST /api/v1/resources/toc

Доступ: администратор, аналитик, оператор.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательный	Описание	Пример значения
fileID	string	Да	Идентификатор файла, полученный в результате выполнения загрузки файла с ресурсами.	00000000-0000-0000-0000-000000000000
password	string	Да	Пароль файла с ресурсами.	SomePassword!88

Ответ

HTTP-код: 200

Формат: JSON

Версия файла, список ресурсов, категорий, папок.

Идентификатор полученных ресурсов необходимо использовать при импорте.

```
type Package struct {
    Version         string                          `json:"version"`
    AssetCategories []*categories.Category         `json:"assetCategories"
`
    Folders         []*folders.Folder               `json:"folders"`
    Resources       []*resources.ExportedResource `json:"resources"`
}
```

kaspersky

Импорт ресурсов

POST /api/v1/resources/import

Доступ: администратор, аналитик.

Тело запроса

Имя	Тип данных	Обязательный	Описание	Пример значения
fileID	string	Да	Идентификатор файла, полученный в результате выполнения загрузки файла с ресурсами.	00000000-0000-0000-0000-000000000000
password	string	Да	Пароль файла с ресурсами.	SomePassword!88
tenantID	string	Да	Идентификтор целевого тенанта	00000000-0000-0000-0000-000000000000

actions	map[string]uint8	Да	Маппинг идентификатора ресурса к действию, которое нужно предпринять в отношении него.	0 – не импортировать (используется при разрешении конфликтов)
				1 – импортировать (изначально должно быть присвоено каждому ресурсу)
				2 – заменить (используется при разрешении конфликтов)
				`{`
				`"00000000-0000-0000-0000-000000000000": 0,`
				`"00000000-0000-0000-0000-000000000001": 1,`
				`"00000000-0000-0000-0000-000000000002": 2,`
				`}`

Ответ

HTTP-код	Тело
204	

409	Идентификаторы импортируемых ресурсов, конфликтующих с уже существующими по ID. В этом случае необходимо повторить операцию импорта, указав для данных ресурсов следующие действия:
	0 – не импортировать
	2 – заменить
	`type ImportConflictsError struct {`
	`HardConflicts []string `json:"conflicts"``
	`}`

kaspersky

Экспорт ресурсов

POST /api/v1/resources/export

Доступ: администратор, аналитик.

Тело запроса

Формат: JSON

Имя	Тип данных	Обязательный	Описание	Пример значения
ids	[]string	Да	Идентификаторы ресурсов, которые необходимо экспортировать	["00000000-0000-0000-0000-000000000000"]
password	string	Да	Пароль файла с экспортированными ресурсами	SomePassword!88
tenantID	string	Да	Идентификатор тенанта, которому принадлежат экспортируемые ресурсы	00000000-0000-0000-0000-000000000000

Ответ

HTTP-код: 200

Формат: JSON

Идентификатор файла с экспортированными ресурсами. Следует использовать его в запросе на скачивание файла с ресурсами.

```
type ExportResponse struct {
    FileID string `json:"fileID"`
}
```

kaspersky

Скачивание файла с ресурсами

GET /api/v1/resources/download/<id>

Здесь id – идентификатор файла, полученный в результате выполнения запроса на экспорт ресурсов.

Доступ: администратор, аналитик.

Ответ

HTTP-код: 200

Зашифрованное содержимое файла с ресурсами в бинарном формате.

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Не указан идентификатор файла	route parameter required	id
400	Идентификатор файла не является валидным UUID	id is not a valid UUID	
403	Пользователь не имеет необходимых ролей ни в одном из тенантов	access denied	
404	Файл не найден	file not found	
406	Файл является директорией	not regular file	
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Поиск сервисов

GET /api/v1/services

Доступ: администратор, аналитик.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	Пример значения
page	number	Нет	Номер страницы. Начинается с 1. Размер страницы - 250 записей. Если параметр не указан, то используется значение по умолчанию - 1.	1
id	string	Нет	Идентификатор сервиса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
tenantID	string	Нет	Идентификатор тенанта сервиса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ. Если пользователь не имеет необходимой роли в указанном тенанте, то данный тенант игнорируется.	00000000-0000-0000-0000-000000000000
name	string	Нет	Имя сервиса. Регистронезависимое регулярное выражение (PCRE).	service ^My service$
kind	string	Нет	Тип сервиса. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ	collector, correlator, storage, agent
fqdn	string	Нет	FQDN сервиса. Регистронезависимое регулярное выражение (PCRE).	hostname ^hostname.example.com$

paired	bool	Нет	Выводить только те сервисы, которые выполнили первый запуск. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются. Пример: /api/v1/services?paired	

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Service


type Service struct {
    ID         string `json:"id"`
    TenantID   string `json:"tenantID"`
    TenantName string `json:"tenantName"`
    ResourceID string `json:"resourceID"`
    Kind       string `json:"kind"`
    Name       string `json:"name"`
    Address    string `json:"address"`
    FQDN       string `json:"fqdn"`
    Status     string `json:"status"`
    Warning    string `json:"warning"`
    APIPort    string `json:"apiPort"`
    Uptime     string `json:"uptime"`
    Version    string `json:"version"`
    Created    string `json:"created"`
    Updated    string `json:"updated"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Неверное значение параметра page	invalid query parameter value	page
400	Неверное значение параметр kind	invalid kind	<kind>
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Поиск тенантов

GET /api/v1/tenants

Выводятся только доступные пользователю тенанты.

Доступ: администратор, аналитик.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	Пример значения
page	number	Нет	Номер страницы. Начинается с 1. Размер страницы - 250 записей. Если параметр не указан, то используется значение по умолчанию - 1.	1
id	string	Нет	Идентификатор тенанта. Если параметр указан несколько раз, то формируется список и применяется логический оператор ИЛИ.	00000000-0000-0000-0000-000000000000
name	string	Нет	Название тенанта. Регистронезависимое регулярное выражение (PCRE).	tenant ^My tenant$
main	bool	Нет	Вывести только основной тенант. Если параметр присутствует в URL query, его значение принимается за true. Указанные пользователем значения игнорируются. Пример: /api/v1/tenants?main	

Ответ

HTTP-код: 200

Формат: JSON

```
type Response []Tenant


type Tenant struct {
    ID          string `json:"id"`
    Name        string `json:"name"`
    Main        bool   `json:"main"`
    Description string `json:"description"`
    EPS         uint64 `json:"eps"`
    EPSLimit    uint64 `json:"epsLimit"`
    Created     string `json:"created"`
    Updated     string `json:"updated"`
}
```

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Неверное значение параметра page	invalid query parameter value	page
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Просмотр информации о предъявителе токена

GET /api/v1/users/whoami

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
    ID      string          `json:"id"`
    Name    string          `json:"name"`
    Login   string          `json:"login"`
    Email   string          `json:"email"`
    Tenants []TenantAccess `json:"tenants"`
}

type TenantAccess struct {
    ID   string `json:"id"`
    Name string `json:"name"`
    Role string `json:"role"`
}
```

kaspersky

Обновление словаря в сервисах

POST /api/v1/dictionaries/update

Обновить можно только словари в ресурсах словарей типа таблица.

Доступ: администратор, аналитик.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	Пример значения
collectorID	string	Нет	ID коллекторов, на которых будет обновлен словарь. Можно указать несколько значений, тогда словарь будет обновлен на каждом из сервисов.	00000000-0000-0000-0000-000000000000
correlatorID	string	Нет	ID коррелляторов, на которых будет обновлен словарь. Можно указать несколько значений, тогда словарь будет обновле на каждом из сервисов.	00000000-0000-0000-0000-000000000000
dictionaryID	string	Да	ID словаря, который будет обновлен.	00000000-0000-0000-0000-000000000000

Если обновление на одном из сервисов заканчивается ошибкой, это не прерывает обновления на других сервисах.

Тело запроса

Имя поля multipart	Тип данных	Обязательный	Описание	Пример значения
file	CSV-файл	Да	Запрос содержит CSV-файл. Данные существующего словаря заменяются на данные этого файла. Первая строка CSV-файла с названиями столбцов не должна меняться.	key columns,column1,column2 key1,k1col1,k1col2 key2,k2col1,k2col2

Ответ

HTTP-код: 200

Формат: JSON

```
type Response struct {
    ServicesFailedToUpdate []UpdateError `json:"servicesFailedToUpdate"`
}
type UpdateError struct {
    ID   string `json:"id"`
    Err error   `json:"err"`
}
```

Возвращает только ошибки для сервисов, на которых словари не были обновлены.

Возможные ошибки

HTTP-код	Описание	Значение поля message (см. раздел "Стандартная ошибка" на стр. 415)	Значение поля details (см. раздел "Стандартная ошибка" на стр. 415)
400	Неверное тело запроса	request body decode failed	возникшая ошибка
400	Нулевое количество строк словаря	request body required	
400	Не указан ID словаря	invalid value	dictionaryID
400	Некорректное значение строки словаря	invalid value	rows или rows[i]
400	Словарь с указанным ID имеет неверный вид (не таблица)	can only update table dictionary	
400	Попытка изменить столбцы словаря	columns must not change with update	
403	Нет доступа к запрашиваемому ресурсу	access denied	
404	Сервис не найден	service not found	
404	Словарь не найден	dictionary not found	идентификатор сервиса
500	Любые другие внутренние ошибки	вариативное	вариативное

kaspersky

Получение словаря

GET /api/v1/dictionaries

Получить можно только словари в ресурсах словарей типа таблица.

Доступ: администратор, аналитик.

Параметры запроса (URL Query)

Имя	Тип данных	Обязательный	Описание	Пример значения
dictionaryID	string	Да	ID словаря, который будет получен	00000000-0000-0000-0000-000000000000

Ответ

HTTP-код: 200

Формат: text/plain; charset=utf-8

Возвращается CSV-файл с данными словаря в теле ответа.

kaspersky

Команды для запуска и установки компонентов вручную

В этом разделе описаны параметры исполняемого файла KUMA /opt/kaspersky/kuma/kuma, с помощью которого можно вручную запустить или установить компоненты KUMA. Это может пригодиться в случае, если вам нужно увидеть выходные данные в консоли операционной системы сервера.

Таблица 7. Параметры команд

Команды	Описание
`tools`	Запуск инструментов управления KUMA.
`collector`	Установка, запуск или удаление сервиса коллектора.
`core`	Установка, запуск или удаление сервиса Ядра.
`correlator`	Установка, запуск или удаление сервиса коррелятора.
`agent`	Установка, запуск или удаление сервиса агента.
`help`	Получение информации о доступных командах и параметрах.
`license`	Получение информации о лицензии.
`storage`	Запуск или установка Хранилища.
`version`	Получение информации о версии программы.

Флаги:

`-h`, `--h` используются для получения справочной информации о командах файла kuma. Например: `kuma <компонент> --help`.

Примеры:

- `kuma version` – получение информации о версии установщика KUMA.
- `kuma core -h` – получение справки по команде `core` установщика KUMA.
- `kuma collector --core <адрес сервера, где должен получить свои параметры коллектор> --id <идентификатор устанавливаемого сервиса> --api.port <порт>` используется запуска установки сервиса коллектора.

kaspersky

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программы, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (https://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe).

Порядок получения критических обновлений изложен в формуляре.

Лицо, ответственное за эксплуатацию программы, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в программе, используя веб-сайт "Лаборатории Касперского" (https://support.kaspersky.ru/vulnerability), банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru) и иные общедоступные источники.

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского" (https://community.kaspersky.com/).

kaspersky

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. раздел "Способы получения технической поддержки" на стр. 465).

kaspersky

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о KUMA, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании KUMA.

Kaspersky предоставляет поддержку KUMA в течение жизненного цикла (см. страницу жизненного цикла программ (https://support.kaspersky.com/corporate/lifecycle)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.ru/support/rules#ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить сайт Службы технической поддержки (https://support.kaspersky.ru/b2c) ;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

kaspersky

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского":	https://www.kaspersky.ru
Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com (https://community.kaspersky.com/)

Информация о стороннем коде

Информация о стороннем коде содержится в файле LEGAL_NOTICES, расположенном в директории /opt/kaspersky/kuma/LEGAL_NOTICES.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

AMD – товарный знак или зарегистрированный товарный знак Advanced Micro Devices, Inc.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

Cisco является зарегистрированным товарным знаком или товарным знаком Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Словесный знак Grafana и логотип Grafana являются зарегистрированными товарными знаками/знаками обслуживания или товарными знаками/знаками обслуживания Coding Instinct AB в США и других странах и используются с разрешения Coding Instinct. Мы не являемся аффилированной, поддерживаемой или спонсируемой со стороны Coding Instinct или сообщества Grafana компанией.

Firebird – зарегистрированный товарный знак Firebird Foundation.

Google, Chrome – товарные знаки Google LLC.

Huawei – товарный знак Huawei Technologies Co., Ltd.

Intel – товарный знак Intel Corporation, зарегистрированный в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Active Directory, Windows и Windows Server являются товарными знаками группы компаний Microsoft.

CVE – зарегистрированный товарный знак MITRE Corporation.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

Oracle – зарегистрированный товарный знак компании Oracle и/или аффилированных компаний.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Ansible – товарный знак или зарегистрированный в США и других странах товарный знак Red Hat, Inc. или дочерних компаний.

ClickHouse – товарный знак компании YANDEX LLC.

kaspersky

Приложения

В этом разделе представлена приложения к основному тексту документа.

В этом разделе

Модель данных нормализованного события 471

Модель данных алерта 488

Модель данных актива 491

Модель данных учетной записи 499

Поля событий аудита 502

Модель данных нормализованного события

В этом разделе вы можете найти модель данных нормализованного события KUMA. Все события, которые обрабатываются коррелляторами KUMA с целью обнаружения алертов, должны соответствовать этой модели.

События, несовместимые с этой моделью данных, необходимо преобразовывать в этот формат (нормализовать) с помощью коллекторов.

Таблица 8. Модель данных нормализованного события

Название поля	Тип значения	Описание
Поля внутреннего стандарта		
ID	Строка	Уникальный идентификатор события типа UID. Никогда не меняет своего значения Для базового события, генерируемого на коллекторе, идентификатор генерируется коллектором. Идентификатор корреляционного события генерируется коррелятором.
Timestamp	Число, timestamp	Время создания базового и корреляционного событий в коллекторе. Время создания корреляционного события в коррелляторе. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
TenantID	Строка	Идентификатор тенанта.

ServiceID	Строка	Идентификатор экземпляра сервиса: коррелятора, коллектора, хранилища.
ServiceName	Строка	Название экземпляра сервиса, задается администратором KUMA при создании сервиса.
AggregationRuleName	Строка	Название правила агрегации, которое обработало событие.
AggregationRuleID	Строка	Идентификатор правила агрегации, которое обработало событие.
CorrelationRuleName	Строка	Название правила корреляции, по которому было создано корреляционное событие. Заполняется только для корреляционного события.
CorrelationRuleID	Строка	Идентификатор правила корреляции, по которому было создано корреляционное событие. Заполняется только для корреляционного события.
GroupedBy	Вложенный список строк	Список названий полей, по которым была группировка в корреляционном правиле. Заполняется только для корреляционного события.
Priority	Число	Уровень важности события.
Code	Строка	В базовом событии это код возврата процесса, функции или операции из источника. В корреляционном событии в это поле записывается код алерта для первой линии поддержки, либо код шаблона уведомления, которое будет отправлено.
Tactic	Строка	Название тактики из MITRE.
Technique	Строка	Название техники из MITRE.
ReplayID	Строка	Идентификатор ретроспективной проверки, в процессе которой было создано событие.
Raw	Строка	Неизмененный текст исходного, "сырого" события.
SourceAssetID	Строка	Идентификатор целевого актива.
DestinationAssetID	Строка	Идентификатор актива-источника.
DeviceAssetID	Строка	Идентификатор актива.
SourceAccountID	Строка	Идентификатор целевой учетной

		записи.
DestinationAccountID	Строка	Идентификатор учетной записи-источника.
SpaceID	Строка	Идентификатор пространства.
BaseEvents	Вложенный список [Event]	Вложенная структура со списком базовых событий. Поле может быть заполнено у корреляционных событий.
TI	Вложенный словарь [строка:строка]	Поле, в котором в формате словаря содержатся категории, полученные от внешнего источника Threat Intelligence по индикаторам из события.
Extra	Вложенный словарь [строка:строка]	Поле, в которое во время нормализации "сырого" события можно поместить те его поля, для которых не настроено сопоставление с полями события KUMA. Это поле может быть заполнено только у базовых событий.
AffectedAssets	Вложенная структура [Affected]	Вложенная структура, из которой можно обратиться к связанным с алертам активам и учетным записям, а также узнать, сколько раз они фигурируют в событиях алерта.
Поля по стандарту CEF		
DeviceVendor	Строка	Название производителя источника журнала. Значение берется из "сырого" события. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.
DeviceProduct	Строка	Название продукта из источника журнала. Значение берется из "сырого" события. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.
DeviceVersion	Строка	Версия продукта из источника журнала. Значение берется из "сырого" события. DeviceVendor, DeviceProduct и DeviceVersion однозначно идентифицируют источник журнала.
DeviceEventClassID	Строка	Уникальный идентификатор типа события из источника журнала. Некоторые источники журнала

		определяют категорию событий.
Name	Строка	Название события в "сыром" событии.
Severity	Строка	Уровень важности ошибки из "сырого" события.
DeviceAction	Строка	Действие, совершенное устройством или предпринятое источником журнала. Например, blocked, detected.
ApplicationProtocol	Строка	Протокол уровня приложений, например HTTP, Telnet.
DeviceCustomIPv6Address1	Строка	Поле для отображения значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных. Может использоваться для обработки журналов сетевых устройств, где необходимо отличать IP-адреса разных устройств (например, для брандмауэров). Поле настраивается.
DeviceCustomIPv6Address1Label	Строка	Описание назначения поля DeviceCustomIPv6Address1.
DeviceCustomIPv6Address2	Строка	Поле для отображения значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных. Может использоваться для обработки журналов сетевых устройств, где необходимо отличать IP-адреса разных устройств (например, для брандмауэров). Поле настраивается.
DeviceCustomIPv6Address2Label	Строка	Описание назначения поля DeviceCustomIPv6Address2.
DeviceCustomIPv6Address3	Строка	Поле для отображения значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных. Может использоваться для обработки журналов сетевых устройств, где необходимо отличать IP-адреса разных устройств (например, для брандмауэров). Поле настраивается.
DeviceCustomIPv6Address3Label	Строка	Описание назначения поля

		DeviceCustomIPv6Address3.
DeviceCustomIPv6Address4	Строка	Поле для отображения значения адреса IPv6, которое не может быть сопоставлено любому другому элементу модели данных. Может использоваться для обработки журналов сетевых устройств, где необходимо отличать IP-адреса разных устройств (например, для брандмауэров). Поле настраивается.
DeviceCustomIPv6Address4Label	Строка	Описание назначения поля DeviceCustomIPv6Address4.
DeviceEventCategory	Строка	Категория "сырого" события из схемы определения категорий событий источника журнала.
DeviceCustomFloatingPoint1	Число	Поле для значения типа Float, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomFloatingPoint1Label	Строка	Описание назначения поля DeviceCustomFloatingPoint1.
DeviceCustomFloatingPoint2	Число	Поле для значения типа Float, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomFloatingPoint2Label	Строка	Описание назначения поля DeviceCustomFloatingPoint2.
DeviceCustomFloatingPoint3	Число	Поле для значения типа Float, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomFloatingPoint3Label	Строка	Описание назначения поля DeviceCustomFloatingPoint3.
DeviceCustomFloatingPoint4	Число	Поле для значения типа Float, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomFloatingPoint4Label	Строка	Описание назначения поля DeviceCustomFloatingPoint4.
DeviceCustomNumber1	Число	Поле для целочисленного значения, которое не может быть сопоставлено

		любому другому полю модели данных. Поле настраивается.
DeviceCustomNumber1Label	Строка	Описание назначения поля DeviceCustomNumber1.
DeviceCustomNumber2	Число	Поле для целочисленного значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomNumber2Label	Строка	Описание назначения поля DeviceCustomNumber2.
DeviceCustomNumber3	Число	Поле для целочисленного значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomNumber3Label	Строка	Описание назначения поля DeviceCustomNumber3.
BaseEventCount	Число	Количество базовых событий, объединенных в агрегированном событии.
DeviceCustomString1	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomString1Label	Строка	Описания назначения поля DeviceCustomString1.
DeviceCustomString2	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomString2Label	Строка	Описания назначения поля DeviceCustomString2.
DeviceCustomString3	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.

DeviceCustomString3Label	Строка	Описания назначения поля DeviceCustomString3.
DeviceCustomString4	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomString4Label	Строка	Описания назначения поля DeviceCustomString4.
DeviceCustomString5	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomString5Label	Строка	Описания назначения поля DeviceCustomString5.
DeviceCustomString6	Строка	Поле для строкового значения, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
DeviceCustomString6Label	Строка	Описания назначения поля DeviceCustomString6.
DestinationDnsDomain	Строка	DNS-часть полного доменного имени (FQDN) точки назначения, если "сырое" событие содержит сведения об отправителе и получателе данных. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationServiceName	Строка	Название сервиса на стороне приемника трафика. Например, "sshd". Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationTranslatedAddress	Строка	IP-адрес устройства приемника трафика (после трансляции). Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationTranslatedPort	Число	Номер порта на устройстве

		приемника трафика (после трансляции адреса приемника). Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DeviceCustomDate1	Число, timestamp	Поле для значения типа Timestamp, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
DeviceCustomDate1Label	Строка	Поле для описания назначения поля DeviceCustomDate1.
DeviceCustomDate2	Число, timestamp	Поле для значения типа Timestamp, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
DeviceCustomDate2Label	Строка	Поле для описания назначения поля DeviceCustomDate2.
DeviceDirection	Число	Поле для описания направления соединения из "сырого" события. • 0 – входящее соединение. • 1 – исходящее соединение.
DeviceDnsDomain	Строка	DNS-часть полного доменного имени (FQDN) IP-адреса устройства, с которого пришло "сырое" событие.
DeviceExternalID	Строка	Внешний уникальный идентификатор устройства, если такой передается в "сыром" событии.
DeviceFacility	Строка	Facility из "сырого" события, если есть. Например, в Syslog в поле Facility может передаваться название компоненты ОС, в которой произошла ошибка.

DeviceInboundInterface	Строка	Название интерфейса входящего соединения.
DeviceNtDomain	Строка	Доменное имя Windows устройства.
DeviceOutboundInterface	Строка	Название интерфейса исходящего соединения.
DevicePayloadID	Строка	Уникальный идентификатор полезной нагрузки, который ассоциирован с "сырым" событием.
DeviceProcessName	Строка	Название процесса из "сырого" события.
DeviceTranslatedAddress	Строка	Ретранслированный IP-адрес устройства, с которого пришло "сырого" событие.
DestinationHostName	Строка	Название хоста приемника трафика. Полное доменное имя приемника трафика, если доступно. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationMacAddress	Строка	MAC-адрес устройства приемника трафика. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationNtDomain	Строка	Доменное имя Windows устройства приемника трафика. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationProcessID	Число	Идентификатор системного процесса, ассоциированного с приемником трафика в "сыром" событии. Например, если в событии указано Process ID 105, то DestinationProcessId=105. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationUserPrivileges	Строка	Названия security ролей, которые идентифицируют пользовательские привилегии на стороне точки назначения. Например, "User",

		"Guest", "Administrator". Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationProcessName	Строка	Название системного процесса в точке назначения. Например, "sshd", "telnet". Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationPort	Число	Номер порта на стороне точке назначения. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationAddress	Строка	IPv4-адрес точки назначения. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DeviceTimeZone	Строка	Часовой пояс устройства, на котором было сгенерировано событие. По умолчанию указывается часовой пояс системного времени коллектора или коррелятора. Если настроено обогащение события сведениями о часовом поясе, в поле указывается часовой пояс из правила обогащения. Если в "сыром" событии был указан часовой пояс источника события и при нормализации эти данные были сохранены, в поле события сохраняются сведения о часовом поясе источника события. Формат значения поля: +-чч:мм.
DestinationUserID	Строка	Идентификатор пользователя на стороне точки назначения. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DestinationUserName	Строка	Имя пользователя на стороне точки назначения. Может содержать адрес электронной почты пользователя. Используется для обработки

		журналов сетевого трафика, где необходимо отличать источник и точку назначения.
DeviceAddress	Строка	IPv4-адрес устройства, с которого получено событие.
DeviceHostName	Строка	Название хоста устройства, с которого было получено событие. Полное доменное имя устройства, если доступно.
DeviceMacAddress	Строка	MAC-адрес устройства, с которого было получено событие. Полное доменное имя устройства, если доступно.
DeviceProcessID	Число	Идентификатор системного процесса устройства, которое создало событие.
EndTime	Число	Время завершения события. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
ExternalID	Строка	Идентификатор устройства, которое создало событие.
FileCreateTime	Число	Время создания файла из события. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
FileHash	Строка	Хеш-код файла.
FileID	Строка	Идентификатор файла.
FileModificationTime	Число	Время последней модификации файла. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
FilePath	Строка	Путь к файлу, включая имя файла.
FilePermission	Строка	Список разрешений к файлу.
FileType	Строка	Тип файла. Например, application, pipe, socket.
FlexDate1	Число, timestamp	Поле для значения типа Timestamp, которое не может быть сопоставлено любому другому полю модели

		данных. Поле настраивается. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
FlexDate1Label	Строка	Описание назначения поля flexDate1.
FlexString1	Строка	Поле для значения типа String, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
FlexString1Label	Строка	Описание назначения поля flexString1.
FlexString2	Строка	Поле для значения типа String, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
FlexString2Label	Строка	Описание назначения поля flexString2.
FlexNumber1	Число	Поле для целочисленного типа, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
FlexNumber1Label	Строка	Описание назначения поля flexNumber1.
FlexNumber2	Число	Поле для целочисленного типа, которое не может быть сопоставлено любому другому полю модели данных. Поле настраивается.
FlexNumber2Label	Строка	Описание назначения поля flexNumber2.
FileName	Строка	Имя файла, без указания пути к файлу.
FileSize	Число	Размер файла.
BytesIn	Число	Количество полученных источником и переданных получателю байтов. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и

		точку назначения.
Message	Строка	Краткое описание ошибки или проблемы из "сырого" события.
OldFileCreateTime	Число	Время создания OLD-файла из события. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
OldFileHash	Строка	Хеш-код OLD-файла.
OldFileID	Строка	Идентификатор OLD-файла.
OldFileModificationTime	Число	Время последней модификации OLD-файла. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
OldFileName	Строка	Имя OLD-файла (без пути).
OldFilePath	Строка	Путь к OLD-файлу, включая имя файла.
OldFilePermission	Строка	Путь к OLD-файлу, включая имя файла.
OldFileSize	Число	Размер OLD-файла.
OldFileType	Строка	Тип файла. Например, application, pipe, socket.
BytesOut	Число	Количество отправленных байтов. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
EventOutcome	Строка	Результат выполнения действия. Например, "success", "failure".
TransportProtocol	Строка	Название протокола 4-уровня OSI (например, TCP, UDP).
Reason	Строка	Краткое описание причины аудита в сообщениях аудита.
RequestUrl	Строка	URL запроса.
RequestClientApplication	Строка	Агент, который обрабатывал запрос.

RequestContext	Строка	Описание контекста запроса.
RequestCookies	Строка	Файлы cookie, связанные с запросом.
RequestMethod	Строка	Метод, который использовался для доступа к веб-адресу (например, POST, GET).
DeviceReceiptTime	Число	Время получения события. Время указывается в UTC0. В веб-интерфейсе KUMA значение отображается по часовому поясу браузера пользователя.
SourceHostName	Строка	Название хоста источника трафика. Полное доменное имя источника трафика, если доступно. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceDnsDomain	Строка	Доменное имя Windows-устройства источника трафика. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceServiceName	Строка	Название сервиса на стороне источника трафика. Например, "sshd". Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceTranslatedAddress	Строка	IPv4-адрес перехода источника. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceTranslatedPort	Число	Номер порта перехода на стороне источника. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceMacAddress	Строка	MAC-адрес устройства источника трафика. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и

		точку назначения.
SourceNtDomain	Строка	Доменное имя Windows устройства источника трафика. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceProcessID	Число	Идентификатор системного процесса, ассоциированного с источником трафика в "сыром" событии. Например, если в событии указано Process ID 105, то SourceProcessId=105. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceUserPrivileges	Строка	Названия security ролей, которые идентифицируют пользовательские привилегии на стороне источника. Например, "User", "Guest", "Administrator". Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceProcessName	Строка	Название системного процесса на стороне источника. Например, "sshd", "telnet". Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourcePort	Число	Номер порта на стороне источника. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceAddress	Строка	IPv4-адрес источника. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
StartTime	Число	Время, когда началось связанное с событием действие. Время указывается в UTC0. В веб-интерфейсе KUMA значение

		отображается по часовому поясу браузера пользователя.
SourceUserID	Строка	Идентификатор пользователя на стороне источника. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
SourceUserName	Строка	Имя пользователя на стороне источника. Может содержать адрес электронной почты пользователя. Используется для обработки журналов сетевого трафика, где необходимо отличать источник и точку назначения.
Type	Число	Тип события. Доступны следующие значения: • 1 – базовое событие. • 2 – агрегированное событие. • 3 – корреляционное событие. • 4 – событие аудита. • 5 – событие мониторинга.
Поля с геоданными		
SourceCountry	Строка	Страна, соответствующая IPv4-адресу источника из поля SourceAddress.
SourceRegion	Строка	Регион, соответствующий IPv4-адресу источника из поля SourceAddress.
SourceCity	Строка	Город, соответствующий IPv4-адресу источника из поля SourceAddress.
SourceLatitude	Число	Долгота, соответствующая IPv4-адресу источника из поля SourceAddress.
SourceLongitude	Число	Широта, соответствующая IPv4-адресу источника из поля SourceAddress.
DestinationCountry	Строка	Страна, соответствующая IPv4-адресу точки назначения из поля DestinationAddress.
DestinationRegion	Строка	Регион, соответствующий IPv4-адресу точки назначения из поля DestinationAddress.
DestinationCity	Строка	Город, соответствующий IPv4-адресу точки назначения из поля DestinationAddress.

DestinationLatitude	Число	Долгота, соответствующая IPv4-адресу точки назначения из поля DestinationAddress.
DestinationLongitude	Число	Широта, соответствующая IPv4-адресу точки назначения из поля DestinationAddress.
DeviceCountry	Строка	Страна, соответствующая IPv4-адресу устройства из поля DeviceAddress.
DeviceRegion	Строка	Регион, соответствующий IPv4-адресу устройства из поля DeviceAddress.
DeviceCity	Строка	Город, соответствующий IPv4-адресу устройства из поля DeviceAddress.
DeviceLatitude	Число	Долгота, соответствующая IPv4-адресу устройства из поля DeviceAddress.
DeviceLongitude	Число	Широта, соответствующая IPv4-адресу устройства из поля DeviceAddress.

Вложенная структура `Affected`

Поле	Тип данных	Описание
`Assets`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом активов.
`Accounts`	Вложенный список `[AffectedRecord]`	Перечень и количество связанных с алертом учетных записей.

Вложенная структура `AffectedRecord`

Поле	Тип данных	Описание
`Value`	Строка	Идентификатор актива или учетной записи.
`Count`	Число	Количество раз актив или учетная запись фигурирует в связанных с алертом событиях.

kaspersky

Модель данных алерта

В этом разделе описана модель данных алерта KUMA. Алерты создаются корреляторами при выявлении с помощью правил корреляции угроз безопасности информации. Алерты необходимо расследовать для устранения этих угроз.

Поле алерта	Тип данных	Описание
`ID`	Строка	Уникальный идентификатор алерта.
`TenantID`	Строка	Идентификатор тенанта, которому принадлежит алерт. Значение наследуется от коррелятора, создавшего алерт.
`TenantName`	Строка	Название тенанта.
`CorrelationRuleID`	Строка	Идентификатор правила, на основании которого был создан алерт.
`CorrelationRuleName`	Строка	Название правила корреляции, на основании которого был создан алерт.
`Status`	Строка	Статус алерта. Возможные значения: • `New` – новый алерт. • `Assigned` – алерт назначен пользователю. • `Closed` – алерт закрыт. • `Exported to IRP` – алерт выгружен IRP-систему для дальнейшего расследования. • `Escalated` – на основе алерта создан инцидент.
`Priority`	Число	Уровень важности алерта. Возможные значения: • 1–4 – Низкий. • 5–8 – Средний. • 9–12 – Высокий. • 13–16 – Критический.
`ManualPriority`	Строка `TRUE/FALSE`	Параметр, показывающий, как был определен уровень важности алерта. Возможные значения: • `true` – задан пользователем. • `false` (значение по умолчанию) – рассчитан автоматически.
`FirstSeen`	Число	Время создания первого корреляционного события из алерта.
`LastSeen`	Число	Время создания последнего корреляционного события из алерта.
`UpdatedAt`	Число	Дата последнего изменения параметров алерта.
`UserID`	Строка	Идентификатор пользователя KUMA, которому алерт назначен на рассмотрение.
`UserName`	Строка	Имя пользователя KUMA, которому алерт назначен на рассмотрение.

`GroupedBy`	Вложенный список строк	Перечень полей событий, по которым группировались событий в правиле корреляции.
`ClosingReason`	Строка	Причина закрытия алерта. Возможные значения: • `False Positive (Incorrect Correlation Rule)` – алерт был ложным, а полученные события не указывают на угрозу безопасности. Возможно, требуется коррекция правила корреляции. • `False Positive (Incorrect Data)` – алерт был ложным, а полученные события не указывают на угрозу безопасности. • `Responded` – были приняты необходимые меры по устранению угрозы безопасности.
`Overflow`	Строка `TRUE/FALSE`	Признак, обозначающий что алерт переполнен, то есть размер алерта и првязанных к нему событий превышает 16 МБ. Возможные значения: • `true` • `false`
`MaxAssetsWeightStr`	Строка	Максимальный уровень важности категорий активов, связанных с алертом.
`IntegrationID`	Строка	Идентификатор алерта в программе IRP / SOAR, если в KUMA настроена интеграция с такой программой.
`ExternalReference`	Строка	Ссылка на раздел в программе IRP / SOAR, в котором отображаются сведения об импортированном из KUMA алерте.
`IncidentID`	Строка	Идентификатор инцидента, к которому привязан алерт.
`IncidentName`	Строка	Название инцидента, к которому привязан алерт.
`SegmentationRuleName`	Строка	Название правила сегментации, по которому корреляционные события сгруппированы в алерте.
`BranchID`	Строка	Идентификатор ветви иерархии, в которой был создан алерт. Указывается при иерархическом развертывании KUMA.
`BranchName`	Строка	Название ветви иерархии, в которой был создан алерт. Указывается при иерархическом развертывании KUMA.
`Actions`	Вложенная структура `[Action]`	Вложенная структура со строками, в которых указаны изменения статусов и назначений алерта, пользовательские комментарии.
`Events`	Вложенная структура `[EventWrapper]`	Вложенная структура, из которой можно обратиться к связанным с алертом корреляционным событиям (см. раздел "Модель

		данных нормализованного события" на стр. 471).
Assets	Вложенная структура [Asset (см. раздел "Модель данных актива" на стр. 491)]	Вложенная структура, из которой можно обратиться к связанным с алертом активам (см. раздел "Модель данных актива" на стр. 491).
Accounts	Вложенная структура [Account (см. раздел "Модель данных учетной записи" на стр. 499)]	Вложенная структура, из которой можно обратиться к связанным с алертом учетным записям (см. раздел "Модель данных учетной записи" на стр. 499).
AffectedAssets	Вложенная структура [Affected]	Вложенная структура, из которой можно обратиться к связанным с алертам активам (см. раздел "Модель данных актива" на стр. 491) и учетным записям (см. раздел "Модель данных учетной записи" на стр. 499), а также узнать, сколько раз они фигурируют в событиях алерта.

Вложенная структура `Affected`

Поле	Тип данных	Описание
Assets	Вложенный список [AffectedRecord]	Перечень и количество связанных с алертом активов.
Accounts	Вложенный список [AffectedRecord]	Перечень и количество связанных с алертом учетных записей.

Вложенная структура `AffectedRecord`

Поле	Тип данных	Описание
Value	Строка	Идентификатор актива или учетной записи.
Count	Число	Количество раз актив или учетная запись фигурирует в связанных с алертом событиях.

Вложенная структура `EventWrapper`

Поле	Тип данных	Описание
`Event`	Вложенная структура `[Event (см. раздел "Модель данных нормализованного события" на стр. 471)]`	Поля события.
`Comment`	Строка	Комментарий, добавленный при добавлении событий к алерту.
`LinkedAt`	Число	Дата добавления событий к алерту.

Вложенная структура `Action`

Поле	Тип данных	Описание
`CreatedAt`	Число	Дата, когда действие над алертом было произведено.
`UserID`	Строка	Идентификатор пользователя.
`Kind`	Строка	Тип действия.
`Value`	Строка	Значение.
`Event`	Вложенная структура `[Event (см. раздел "Модель данных нормализованного события" на стр. 471)]`	Поля события.
`ClusterID`	Строка	Идентификатор кластера.

Модель данных актива

Структура актива представлена полями, в которых содержатся значения. Поля также могут содержать вложенные структуры.

Поле актива	Тип значения	Описание
`ID`	Строка	Идентификатор актива.
`TenantName`	Строка	Название тенанта.
`DeletedAt`	Число	Дата удаления актива.
`CreatedAt`	Число	Дата создания актива.
`TenantID`	Строка	Идентификатор тенанта.
`DirectCategories`	Вложенный список строк	Категории актива.
`CategoryModels`	Вложенная структура `[Category]`	Изменение категорий актива.

AffectedByIncidents	Вложенный словарь: [строка:строка TRUE/FALSE]	Идентификаторы инцидентов.
IPAddress	Вложенный список строк	IP-адреса актива.
FQDN	Строка	FQDN актива.
Weight	Число	Уровень важности актива.
Deleted	Строка со значениями TRUE/FALSE	Помечен ли актив на удаление из KUMA.
UpdatedAt	Число	Дата последнего обновления актива.
MACAddress	Вложенный список строк	MAC-адреса актива.
IPAddressInt	Вложенный список чисел	IP-адрес в виде числа.
Owner	Вложенная структура [OwnerInfo]	Сведения о владельце актива.
OS	Вложенная структура [OS]	Сведения об операционной системы актива.
DisplayName	Строка	Название актива.
APISoft	Вложенная структура [Software]	ПО, установленное на активе.
APIVulns	Вложенная структура [Vulnerability]	Уязвимости актива.
KICSServerIp	Строка	IP-адрес сервера KICS for Networks.
KICSConnectorID	Число	Идентификатор коннектора KICS for Networks.
KICSDeviceID	Число	Идентификатор актива в KICS for Networks.
KICSStatus	Строка	Статус актива актива в KICS for Networks.
KICSHardware	Вложенная структура [KICSSystemInfo]	Аппаратные сведения об активе, полученные из KICS for Networks.
KICSSoft	Вложенная структура [KICSSystemInfo]	Сведения о ПО актива, полученные из KICS for Networks.
KICSRisks	Вложенная структура [KICSRisk]	Сведения об уязвимостях актива, полученные из KICS for Networks.
Sources	Вложенная структура [Sources]	Основные сведения об активе, поступавшие из разных источников.

FromKSC	Строка со значениями TRUE/FALSE	Индикатор, указывающий, что сведения об активе импортированы из KSC.
NAgentID	Строка	Идентификатор агента KSC, от которого получены сведения об активе.
KSCServerFQDN	Строка	FQDN сервера KSC.
KSCInstanceID	Строка	Идентификатор экземпляра KSC.
KSCMasterHostname	Строка	Имя хоста сервера KSC.
KSCGroupID	Число	Идентификатор группы KSC.
KSCGroupName	Строка	Название группы KSC.
LastVisible	Число	Дата, когда от KSC в последний раз были получены сведения об активе.
Products	Вложенный словарь: [строка:вложенная структура [ProductInfo]]	Сведения об установленных на активе приложениях Kaspersky, полученные из KSC.
Hardware	Вложенная структура [Hardware]	Аппаратные сведения об активе, полученные из KSC.
KSCSoft	Вложенная структура [Software]	Сведения о ПО актива, полученные из KSC.
KSCVulns	Вложенная структура [Vulnerability]	Сведения об уязвимостях актива, полученные из KSC.

Вложенная структура `Category`

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор категории.
`TenantID`	Строка	Идентификатор тенанта.
`TenantName`	Строка	Название тенанта.
`Parent`	Строка	Родительская категория.
`Path`	Вложенный список строк	Структура категорий.
`Name`	Строка	Название категории.
`UpdatedAt`	Число	Последнее обновление категории.
`CreatedAt`	Число	Дата создания категории.
`Description`	Строка	Описание категории.
`Weight`	Число	Уровень важности категории.
`CategorizationKind`	Строка	Тип присвоения категории активам.
`CategorizationAt`	Число	Дата категоризации.
`CategorizationInterval`	Строка	Интервал присвоения категорий.

Вложенная структура `OwnerInfo`

Поле	Тип значения	Описание
`DisplayName`	Строка	Имя владельца актива.

Вложенная структура `OS`

Поле	Тип значения	Описание
`Name`	Строка	Название операционной системы.
`BuildNumber`	Число	Версия операционной системы.

Вложенная структура `Software`

Поле	Тип значения	Описание
`DisplayName`	Строка	Название ПО.
`DisplayVersion`	Строка	Версия ПО.
`Publisher`	Строка	Издатель ПО.
`InstallDate`	Строка	Дата установки.
`HasMSIInstaller`	Строка `TRUE/FALSE`	Признак, имеет ли ПО MSI-установщик.

Вложенная структура `Vulnerability`

Поле	Тип значения	Описание
`KasperskyID`	Строка	Идентификатор уязвимости, присвоенный Kaspersky.
`ProductName`	Строка	Название ПО.
`DescriptionURL`	Строка	URL с описанием уязвимости.
`RecommendedMajorPatch`	Строка	Рекомендуемое обновление.
`RecommendedMinorPatch`	Строка	Рекомендуемое обновление.
`SeverityStr`	Строка	Уровень важности уязвимости.
`Severity`	Число	Уровень важности уязвимости.
`CVE`	Вложенный список строк	Идентификатор уязвимости CVE.
`ExploitExists`	Строка `TRUE/FALSE`	Существует ли эксплойт.
`MalwareExists`	Строка `TRUE/FALSE`	Существует ли вредоносная программа.

Вложенная структура `KICSSystemInfo`

Поле	Тип значения	Описание
`Model`	Строка	Модель устройства.
`Version`	Строка	Версия устройства.
`Vendor`	Строка	Производитель.

Вложенная структура `KICSRisk`

Поле	Тип значения	Описание
`ID`	Число	Идентификатор риска KICS for Networks.
`Name`	Строка	Название риска.
`Category`	Строка	Тип риска.
`Description`	Строка	Описание риска.
`DescriptionUrl`	Строка	Ссылка на описание риска.
`Severity`	Число	Уровень важности риска.
`Cvss`	Число	Оценка CVSS.

Вложенная структура `Sources`

Поле	Тип значения	Описание
`KSC`	Вложенная структура `[SourceInfo]`	Сведения об активе, поступившие из KSC.
`API`	Вложенная структура `[SourceInfo]`	Сведения об активе, поступившие через REST API.
`Manual`	Вложенная структура `[SourceInfo]`	Сведения об активе, введенные вручную.
`KICS`	Вложенная структура `[SourceInfo]`	Сведения об активе, поступившие из KICS for Networks.

Вложенная структура `Sources`

Поле	Тип значения	Описание
`MACAddress`	Вложенный список строк	MAC-адреса актива.
`IPAddressInt`	Вложенный список чисел	IP-адрес в виде числа.
`Owner`	Вложенная структура `[OwnerInfo]`	Сведения о владельце актива.
`OS`	Вложенная структура `[OS]`	Сведения об операционной системы актива.
`DisplayName`	Строка	Название актива.
`IPAddress`	Вложенный список строк	IP-адреса актива.
`FQDN`	Строка	FQDN актива.
`Weight`	Число	Уровень важности актива.
`Deleted`	Строка со значениями `TRUE/FALSE`	Помечен ли актив на удаление из KUMA.
`UpdatedAt`	Число	Дата последнего обновления актива.

Вложенная структура `ProductInfo`

Поле	Тип значения	Описание
`ProductVersion`	Строка	Версия ПО.
`ProductName`	Строка	Название ПО.

Вложенная структура `Hardware`

Поле	Тип значения	Описание
`NetCards`	Вложенная структура `[NetCard]`	Перечень сетевых карт актива.
`CPU`	Вложенная структура `[CPU]`	Перечень процессоров актива.
`RAM`	Вложенная структура `[RAM]`	Перечень ОЗУ актива.
`Disk`	Вложенная структура `[Disk]`	Перечень дисков актива.

Вложенная структура `NetCard`

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор сетевой карты.
`MACAddresses`	Вложенный список строк	MAC-адреса сетевой карты.
`Name`	Строка	Название сетевой карты.
`Manufacture`	Строка	Производитель сетевой карты.
`DriverVersion`	Строка	Версия драйвера.

Вложенная структура `RAM`

Поле	Тип значения	Описание
`Frequency`	Строка	Частота ОЗУ.
`TotalBytes`	Число	Объем ОЗУ в байтах.

Вложенная структура `CPU`

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор процессора.
`Name`	Строка	Название процессора.
`CoreCount`	Строка	Количество ядер.
`CoreSpeed`	Строка	Частота.

Вложенная структура `Disk`

Поле	Тип значения	Описание
`FreeBytes`	Число	Свободное пространство на диске.
`TotalBytes`	Число	Общее пространство на диске.

kaspersky

Модель данных учетной записи

К полям учетной записи можно обращаться из шаблонов электронной почты, а также при корреляции событий.

Поле	Тип значения	Описание
`ID`	Строка	Идентификатор учетной записи.
`ObjectGUID`	Строка	Атрибут Active Directory. Идентификатор учетной записи в Active Directory.
`TenantID`	Строка	Идентификатор тенанта.
`TenantName`	Строка	Название тенанта.
`UpdatedAt`	Число	Последнее обновление учетной записи.
`Domain`	Строка	Домен.
`CN`	Строка	Атрибут Active Directory. Имя пользователя.
`DisplayName`	Строка	Атрибут Active Directory. Отображаемое имя пользователя. По этому атрибуту события можно искать при корреляции.
`DistinguishedName`	Строка	Атрибут Active Directory. Название объекта LDAP. По этому атрибуту события можно искать при корреляции.
`EmployeeID`	Строка	Атрибут Active Directory. Идентификатор сотрудника.
`Mail`	Строка	Атрибут Active Directory. Электронная почта пользователя. По этому атрибуту события можно искать при корреляции.
`MailNickname`	Строка	Атрибут Active Directory. Альтернативный адрес электронной почты.
`Mobile`	Строка	Атрибут Active Directory. Номер мобильного телефона.
`ObjectSID`	Строка	Атрибут Active Directory. Идентификатор безопасности.
`SAMAccountName`	Строка	Атрибут Active Directory. Логин. По этому атрибуту события можно искать при корреляции.
`TelephoneNumber`	Строка	Атрибут Active Directory. Номер телефона.

UserPrincipalName	Строка	Атрибут Active Directory. Имя участника-пользователя. По этому атрибуту события можно искать при корреляции.
Archived	Строка TRUE/FALSE	Признак, определяющий, является ли учетная запись устаревшей.
MemberOf	Список строк	Атрибут Active Directory. Группы AD, в которые внесен пользователь. По этому атрибуту события можно искать при корреляции.
PreliminarilyArchived	Строка TRUE/FALSE	Признак, определяющий, требуется ли обозначить учетную запись как устаревшую.
CreatedAt	Число	Дата создания учетной записи.
SN	Строка	Атрибут Active Directory. Фамилия пользователя. По этому атрибуту события можно искать при корреляции.
SAMAccountType	Строка	Атрибут Active Directory. Тип учетной записи.
Title	Строка	Атрибут Active Directory. Должность пользователя.
Division	Строка	Атрибут Active Directory. Подразделение пользователя.
Department	Строка	Атрибут Active Directory. Отдел пользователя.
Manager	Строка	Атрибут Active Directory. Руководитель пользователя.
Location	Строка	Атрибут Active Directory. Местоположение пользователя.
Company	Строка	Атрибут Active Directory. Компания пользователя.
StreetAddress	Строка	Атрибут Active Directory. Адрес компании.
PhysicalDeliveryOfficeName	Строка	Атрибут Active Directory. Адрес для доставки.
ManagedObjects	Список строк	Атрибут Active Directory. Объекты, находящиеся под управлением пользователя.
UserAccountControl	Число	Атрибут Active Directory. Тип учетной записи AD. По этому атрибуту события можно искать при корреляции.

`WhenCreated`	Число	Атрибут Active Directory. Дата создания учетной записи.
`WhenChanged`	Число	Атрибут Active Directory. Дата изменения учетной записи.
`AccountExpires`	Число	Атрибут Active Directory. Дата истечения срока учетной записи.
`BadPasswordTime`	Число	Атрибут Active Directory. Дата последней неудачной попытки входа в систему.

kaspersky

Поля событий аудита

События аудита создаются при выполнении в KUMA определенных действий, связанных с безопасностью, и используются для обеспечения целостности системы. Этот раздел содержит информацию о полях событий аудита.

В этом разделе

Поля событий с общей информацией 503
Пользователь успешно вошел в систему или не смог войти 504
Логин пользователя успешно изменен 505
Роль пользователя успешно изменена 506
Другие данные пользователя успешно изменены 507
Пользователь успешно вышел из системы 508
Пароль пользователя успешно изменен 509
Пользователь успешно создан 510
Токен доступа пользователя успешно изменен 511
Сервис успешно создан 512
Сервис успешно удален 513
Сервис успешно перезагружен 514
Сервис успешно перезапущен 515
Сервис успешно запущен 516
Сервис успешно сопряжен 517
Статус сервиса изменен 517
Индекс хранилища удален пользователем 518
Раздел хранилища автоматически удален в связи с истечением срока действия 518
Активный лист успешно очищен или операция завершилась с ошибкой 519
Элемент активного листа успешно удален или операция завершилась с ошибкой 520
Активный лист успешно импортирован или операция завершилась с ошибкой 521
Активный лист успешно экспортирован 522
Ресурс успешно добавлен 523
Ресурс успешно удален 524
Ресурс успешно обновлен 525
Актив успешно создан 526
Актив успешно удален 527
Категория актива успешно добавлена 528
Категория актива успешно удалена 528
Параметры успешно обновлены 529

kaspersky

Поля событий с общей информацией

Каждое событие аудита имеет поля событий, описанные ниже.

Название поля события	Значение поля
ID	Уникальный идентификатор события в виде UUID.
Timestamp	Время события.
DeviceHostName	Хост источника события. Для событий аудита это имя хоста, на котором установлена служба kuma-core, потому что она является источником событий.
DeviceTimeZone	Часовой пояс системного времени сервера, на котором установлено Ядро KUMA в формате +-`чч:мм`.
Type	Тип события аудита. Событию аудита соответствует значение `4`.
TenantID	Идентификатор главного тенанта.
Priority	`Low` (значение по умолчанию).
DeviceVendor	`Kaspersky`
DeviceProduct	`KUMA`
EndTime	Время создания события.

kaspersky

Пользователь успешно вошел в систему или не смог войти

Название поля события	Значение поля
DeviceAction	`user login`
EventOutcome	`succeeded` или `failed` – статус зависит от исхода операции.
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя.
SourceUserID	Идентификатор пользователя.
Message	Описание ошибки; появляется только в том случае, если при входе в систему произошла ошибка. В противном случае поле будет пустым.

kaspersky

Логин пользователя успешно изменен

Название поля события	Значение поля
DeviceAction	`user login changed`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для изменения данных.
SourceUserID	ID пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	ID пользователя, данные которого были изменены.
DeviceCustomString1	Текущее значение логина.
DeviceCustomString1Label	`new login`
DeviceCustomString2	Значение логина до его изменения.
DeviceCustomString2Label	`old login`

kaspersky

Роль пользователя успешно изменена

Название поля события	Значение поля
DeviceAction	`user role changed`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для изменения данных.
SourceUserID	ID пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	ID пользователя, данные которого были изменены.
DeviceCustomString1	Текущее значение роли.
DeviceCustomString1Label	`new role`
DeviceCustomString2	Значение роли до ее изменения.
DeviceCustomString2Label	`old role`

Другие данные пользователя успешно изменены

Название поля события	Значение поля
DeviceAction	`user other info changed`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для изменения данных.
SourceUserID	ID пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	ID пользователя, данные которого были изменены.

kaspersky

Пользователь успешно вышел из системы

Это событие создается только тогда, когда пользователь нажимает кнопку выхода.

Это событие не создается, если пользователь покидает систему из-за окончания сеанса или если пользователь снова входит в систему из другого браузера.

Название поля события	Значение поля
DeviceAction	`user logout`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя.
SourceUserID	Идентификатор пользователя.

Пароль пользователя успешно изменен

Название поля события	Значение поля
DeviceAction	`user password changed`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для изменения данных.
SourceUserID	ID пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	ID пользователя, данные которого были изменены.

Пользователь успешно создан

Название поля события	Значение поля
DeviceAction	`user created`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для создания учетной записи.
SourceUserID	Идентификатор пользователя, который использовался для создания учетной записи.
DestinationUserName	Логин пользователя, для которого была создана учетная запись.
DestinationUserID	Идентификатор пользователя, для которого была создана учетная запись.
DeviceCustomString1	Роль созданного пользователя.
DeviceCustomString1Label	`role`

Токен доступа пользователя успешно изменен

Название поля события	Значение поля
DeviceAction	`user access token changed`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для изменения данных.
SourceUserID	ID пользователя, который использовался для изменения данных.
DestinationUserName	Логин пользователя, данные которого были изменены.
DestinationUserID	ID пользователя, данные которого были изменены.

kaspersky

Сервис успешно создан

Название поля события	Значение поля
DeviceAction	`service created`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
DeviceExternalID	ID сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.

kaspersky

Сервис успешно удален

Название поля события	Значение поля
DeviceAction	`service deleted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для удаления сервиса.
SourceUserID	Идентификатор пользователя, который использовался для удаления сервиса.
DeviceExternalID	ID сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес машины, с которой был запущен сервис. Если сервис никогда раньше не запускался, поле будет пустым.
DestinationHostName	Полное доменное имя компьютера, с которого был запущен сервис. Если сервис никогда раньше не запускался, поле будет пустым.

kaspersky

Сервис успешно перезагружен

Название поля события	Значение поля
DeviceAction	`service reloaded`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
DeviceExternalID	ID сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.

Сервис успешно перезапущен

Название поля события	Значение поля
DeviceAction	`service restarted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
DeviceExternalID	ID сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.

Сервис успешно запущен

Название поля события	Значение поля
DeviceAction	`service started`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, который сообщил информацию о запуске сервиса. Это может быть адрес прокси-сервера, если информация передается через прокси.
SourcePort	Порт, передавший информацию о запуске сервиса. Это может быть порт прокси-сервера, если информация передается через прокси.
DeviceExternalID	ID сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес машины, на которой был запущен сервис.
DestinationHostName	Полное доменное имя машины, на которой был запущен сервис.

Сервис успешно сопряжен

Название поля события	Значение поля
DeviceAction	`service paired`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого был отправлен запрос на сопряжение сервисов. Это может быть адрес прокси-сервера, если запрос передается через прокси.
SourcePort	Порт, отправивший запрос на сопряжение сервисов. Это может быть порт прокси-сервера, если запрос передается через прокси.
DeviceExternalID	ID сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.

Статус сервиса изменен

Название поля события	Значение поля
DeviceAction	`service status changed`
DeviceExternalID	ID сервиса.
DeviceProcessName	Название сервиса.
DeviceFacility	Тип сервиса.
DestinationAddress	Адрес машины, на которой был запущен сервис.
DestinationHostName	Полное доменное имя машины, на которой был запущен сервис.
DeviceCustomString1	`green`, `yellow` или `red`
DeviceCustomString1Label	`new status`
DeviceCustomString2	`green`, `yellow` или `red`
DeviceCustomString2Label	`old status`

kaspersky

Индекс хранилища удален пользователем

Название поля события	Значение поля
DeviceAction	`partition deleted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для создания сервиса.
SourceUserID	Идентификатор пользователя, который использовался для создания сервиса.
Name	Имя индекса.
Message	`deleted by user`

Раздел хранилища автоматически удален в связи с истечением срока действия

Название поля события	Значение поля
DeviceAction	`partition deleted`
EventOutcome	`succeeded`
Name	Имя индекса
SourceServiceName	`scheduler`
Message	`deleted by retention period settings`

kaspersky

Активный лист успешно очищен или операция завершилась с ошибкой

Это событие может поступить со статусами `succeeded` или `failed`.

Поскольку запрос на очистку активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть как до удаления, так и после удаления.

Это означает, что активные лист может быть очищен успешно, но событие все равно будет иметь статус `failed`. Фактически, EventOutcome возвращает статус TCP/IP-соединения запроса, а статус проверки того, был ли очищен активные лист.

Название поля события	Значение поля
DeviceAction	`active list cleared`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для очистки активного листа.
SourceUserID	Идентификатор пользователя, который использовался для очистки активного листа.
DeviceExternalID	Идентификатор сервиса, активные лист которого был очищен.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.

kaspersky

Элемент активного листа успешно удален или операция завершилась с ошибкой

Это событие может поступить со статусами `succeeded` или `failed`.

Поскольку запрос на удаление элемента активного листа осуществляется через удаленное соединение, ошибка передачи данных может возникнуть как до удаления, так и после удаления.

Это означает, что элемент активного листа может быть удален успешно, но событие все равно будет иметь статус `failed`. Фактически, EventOutcome возвращает статус TCP/IP-соединения запроса, а статус проверки того, был ли удален элемент активного листа.

Название поля события	Значение поля
DeviceAction	`active list item deleted`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для удаления элемента активного листа.
SourceUserID	Идентификатор пользователя, который использовался для удаления элемента активного листа.
DeviceExternalID	Идентификатор сервиса, активные лист которого был очищен.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
DeviceCustomString1	Название ключа.
DeviceCustomString1Label	`key`
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.

kaspersky

Активный лист успешно импортирован или операция завершилась с ошибкой

Частично импортировано через удаленное подключение.

Во время операции может произойти ошибка, что означает, что EventOutcome = `failed` также может означать ошибку подключения, при которой данные могут быть частично или полностью импортированы.

Однако в большинстве случаев ошибка означает, что данные не были импортированы или были импортированы лишь частично.

Название поля события	Значение поля
DeviceAction	`active list imported`
EventOutcome	`succeeded` или `failed`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для выполнения импорта.
SourceUserID	Идентификатор пользователя, который использовался для импорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен импорт.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.
Message	Если EventOutcome = `failed`, в этом поле будет отображаться сообщение об ошибке.

kaspersky

Активный лист успешно экспортирован

Название поля события	Значение поля
DeviceAction	`active list exported`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для выполнения экспорта.
SourceUserID	Идентификатор пользователя, который использовался для экспорта.
DeviceExternalID	Идентификатор сервиса, для которого был выполнен экспорт.
ExternalID	Идентификатор активного листа.
Name	Название активного листа.

kaspersky

Ресурс успешно добавлен

Название поля события	Значение поля
DeviceAction	`resource added`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для добавления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для добавления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName	Название ресурса.
DeviceFacility	Тип ресурса: • `activeList` • `agent` • `aggregationRule` • `collector` • `connection` • `connector` • `correlationRule` • `correlator` • `destination` • `dictionary` • `enrichmentRule` • `filter` • `normalizer` • `proxy` • `responseRule` • `storage`

kaspersky

Ресурс успешно удален

Название поля события	Значение поля
DeviceAction	`resource deleted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для удаления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для удаления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName	Название ресурса.
DeviceFacility	Тип ресурса: • `activeList` • `agent` • `aggregationRule` • `collector` • `connection` • `connector` • `correlationRule` • `correlator` • `destination` • `dictionary` • `enrichmentRule` • `filter` • `normalizer` • `proxy` • `responseRule` • `storage`

kaspersky

Ресурс успешно обновлен

Название поля события	Значение поля
DeviceAction	`resource updated`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для обновления ресурса.
SourceUserID	Идентификатор пользователя, который использовался для обновления ресурса.
DeviceExternalID	Идентификатор ресурса.
DeviceProcessName	Название ресурса.
DeviceFacility	Тип ресурса: • `activeList` • `agent` • `aggregationRule` • `collector` • `connection` • `connector` • `correlationRule` • `correlator` • `destination` • `dictionary` • `enrichmentRule` • `filter` • `normalizer` • `proxy` • `responseRule` • `storage`

kaspersky

Актив успешно создан

Название поля события	Значение поля
DeviceAction	`asset created`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для добавления актива.
SourceUserID	Идентификатор пользователя, который использовался для добавления актива.
DeviceExternalID	Идентификатор актива.
SourceHostName	Идентификатор актива.
Name	Название актива.
DeviceCustomString1	Разделенные запятыми IP-адреса актива.
DeviceCustomString1Label	`addresses`

kaspersky

Актив успешно удален

Название поля события	Значение поля
DeviceAction	`asset deleted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для добавления актива.
SourceUserID	Идентификатор пользователя, который использовался для добавления актива.
DeviceExternalID	Идентификатор актива.
SourceHostName	Идентификатор актива.
Name	Название актива.
DeviceCustomString1	Разделенные запятыми IP-адреса актива.
DeviceCustomString1Label	`addresses`

kaspersky

Категория актива успешно добавлена

Название поля события	Значение поля
DeviceAction	`category created`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для добавления категории.
SourceUserID	Идентификатор пользователя, который использовался для добавления категории.
DeviceExternalID	Идентификатор категории.
Name	Название категории.

Категория актива успешно удалена

Название поля события	Значение поля
DeviceAction	`category deleted`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для удаления категории.
SourceUserID	Идентификатор пользователя, который использовался для удаления категории.
DeviceExternalID	Идентификатор категории.
Name	Название категории.

kaspersky

Параметры успешно обновлены

Название поля события	Значение поля
DeviceAction	`settings updated`
EventOutcome	`succeeded`
SourceTranslatedAddress	Это поле содержит значение HTTP-заголовка x-real-ip или x-forwarded-for. Если эти заголовки отсутствуют, поле будет пустым.
SourceAddress	Адрес, с которого пользователь вошел в систему. Если пользователь вошел в систему с помощью прокси, будет указан прокси-адрес.
SourcePort	Порт, с которого пользователь вошел в систему. Если пользователь вошел в систему через прокси, будет указан порт на стороне прокси.
SourceUserName	Логин пользователя, который использовался для обновления параметров.
SourceUserID	Идентификатор пользователя, который использовался для обновления параметров.
DeviceFacility	Тип параметров.

kaspersky

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 9. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
виртуальная инфраструктура VMware	среда функционирования
файл виртуальной машины	объект воздействия
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

kaspersky

Приложение. Значения параметров программы в сертифицированной конфигурации

Этот раздел содержит перечень параметров программы, влияющих на безопасное состояние программы, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение каких-либо из перечисленных параметров с их значений (диапазона значений) в сертифицированном конфигурации на другие значения, выводит программу из безопасного состояния.

Таблица 10. Параметры и их безопасные значения для программы в сертифицированной конфигурации

Сущность, к которой относится параметр	Название параметра	Безопасное значение или диапазон значений параметра (сертифицированная конфигурация)
Общие	Параметры подключения к SMTP-серверу	Должна быть осуществлена настройка подключения к SMTP-серверу (по умолчанию настройки отсутствуют).
Общие - Параметры подключения к SMTP-серверу	Чекбокс **Выключено**	Чекбокс **Выключено** должен быть отключен (по умолчанию отключен).
Подключение к LDAP – Setting/**LDAP-сервер**	Тип	ssl или startTLS
Подключение к Active directory – Setting/**Доменная авторизация**	Режим TLS	ssl или startTLS
Взаимодействия источников логов с коллекторами – **Коннекторы** (для получения событий) при использовании следующих типов: Internal, tcp, nats, kafka, http	Дополнительные параметры/Режим TLS	Должно быть указано одно из следующих значений: **Включено**, **С верификацией**, **Нестандартный CA.**