

Отчеты

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в онлайн-справке на продукт: <https://support.kaspersky.ru/kuma/4.0/217966>

Видео «Типовые операции с панелями мониторинга и отчетами»:
<https://rutube.ru/video/304bc4fd81bae7219ade8c3a3d717213/>

В KUMA можно настроить регулярное формирование отчетов по собранным/обработанным данным, статистике по алертам или инцидентам и другим аналитическим данным.

Отчеты формируются с помощью шаблонов отчетов, которые хранятся на вкладке **Шаблоны** раздела **Отчеты**. Пользователи с ролью Главного администратора, Администратора тенанта, Аналитика второго уровня и Аналитика первого уровня могут создавать, редактировать и удалять шаблоны отчетов. Отчеты, созданные с использованием шаблонов отчетов, отображаются на вкладке Сформированные отчеты. Вы можете создавать шаблоны самостоятельно или воспользоваться преднастроенными шаблонами.



Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты 1

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Отчеты

Шаблоны

Сформированные отчеты

Новый шаблон

Название	Расписание	Создал	Последнее обновление ↓	Последний отчет	Отправить по электронной поч...	Тенант
Alerts Overview	выключено		21.12.2020 23:08	18.07.2024 14:24		Main
Incidents Overview	выключено		21.12.2020 23:08			Main
Network Overview	выключено		17.12.2020 11:00			Main

Шаблон отчета идентичен макету **Панели мониторинга**, так как также состоит из набора виджетов, которые визуализируют аналитические данные.

Чтобы создать шаблон отчета:

- Перейдите в раздел **Отчеты** → **Шаблоны**.
- Нажмите на кнопку **Новый шаблон**.
- Откроется окно **Новый шаблон отчета**.
- В раскрывающемся списке **Тенанты** выберите тенанты (в нашем примере Main), которым будет принадлежать создаваемый шаблон.
- В раскрывающемся списке **Период** выберите период времени, по которому требуется аналитика. В нашем примере будет использоваться период **Сегодня**.
- В поле **Срок хранения** укажите на протяжении какого времени следует хранить сформированные по этому шаблону отчеты. В нашем примере **Сохранять в течение 1 месяца**.
- В поле **Название шаблона** укажите название шаблона.

Первым создадим виджет со статистикой по количеству нормализованных событий от каждого типа источника.

Чтобы добавить виджет:

- В раскрывающемся списке **Добавить виджет** выберите виджет **События**. Данный тип виджета будет строиться на основе событий из хранилища.

Касперский
Unified Monitoring and
Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты 1

Ресурсы

Диспетчер задач

Отчеты >
Новый шаблон отчета

Добавить виджет 6

Тенанты* Main 2

Период: Сегодня 3

Срок хранения: Сохранять в течение 1 мес. 4

Название шаблона* Статистика KUMA 5

☐ Отображать данные по КИИ 1

+ Загрузить логотип

Изображение должно быть в одном из следующих форматов: jpg, png или gif. Максимальный размер изображения: 3 МБ.

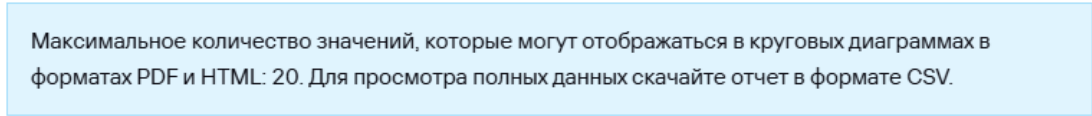
Статистика KUMA

Создайте макет с помощью виджетов

- В появившемся окне справа укажите:
 - Во вкладке :
 - **График** – Круговая диаграмма
 - **Тенант** – Main
 - **Период** – Как на макете
 - **Хранилище** – выберите сервис хранилища. В нашем примере **[ООТВ] Storage**.
 - В поле SQL-запроса (т.е. данные на основании, которых будет строиться виджет) укажите следующий поисковый запрос:

```
SELECT count(ID) AS `metric`, DeviceProduct AS `value` FROM `events` WHERE DeviceProduct != ''  
GROUP BY DeviceProduct ORDER BY metric DESC LIMIT 10
```

-



```
SELECT count(ID) AS `metric`, DeviceProduct AS `value` FROM `events` WHERE  
DeviceProduct != '' GROUP BY DeviceProduct ORDER BY metric DESC LIMIT 10
```

7

Предварительный просмотр

Добавить

Отмена

-

- Виджет будет добавлен в шаблон. Виджеты можно перетаскивать по окну и изменять их размер с помощью кнопки  , которая появляется при наведении указателя мыши на виджет.

Отчеты >

Добавить виджет

Тенанты*

Main

Период:

Сегодня

Срок хранения:

Сохранять в течение 1 мес.

Название шаблона*

Статистика KUMA

☐ Отображать данные по КИИ

+ Загрузить логотип

Изображение должно быть в одном из следующих форматов: jpg, png или gif. Максимальный размер изображения: 3 МБ.

Статистика KUMA

Количество нормализованных событий от каждого типа источника

331 806

Всего

331 806 (100%)

Windows

303 480 (91.46%)

auditd

25 387 (7.65%)

KSC

2 892 (0.87%)

KUMA

47 (0.01%)

1

2

Сохранить

Отмена

- Нажмите **Сохранить** для сохранения шаблона.

Вторым создадим виджет со статистикой по количеству и типу действий пользователей в KUMA.

Чтобы добавить новый виджет в шаблон отчета:

- Во вкладке **Шаблоны** нажмите на название шаблона **Статистика KUMA** и в раскрывающемся списке выберите **Изменить шаблон отчета**.

Касперский
Unified Monitoring and
Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты 1

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Отчеты

Шаблоны

Сформированные отчеты

Название	Расписание	Создал	Последнее обновление ↓	Последний отчет	Отправить по электронной поч...	Тенант
Статистика KUMA	выключено	Administrator	06.03.2025 20:38			Main
Создать отчет	выключено		21.12.2020 23:08	18.07.2024 14:24		Main
Изменить расписание						
Изменить шаблон отчета	выключено		21.12.2020 23:08			Main
Дублировать шаблон отчета	выключено		17.12.2020 11:00			Main
Удалить шаблон отчета						

- В появившемся окне **Изменить шаблон отчета** нажмите **Добавить виджет** и выберите виджет **События**.
- В появившемся окне справа укажите:
 - Во вкладке :
 - **График** – Столбчатая диаграмма
 - **Тенант** – Main
 - **Период** – Как на макете
 - **Хранилище** – выберите сервис Хранилища. В нашем примере **[ООТВ] Storage**.
 - Возле поля SQL-запроса нажмите на кнопку  для формирования SQL-запроса с помощью конструктора.
 - В появившемся окне **Формирование SQL-запроса** заполните поля как на скриншоте ниже и нажмите **Применить**.

Формирование SQL-запроса



Поля событий, указанные в блоках SELECT и WHERE, будут добавлены в таблицу событий в качестве столбцов. Поля событий из блока WHERE помещаются в таблицу, только если для них выбран оператор, отличный от "=".

SELECT

[-]

ID

▼

metric

count

▼

[-]

DeviceAction

▼

value

1

FROM

events ▼

WHERE

AND

Добавить условие

Добавить группу

⋮

Type

▼

=

▼

Audit

▼

×

2

GROUP BY

DeviceAction ▼

3

ORDER BY

[-]

metric

▼

↓ DESC

▼

LIMIT

50

4

При нажатии на кнопку Применить текущий SQL-запрос будет перезаписан.



5

Применить

Запрос по умолчанию

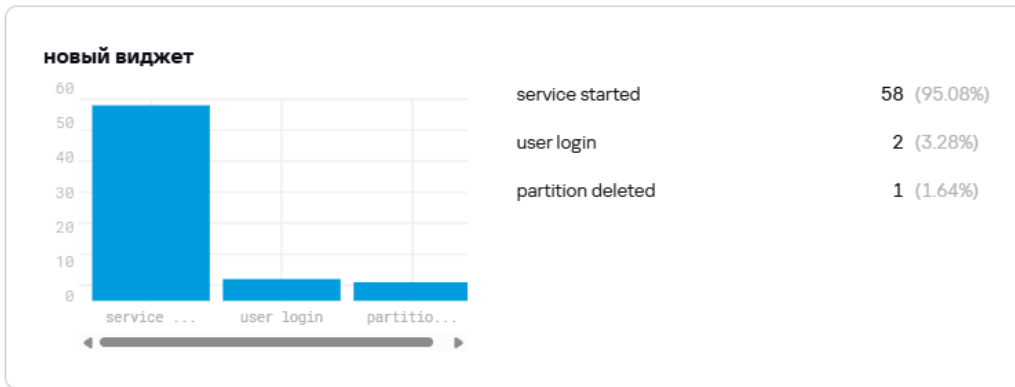
- Сформированный запрос из конструктора появится в поле SQL-запроса.



```
SELECT count(ID) AS `metric`, DeviceAction AS `value` FROM `events` WHERE Type = 4  
GROUP BY DeviceAction ORDER BY metric DESC LIMIT 50
```

•

Нажмите **Предварительный просмотр**, чтобы убедиться, что SQL-запрос корректен и выполняется успешное построение виджета.



График

Столбчатая диаграмма

1



Тенант

Main

2



Период

Как на макете

3

Показывать данные за предыдущий период



Хранилище*

Хранилище: [OOTB] Storage

4

Максимальное количество значений, которые могут отображаться в столбчатых и календарных диаграммах в форматах PDF и HTML: 40. Для просмотра полных данных скачайте отчет в формате CSV.



```
SELECT count(ID) AS `metric`, DeviceAction AS `value` FROM `events` WHERE Type = 4
GROUP BY DeviceAction ORDER BY metric DESC LIMIT 50
```

5

Предварительный просмотр

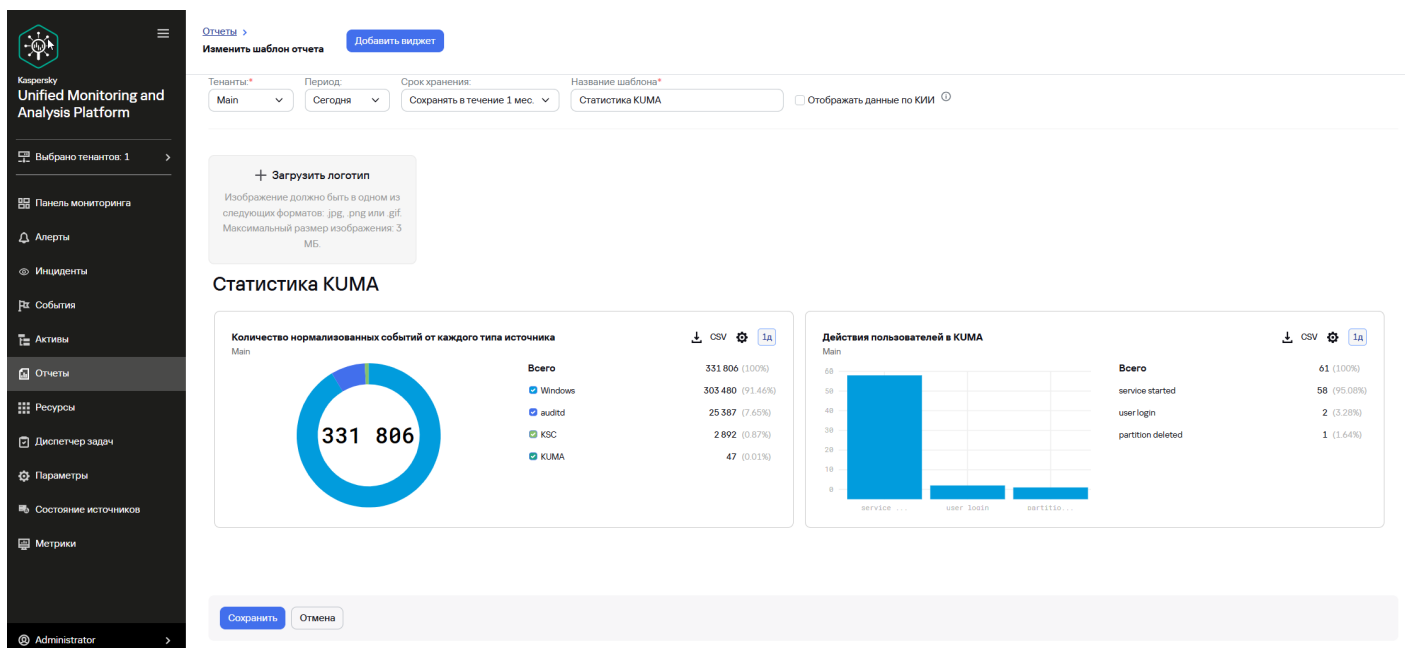
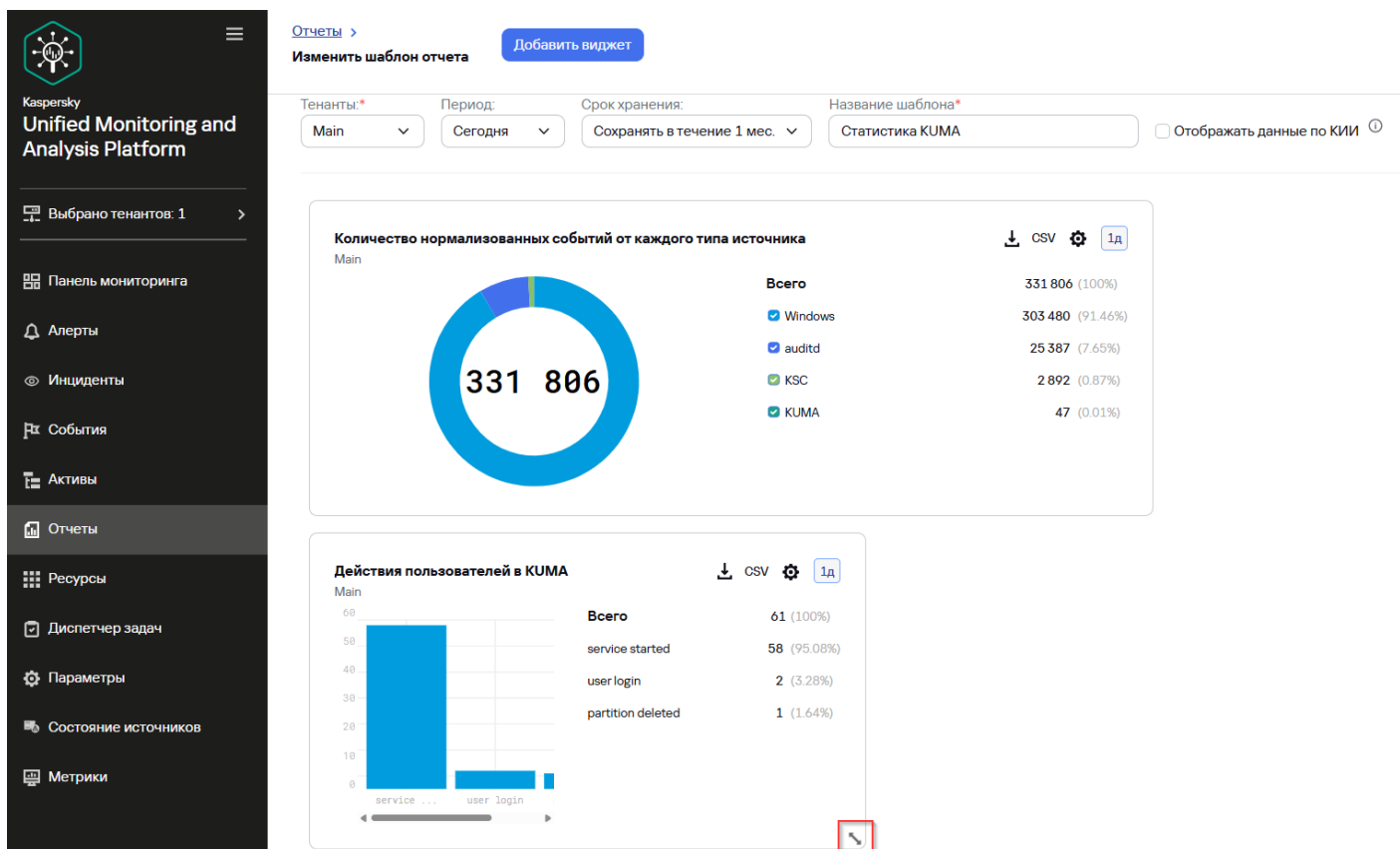
6

Добавить

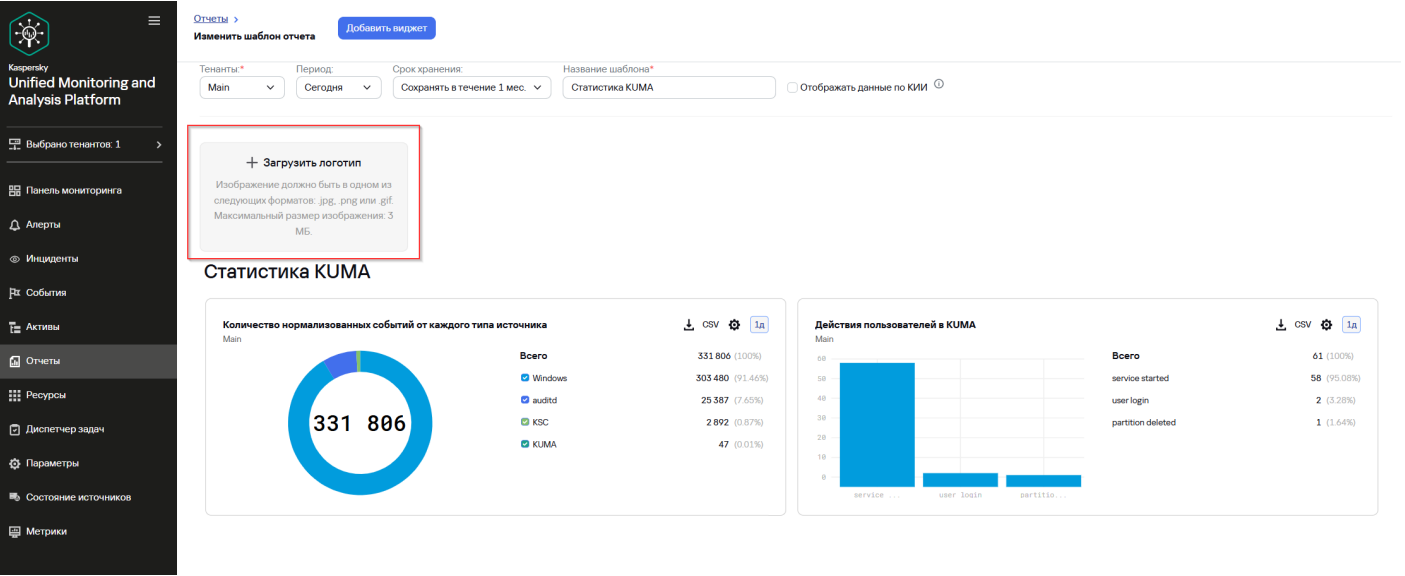
Отмена

Во вкладке :

- Укажите **Название виджета**. В нашем примере **Действия пользователей в KUMA**.
- Активируйте параметр **Итоговые значения**.
- Нажмите **Добавить**.
- Виджет будет добавлен в шаблон отчета. Виджеты можно перетаскивать по окну и изменять их размер с помощью кнопки , которая появляется при наведении указателя мыши на виджет.



- При необходимости можно поменять логотип шаблона отчетов с помощью кнопки **Загрузить логотип**. Если нажать на кнопку **Загрузить 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.



- Нажмите **Сохранить** для сохранения шаблона отчета.

Новый шаблон отчета создан и доступен во вкладке **Шаблоны** в разделе **Отчеты** веб-интерфейса KUMA. Вы можете сформировать этот отчет вручную. Если вы хотите, чтобы отчеты создавались автоматически, требуется настроить расписание.

Чтобы создать отчет вручную (на примере ранее созданного шаблона отчета **Статистика KUMA**):

- Перейдите раздел **Отчеты** → **Шаблоны**.
- В таблице шаблонов отчета нажмите имя шаблона отчета **Статистика KUMA** и в раскрывающемся списке выберите **Создать отчет**.

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты 1

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Отчеты

Шаблоны

Сформированные отчеты

Название	Расписание	Создал	Последнее обновление ↓	Последний отчет	Отправить по электронной поч...	Тенант
Статистика KUMA 2	выключено	Administrator	07.03.2025 11:53			Main
Создать отчет 3	выключено		21.12.2020 23:08	18.07.2024 14:24		Main
Изменить расписание						
Изменить шаблон отчета	выключено		21.12.2020 23:08			Main
Дублировать шаблон отчета						
Удалить шаблон отчета	выключено		17.12.2020 11:00			Main

Созданный отчет будет доступен на вкладке **Отчеты** → **Сформированные отчеты**.

Чтобы просмотреть отчет:

- На вкладке **Сформированные отчеты** нажмите на название сформированного отчета и выберите **Открыть отчет**.



Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Отчеты

Шаблоны

Сформированные отчеты

Название	Период	Последний отчет ↓	Тенант	Пользователь
Статистика KUMA	07.03.2025 00:00 - 07.03.2025 12:52	07.03.2025 12:52	Main	Administrator

Открыть отчет

Сохранить как

Создать отчет

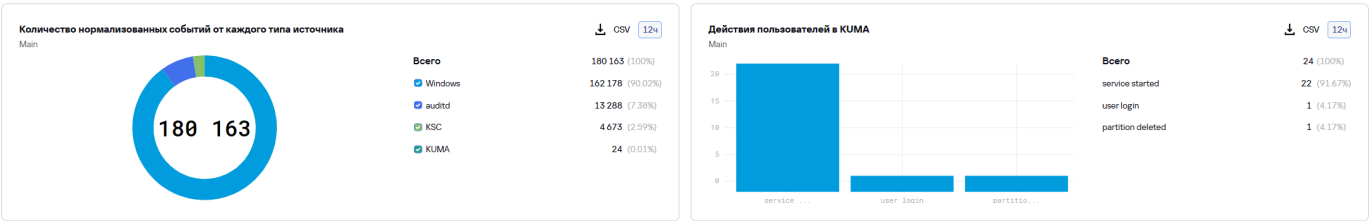
Изменить шаблон отчета

Удалить отчет

- Откроется новая вкладка браузера с виджетами сформированного отчета.

Сохранить как

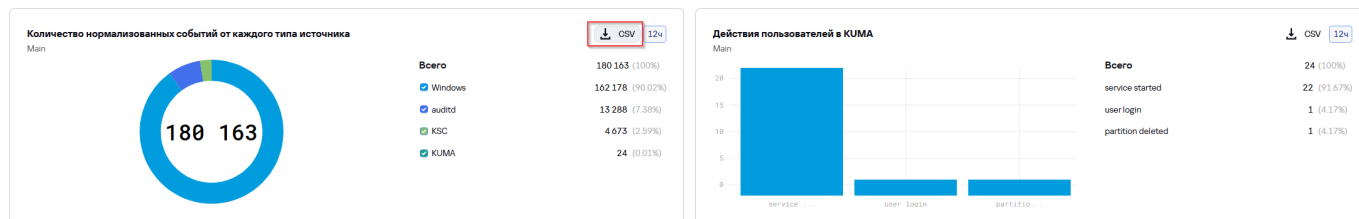
Статистика KUMA



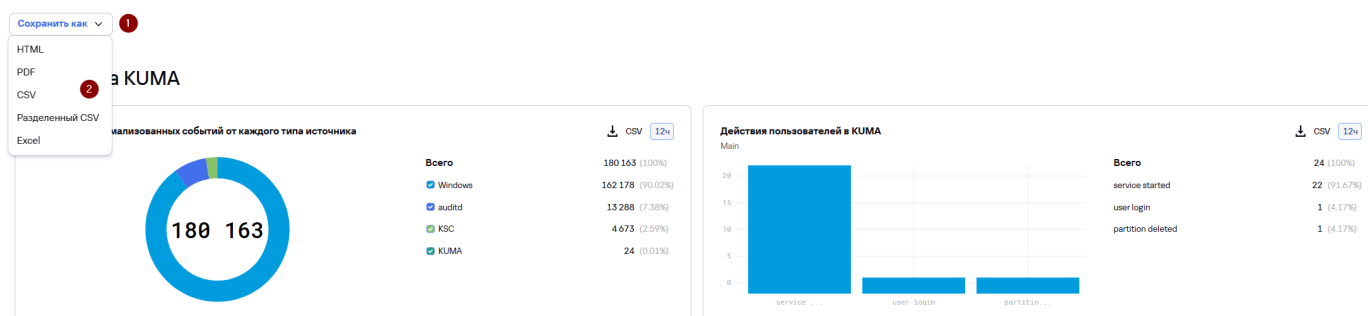
- С помощью кнопки CSV данные, отображаемые на каждом виджете, можно скачать в формате CSV в кодировке UTF-8. Название скачиваемого файла имеет формат <название виджета>_<дата скачивания (ГГГГММДД)>_<время скачивания (ЧЧММСС)>.CSV.

Сохранить как ▾

Статистика KUMA



- Отчет можно сохранить в выбранном формате с помощью кнопки **Сохранить как**, выбрав нужный формат: HTML, PDF, CSV, разделенный CSV, Excel. Отчет сохраняется в папку загрузки, настроенную в вашем браузере.



Если необходимо формировать отчет автоматически по расписанию (на примере ранее созданного шаблона отчета Статистика KUMA):

- Перейдите в раздел **Отчеты → Шаблоны**.
- В таблице шаблонов отчета нажмите на имя шаблона отчета **Статистика KUMA** и в раскрывающемся списке выберите **Изменить расписание**.



Касперский
Unified Monitoring and
Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты 1

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Отчеты

Шаблоны 2

Сформированные отчеты

Название	Расписание	Создал	Последнее обновление ↓	Последний отчет	Отправить по электронной поч...	Тенант
Статистика KUMA	выключено	Administrator	07.03.2025 11:53	07.03.2025 12:52		Main
Создать отчет	выключено		21.12.2020 23:08	18.07.2024 14:24		Main
Изменить расписание 3	выключено		21.12.2020 23:08			Main
Изменить шаблон отчета	выключено		21.12.2020 23:08			Main
Дублировать шаблон отчета	выключено		17.12.2020 11:00			Main
Удалить шаблон отчета						

- Откроется окно **Параметры отчета**.
- Если вы хотите, чтобы отчет формировался, например, каждый понедельник в 10 утра:
 - Включите переключатель **Расписание**.
 - В группе настроек **Повторять каждый** укажите:
 - **1 Неделя**
 - **День** – ПН
 - В поле **Время** укажите время, когда должен быть сформирован отчет. В нашем примере 10:00 часов.
 - В поле **Часовой пояс** укажите часовой пояс. В нашем примере UTC +03:00 (для Москвы).
- Чтобы выбрать формат отчета и указать адресатов для рассылки, настройте следующие параметры:
 - В группе настроек **Отправить** нажмите **Добавить**.

Параметры отчета

Шаблон "Статистика KUMA"

Расписание ☒ Включено 1

Повторять каждый 1 Неделя 2

День пн вт ср чт пт сб вс 3

Время 10:00 4

Часовой пояс Europe/Moscow (UTC+03:00) 5

Отправить

6

Добавить

Удалить

☐ Адрес электронной почты

Формат

- В открывшемся окне **Добавление адресов электронной почты** в разделе **Группы пользователей** нажмите **Добавить группу**.
- В появившемся поле укажите адрес электронной почты, выберите формат отчета (доступные форматы: PDF, HTML, CSV, разделенный CSV, Excel) и нажмите **Enter** или щелкните вне поля ввода - адрес электронной почты будет добавлен. Можно добавить несколько адресов. Отчеты будут отправлены по указанным адресам каждый раз, когда вы сформируете отчет вручную или KUMA сформирует отчет автоматически по расписанию.

Добавление адресов электронной почты

Группы пользователей

+ Добавить группу

Введите адрес электронной почты 1

PDF 2

×

Нажмите Enter или щелкните вне поля ввода для добавления адреса.

admin@truecompany.local ×

 3

Чтобы сформированные отчеты можно было отправлять по электронной почте необходимо настроить интеграцию с почтовым сервером (см. Раздел Уведомления об алертах).

- Если адресаты, которым отчет пришел на почту, являются пользователями KUMA, они смогут скачать отчет или просмотреть отчет по ссылкам из письма. Если адресаты не являются пользователями KUMA, переход по ссылкам будет доступен, но авторизоваться в KUMA адресаты не смогут, поэтому им будут доступны только вложения.

Вы можете отправить письмо без вложений, тогда адресатам будут доступны отчеты только по ссылкам и только с авторизацией в KUMA, без ограничений по ролям или тенантам.

- Нажмите **Сохранить**.
- Нажмите **Сохранить**.

Параметры отчета

Шаблон "Статистика KUMA"

Расписание ☒ Включено

Повторять каждый Неделя ▼

День пн вт ср чт пт сб вс

Время 🕒

Часовой пояс Europe/Moscow (UTC+03:00) ▼

Отправить

Добавить

Удалить

☐ Адрес электронной почты

Формат

☐ admin@truecompany.local

PDF

1

Сохранить

Отмена

Автоматическое формирование отчета и отправка по расписанию настроены.

Kaspersky

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты1

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

Отчеты

Шаблоны

Сформированные отчеты

Название	Расписание	Создал	Последнее обновление ↓	Последний отчет	Отправить по электронной поч...	Тенант
Статистика KUMA	периодичность: 1 нед.	Administrator	07.03.2025 13:56		✓	Main
Alerts Overview	выключено		21.12.2020 23:08	18.07.2024 14:24		Main
Incidents Overview	выключено		21.12.2020 23:08			Main
Network Overview	выключено		17.12.2020 11:00			Main

Входящие

Получить Создать Метка Быстрый фильтр

Поиск <Ctrl+K>

Непрочитанные Звёздочка Контакт Метки Вложения

Фильтровать эти сообщения <Ctrl+Shift+K>

Тема	Отправители	Дата
KUMA: report "Статистика KUMA" is ready	kuma-aio@truecompany.local	10:00

От kuma-aio@truecompany.local

Кому Мне

Тема KUMA: report "Статистика KUMA" is ready

10:00

Ответить Переслать Архивировать Спам Удалить Больше

Hello,

KUMA has just finished generating report "Статистика KUMA" with data for 11.03.2025 00:00 - 11.03.2025 10:00.

You can [preview](#) or [download](#) report.

Kaspersky Unified Monitoring and Analysis Platform automatic notification

Здравствуйте!

В KUMA был создан отчет "Статистика KUMA" с данными за следующий период: 11.03.2025 00:00 - 11.03.2025 10:00.

Отчет можно [просмотреть](#) или [загрузить](#).

Автоматическое уведомление Kaspersky Unified Monitoring and Analysis Platform

1 вложение: Статистика KUMA.pdf 65,1 КБ

Статистика KUMA.pdf 65,1 КБ

Сохранить