Работа с алертами

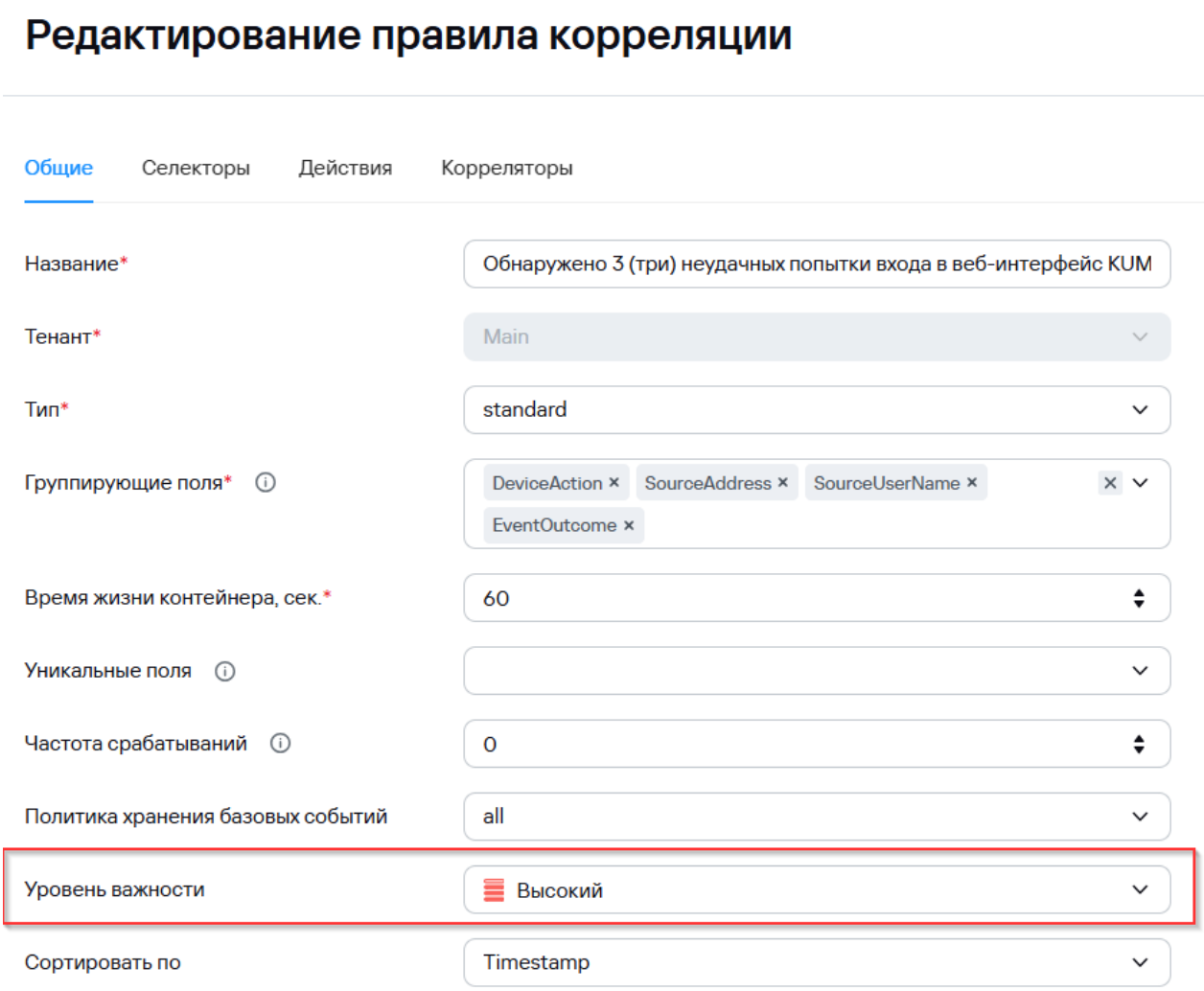
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

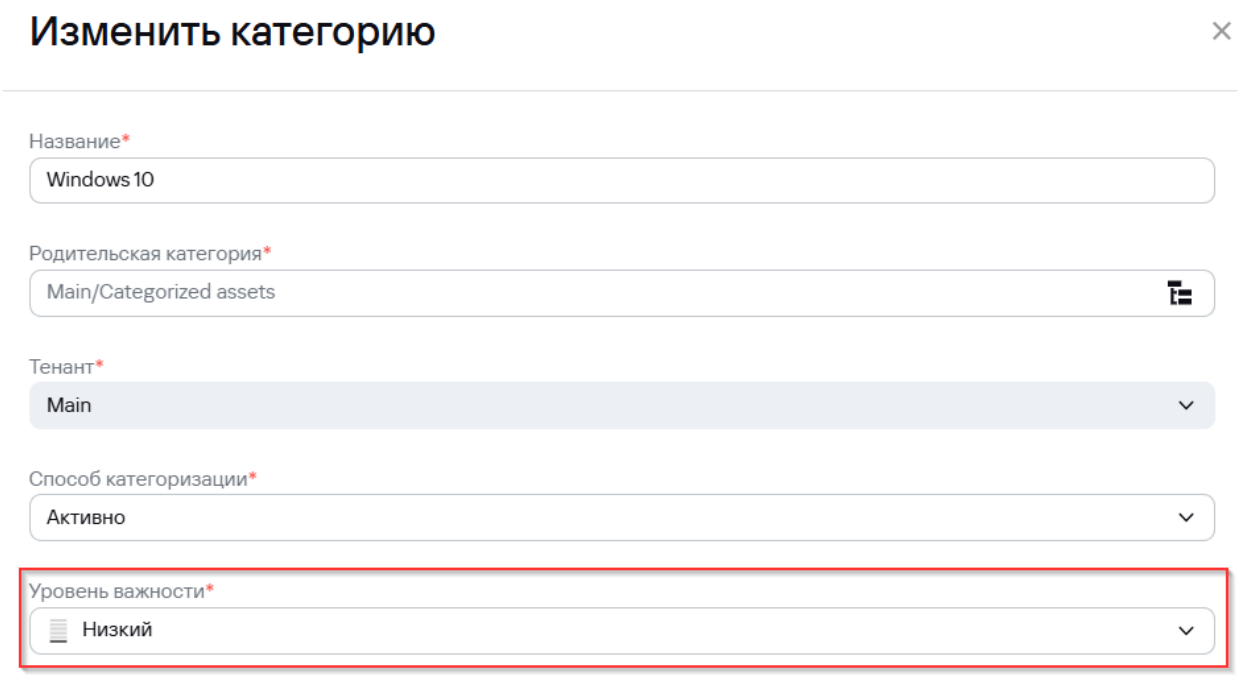
> Официальная документация по данному разделу приведена в онлайн-справке на продукт: https://support.kaspersky.ru/kuma/4.0/218046

Алерт - это уведомление (оповещение), создаваемое в KUMA, при получении события или последовательности событий, которое приводит к срабатыванию правила корреляции.

KUMA автоматически присваивает уровень важности каждому алерту. Уровень важности отражает насколько критичны для безопасности действия/выполненные команды/запущенные процессы и файлы, обнаруженные в событии. Уровень важности зависит от уровня важности сработавшего правила корреляции и категории актива, который вовлечен в алерт.
Возможные значения уровня важности:

- Низкий
- Средний
- Высокий
- Критический





В первую очередь следует обрабатывать алерты с более высоким уровнем важности. Значение уровня важности автоматически обновляется при получении новых корреляционных событий в результате срабатывания правил корреляции, но аналитик

также может задать уровень важности вручную. В этом случае уровень важности алерта больше не обновляется автоматически.
В разделе **Алерты** веб-интерфейса KUMA можно просматривать и обрабатывать алерты, зарегистрированные KUMA.

Жизненный цикл алертов

- KUMA создает алерт при срабатывании правила корреляции. Алерт именуется по породившему его правилу корреляции. Алерту присваивается статус **Новый**.
- Алерты в статусе **Новый** продолжают наполняться данными при последующих срабатываниях того же правила корреляции (если не используются правила сегментации). При изменении статуса алерта на любой другой, алерт больше не обновляется и, если правило корреляции срабатывает снова, создается новый алерт.

> С помощью правил сегментации поток однотипных корреляционных событий можно разделять, создавая более одного алерта.

- Алерт назначается пользователю (аналитику) для дальнейшего расследования. Статус алерта меняется на **Назначен**.
- Аналитик 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**).
  - Создает на основе алерта инцидент (статус алерта меняется на **В инциденте**).

Наполнение алертов событиями

По умолчанию количество привязанных событий к алерту не может превышать 10 000. Когда количество событий привязанных к алерту достигает 10 000, создается новый алерт с таким же названием, но новым идентификатором. Идентификатор алерта можно просмотреть в деталях алерта. При необходимости вы можете изменить это значение в свойствах правила сегментации в поле **Количество корреляционных событий**. Правило сегментации при этом должно быть включено и привязано к правилам корреляции алертов тенанта.

Поиск алертов

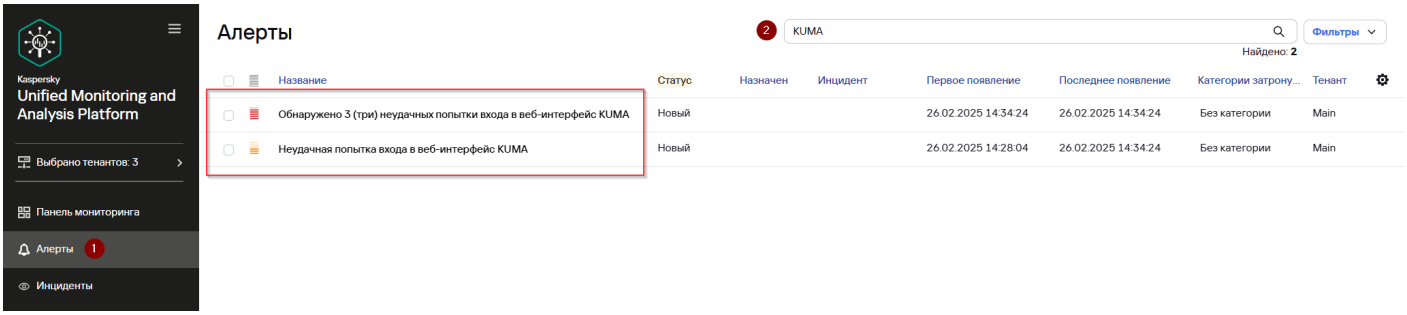
Чтобы выполнить поиск алертов:

- Перейдите в **Алерты**
- Введи в поле **Поиск** искомое имя алерта, например, «KUMA»

>

> Пример алерта с именем«KUMA» будет доступен при создании правила типа Simple или Standard.

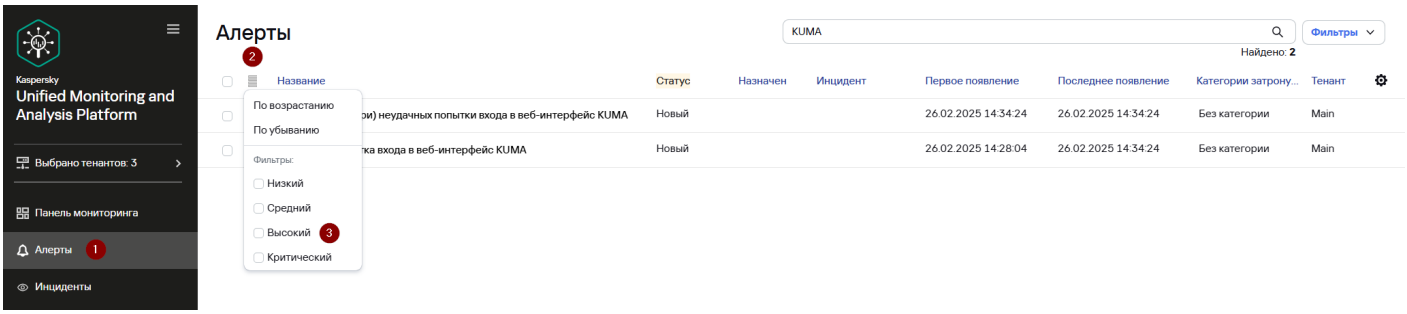
- Убедитесь, что в таблице отображаются только алерты в названии, которых содержится слово "KUMA"

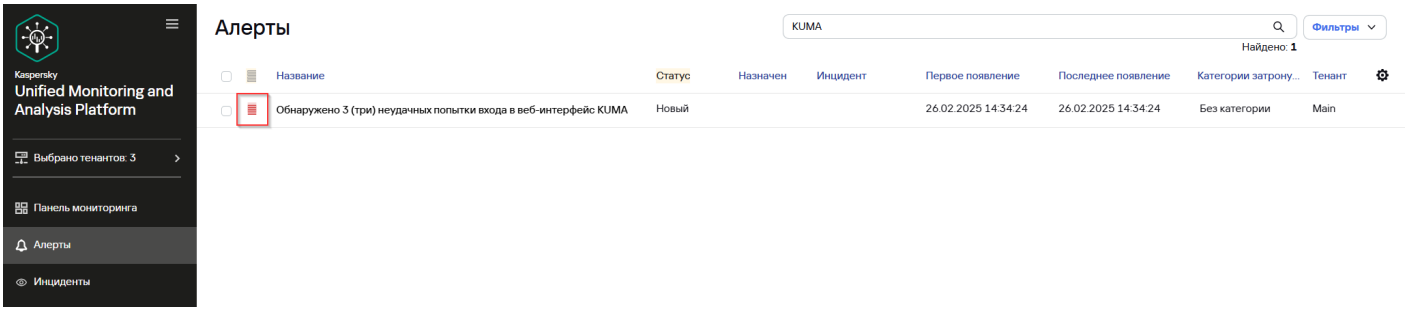


Параметры, по которым производится поиск:

- 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 нажатии на заголовки столбцов вы можете просмотреть значения для фильтрации алертов. При фильтрации алертов по какому-либо параметру соответствующий заголовок таблицы алертов подсвечивается желтым цветом.

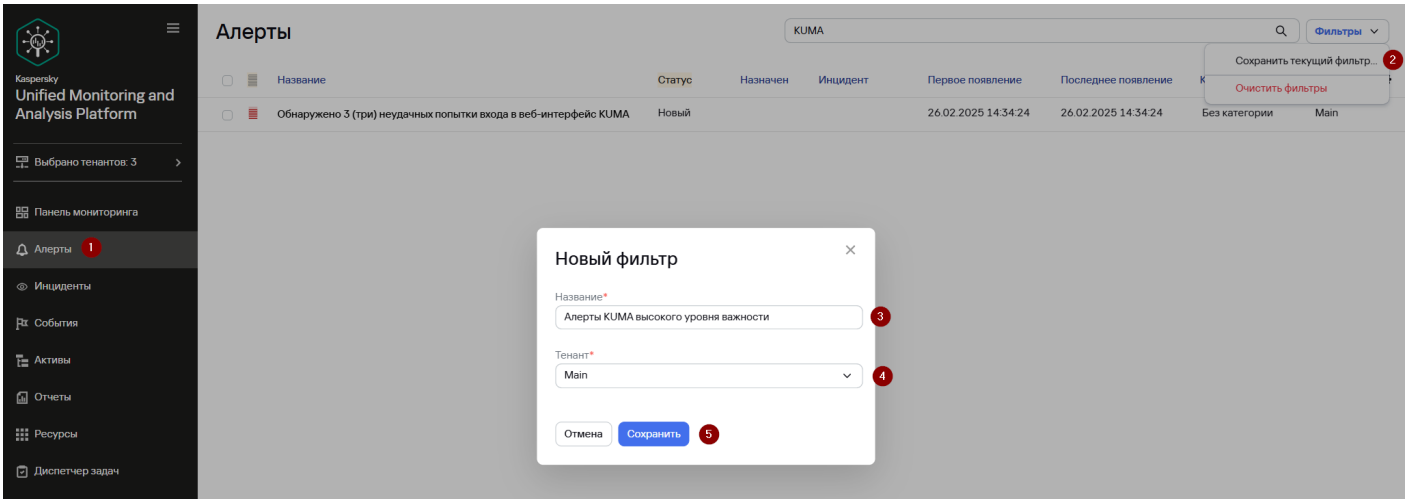




Чтобы сохранить текущие параметры фильтрации алертов:

- В разделе **Алерты** откройте раскрывающийся список **Фильтры**.

- Выберите **Сохранить текущий фильтр**.
- Появится поле для ввода названия нового фильтра и выбора тенанта, которому он будет принадлежать.
- Введите название фильтра.
- В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать фильтр, и нажмите **Сохранить**.
  Фильтр сохранен.

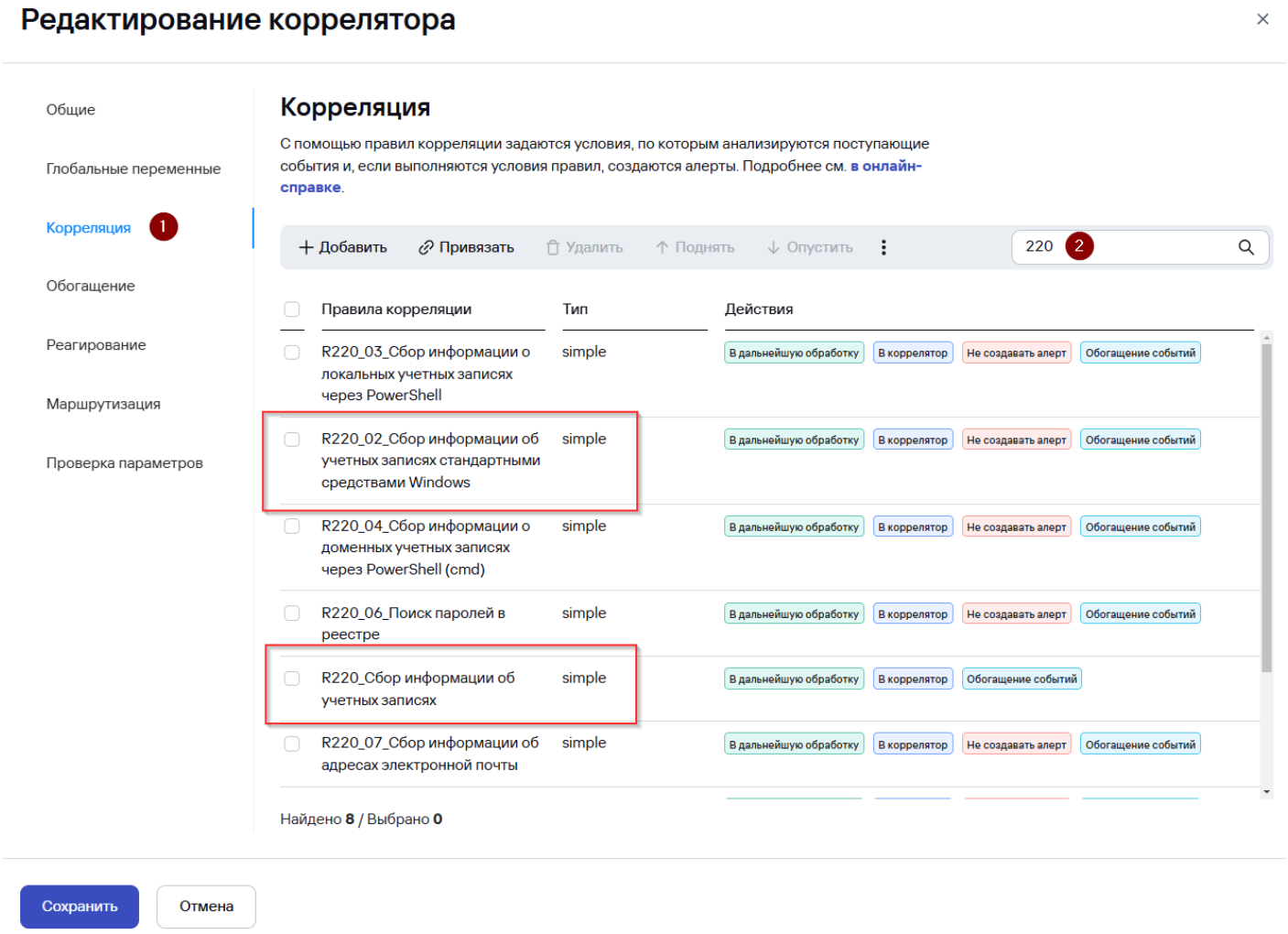


Чтобы сбросить текущие настройки фильтра, откройте раскрывающийся список **Фильтры** и выберите **Очистить фильтры**.

Просмотр информации об алерте

Для примера можно использовать уже сформированный алерт в KUMA (при наличии) или выполнить следующие действия для создания алерта:

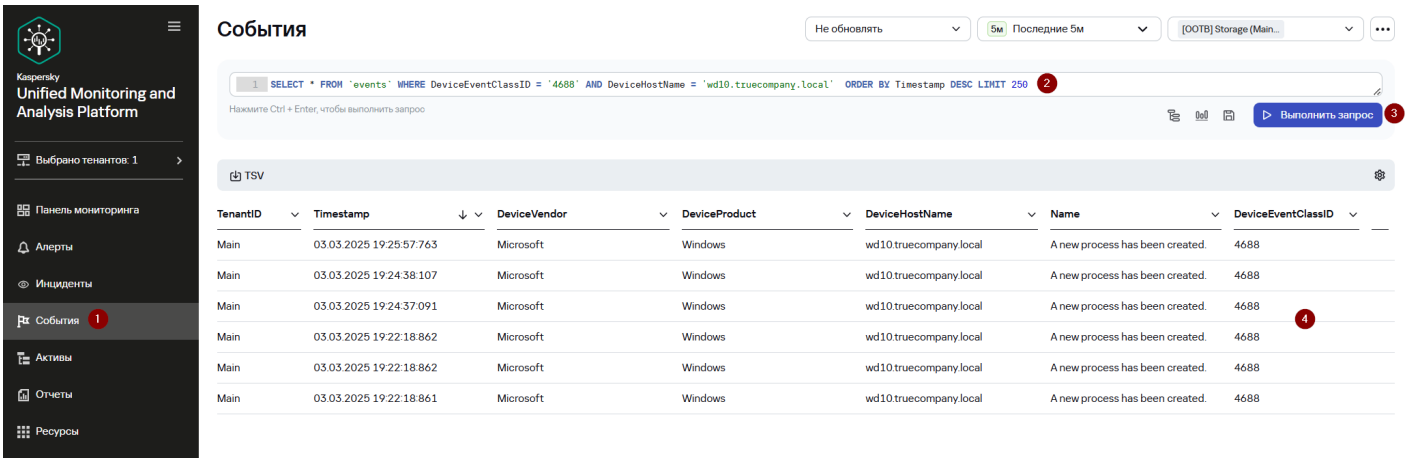
- Убедитесь, что правила **R220_02_Сбор информации об учетных записях стандартными средствами Windows** и **R220_Сбор информации об учетных записях** привязаны к коррелятору. Для этого:
  - Перейдите в **Ресурсы → Активные сервисы**
  - Выберите сервис коррелятора
  - В окне **Редактирование коррелятора** перейдите на шаг **Корреляция**
  - В поле **Поиск** введите «220»
  - Убедитесь, что правила **R220_02_Сбор информации об учетных записях стандартными средствами Windows** и **R220_Сбор информации об учетных записях** присутствуют в списке.
  - Если правила отсутствуют в списке выполните привязку правил аналогично статьям Простое правило (simple) и Стандартное правило (standard).



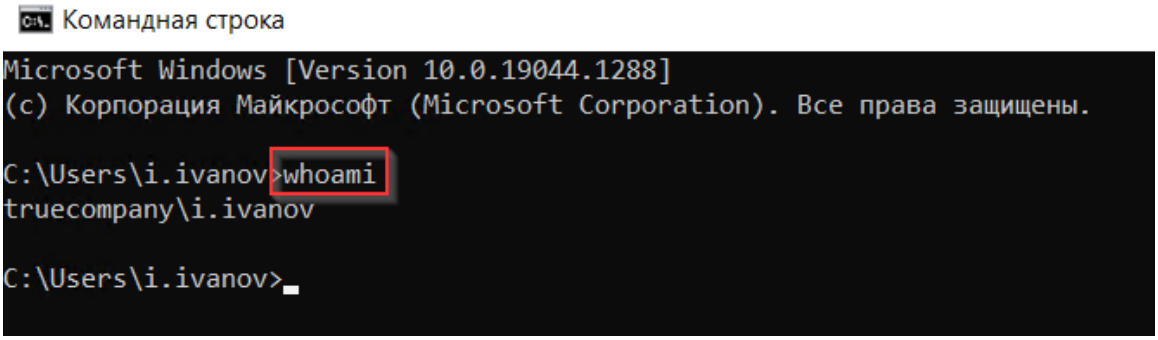
- Убедитесь, что события Windows **A new process has been created (Event ID 4688)** поступают с тестовой рабочей станции. Для этого:
  - Перейдите в раздел **События**.
  - Укажите следующий поисковый запрос:

```
SELECT * FROM `events` WHERE DeviceEventClassID = '4688' AND DeviceHostName = '<имя тестовой рабочей станции>'  ORDER BY Timestamp DESC LIMIT 250
```

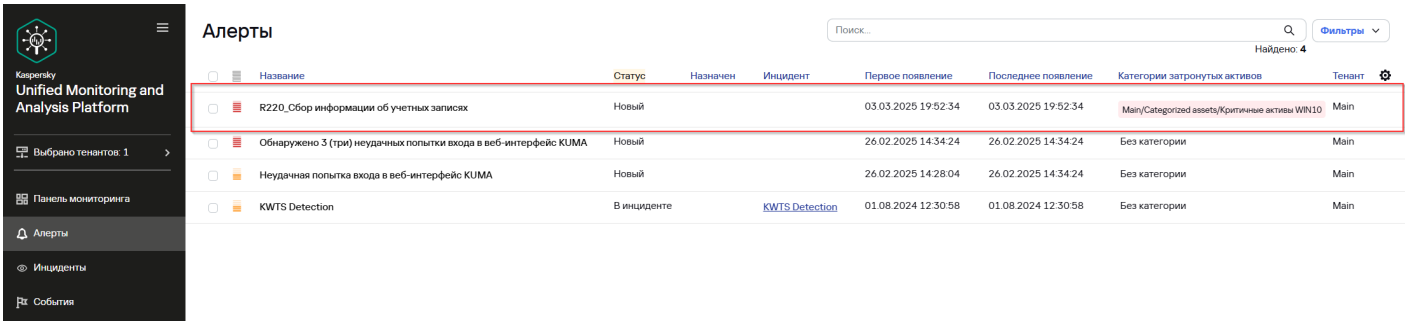
  - Нажмите **Выполнить запрос**
  - Убедитесь, что события **A new process has been created** отображаются в таблице событий.
  - Если события **A new process has been created** отсутствуют в таблице событий выполните настройку сбора событий с EventID 4688 одним из описанных способов.



- На тестовой рабочей станции запустите командую строку и выполните команду whoami для отображения имени текущего пользователя.

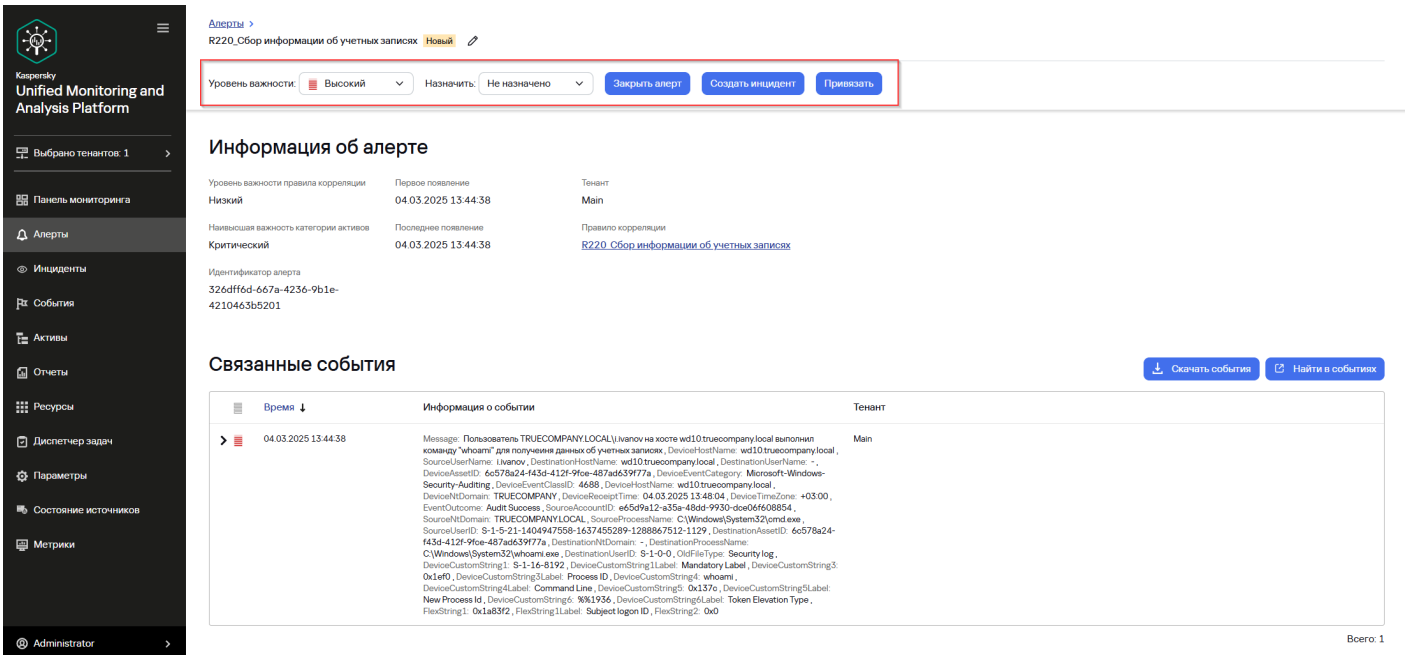


- В веб-интерфейсе KUMA перейдите в раздел **Алерты** и убедитесь, что алерт **R220_Сбор информации об учетных записях** появился в таблице алертов.



Чтобы просмотреть информацию об алерте:

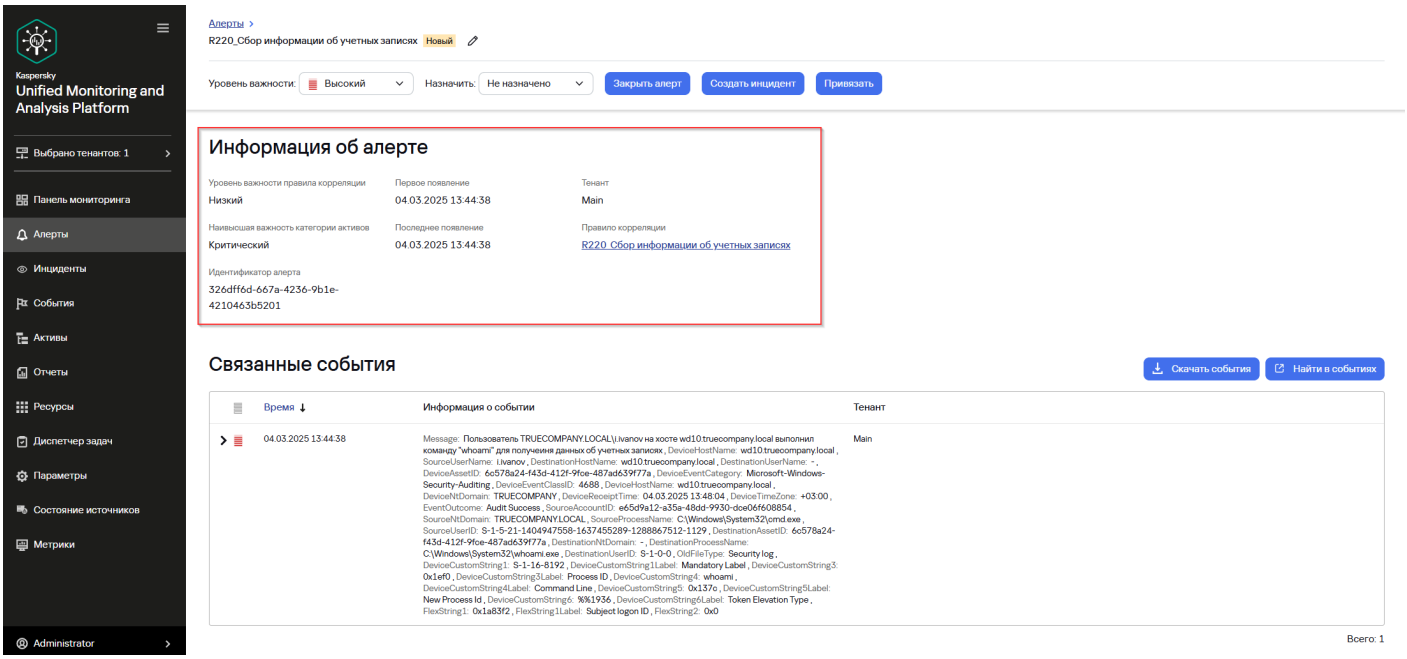
- Перейдите в раздел **Алерты**.
- Нажмите на название алерта, информацию о котором вы хотите просмотреть. В нашем примере это алерт **R220_Сбор информации об учетных записях.**
- Откроется окно с информацией об алерте.
  В верхней части окна с информацией об алерте расположена панель инструментов, а также указаны уровень важности алерта и имя пользователя, которому назначен этот алерт. В этом окне можно обработать алерт: изменить его уровень важности, назначить его пользователю, закрыть, создать на его основе инцидент (подробнее см. Раздел Обработка алертов).



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. Если алерт не привязан к инциденту, поле не заполнено.
- **Первое появление** – дата и время создания первого корреляционного события, приведшего к созданию алерта.
- **Последнее появление** – дата и время создания последнего корреляционного события, приведшего к созданию или обновлению алерта.
- **Идентификатор алерта** – уникальный идентификатор алерта в KUMA.
- **Тенант** – название тенанта, которому принадлежит алерт.
- **Правило корреляции** – название правила корреляции, в результате срабатывания которого создан алерт. Название правила представлено в виде ссылки, по которой можно перейти к настройкам этого правила корреляции.

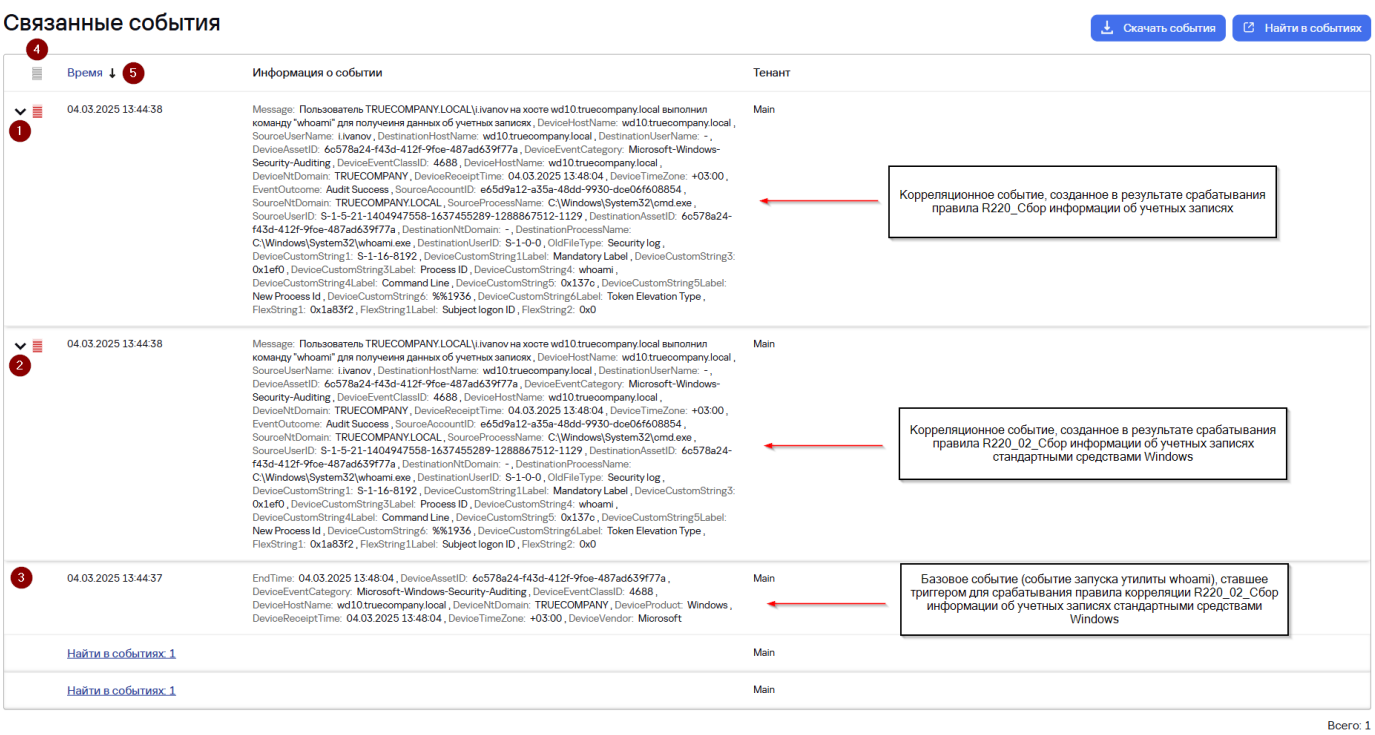


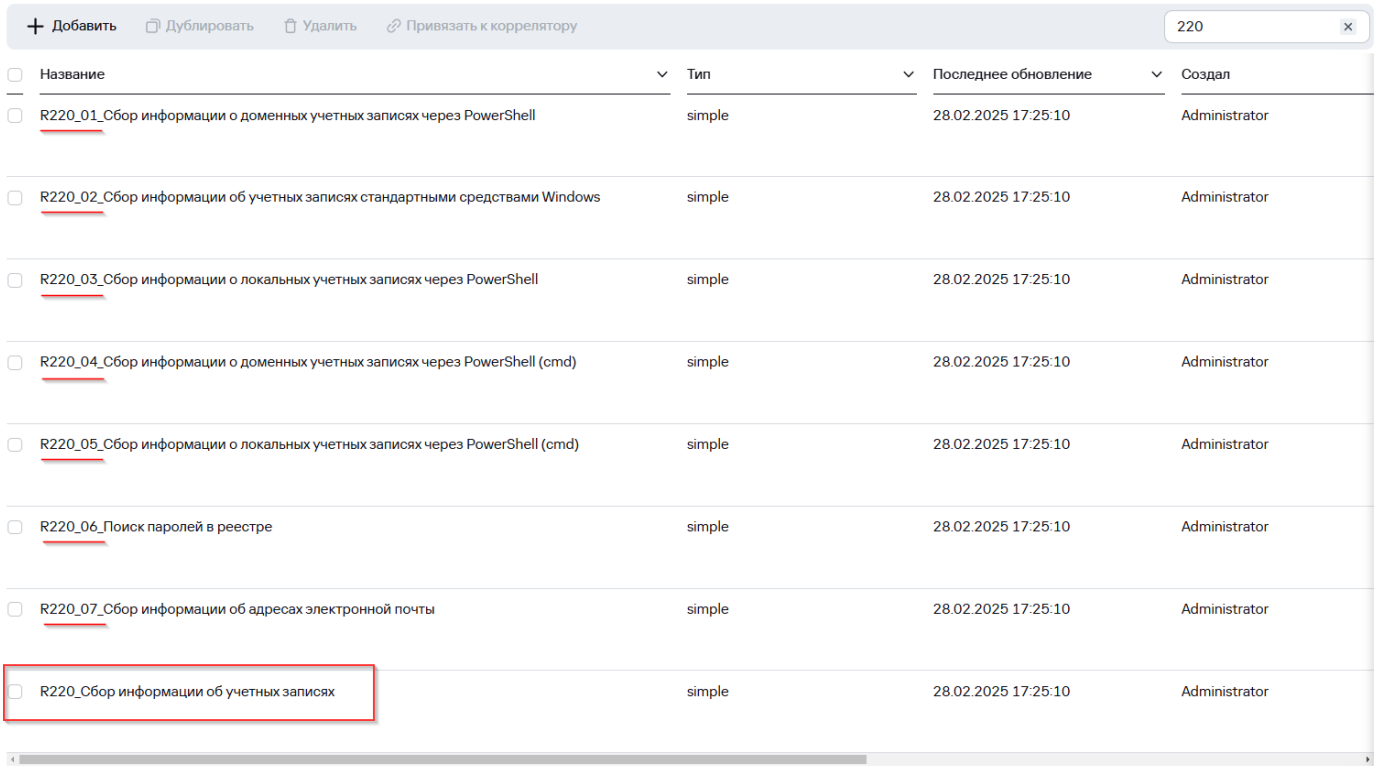
Раздел Связанные события

Этот раздел содержит таблицу событий, относящихся к алерту. Если нажать на значок › рядом с корреляционным событием, отобразятся базовые события, которые стали триггером срабатывания правила корреляции.

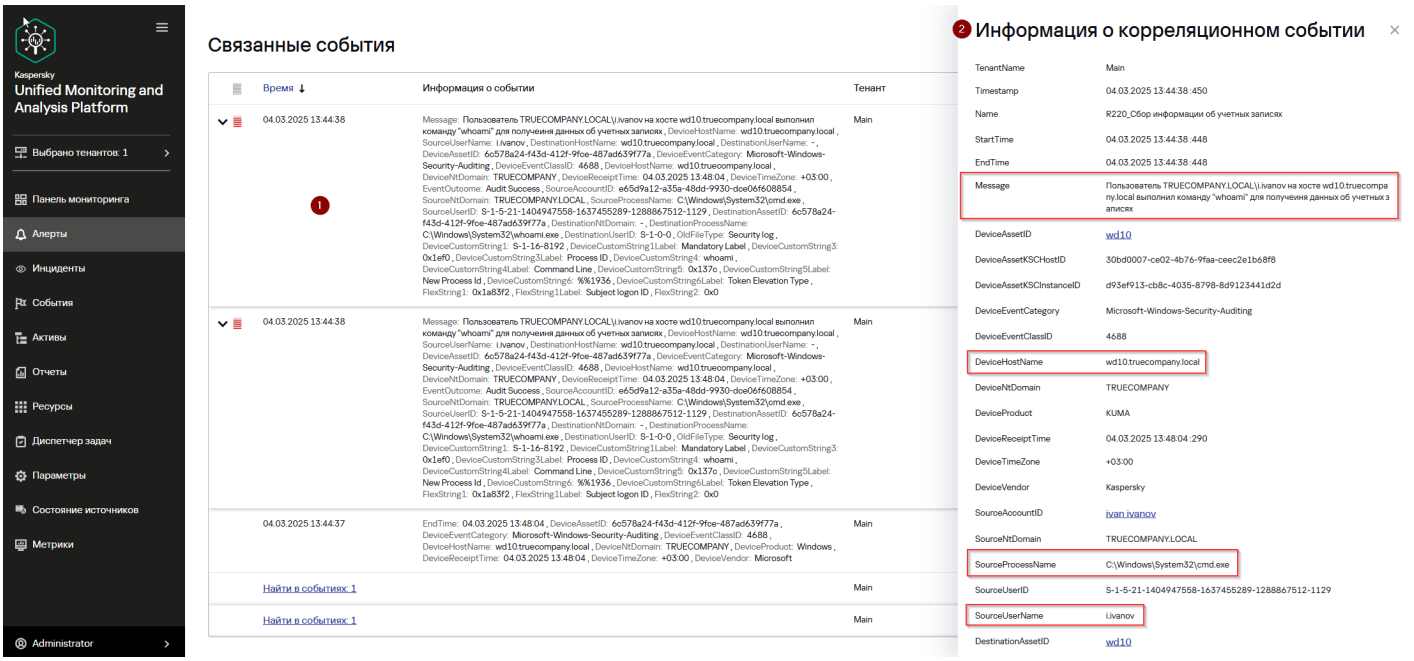
> **Базовое событие**. Событие, которое было получено от источника и было нормализовано.
> **Корреляционное событие.** При обнаружении события или последовательности событий, удовлетворяющих условиям правила корреляции, коррелятор создает корреляционное событие.

В нашем примере используется «вложенное» правило корреляции **R220_02_Сбор информации об учетных записях стандартными средствами Windows**, срабатывание которого приводит к срабатыванию вышестоящего (обобщающего) правила **R220_Сбор информации об учетных записях**. Поэтому при нажатии на значок › отображается сначала еще одно корреляционное событие (результат срабатывания **R220_02_Сбор информации об учетных записях стандартными средствами Windows**), а уже затем отображается базовое событие.





При выборе события в таблице открывается область деталей, содержащая информацию о выбранном событии.



Информация о корреляционном событии

DestinationHostName	wd10.truecompany.local
DestinationNtDomain	-
DestinationProcessName	C:\Windows\System32\whoami.exe
DestinationUserID	S-1-0-0
DestinationUserName	-
DeviceCustomString1	S-1-16-8192
DeviceCustomString1Label	Mandatory Label
DeviceCustomString3	0x1ef0
DeviceCustomString3Label	Process ID
DeviceCustomString4	whoami
DeviceCustomString4Label	Command Line
DeviceCustomString5	0x137c
DeviceCustomString5Label	New Process Id
DeviceCustomString6	%%1936
DeviceCustomString6Label	Token Elevation Type
CorrelationRule	R220_Сбор информации об учетных записях
Service	[OOTB] Correlator
BaseEventCount	1
EventOutcome	Audit Success
ExternalID	R220

Кнопка **Найти в событиях** справа от заголовка раздела используется для перехода к расследованию алерта.

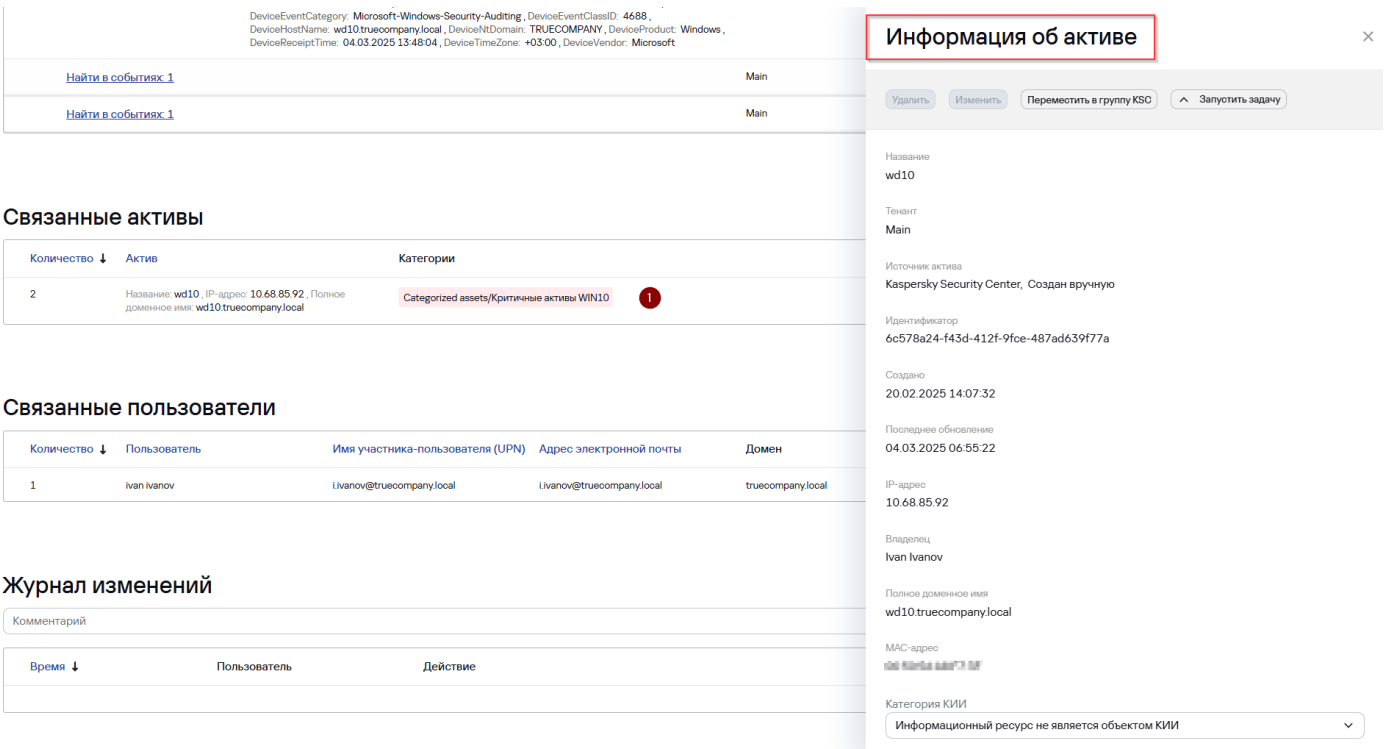
> Подробнее про расследование алерта:
>
> https://support.kaspersky.ru/kuma/4.0/217847
>
> Пример расследования инцидента с помощью KUMA:
>
> https://support.kaspersky.ru/kuma/4.0/245892

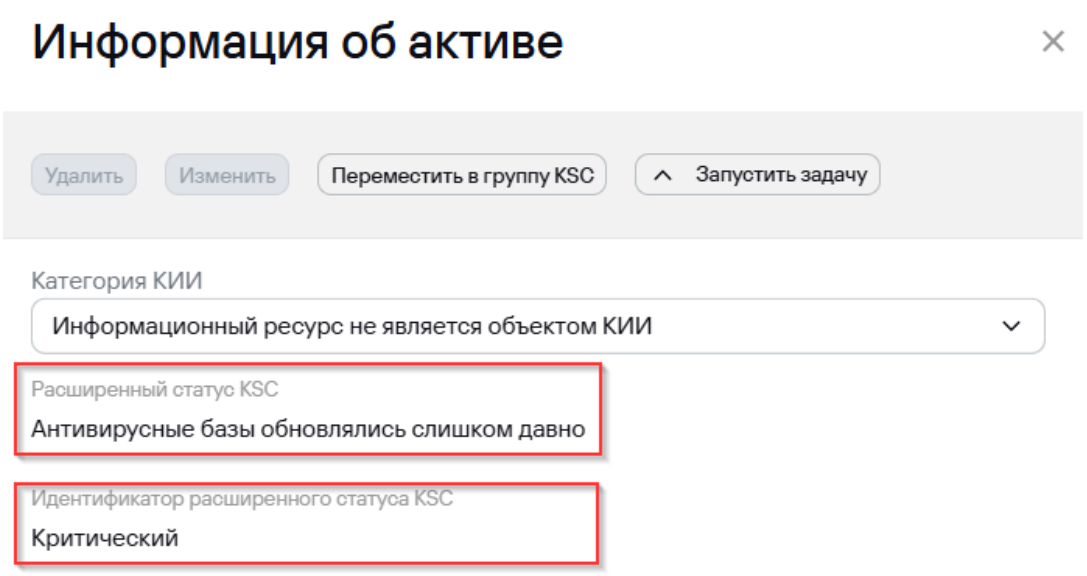
С помощью кнопки **Скачать события** вы можете скачать информацию о связанных событиях в виде файла в формате CSV (в кодировке UTF-8).

Раздел Связанные активы

Этот раздел содержит таблицу активов, связанных с алертом. Информация об активах поступает из событий, связанных с алертом. С помощью поля **Поиск по IP или FQDN** можно искать нужные активы. Активы можно сортировать по столбцам **Количество** и **Актив**.

При нажатии на название актива открывается окно **Информация об активе**, в котором можно посмотреть владельца актива, состояние защиты (статусы KSC), информацию о ПО, аппаратном обеспечении и уязвимостях (опционально).

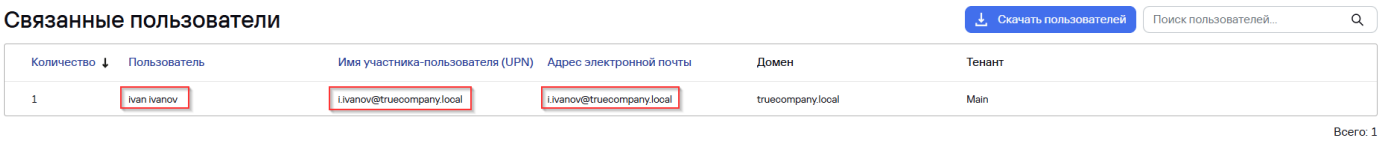




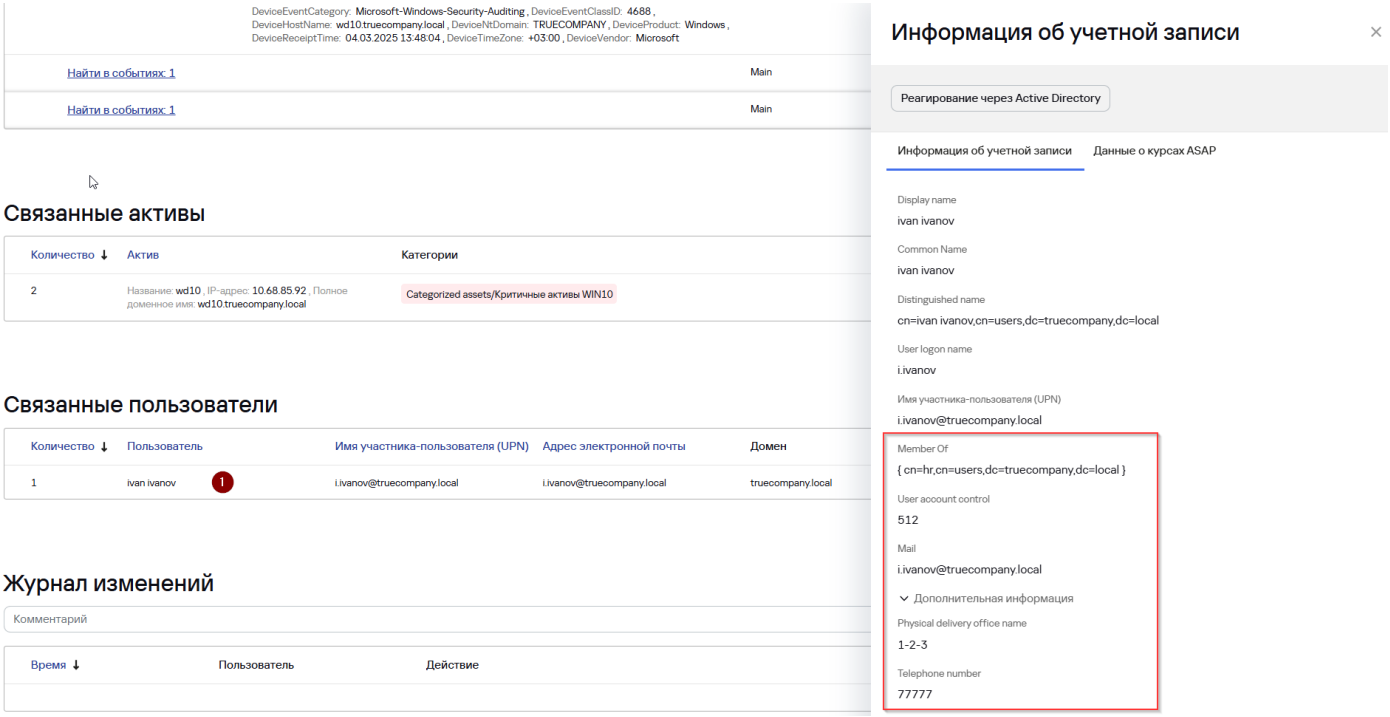
С помощью кнопки **Скачать активы** вы можете скачать информацию о связанных активах в виде файла в формате CSV (в кодировке UTF-8).

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**.



При нажатии на имя пользователя открывается окно **Информация об учетной записи**, в котором можно посмотреть данные учетной записи: в каких группах состоит учетная запись, UAC, контактные данные, местонахождение пользователя и другие атрибуты, которые были импортировать из MS Active Directory.

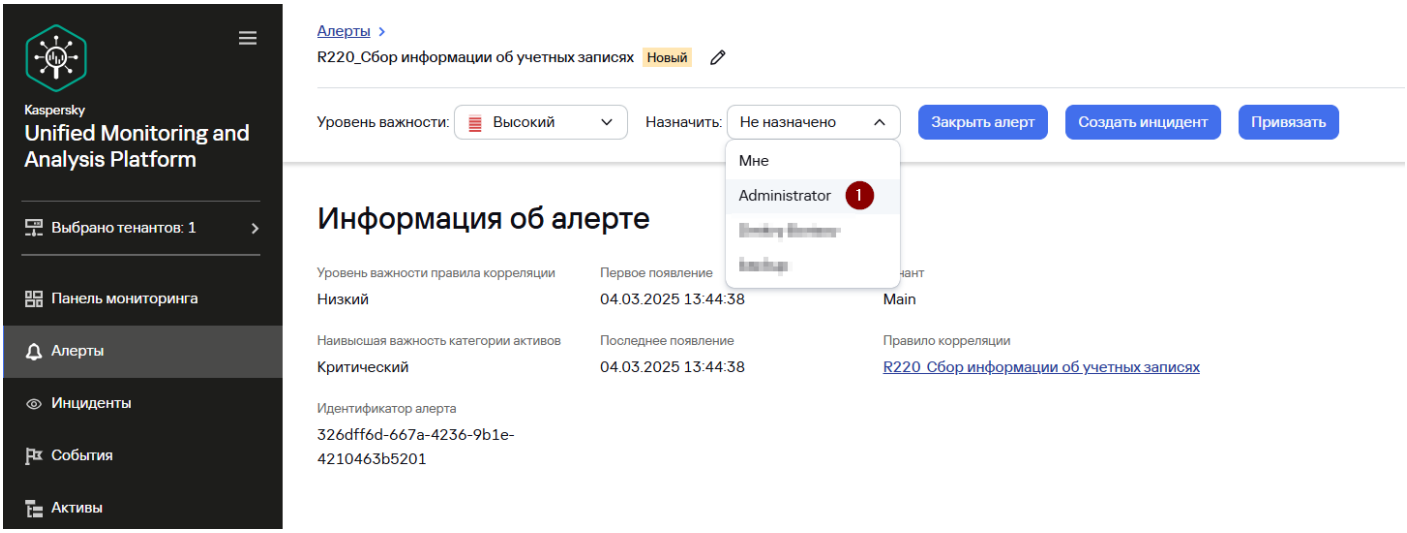


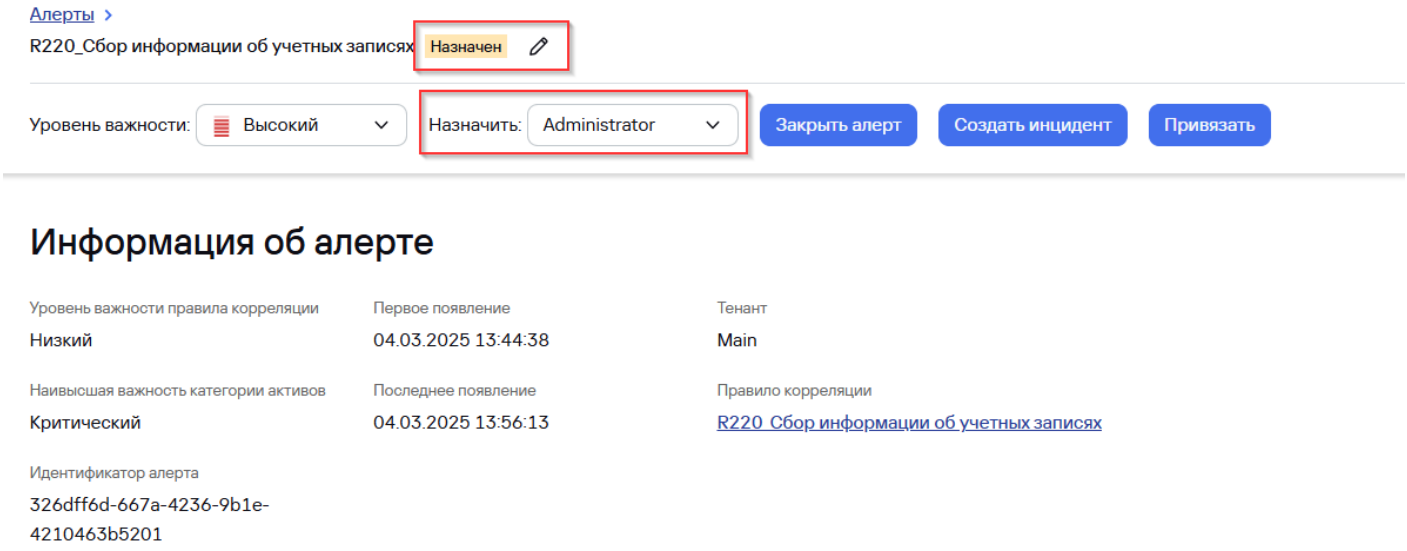
С помощью кнопки **Скачать пользователей** вы можете скачать информацию о связанных пользователях в виде файла в формате CSV (в кодировке UTF-8).

Раздел Журнал изменений

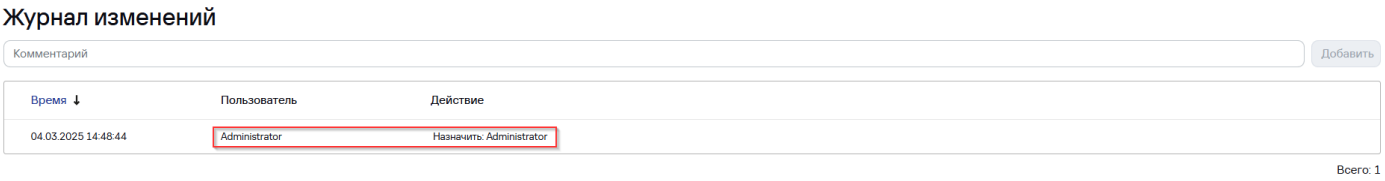
Этот раздел содержит записи об изменениях, которые пользователи внесли в алерт. Изменения регистрируются автоматически, при этом есть возможность вручную добавлять комментарии. Комментарии можно сортировать по столбцу **Время**.

Например, назначьте алерт пользователю **Administrator**. Статус алерта изменится с **Новый** на **Назначен**.





Убедитесь, что в разделе **Журнал изменений** появилась запись о назначении алерта пользователю **Administrator**.



При необходимости в поле **Комментарий** вы можете внести комментарий к алерту и нажать **Добавить**, чтобы сохранить его.

Обработка алертов

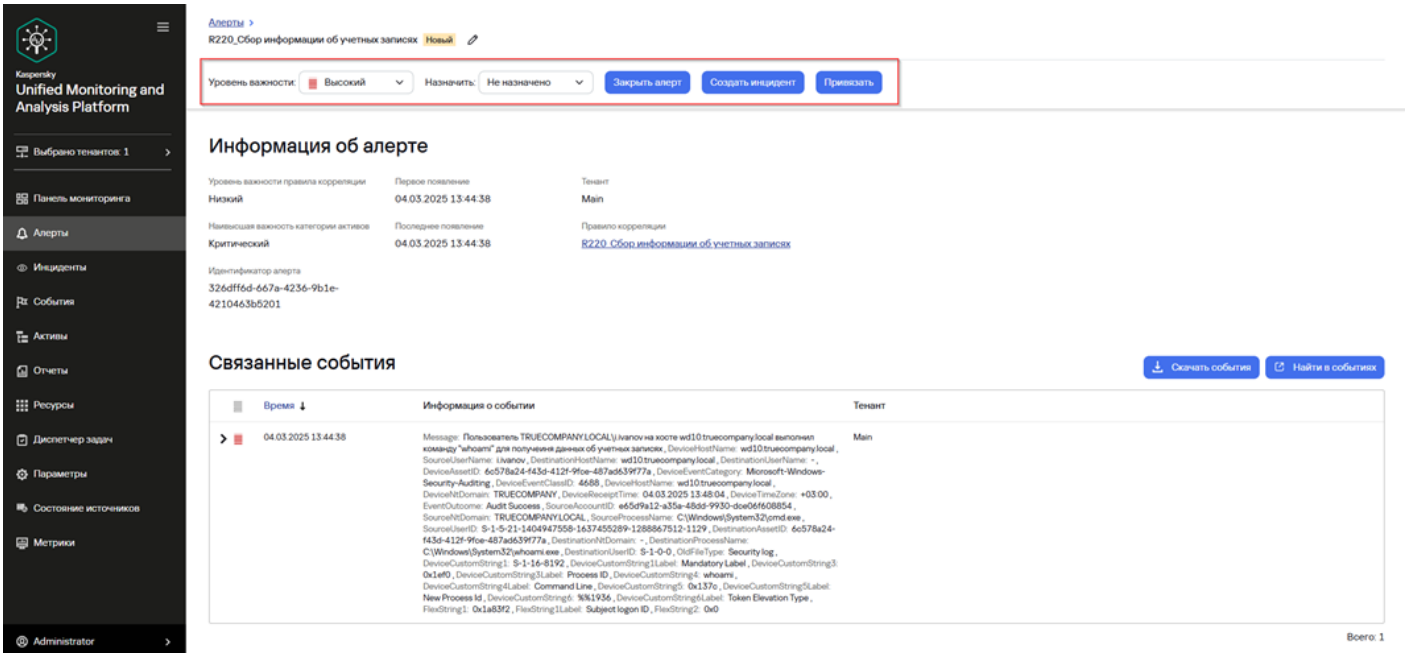
Вы можете изменить уровень важности алерта, назначить алерт пользователю, закрыть алерт или создать на основе алерта **инцидент**.

> В терминах Лаборатории Касперского **инцидент** — это подтвержденный алерт (другими словами, подтвержденная угроза информационной безопасности). Инцидент может объединять несколько алертов, например, в рамках расследования аналитик обнаружил первичное заражение и боковое перемещение и привязал эти алерты к одному инциденту.

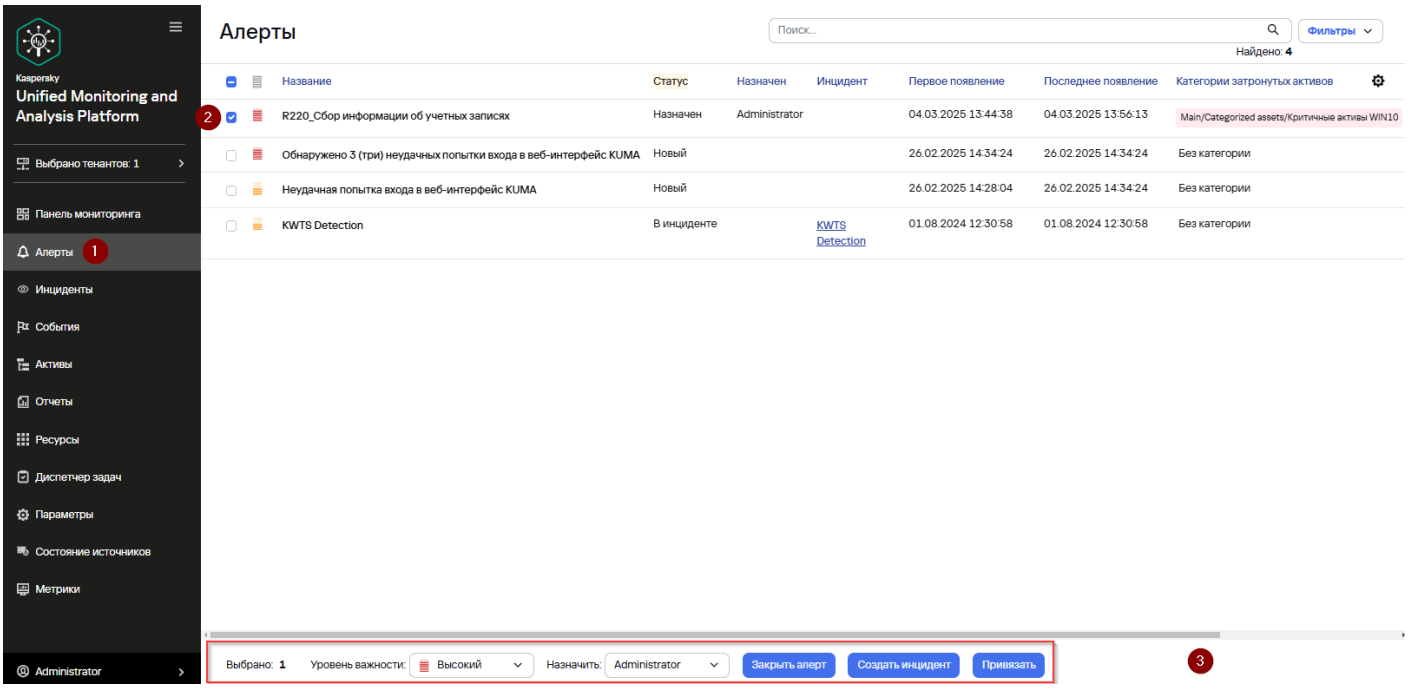
Чтобы обработать алерт:

- Выберите необходимый алерт одним из следующих способов:
  - В разделе **Алерты** веб-интерфейса KUMA нажмите на алерт, сведения о котором вы хотите просмотреть. Откроется 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). В нижней части окна отобразится панель инструментов.

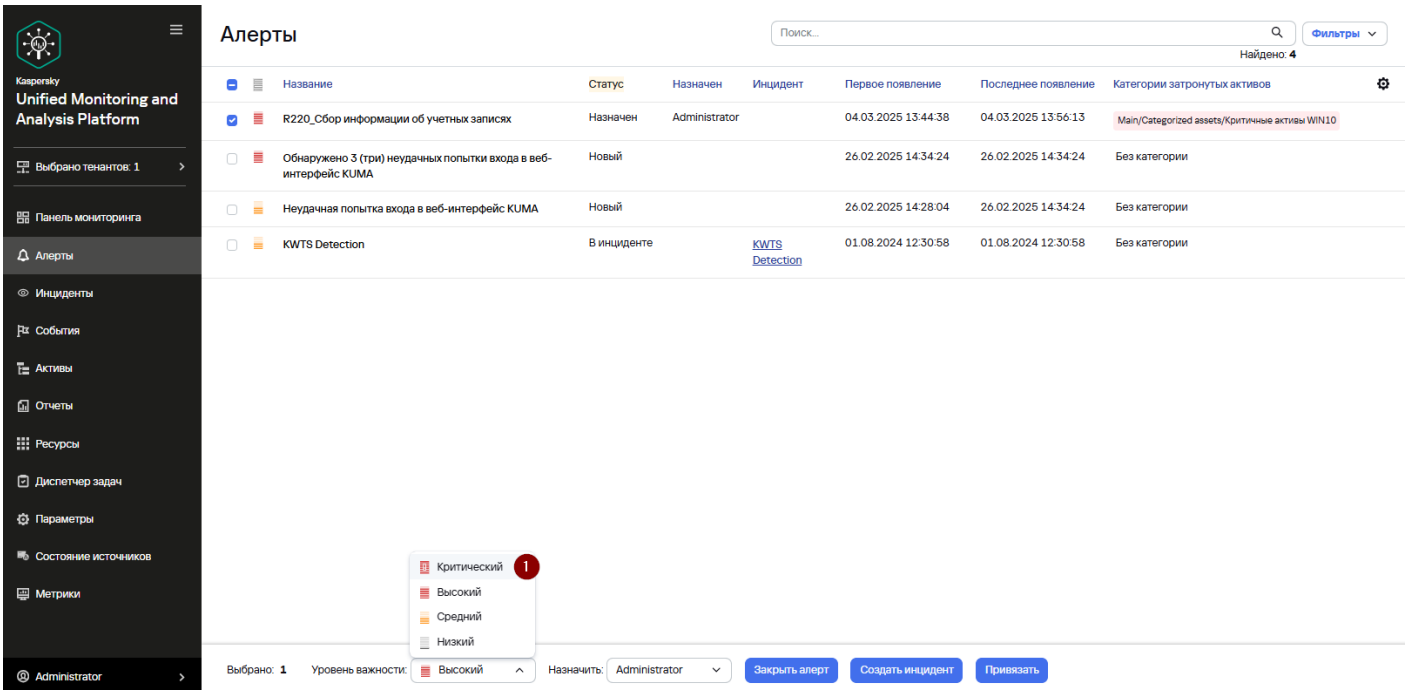


> Алерты со статусом **Закрыт** не могут быть выбраны для обработки.

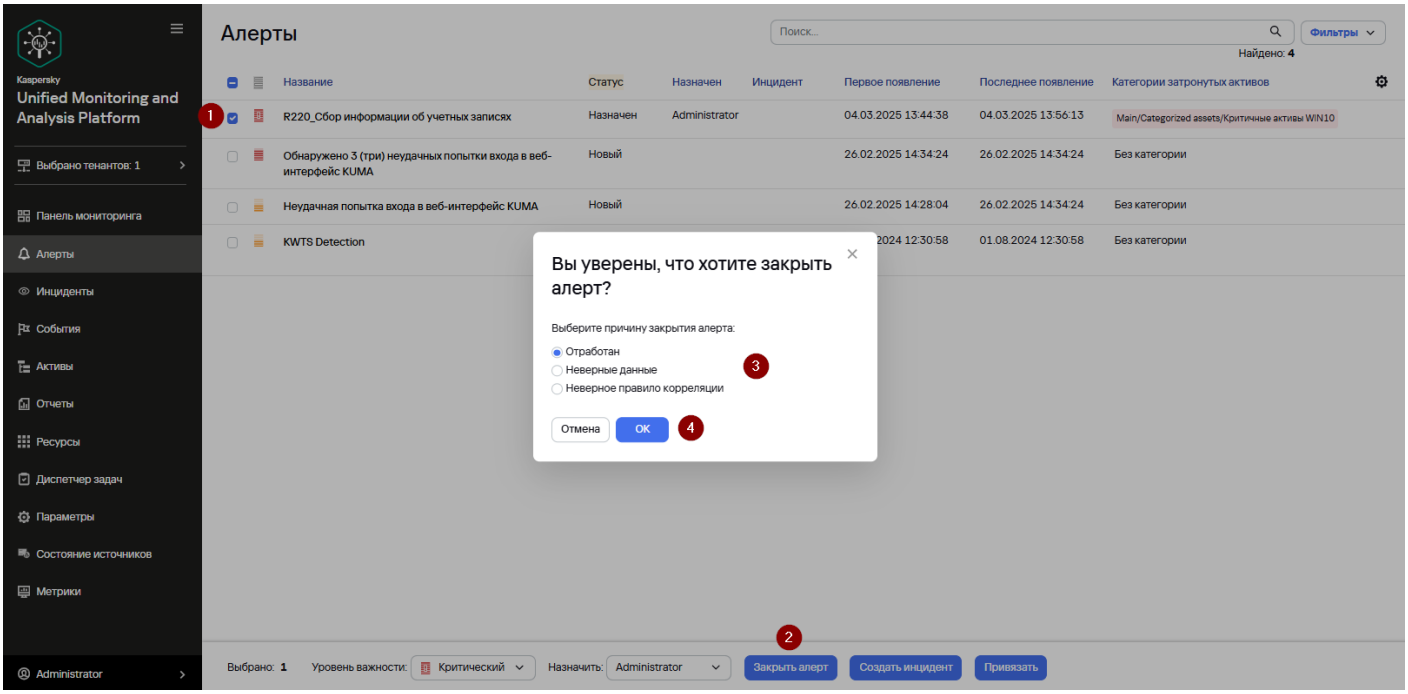
- Измените уровень важности алерта с помощью раскрывающегося списка Уровень важности:
  - Низкий.
  - Средний.

- Высокий.
- Критический.

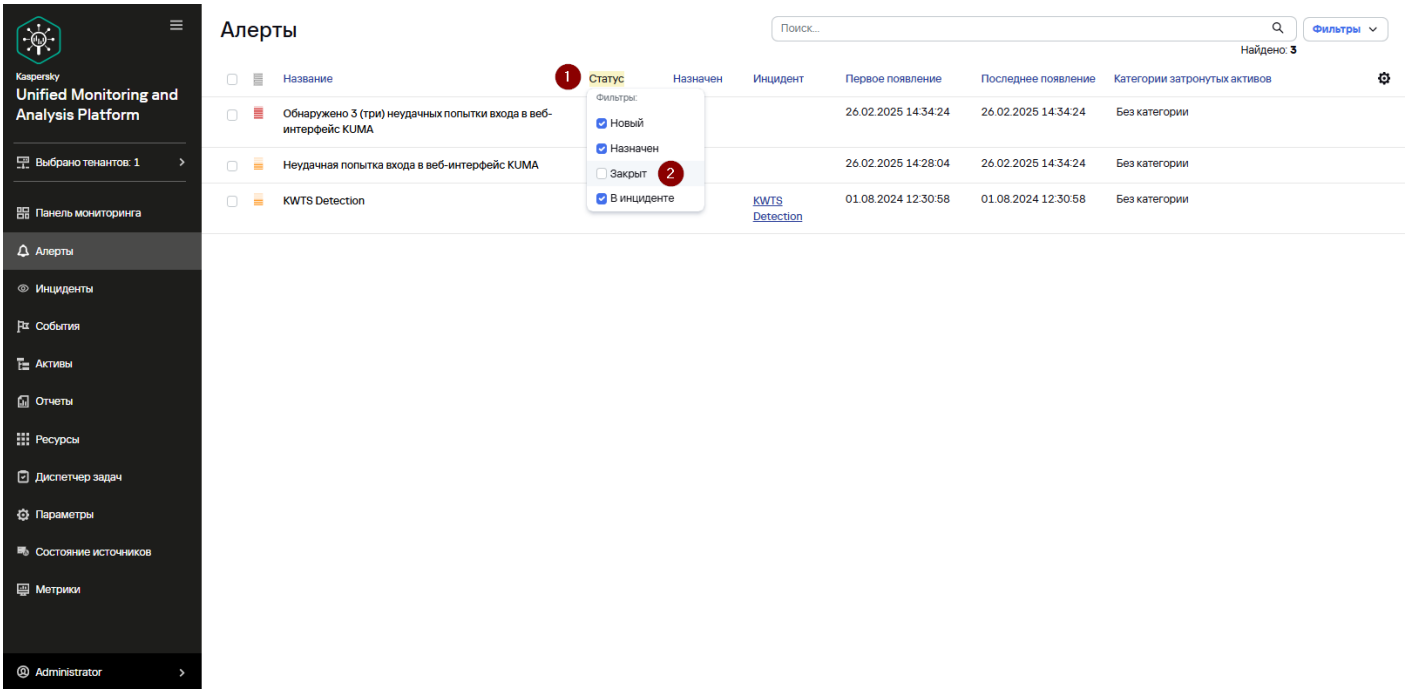
В нашем примере измените **Уровень важности** с **Высокий** на **Критический**.

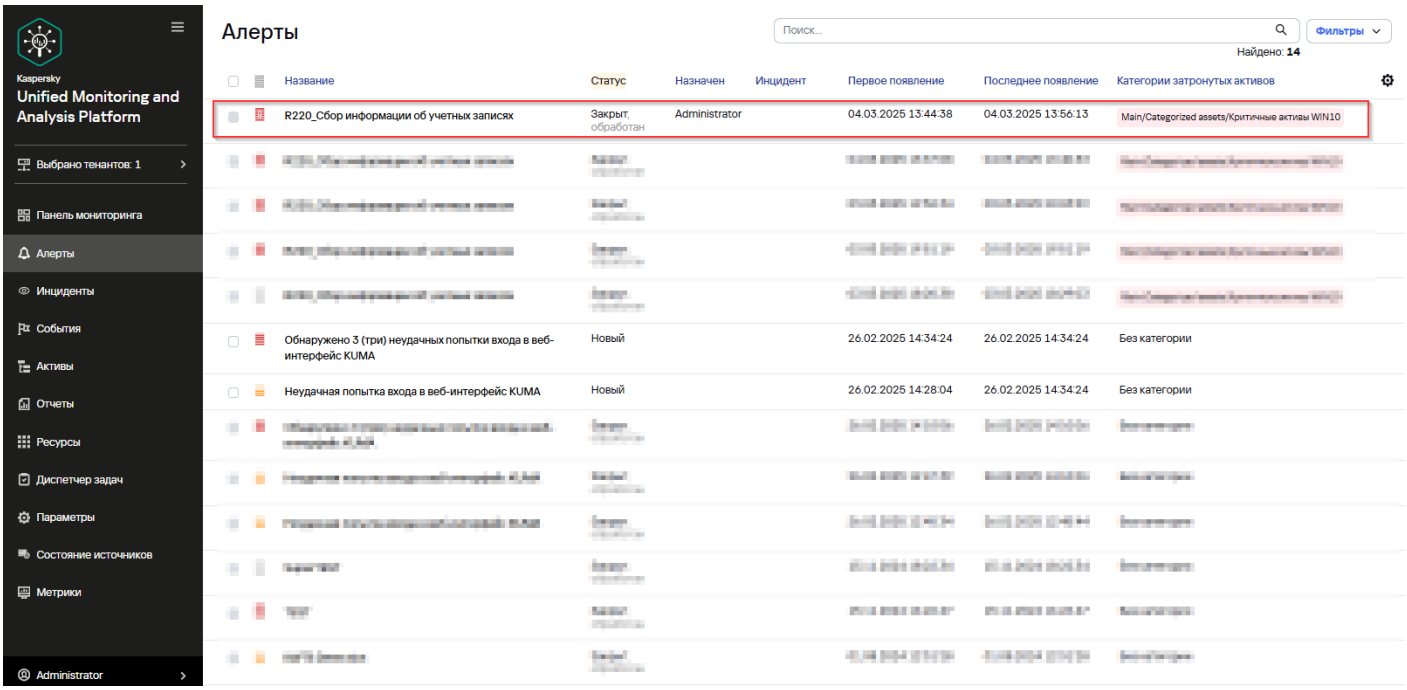


- Алерт можно назначить пользователю для дальнейшего анализа. Ранее в Разделе **Просмотр информации об алерте** мы уже назначили алерт пользователю **Administrator**. Статус алерта в таком случае изменяется на **Назначен,** а в раскрывающемся списке **Назначить** отобразится имя выбранного пользователя.
- Если алерт признан ложным срабатыванием или расследование алерта завершено закройте алерт. Для этого:
  - Нажмите **Закрыть алерт** (это можно сделать в карточке алерта или в таблице алертов, выбрав соответствующий алерт, как на скриншоте выше).
  - В появившемся окне подтверждения укажите причину закрытия алерта:
    - **Отработан**. Это означает, что было проведено расследование алерта и 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.
  - Нажмите **OK**.

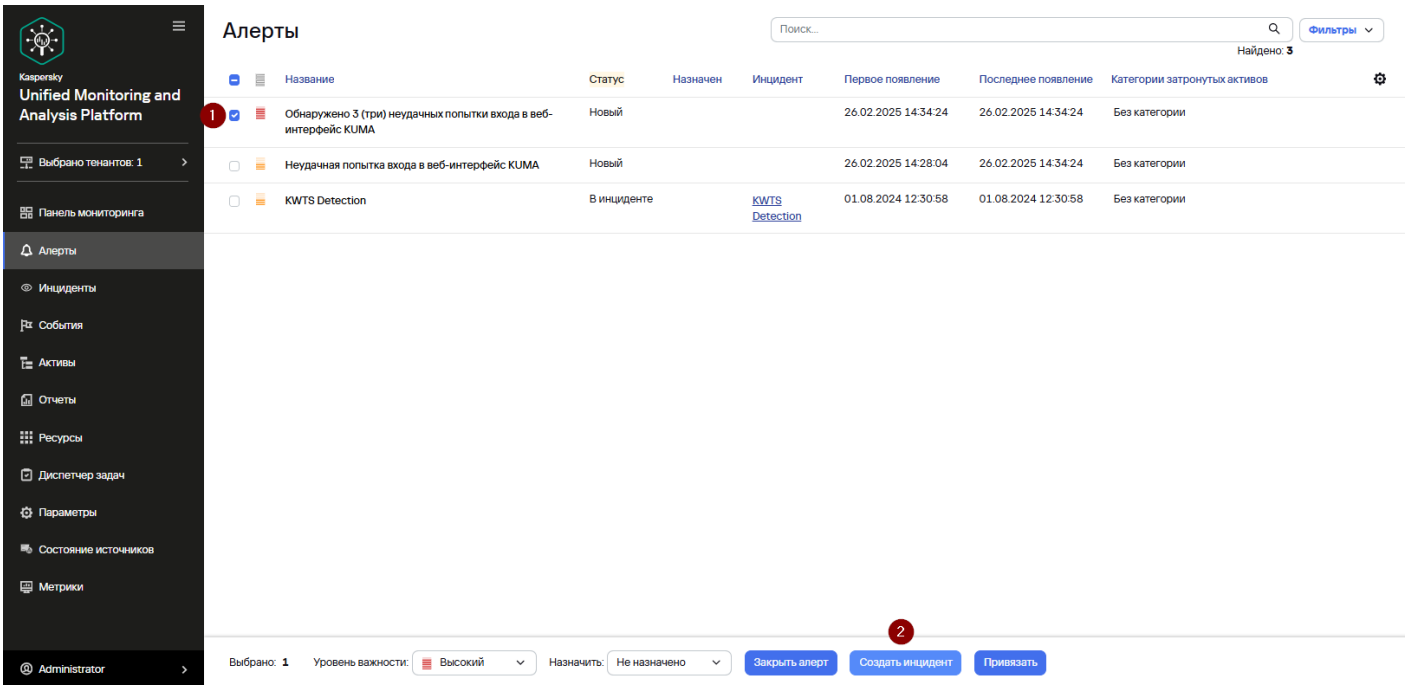


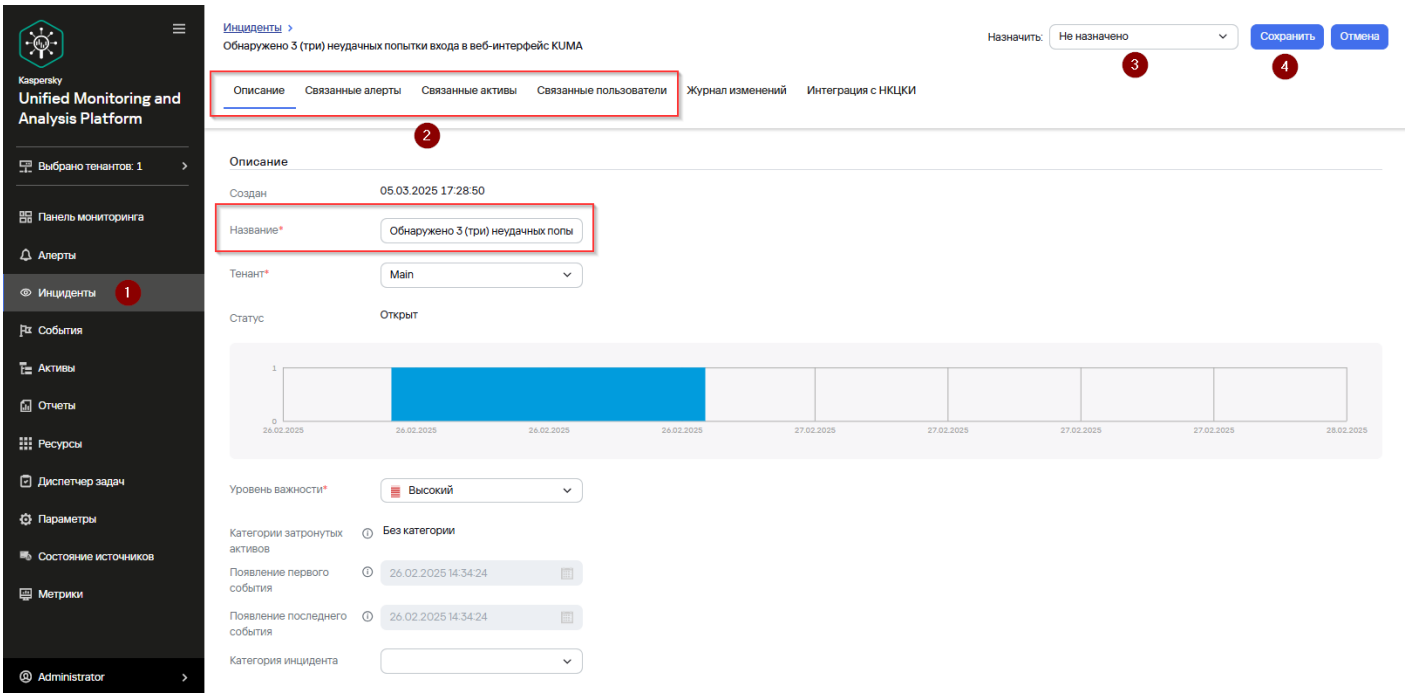
- Статус алерта будет изменен на **Закрыт**. Алерты с таким статусом не обновляются новыми корреляционными событиями и отображаются в таблице алертов, только если в раскрывающемся списке **Статус** установлен флажок **Закрыт**. Изменить статус закрытого алерта или назначить его другому пользователю невозможно.

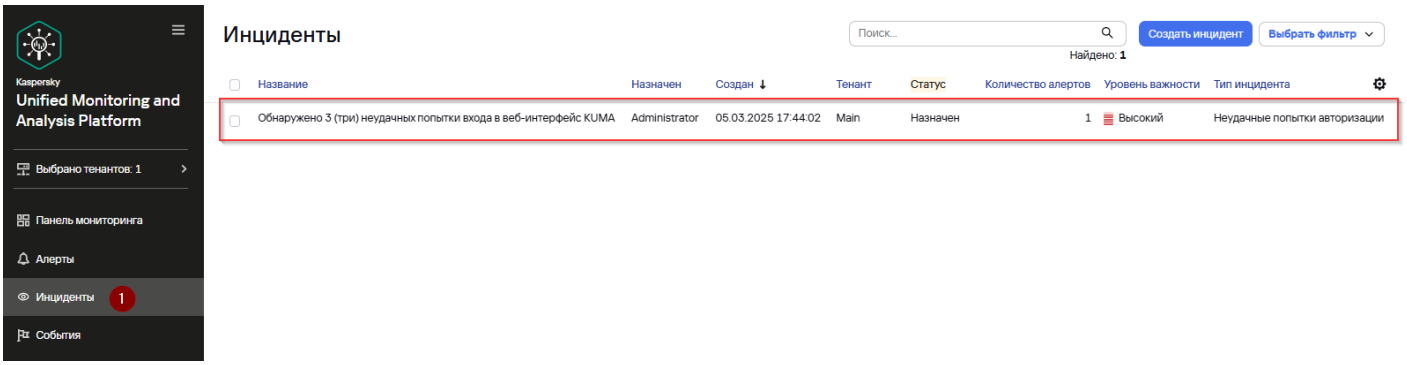


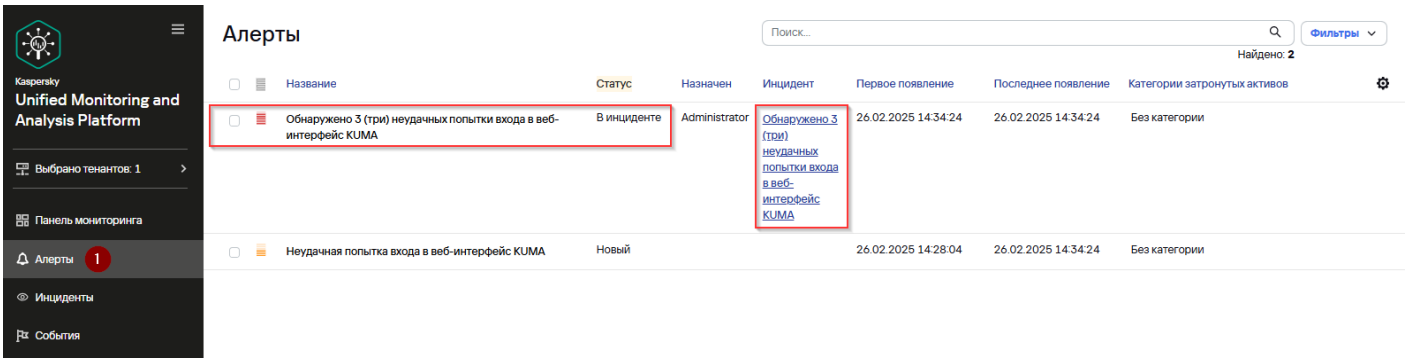


- Если в процессе расследования алерта Вы выявили и подтвердили вредоносные действия, а также предполагаете наличие других алертов, связанных с данной вредоносной активностью, создайте на основе алерта инцидент:
  - Нажмите **Создать инцидент**.
  - Откроется окно создания инцидента. В качестве названия инцидента используется название алерта.
  - При необходимости измените параметры инцидента и нажмите **Сохранить**.
  - Инцидент будет создан, статус алерта изменится на **В инциденте**. При необходимости алерт можно отвязать от инцидента, выбрав его и нажав **Отвязать**.









> Подробнее про работу с инцидентами:
>
> https://support.kaspersky.ru/kuma/4.0/220213

Уведомления об алертах

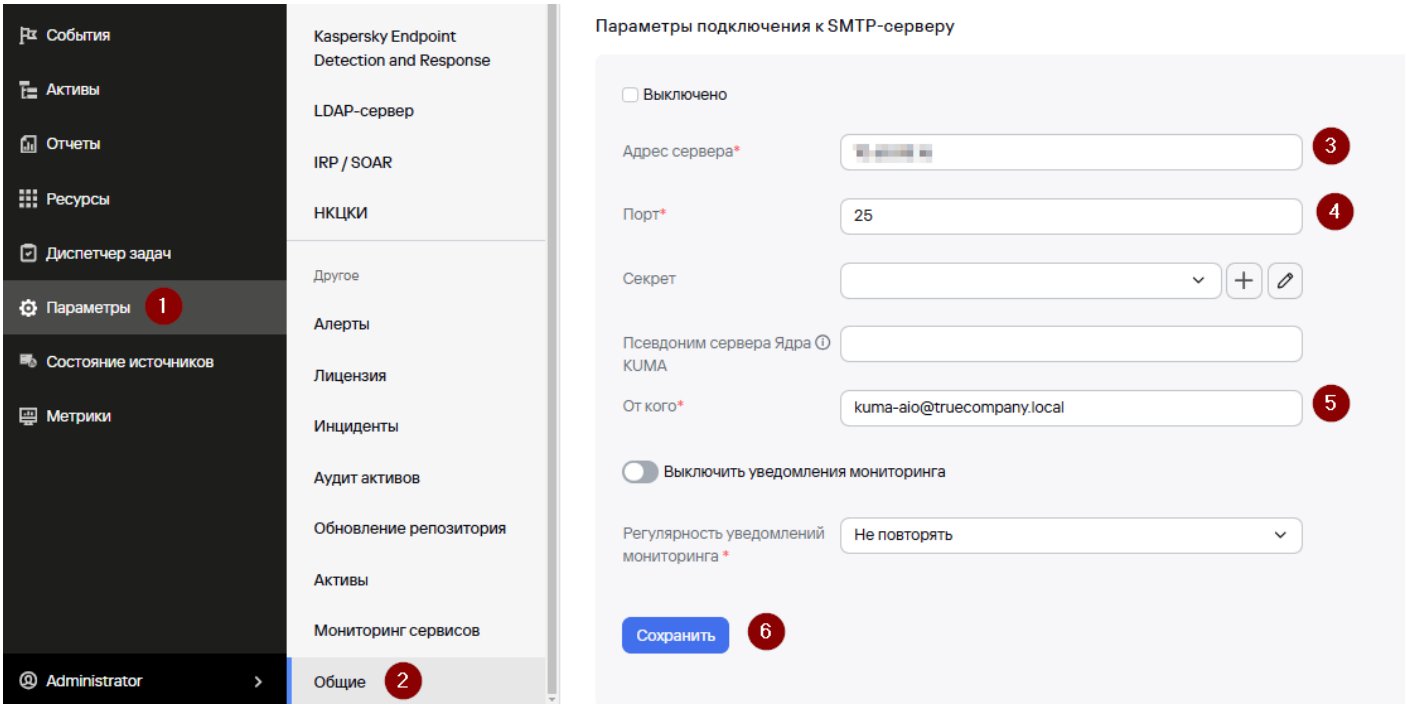
При создании и назначении алертов по электронной почте рассылаются стандартные уведомления KUMA. Предварительно необходимо настроить подключение к SMTP-серверу

организации, а также установить флажок **Получать уведомления по почте** в карточке пользователя.

Чтобы настроить подключение к SMTP-серверу:

- Перейдите в раздел **Параметры** → **Общие**.
- В секции **Параметры подключения к SMTP-серверу** укажите необходимые параметры:
  - **Адрес сервера** – адрес SMTP-сервера в одном из следующих форматов: hostname, IPv4, IPv6.
  - **Порт** – порт подключения к почтовому серверу.
  - **От кого** – адрес электронной почты отправителя сообщения. Например, kuma-aio@truecompany.local.
  - (Опционально) Если при подключении к почтовому серверу необходимо пройти аутентификацию в поле **Секрет** выберите или создайте секрет типа credentials, в котором будут указаны учетные данные для подключения к SMTP-серверу.
- Нажмите **Сохранить**.

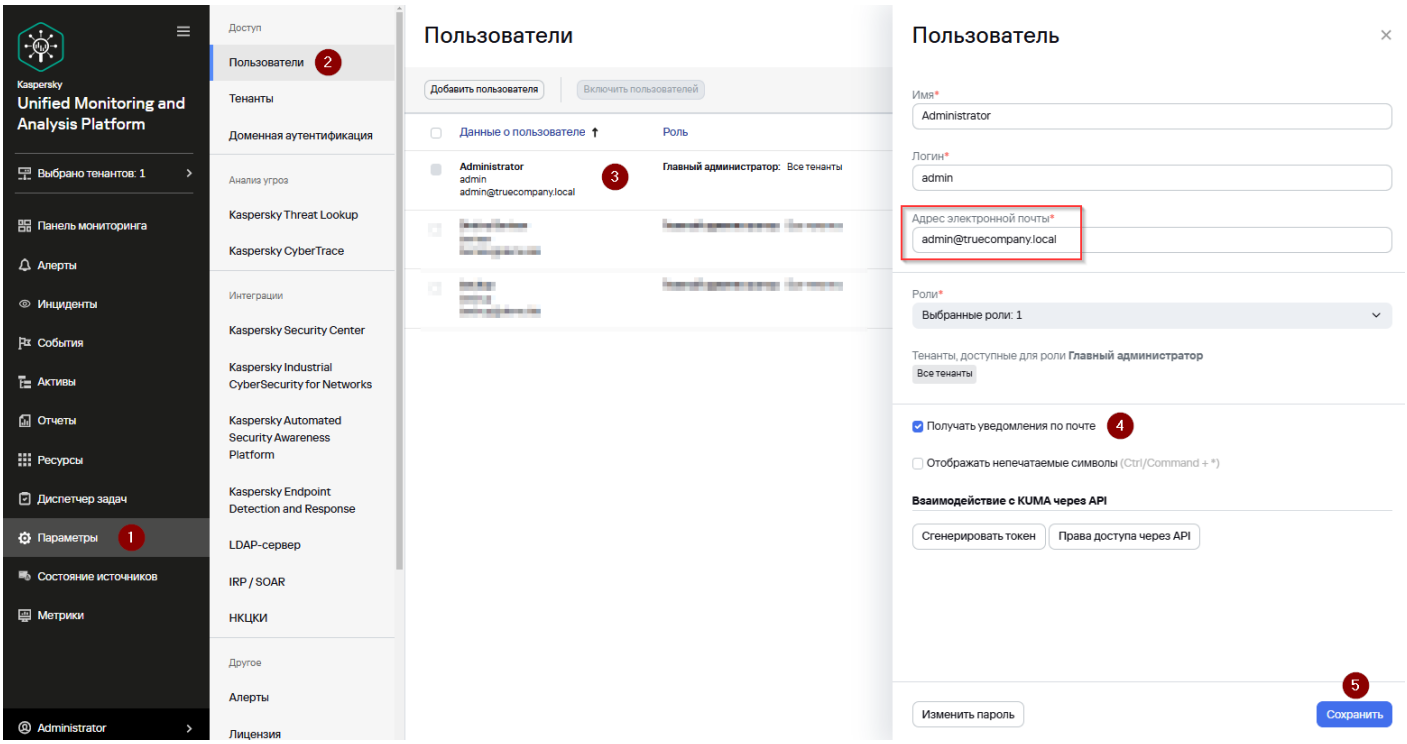
Соединение с SMTP-сервером настроено.



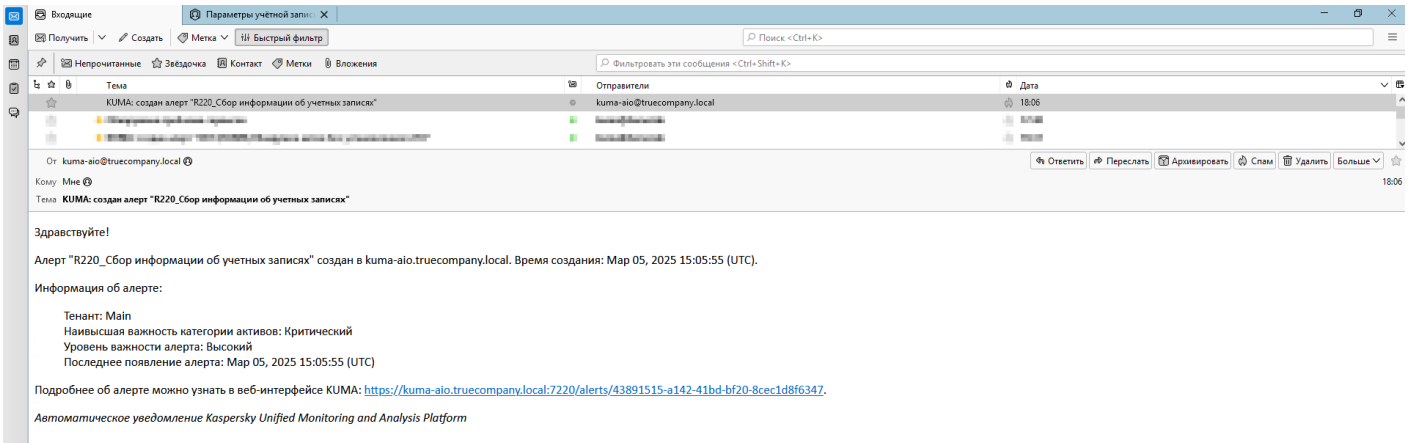
Для того, чтобы пользователи смогли получать сообщения электронной почты от KUMA также необходимо в карточке пользователей установить флажок **Получать уведомления по почте**. Для этого:

- Перейдите в раздел **Параметры** → **Пользователи**.
- Нажмите на пользователя, для которого необходимо настроить получение уведомлений.

- В появившемся окне справа **Пользователи** установите флажок **Получать уведомления по почте**.
- Нажмите **Сохранить.**



Сгенерируйте тестовый алерт (см. **Раздел Просмотр информации об алерте**). Убедитесь, что на почтовый ящик пользователя пришло почтовое сообщение с уведомлением о созданном алерте.



> Вместо стандартных уведомлений KUMA о создании алертов (как на скриншоте выше) можно рассылать уведомления на основании пользовательских шаблонов. Подробнее:
>
> https://support.kaspersky.ru/kuma/4.0/233518

> Также в KUMA поддерживается отправка уведомлений в Telegram:
> Статья онлайн-справки «Отправка уведомлений в Telegram»:
>
> https://support.kaspersky.ru/kuma/4.0/258846

Community-скрипт с расширенными возможностями уведомлений и управления через Telegram:

https://github.com/KUMA-Community/kuma_telebot

Revision #4
Created 2026-08-10 13:48:47 UTC by Dmitry Borisov
Updated 2026-08-11 14:19:02 UTC by Dmitry Borisov