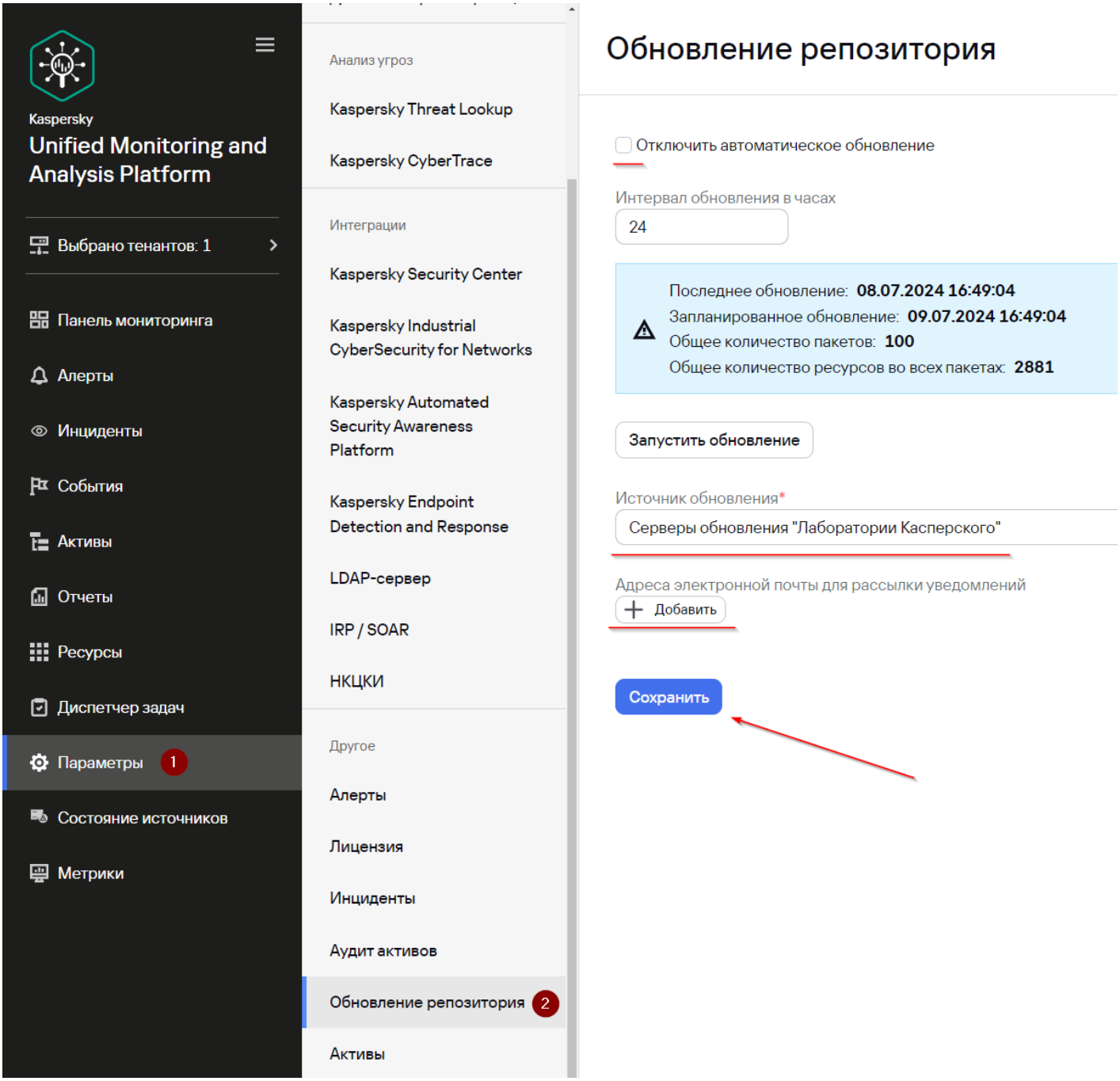
Где брать официальный контент для KUMA? (Обновление контента)

> Начиная с версии KUMA 2.1 контент от Лаборатории Касперского (правила корреляции, нормализаторы, коннекторы и т.п.) публикуются в репозитории ЛК: https://support.kaspersky.com/help/KUMA/4.0/ru-RU/250594.htm

> Возможно также офлайн обновление с помощью утилиты KUU - https://kb.kuma-community.ru/books/ustanovka-i-obnovlenie/page/obnovlenie-resursov-s-pomoshhiu-kaspersky-update-utility-kuu

Как получить SOC Package и другой коробочный контент? (KUMA < 4.6)

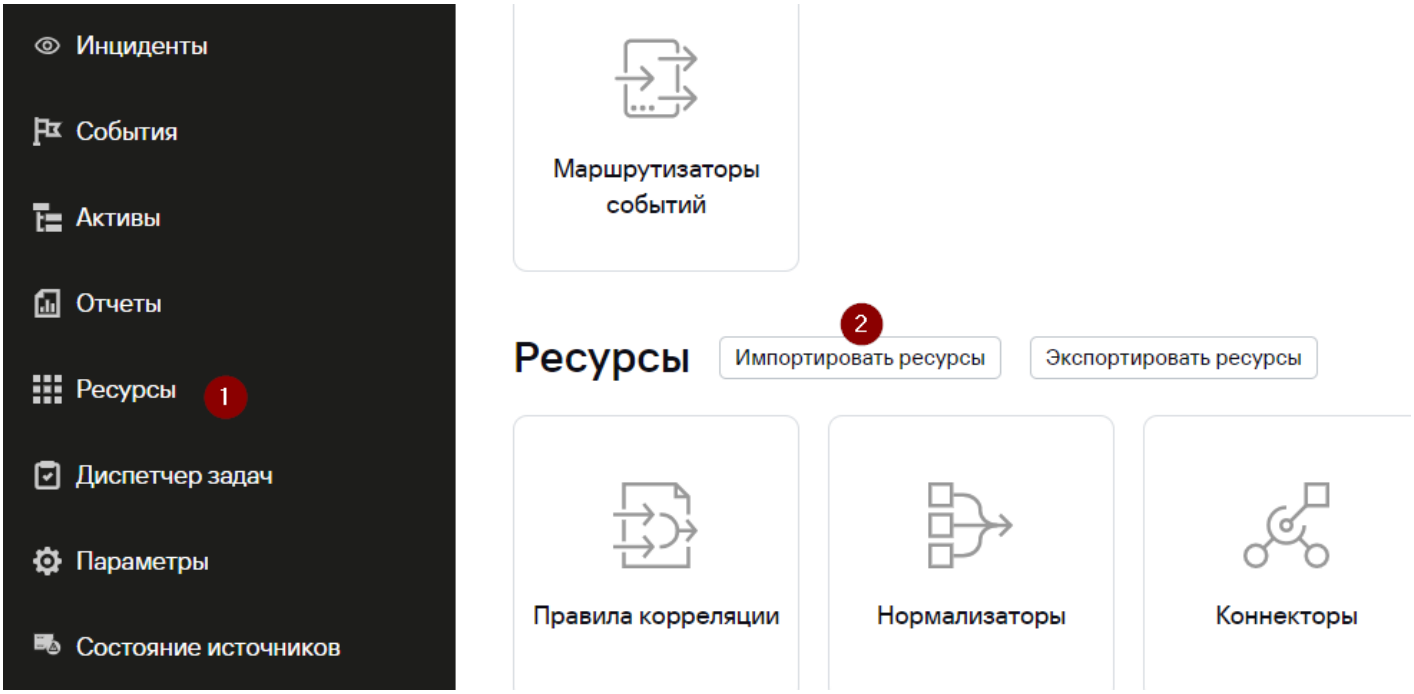
1. В Web-интерфейсе KUMA нужно настроить интеграцию с репозиторием



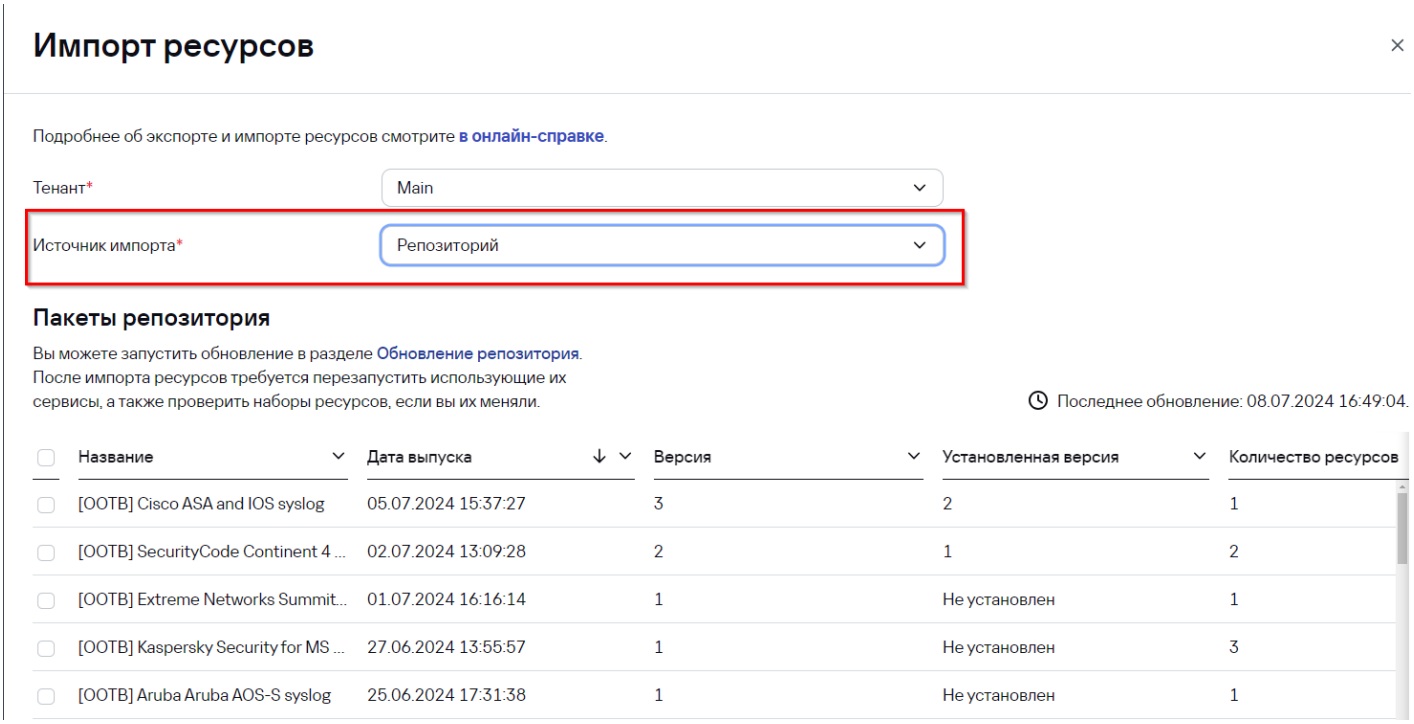
Список серверов, до которых нужно предоставить доступ с KUMA представлен в официальной документации: https://support.kaspersky.ru/common/start/6105

Для обновления напрямую с репозитория **НЕЛЬЗЯ** использовать Proxy для KUMA < 3.4. Если для доступа к репозиторию требуется использование Proxy или у KUMA нет доступа в Интернет напрямую, то следует использовать Kaspersky Update Utility (KUU). Подробнее в статье: https://kb.kuma-community.ru/books/ustanovka-i-obnovlenie/page/obnovlenie-resursov-s-pomoshhiu-kaspersky-update-utility-kuu

2. После настройки интеграции с репозиторием и Запуска обновления перейдите в Ресурсы и выберите Импортировать ресурсы



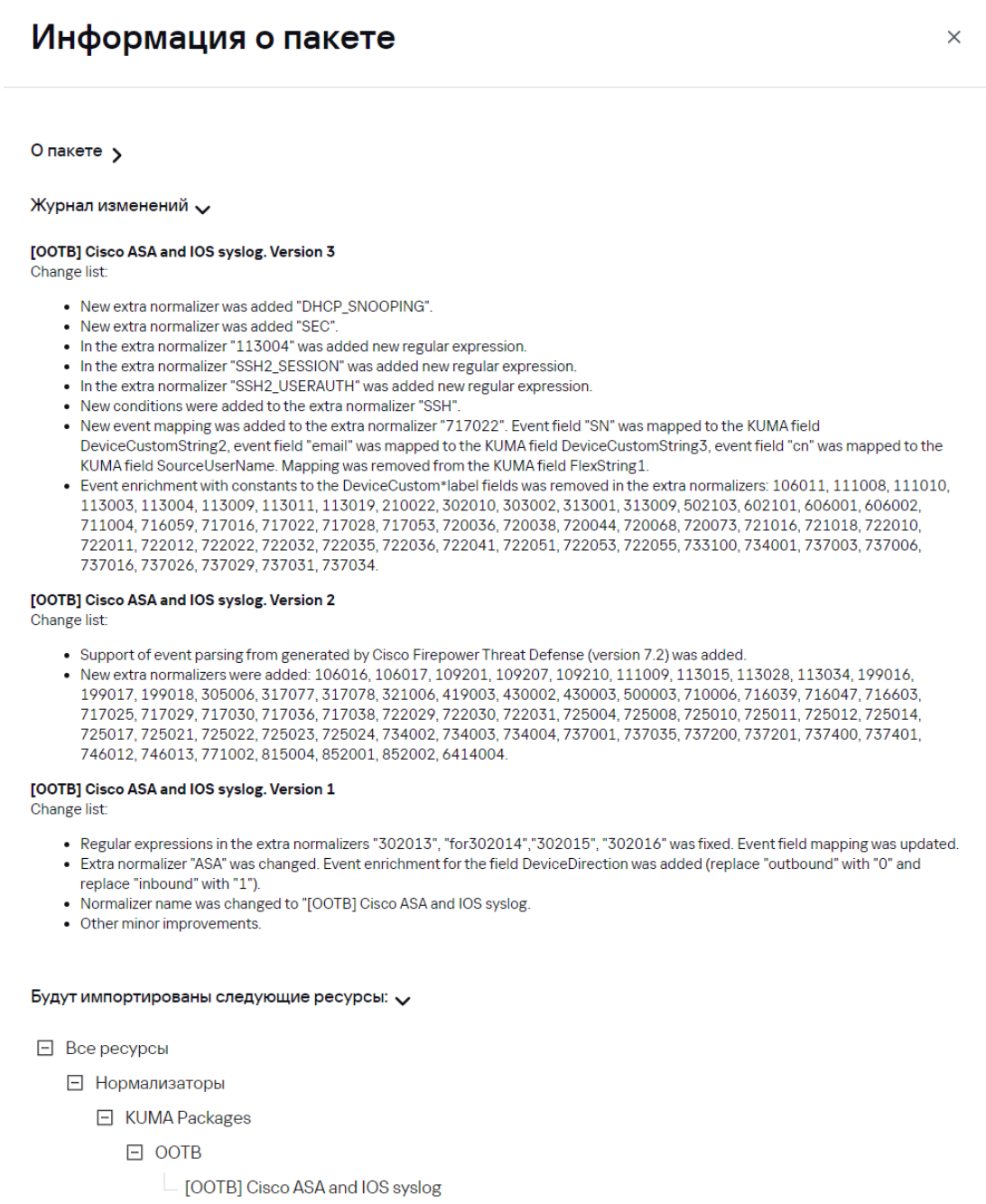
3. Далее выберите Репозиторий в качестве источника



> Контент в системе применяется сверху вниз, проверяйте, что выбирается к применению, чтобы иметь актуальный набор ресурсов

4. Нажав на имя конкретного пакета, вы увидите информацию о пакете, журнал изменений и перечень импортируемых ресурсов.

Информация о пакете



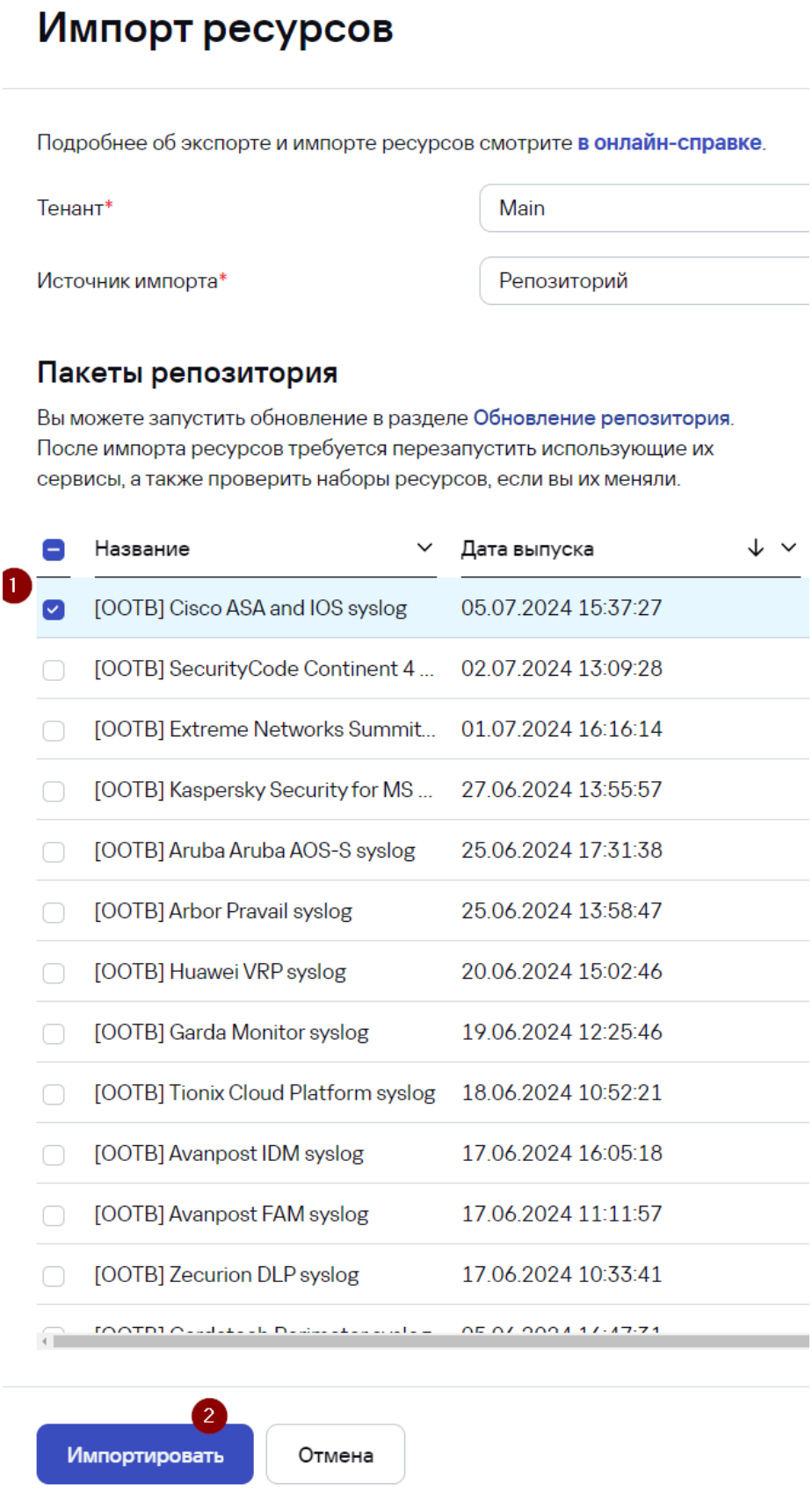
Пакеты для начальной установки

1. Щелкните на столбец Название в пакетах репозитория и отсортируйте по Возрастанию
2. Загрузите ресурс, например `[OOTB] KUMA 4.0 resources`, в соответствии с вашей версией KUMA
3. Для детектирования загрузите:
   - Правила корреляции - `[OOTB] SOC Content - RU`

- Правила корреляции мониторинг событий Kaspersky Security Center - `[OOTB] KSC Package - RU`
- Правила корреляции мониторинг событий Kaspersky Security Mail Gateway - `[OOTB] KSMG Package - RU`
- (Опционально) Правила корреляции, направленные на соблюдение требований стандарта PCI DSS. - `[OOTB] PCIDSS - RU`
- Правила поведенческого анализа - `[OOTB] UEBA package - RU`
- Правила для выявления аномалий в сетевой активности - `[OOTB] Network Package - RU`
- Правила межпродуктовые в рамках экосистемы Kaspersky - `[OOTB] XDR package - RU`
- Загрузите (с помощью кнопки Привязать) эти правила в имеющуюся службу коррелятора (встроенные правила OOTB удалите)

> Описание пакетов на странице справки
>
> https://support.kaspersky.com/help/KUMA/4.0/ru-RU/250594.htm

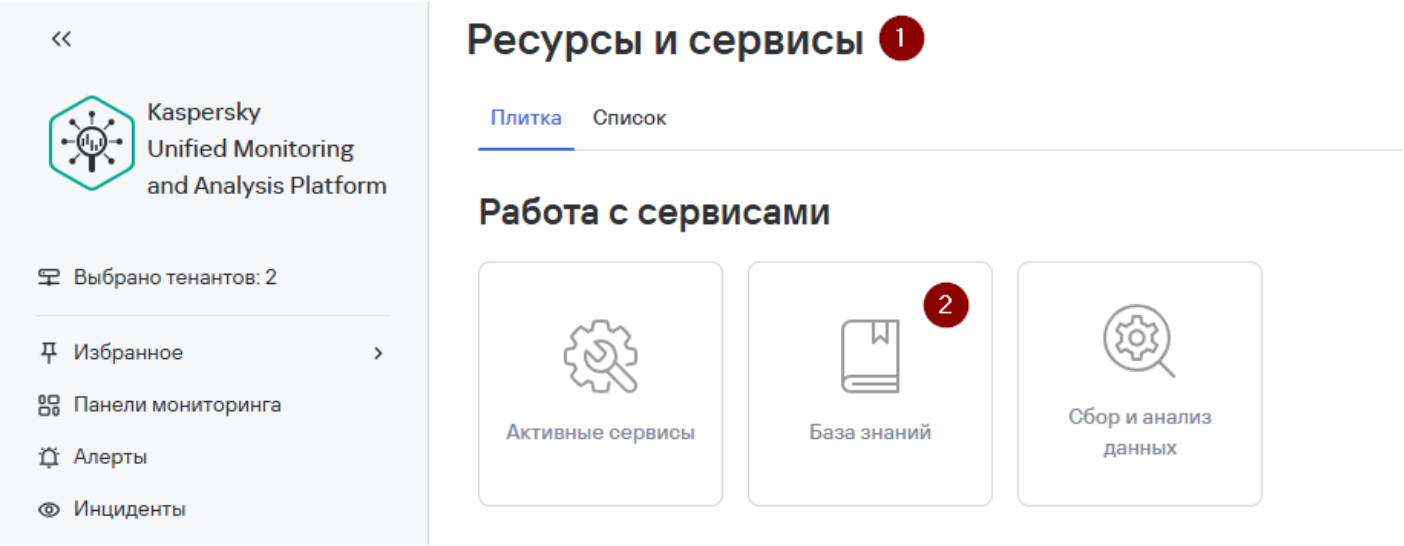
5. Для импорта интересующих ресурсов выберите один или несколько пакетов галочкой слева от имени пакета и нажмите Импортировать внизу окна



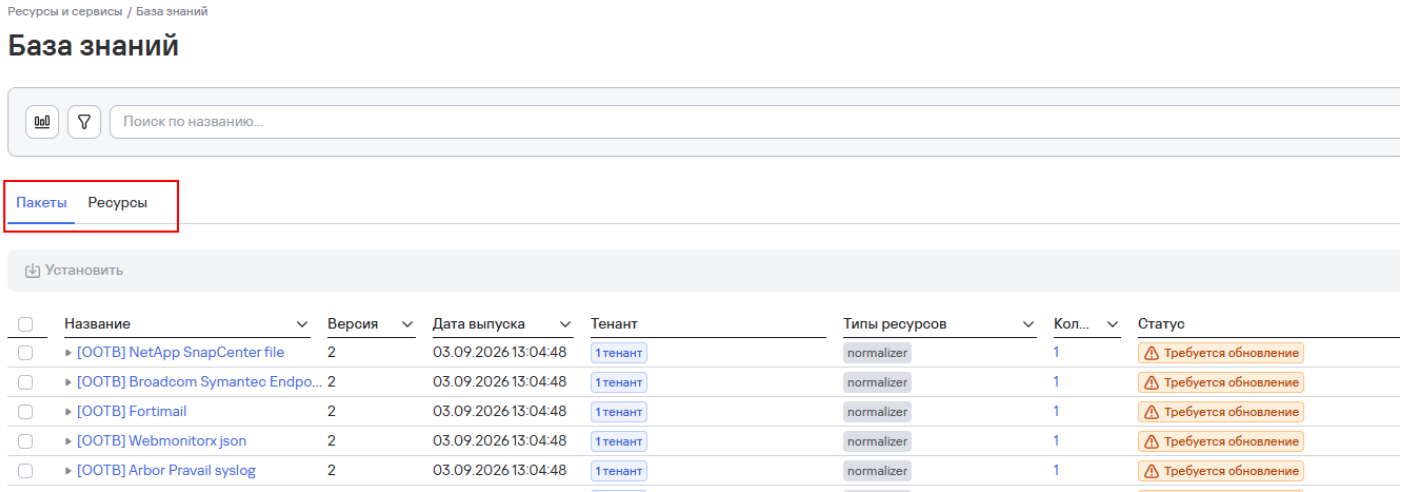
6. Выбранные ресурсы будут импортированы.

Импорт ресурсов для KUMA 4.6

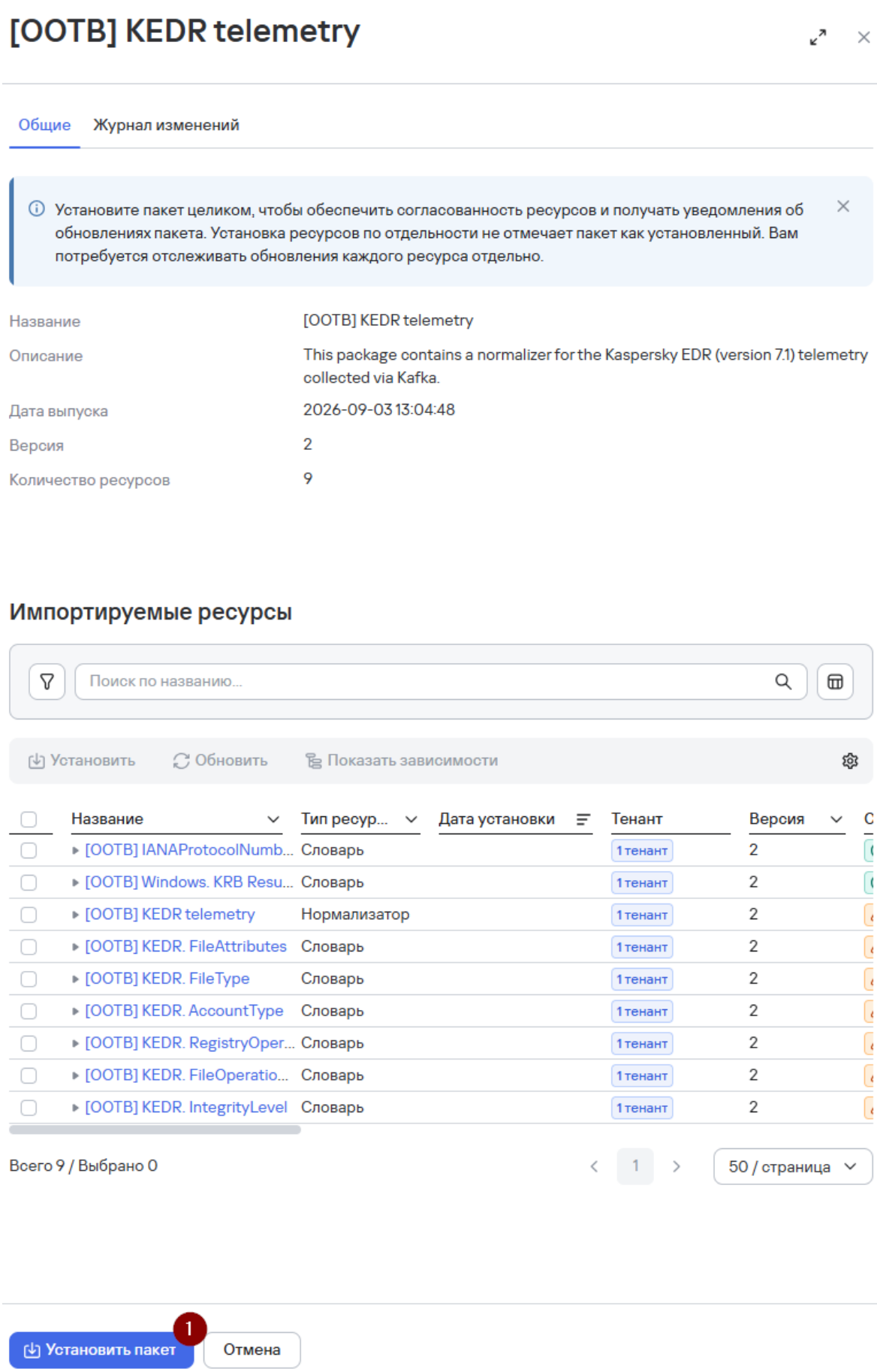
1. Перейдите в меню в "Ресурсы" -> "База знаний"



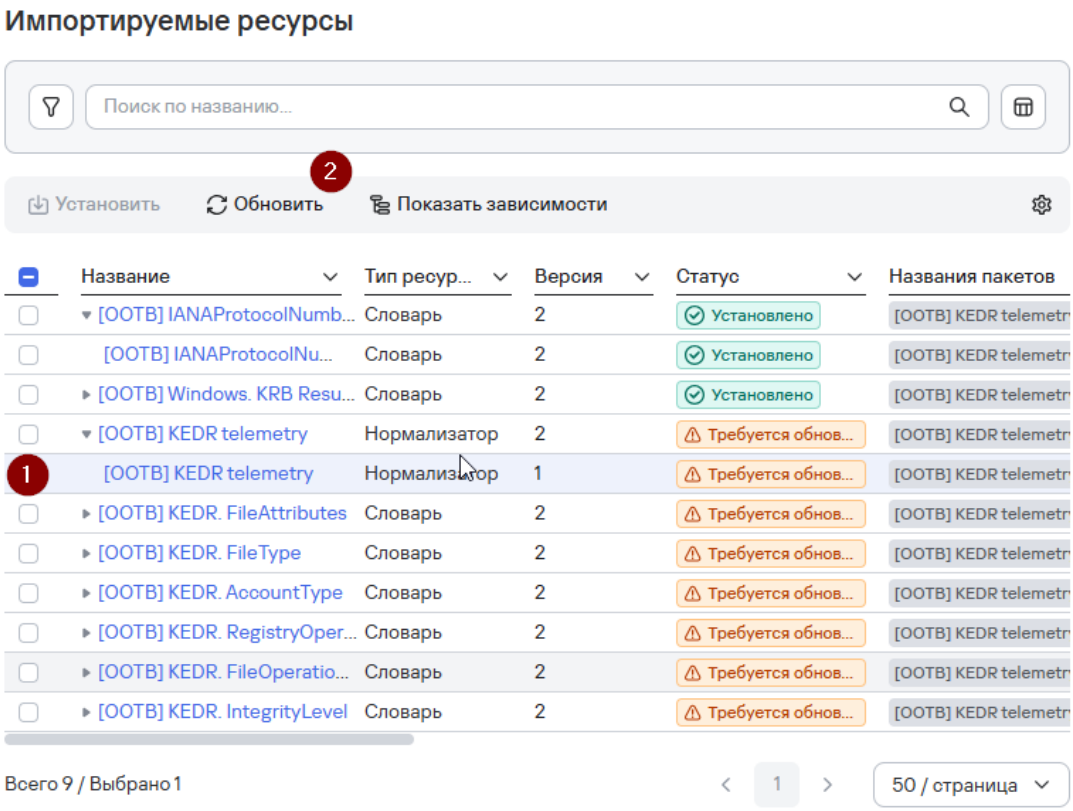
2. Внутри базы знаний вам будут доступны как собранные пакеты с разными типами ресурсов, так и отдельно каждый, если перейти во вкладку ресурсы.



3. Для установки нажмите на выбранный пакет/ресурс, далее "Установить пакет"/"Установить"

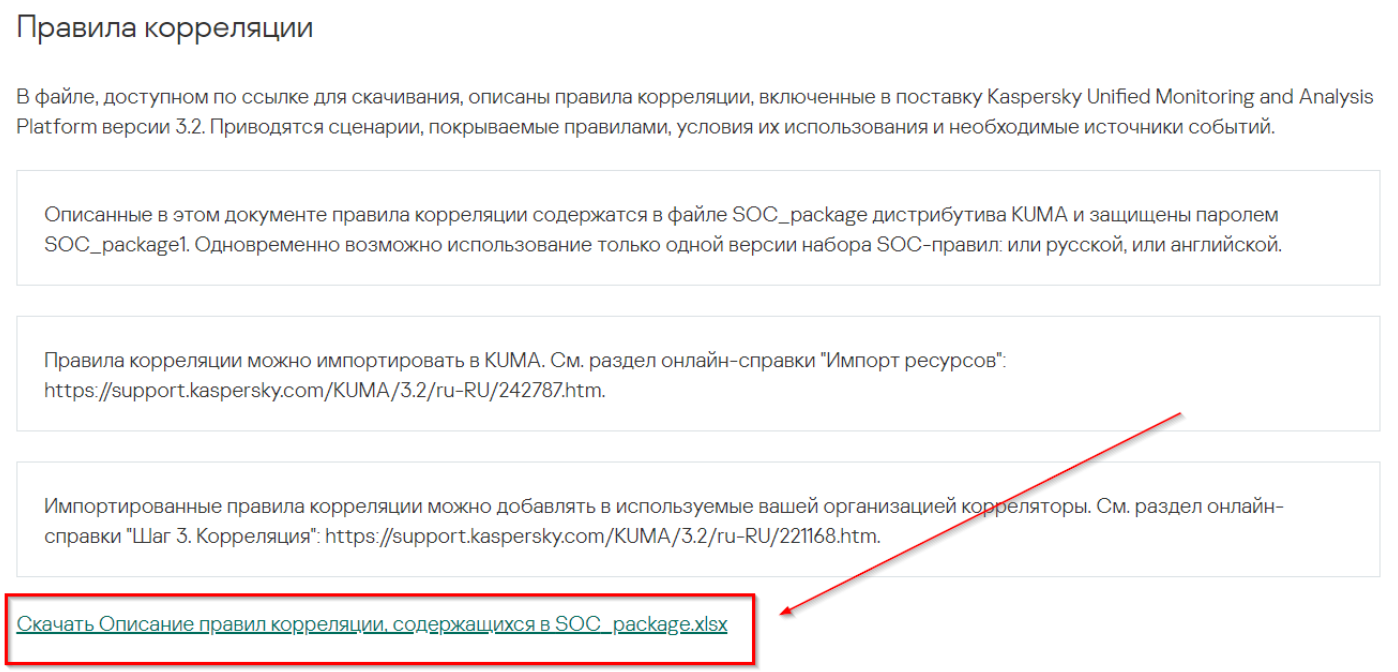


4. При необходимости обновления ресурса, выберите нужный, далее "Обновить"



Где взять описание правил из SOC Package?

> Описание правил из SOC Package можно скачать из официальной документации: https://support.kaspersky.com/help/KUMA/4.2/ru-RU/250594.htm



> Альтернативно, можно воспользоваться интерактивной библиотекой правил по **ссылке**

На что ориентируемся при разработке правил

Вширь:

- Покрытие матрицы MITRE
- Покрытие новых источников событий

Вглубь

- Отчет MDR Report
- Отчет IR Report (GERT)
- Отчет Threat Landscape Report
- Внутренняя экспертиза (EDR, MDR)

Ad-hoc

- Интересные публикации в блогах и телеграмм-каналах
- Замечания/предложения пользователей

Где взять мапинг коробочных нормализаторов?

>

Сопоставление полей коробочных нормализаторов можно скачать из официальной документации: https://support.kaspersky.com/help/KUMA/4.2/ru-RU/267237.htm

Приложения > Сопоставление полей предустановленных нормализаторов

Сопоставление полей предустановленных нормализаторов

В файле, доступном по ссылке для скачивания, представлено описание сопоставления полей предустановленных нормализаторов.

Скачать Описание сопоставления полей предустановленных нормализаторов.ZIP

Revision #19
Created 2024-07-08 14:03:27 UTC by Koala
Updated 2026-10-23 08:27:04 UTC by lerat