



Руководство  
по лицензированию

# Kaspersky Unified Monitoring and Analysis Platform

**kaspersky** активируй  
будущее



## Kaspersky Unified Monitoring and Analysis Platform



В случае если среднее значение превышает ограничение по EPS, указанное в лицензионном ключе, KUMA уведомляет об этом событии в интерфейсе.

А также, если за 7 дней работы KUMA среднее значение EPS превышало ограничение 30% времени и более, KUMA дополнительно отправляет на email-адрес администратора уведомление о превышении количества полученных событий и продолжает подсчёт среднего значения EPS, не блокируя функциональность.



По истечении лицензии блокируются все функции (создание и/или изменение контента SIEM, обработка новых событий, а также создание или изменение правил корреляции, нормализации, дашбордов, отчетов и пр.) за исключением просмотра информации по ранее собранным событиям.

## Модель лицензирования

Лицензирование продукта Kaspersky Unified Monitoring and Analysis Platform (KUMA) производится по среднему количеству обрабатываемых событий в секунду (EPS) за 24 часа. Одна лицензия равна 100 EPS, минимальное количество — 500 EPS.

### Подсчет событий идет после их обработки:

1

#### Событие отфильтровано

Событие, которое в результате обработки коллектором было отфильтровано как ненужное для дальнейшей обработки, учитывается как 0 событий при подсчете EPS

2

#### События агрегированы

События, которые в результате обработки коллектором были агрегированы в одно событие, учитываются как 1 событие при подсчете EPS

3

#### Событие не подошло

Событие, которое было обработано коллектором, но не подошло ни под один фильтр точек назначения, учитывается как 1 событие при подсчете EPS

4

#### Событие подошло под несколько фильтров

Событие, которое подошло под несколько фильтров точек назначения (в коррелятор и хранилище), учитывается как 1 событие при подсчете EPS

5

#### Событие не ушло в хранилище

Событие, которое подошло только под фильтр коррелятора и не ушло в хранилище, учитывается как 1 событие при подсчете EPS

Финальная стоимость продукта зависит в том числе от выбранных дополнительных модулей (Netflow support, GosSOPKA и TI), уровня технической поддержки (Premium, Premium Plus) и наличия у заказчика решения от другого производителя (тип лицензий cross-grade с включенной по умолчанию технической поддержкой уровня Premium). В качестве лицензии выписываются срочные ключи на один, два или три года.

Все лицензии KUMA поддерживают **отказоустойчивость** по умолчанию и не требуют отдельных модулей. Отказоустойчивость системы достигается за счёт встроенных механизмов маршрутизации данных.

| №      | Наименование лицензии                                                                              | Описание                                                                                                                                         | Тип лицензии и срок         | Band*     |
|--------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------|
| KL4032 | Kaspersky Unified Monitoring and Analysis Platform                                                 | <b>KUMA:</b><br>Основная лицензия                                                                                                                | <b>Base Premium</b>         | 5-9       |
|        |                                                                                                    |                                                                                                                                                  | 1 year                      | 10-14     |
|        |                                                                                                    |                                                                                                                                                  | 2 years                     | 15-19     |
|        |                                                                                                    |                                                                                                                                                  | 3 years                     | 20-24     |
| KL4034 | Kaspersky Unified Monitoring and Analysis Platform with Netflow support                            | <b>KUMA + Netflow:</b><br>Лицензия с поддержкой протокола Netflow                                                                                | <b>Base Premium Plus</b>    | 25-49     |
|        |                                                                                                    |                                                                                                                                                  | 1 year                      | 50-99     |
|        |                                                                                                    |                                                                                                                                                  | 2 years                     | 100-149   |
|        |                                                                                                    |                                                                                                                                                  | 3 years                     | 150-249   |
| KL4036 | Kaspersky Unified Monitoring and Analysis Platform, GosSOPKA compatible                            | <b>KUMA + GosSOPKA:</b><br>Лицензия с поддержкой модуля ГосСОПКА                                                                                 | <b>Premium Renewal</b>      | 250-499   |
|        |                                                                                                    |                                                                                                                                                  | 1 year                      | 500-999   |
|        |                                                                                                    |                                                                                                                                                  | 2 years                     | 1000-1499 |
|        |                                                                                                    |                                                                                                                                                  | 3 years                     | 1500-2499 |
| KL4038 | Kaspersky Unified Monitoring and Analysis Platform GosSOPKA compatible with Netflow support        | <b>KUMA + GosSOPKA + Netflow:</b><br>Лицензия с поддержкой модуля ГосСОПКА и протокола Netflow                                                   | <b>Premium Plus Renewal</b> | 2500-4999 |
|        |                                                                                                    |                                                                                                                                                  | 1 year                      | 5000+     |
|        |                                                                                                    |                                                                                                                                                  | 2 years                     |           |
|        |                                                                                                    |                                                                                                                                                  | 3 years                     |           |
| KL4048 | Kaspersky Unified Monitoring and Analysis Platform with TI                                         | <b>KUMA + TI:</b><br>Лицензия с поддержкой Threat Intelligence                                                                                   | <b>Cross-grade</b>          |           |
|        |                                                                                                    |                                                                                                                                                  | 1 year                      |           |
|        |                                                                                                    |                                                                                                                                                  | 2 years                     |           |
|        |                                                                                                    |                                                                                                                                                  | 3 years                     |           |
| KL4047 | Kaspersky Unified Monitoring and Analysis Platform with Netflow support and TI                     | <b>KUMA + Netflow + TI:</b><br>Лицензия с поддержкой протокола Netflow и поддержкой Threat Intelligence                                          |                             |           |
| KL4049 | Kaspersky Unified Monitoring and Analysis Platform GosSOPKA compatible with TI                     | <b>KUMA + GosSOPKA + TI:</b><br>Лицензия с поддержкой модуля ГосСОПКА и поддержкой Threat Intelligence                                           |                             |           |
| KL4051 | Kaspersky Unified Monitoring and Analysis Platform GosSOPKA compatible with Netflow support and TI | <b>KUMA + GosSOPKA + Netflow + TI:</b><br>Лицензия с поддержкой модуля ГосСОПКА, с поддержкой протокола Netflow и поддержкой Threat Intelligence |                             |           |

\* Количество EPS = Band×100. Например, band 5-9 = 500-900 EPS

# Описание модулей

## Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Решение класса SIEM (Security Information and Event Management), предназначенное для централизованного сбора, анализа и корреляции событий информационной безопасности с различных источников данных. Решение содержит единую консоль мониторинга, анализа и реагирования на угрозы ИБ, объединяя как решения «Лаборатории Касперского», так и сторонних производителей. Поддерживается развёртывание в режиме отказоустойчивости, при котором отказ одного или нескольких узлов не приводит к нарушению потоковой обработки событий и выявления инцидентов. Дополнительных лицензий и лицензионного ключа для отказоустойчивости не требуется.

## Netflow Support (Netflow)

События телеметрии о трафике, которые помогают в обнаружении аномалий на сетевом уровне и расследовании инцидентов. KUMA выполняет приём и обработку Netflow событий без ограничений, при этом данные Netflow не учитываются в счётчике EPS.

## GosSOPKA (ГосСОПКА)

Модуль, обеспечивающий возможность интеграции с технической инфраструктурой НКЦКИ (Национальный координационный центр по компьютерным инцидентам). Модуль ГосСОПКА позволяет передавать инциденты, выявленные SIEM «по требованию» (т. е. по явному указанию пользователя), в техническую инфраструктуру НКЦКИ через API и получать рекомендации по реагированию на эти инциденты. Модуль ГосСОПКА регулирует только взаимодействие с НКЦКИ по инцидентам.

## Threat Intelligence (TI)

В рамках данного модуля поставляются платформа для управления данными об угрозах Kaspersky CyberTrace и потоки данных об угрозах Kaspersky Threat Data Feeds. Наличие лицензии упрощает интеграцию потоков данных с KUMA для дальнейшего использования аналитики угроз в повседневной работе ИБ-служб. KUMA собирает журналы с различных устройств, ИТ-систем и ИБ-инструментов и отправляет данные о событиях с URL, IP-адресами и хешами в Kaspersky CyberTrace на анализ, который сопоставляет поступающие события с потоками данных об угрозах и отправляет данные об обнаруженных угрозах обратно в KUMA и Kaspersky CyberTrace Web. Аналитик ИБ получает оповещения об обнаруженных угрозах с дополнительным контекстом и может провести первоначальное расследование и инициировать процесс реагирования на основе полученного контекста.

Платформа взаимодействует с любыми типами потоков аналитических данных об угрозах («Лаборатории Касперского», других поставщиков, из открытых источников или иных каналов) в форматах JSON, STIX/TAXII, XML и CSV и поддерживает интеграции с рассылками НКЦКИ и бюллетенями ФинЦЕПТ. В рамках данного модуля доступны следующие **потоки данных об угрозах: Malicious URL, BotnetCnC URL и Phishing URL, IP reputation и Ransomware URL**. Использовать фиды и Kaspersky CyberTrace, приобретённые в рамках данного модуля, можно только для обогащения событий, получаемых KUMA (использовать их с другими SIEM-системами, а также для интеграции с системами других классов недопустимо).



В лицензию KUMA включены до 100 запросов в Kaspersky Threat Intelligence Portal и до 10 запросов Kaspersky Threat Analysis (Cloud Sandbox, Cloud Threat Attribution Engine, Similarity) для получения дополнительного контекста в ходе проведения расследования. Доступ предоставляется через запрос от аккаунт менеджера.

# Предлагаемая техническая поддержка

| Каналы связи                                          | Premium | Premium Plus |
|-------------------------------------------------------|---------|--------------|
| Company account (веб-портал, уведомления через почту) | ●       | ●            |
| Телефон                                               | ●       | ●            |

## Время реакции в зависимости от уровня критичности

|                          |          |          |
|--------------------------|----------|----------|
| Критический (24 / 7)     | 2 часа   | 0,5 часа |
| Высокий (в рабочие часы) | 6 часов  | 4 часа   |
| Средний (в рабочие часы) | 8 часов  | 6 часов  |
| Низкий (в рабочие часы)  | 10 часов | 8 часов  |

## Доступные услуги

|                                                                                           |    |                      |
|-------------------------------------------------------------------------------------------|----|----------------------|
| Программные исправления                                                                   | ●  | ●                    |
| Удаленное подключение для диагностики проблем                                             | ●  | ●                    |
| Постпроектная поддержка*                                                                  | ●  | ●                    |
| Частные исправления                                                                       | ●  | ●                    |
| Рекомендации по оптимизации                                                               | ●  | ●                    |
| Персональный технический аккаунт-менеджер (ТАМ)                                           | ●  | ●                    |
| Регулярные статус-встречи с ТАМ для анализа зарегистрированных инцидентов, связанных с ТП | ●  | Ежеквартальный отчет |
| Разработка нормализаторов для нестандартных источников событий                            | 10 | 20                   |

● Доступно      ● Отсутствует

\* Консультации по донстройке в среде заказчика проводятся только по продукту KUMA и при наличии информации об инфраструктуре и схеме развертывания продукта.