kaspersky

Лицензии типа Premium и Premium Plus для Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Программа технической поддержки

kaspersky

1. Общие условия

Настоящая программа поддержки определяет перечень и порядок оказания технической поддержки владельцу лицензий типа Premium или Premium Plus для решения Kaspersky Unified Monitoring and Analysis Platform (KUMA).

2. Определения

«Company Account» – web-система обработки инцидентов Службой Технической Поддержки Лаборатории Касперского (https://companyaccount.kaspersky.com)

«Продукт» – программа для ЭВМ, разработанная АО «Лаборатория Касперского».

«Пользователь» – юридическое лицо, имеющее действующую лицензию на использование Продукта, для которого будет оказываться техническая поддержка в соответствии с настоящей программой.

«Персональный Технический Менеджер (ПТМ)» - специалист технической поддержки Лаборатории Касперского, выполняющий роль персонального технического менеджера для клиентов-владельцев лицензии типа Premium Plus.

«Инцидент», «Запрос», «Обращение» – любое событие, сообщенное Пользователем, которое не является частью стандартного функционирования Продукта, и которое вызывает или может вызвать прерывание или снижение качества услуги, производимой Продуктом.

«Проблема» – основная неизвестная причина одного или более инцидентов. Становится известной ошибкой в случае, если корневая причина известна и найдено временное обходное решение или постоянная альтернатива.

«Известная ошибка» – проблема, корневая причина которой стала известна и найдено временное обходное решение или постоянная альтернатива.

«Продуктовая ошибка» – не декларируемое поведение продукта.

«Запрос на обслуживание» – запрос Пользователя на предоставление технической поддержки, информации, совета или документации в случаях, не касающихся некорректного функционирования или прерывания нормальной работы Продукта.

«Критичность инцидента» – означает меру бизнес-критичности инцидента, основанную на потребностях бизнеса Пользователя.

«Время реакции» – время, прошедшее с момента получения АО «Лабораторией Касперского» информации о любом инциденте до момента предоставления Пользователю квалифицированного ответа (посредством Company Account Пользователя на интернет-портале технической поддержки, электронной почты или телефона).

«Обновление» – выпуск АО «Лабораторией Касперского» модификации Продукта, обеспечивающей улучшение функциональности или производительности Продукта и/или содержащей новую функциональность или улучшения Продукта.

«Обходное решение» – процедура, посредством применения которой Пользователь может временно решить инцидент.

«Стандартный источник событий» – устройство или программное обеспечение одной конкретной версии, выполняющее регистрацию и отправку «сырых» событий информационной безопасности. Для стандартных источников событий в KUMA существует нормализатор событий, поддерживаемый Лабораторией Касперского.

«Нестандартный источник событий» – устройство или программное обеспечение одной конкретной версии, выполняющее регистрацию и отправку «сырых» событий информационной безопасности, для событий которого на текущий момент не существует нормализатор событий, поддерживаемый Лабораторией Касперского.

«Тип событий» - разновидность события, описывающая определенный вид поведения контролируемого элемента информационной инфраструктуры. При разработке нормализатора в качестве отдельного типа событий будут учитываться события, которые удовлетворяют хотя бы одному из следующих условий:

- событие требует отдельного типа парсера для разбора;
- событие требует отдельного regex-выражения для разбора;
- более половины полей события требуют настройки индивидуального сопоставления схеме событий KUMA (маппинга).

Как правило для отдельных типов событий вводится уникальный идентификатор, например, EventID в операционной системе Microsoft Windows).

«Нормализатор» – компонент системы, отвечающий за процесс нормализации (обработки) «сырых» событий, поступающих от источников событий. Один нормализатор обрабатывает события от одного устройства или программного обеспечения одной конкретной версии.

«Нормализация» – процесс приведения данных, составляющих событие, в соответствие с полями модели данных KUMA. Во время нормализации могут выполняться определенные преобразования данных по заданным правилам (например, символы верхнего регистра могут заменяться на символы нижнего регистра, определенные последовательности символов могут перезаписываться другими и т.п.).

«Коллектор» – компонент KUMA, который получает сообщения из источников событий, обрабатывает их и передает в хранилище, коррелятор и/или сторонние сервисы для выявления подозрений на инциденты ИБ (алерты).

«Коннектор» – компонент KUMA, обеспечивающий транспорт для приема данных из внешних систем.

«Событие» – случай активности сетевых устройств, прикладного программного обеспечения, средств защиты информации, операционных систем и иных устройств, который можно обнаружить и записать. Например, к событиям относятся: событие успешного входа пользователя, событие очистки журнала, событие отключения антивирусного ПО.

«Сырое событие» - событие, не прошедшее этап нормализации в KUMA.

«Панель мониторинга» – компонент системы KUMA, выполняющий визуализацию данных.

«Корреляционное правило» – ресурс KUMA, используемый для распознавания определенных последовательностей обрабатываемых событий и выполнения определенных действий после распознавания.

«Отчёт» – ресурс KUMA, используемый для формирования набора данных, удовлетворяющих критериям выборки фильтра, задаваемого пользователем.

3. Описание программы поддержки

Прием запросов

Прием и решение вопросов по эксплуатации продукта и запросов на устранение негативных последствий инцидентов ведётся посредством интернет-портала, телефона и электронной почты.

Интернет-портал

Kaspersky Company Account https://companyaccount.kaspersky.com - Интернет-Портал технической поддержки АО «Лаборатория Касперского», доступ к которому с возможностью размещения запросов предоставляется в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни).

Телефон

Приём запросов по телефону приоритетной выделенной линии предоставляется в режиме:

- 24x7x365 для запросов уровня критичности 1 для владельцев лицензии Premium;
- 24x7x365 для запросов уровня критичности 1 и 2, для владельцев лицензии Premium Plus;

- по рабочим дням с 10:00 по 18:30 (время Московское) для запросов уровня критичности 2, 3, 4.

Уровень критичности инцидента	Тип лицензии	
	Лицензия Premium	**Лицензия Premium Plus**
Уровень критичности 1	24x7	24x7
Уровень критичности 2	В будни с 10:00 по 18:30 (время Московское)	24x7
Уровень критичности 3	В будни с 10:00 по 18:30 (время Московское)	В будни с 10:00 по 18:30 (время Московское)
Уровень критичности 4	В будни с 10:00 по 18:30 (время Московское)	В будни с 10:00 по 18:30 (время Московское)

Электронная почта

Приём запросов по электронной почте предоставляется в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни) в случае невозможности создания запроса через Интернет-Портал, из-за его технической недоступности. Запросы, зарегистрированные через почту по умолчанию, имеют уровень критичности 4.

Обработка инцидентов

Обработка инцидентов через web

Web система обработки запросов Центра технической поддержки АО «Лаборатория Касперского» доступна по ссылке https://companyaccount.kaspersky.com.

Посредством данной системы АО «Лаборатория Касперского» предоставляет Пользователю:

- возможность использования персональной учетной записи Пользователя для создания, обновления и мониторинга инцидентов;
- техническую поддержку и консультации по решению инцидентов в процессе установки, конфигурирования и функционирования Продукта;
- техническую поддержку и консультации по лечению файлов, зараженных вредоносным ПО, и самостоятельному удалению вредоносного ПО с программно-аппаратных комплексов, защищенных Продуктом с установленными новейшими обновлениями Продукта и антивирусных баз данных.

Обработка инцидентов: поддержка по телефону

- Поддержка по телефону предоставляется АО «Лаборатория Касперского» только авторизованным сотрудникам Пользователя.

Время реакции на инциденты

АО «Лаборатория Касперского» гарантирует время реакции на обращения Пользователя в зависимости от типа приобретенной лицензии и в соответствии с временными рамками, соответствующими уровням срочности инцидента:

Уровень критичности инцидента	Время реакции	
	Лицензия Premium	**Лицензия Premium Plus**

Уровень критичности 1	2 часа*	30 минут*
Уровень критичности 2	6 рабочих часов*	4 часа*
Уровень критичности 3	8 рабочих часов	6 рабочих часов
Уровень критичности 4	10 рабочих часов	8 рабочих часов

* Необходимо дополнительное обращение по телефону для гарантированного времени реакции

Запросам Пользователей с лицензией Premium и Premium Plus присваивается более высокий приоритет относительно стандартных запросов Пользователей с базовой лицензией.

Уровень критичности инцидента определяется его категорией, выбранной Пользователем при первоначальном обращении (через выбор предустановленных категорий в Company Account). Уровни критичности инцидента 1 и 2 могут быть установлены через обращение по телефону.

АО «Лаборатория Касперского» имеет право впоследствии пересмотреть уровень критичности инцидента, если его описание будет соответствовать другому уровню. Перечень уровней критичности и их описания приведены в Приложении.

Управление качеством

Эскалация инцидентов и управление претензиями

Предъявление претензий и жалоб на качество обслуживания осуществляется согласно нижеследующей схеме:

	1	2
Уровень эскалации	Руководитель службы технической поддержки регионального офиса АО «Лаборатория Касперского»	Менеджер по работе с корпоративными клиентами (бизнес-контакт)

Пользователь может эскалировать нерешенные инциденты в случае, если инцидент находится «на стороне» АО «Лаборатория Касперского».

Контроль решения инцидентов

В любой момент времени инцидент может быть, как в работе у Пользователя (т.е. Пользователь предпринимает действия, способствующие решению инцидента АО «Лаборатория Касперского»), так и в работе в АО «Лаборатория Касперского».

Инцидент считается находящимся в работе у Пользователя, когда АО «Лаборатория Касперского» производит запрос дополнительной информации у Пользователя или предоставляет рекомендации, которые необходимо выполнить Пользователю. После того, как Пользователь предоставляет запрошенную информацию или дает обратную связь по рекомендациям, инцидент считается переданным в работу АО «Лаборатория Касперского». Время нахождения инцидента на стороне клиента не должно превышать 30 календарных дней. В случае превышения этого показателя, текущий инцидент автоматически закрывается.

АО «Лаборатория Касперского» несет ответственность только за время, в течение которого инцидент находился в работе в АО «Лаборатория Касперского».

kaspersky

Опции программы технической поддержки

Предоставление кодов программных коррекций продукта

В процессе исправления известных ошибок компанией АО «Лаборатория Касперского» Пользователю предоставляются общедоступные коды программных коррекций по мере их выпуска.

При обнаружении нестандартной проблемы (в том числе ошибок обновления, включая ошибки парсеров логов, а так же ошибок конфигурации системы), для которой отсутствует общедоступный код программной коррекции, Пользователь вправе запросить АО «Лаборатория Касперского» о выпуске частного решения – кода программной коррекции, специфичного для ситуации (конфигурации, версии, условий использования продукта) Пользователя.

АО «Лаборатория Касперского» организует работы по:

- Обработке запросов Пользователей на выпуск кодов общедоступных и частных коррекций;
- Информированию Пользователя о промежуточных результатах и ходе выполнения его запроса Персональным Техническим Менеджером для владельцев лицензии Premium Plus.

АО «Лаборатория Касперского» приложит коммерчески обоснованные усилия для выпуска частного кода программной коррекции. Коды программных коррекций выпускаются согласно политике поддержки продуктов на разных стадиях жизненного цикла приложения (актуальная версия доступна по ссылке http://support.kaspersky.ru/support/rules)
Условия использования кодов программных коррекций являются предметом лицензионного соглашения, заключенного между АО «Лаборатория Касперского» и Пользователем.

Удаленное подключение для диагностики проблемы

В случае необходимости сотрудники технической поддержки АО «Лаборатории Касперского» могут предложить Пользователю удаленное подключение для более детальной диагностики проблемы. Условия и время подключения оговариваются дополнительно в каждом конкретном случае.

Консультации по настройке и оптимизации

В рамках технической поддержки Пользователь имеет право на консультации по настройке своей продуктивной инсталляции Kaspersky Unified Monitoring and Analysis Platform (KUMA).

Рекомендации по оптимизации

Рекомендации по оптимизации производительности, архитектуры и настроек продукта в рамках инфраструктуры клиента предоставляются однократно в течение одного календарного года при наличии действующей программы технической поддержки.

Разработка нормализаторов для нестандартных источников событий

Ежегодно в рамках действующей лицензии на Kaspersky Unified Monitoring and Analysis Platform (KUMA) Пользователю могут быть разработаны и предоставлены нормализаторы для нестандартных источников событий в количестве, определённом в таблице ниже.

Тип лицензии	Premium	Premium Plus
Количество источников	**10**	**20**

Разработка нормализаторов осуществляется при условии, если от источника событий поступает не более 50 типов событий. Если количество типов событий превышает 50 для одного источника, такой источник считается в двойном (либо тройном) размере (как 2 или 3 источника), в зависимости от количества типов событий.

Когда количество источников, предоставленных в рамках премиальной лицензии, использовано полностью, Пользователь может отдельно докупить услугу профессионального сервиса для разработки нормализаторов для дополнительных источников событий.

Разработка нормализаторов для нестандартных источников, использующих транспортные протоколы(коннекторы), не поддерживаемые KUMA, не выполняется.

Дополнительные привилегии Пользователям лицензии типа Premium Plus

Персональный Технический Менеджер (ПТМ)

Персональный технический менеджер (ПТМ) назначается АО «Лаборатория Касперского» с целью организации единого канала взаимодействия с пользователем. ПТМ является сотрудником компании-производителя и управляет обработкой всех инцидентов Пользователя лицензии типа Premium Plus. В обязанности технического менеджера входит:

- организация работ по технической поддержке специалистами АО «Лаборатория Касперского» для решения технических инцидентов;
- информирование Пользователя о текущем состоянии решения запросов, предоставление ежеквартальной отчётности;
- контроль выполнения задач и обеспечение своевременных эскалаций при обработке инцидентов в процессе оказания технической поддержки;
- поддержка ИТ-департамента Пользователя в понимании и правильном использовании предоставленных рекомендаций;
- проведение совместно с Пользователем регулярного анализа и согласование действий необходимых для решения технических и операционных инцидентов.

ПТМ гарантированно доступен по рабочим дням с 10:00 до 18:30 (время Московское) по телефону, электронной почте и мобильному телефону. В случае недоступности ПТМ (в ночное время и нерабочие дни), запросы Пользователя переадресуются заменяющему на линию технической поддержки.

Пользователь должен сообщить АО «Лаборатория Касперского» имена и контактную информацию сотрудников, назначенных для взаимодействия с ПТМ (контактное лицо) и предоставить их контактную информацию (в частности, адрес электронной почты и номер телефона), посредством которой с контактными лицами или полномочным представителем данного лица можно взаимодействовать во время работ над инцидентами.

Предоставление отчетов

В процессе решения инцидентов АО «Лаборатория Касперского» сделает все возможное для своевременного предоставления информации о статусе открытых инцидентов Пользователю в соответствии с графиком, указанном в нижеследующей таблице.

Уровень критичности	График предоставления отчетов
Уровень критичности 1	По договоренности, но не чаще, чем раз в день (по электронной почте или по телефону)
Уровень критичности 2	В рамках регулярного отчета
Уровень критичности 3	
Уровень критичности 4	

Пользователь имеет право на регулярные статус-звонки с ПТМ-ом и предоставление ежеквартального отчета для ретроспективного анализа зарегистрированных инцидентов, связанных с технической поддержкой.

ПТМ также может предоставлять отчетность качества оказания сервиса и выполнение обязательств при запросе клиента по мере необходимости.

Дополнительные условия поддержки

Для регистрации инцидентов, владелец лицензии типа Premium и Premium Plus, должен предоставить список контактных лиц, имеющих право открывать заявки на оказание технической поддержки.

Количество авторизованных лиц варьируется в зависимости от типа лицензии:

	Лицензия Premium	Лицензия Premium Plus
Количество авторизованных лиц	4	8

Список контактных лиц со стороны Пользователя должен быть определен и предоставлен в техническую поддержку при первом обращении. Для изменения списка контактных лиц Пользователь должен оформить запрос через Company Account. В ответ на запрос об изменении списка контактных лиц, АО Лаборатория Касперского предоставит пользователю обновленный список контактов.

Некоторые инциденты могут потребовать воссоздания условий возникновения инцидента в АО «Лаборатория Касперского» с целью проведения тестирования и верификации вирусного заражения или наличия продуктовой ошибки.

Пользователь обязан предоставить АО «Лаборатория Касперского» всю необходимую информацию и специфическое программное или аппаратное обеспечение необходимое для воспроизведения условий возникновения инцидента в случае, если необходимое программное и/или аппаратное обеспечение отсутствует у АО «Лаборатория Касперского».

АО «Лаборатория Касперского» приложит все необходимые усилия для воспроизведения инцидента, как только будет доступна вся необходимая информация, а также программное и/или аппаратное обеспечение. В случае невозможности воспроизведения условий возникновения инцидента Пользователь обязан предоставить сотрудникам АО «Лаборатория Касперского» доступ к инфицированным системам удаленно.

В случае если инцидент не может быть воспроизведен ни одной из сторон, или клиент не предоставил доступ к рабочему окружению, где инцидент может быть воспроизведен, или установлено, что Продукт не является источником инцидента, инцидент не может быть классифицирован в рамках данной программы поддержки.

Ограничения программы поддержки

В случае приобретения Заказчиком Продуктов с разными типами лицензий, условия поддержки, описанные в данной программе, предоставляются только в отношении тех Продуктов заказчика, которые имеют тип лицензии Premium или Premium Plus.

Техническая поддержка не оказываются в случае возникновения перечисленных ниже инцидентов:

- инциденты, уже решенные для Пользователя (т.е., если возникли инциденты на установленной копии Продукта после того, как аналогичные инциденты были решены для другой копии Продукта);
- поиск и устранение проблем аналогичных или идентичных уже решенным (т.е. инцидентов, для решения которых может быть применено решение предыдущих инцидентов с предоставлением дополнительных инструкций АО «Лаборатория Касперского»);
- инциденты, вызванные неполадками аппаратного обеспечения Пользователя;

- инциденты, возникшие на неподдерживаемых версиях программных платформ (например, на бета-версиях программных платформ, версиях новых пакетов обновлений или дополнений, не одобренных АО «Лаборатория Касперского» в качестве совместимых с Продуктами);
- инциденты, вызванные установкой и запуском сторонних приложений (включая, но не ограничиваясь, списком неподдерживаемого или несовместимого программного обеспечения, указанного в документации или на сайте АО «Лаборатория Касперского»);
- инциденты, о которых Пользователь не может предоставить точную информацию, обоснованно запрошенную АО «Лаборатория Касперского» с целью воспроизведения, расследования и решения инцидента;
- инциденты, возникшие в результате неприменения или неправильного применения инструкций или документации АО «Лаборатория Касперского», в случае правильного использования, которых, возникновение инцидента было бы невозможно.

Предоставление профессиональных сервисов

В качестве дополнительных профессиональных сервисов, не входящих в данное предложение, Пользователь может приобрести право на предоставление профессионального сервиса по следующим направлениям развития KUMA:

- разработка нормализаторов для не стандартного источника событий;
- подключение стандартных источников событий;
- разработка корреляционных правил;
- доработка коробочных правила (с целью оптимизации работы в инфраструктуре Пользователя);
- разработка панелей мониторинга;
- разработка отчётов;
- настройка сетевой модели;
- разработка технической проектной документации.

Также в качестве дополнительных профессиональных сервисов, не входящих в данное предложение, Пользователь может приобрести услуги обзора архитектуры развертывания продуктов Лаборатории Касперского, а также консалтинговые услуги по разработке процессной, операционной и организационной моделей SOC, технической архитектуры, специфических сценариев обнаружения и реагирования SOC, а также правил корреляции.

Подробное описание консалтинговых сервисов SOC предоставляется по запросу. Пожалуйста, обратитесь к вашему аккаунт-менеджеру или партнерскому менеджеру. Условия и сроки оказания сервиса обсуждаются дополнительно, но не менее чем за 2 (две) недели до срока оказания.

4. Приложение

Уровни критичности инцидентов, относящихся к продукту.

«Уровень критичности 1» (критический) означает критическую проблему с Продуктом, влияющую на работоспособность Продукта или операционных систем Пользователя, или вызывающую потерю данных, при этом обходное решение отсутствует.

Перечень инцидентов, связанных с Продуктом и соответствующих Уровню критичности 1, включает в себя следующие инциденты:

- продукт полностью не работоспособен: не удаётся запустить сервисы Продукта;
- полностью прекращён и не осуществляется сбор событий ИБ.

«Уровень критичности 2» (высокий) означает проблему высокого уровня критичности, вызывающую воздействие на функциональность Продукта, но не вызывающую повреждение / потерю данных или полного прерывания работоспособности программного обеспечения. Уровень критичности 1 рассматривается, как Уровень критичности 2, когда известно обходное решение.

Перечень инцидентов, связанных с Продуктом и соответствующих Уровню критичности 2, включает в себя следующие инциденты:

- не работают все корреляционные правила;
- не работает более 70% коллекторов, осуществляющих сбор событий ИБ.

«Уровень критичности 3» (средний) означает некритичную проблему или запрос на обслуживание, не вызывающие отказ в обслуживании Продукта.

Перечень инцидентов, соответствующих Уровню критичности 3, включает в себя следующие инциденты:

- не работают единичные внутренние ресурсы Продукта (корреляционные правила, панель мониторинга, отчёт);
- не работает до 30% коллекторов, осуществляющих сбор событий ИБ.

«Уровень критичности 4» (низкий) означает другие некритичные запросы на обслуживание. Все инциденты, не упомянутые выше, относятся к этому уровню критичности.

www.kaspersky.ru/
www.securelist.ru