kaspersky

Лицензии типа Successive для Kaspersky Container Security for Managed Kubernetes (KL4250RHRMG)

Программа технической поддержки

Содержание

Общие условия

Настоящая программа поддержки определяет перечень и порядок оказания технической поддержки владельцу лицензий на Продукт Kaspersky Container Security for Managed Kubernetes KL4250RHRMG (Kaspersky Container Security Advanced Russian Edition) Лаборатории Касперского типа Successive.

Определения

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

«Продукт» – Kaspersky Container Security for Managed Kubernetes KL4250RHRMG (Kaspersky Container Security Advanced Russian Edition) - 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.

«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.

«Вирусная эпидемия» – кризисная ситуация у Пользователя, возникшая в случае, если вирус не может быть обнаружен Продуктом при применении актуальных антивирусных баз данных, и исполняемые модули вируса негативно воздействуют на непрерывность бизнеса Пользователя.

«Вирусный инцидент / Инцидент, связанный с вредоносным ПО» – инцидент, не связанный с Продуктом, но связанный с необходимостью предоставления Пользователю специфических утилит, удаляющих вредоносное ПО, и/или рекомендаций по удалению и описаний вредоносного ПО.

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

«Время реакции» – время, прошедшее с момента получения «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 «Лабораторией Касперского» антивирусной базы данных с новыми сигнатурами вирусов или модификациями 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.

«Ложное срабатывание» – ситуация, когда Продукт ошибочно воспринимает неинфицированный файл, как инфицированный.

Описание программы поддержки

Прием запросов

Прием и решение вопросов по эксплуатации продукта и запросов на устранение негативных последствий инцидентов ведётся посредством интернет-портала и/или телефона и/или 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 Successive для Kaspersky Container Security for Managed Kubernetes (KL4250RHRMG);
- по рабочим дням с 10:00 по 18:30 (время Московское) для запросов уровня критичности 2, 3, 4.

Уровень критичности инцидента	
Уровень критичности 1	24x7
Уровень критичности 2	В будни с 10:00 по 18:30 (время Московское)
Уровень критичности 3	В будни с 10:00 по 18:30 (время Московское)
Уровень критичности 4	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.

Обработка инцидентов

Обработка инцидентов через web

Web система обработки запросов Центра технической поддержки «Лаборатории 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 «Лабораторией Касперского» только авторизованным сотрудникам Пользователя.

Время реакции на инциденты

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

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

* В нерабочее время, в т. ч. во время выходных и праздников, необходимо обращение по телефону

Запросам Пользователей с лицензией Successive для Kaspersky Container Security for Managed Kubernetes (KL4250RHRMG) 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 уровней в Company Account).

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 «Лаборатории Касперского»	Менеджер по работе с корпоративными клиентами (бизнес-контакт)

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

Контроль решения инцидентов

В любой момент времени инцидент может быть как «на стороне» Пользователя (т.е. Пользователь предпринимает действия, способствующие решению инцидента «Лабораторией Касперского»), так и «на стороне» «Лаборатории Касперского».

Инцидент считается находящимся «на стороне» Пользователя, когда АО «Лаборатория Касперского» производит запрос дополнительной информации у Пользователя. После того, как Пользователь предоставляет запрошенную информацию, инцидент считается переданным в работу «Лаборатории Касперского». Время нахождения инцидента на стороне Пользователя не должно превышать 30 календарных дней. В случае превышения этого показателя, текущий инцидент автоматически закрывается.

Время, в течение которого инцидент находился «на стороне» (в работе) Пользователя – не засчитывается во время реакции, либо общее время работы «на стороне» «Лаборатории Касперского».

Обновление антивирусных баз по запросу пользователя при возникновении вирусного инцидента или ложной тревоги

В случае «ложной тревоги», ошибочном детектировании Продуктом инфицированного файла как неинфицированного, или в обратном случае, при условии, что Пользователем установлены новейшие обновления и антивирусные базы данных, Пользователь может потребовать внесения изменений в базы антивирусных описаний Продукта. АО «Лаборатория Касперского» обеспечивает предоставление Пользователю Обновления Баз, в котором данный файл будет верно детектироваться.

АО «Лаборатория Касперского» организует работы по:

- Обработке запросов, связанных с выпуском антивирусных баз, выделенной группой специалистов, действующих в режиме 24x7x365
- Приоритетному (ускоренному) выпуску обновления для Пользователей владельцев лицензии Successive для Kaspersky Container Security for Managed Kubernetes (KL4250RHRMG)

Дополнительные условия поддержки

Для регистрации инцидентов, владелец лицензии типа Successive для Kaspersky Container Security for Managed Kubernetes (KL4250RHRMG), должен предоставить список контактных лиц, имеющих право открывать заявки на оказание технической поддержки.

Пользователь имеет право назначить до 4 (четырех) контактных лиц, имеющих право открывать заявки на оказание услуг технической поддержки. 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 разумно возможные и 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 (рабочему окружению) удаленно.

В случае, если инцидент не может быть воспроизведен ни одной из сторон, или Пользователь 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

Лаборатория Касперского вправе отказать в премиальной технической поддержке в случае приобретения Пользователем разных типов лицензий для одного Продукта. В таком случае Пользователю будет предоставляться поддержка в соответствии с правилами предоставления поддержки для базовых лицензий, размещенных на http://support.kaspersky.com

В случае приобретения Пользователем Продуктов с разными типами лицензий, условия поддержки, описанные в данной программе, предоставляются только в отношении тех Продуктов Пользователя, которые имеют тип лицензии Successive для Kaspersky Container Security for Managed Kubernetes (KL4250RHRMG).

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 «Лаборатории 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 «Лабораторией 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 «Лаборатории Касперского»);
- инциденты, о которых Пользователь не может предоставить точную информацию, обоснованно запрошенную «Лабораторией Касперского» с целью воспроизведения, расследования и решения инцидента;
- инциденты, возникшие в результате неприменения или неправильного применения инструкций «Лаборатории Касперского» или документации «Лаборатории Касперского», в случае правильного использования которых возникновение инцидента было бы невозможно;
- инциденты, возникшие на виртуальных машинах или серверах, на которых установлен Продукт (например, переполнение жесткого диска, возникшее не по вине Продукта, отсутствие сетевой связности между виртуальными машинами и/или сетью Интернет, нехватка ресурсов в случае их выделения в меньшем количестве, чем указано в Аппаратных и программных требованиях);
- инциденты, возникшие со сторонним программным обеспечением, установленным Пользователем самостоятельно (например, Zabbix, Syslog Server, Open Stack);
- инциденты, вызванные развертыванием и использованием продукта за пределами сервиса Yandex Managed Service for Kubernetes (https://yandex.cloud/ru/services/managed-kubernetes).

Правовые ограничения

1. Пользователь понимает, что его компьютерные системы должны соответствовать минимальным требованиям по аппаратному обеспечению, которые указаны в сопроводительных инструкциях и иметь достаточный доступ в Интернет.
2. Пользователь обязан регулярно (как правило, ежедневно) делать резервные копии своих данных. В случае утраты данных по вине «Лаборатории Касперского»), последняя несёт ответственность только за восстановление данных на основе предоставленных Пользователем резервных копий и при условии регулярного резервного копирования.
3. Пользователь подтверждает, что у него есть в наличии активные подписки или лицензии на ПО третьих лиц, которое используется в связи с оказанием услуг по настоящей Программе.
4. Оказание услуг по настоящей Программе может потребовать доступа к аппаратному или программному обеспечению, которое не производится «Лабораторией Касперского». Гарантии некоторых производителей могут утратить силу, если «Лаборатория Касперского» или кто-либо другой, кроме производителя, будет работать с аппаратным или программным обеспечением.

Пользователь несет ответственность за то, чтобы выполнение услуг по Программе не повлияло на такие гарантии или, если повлияет, чтобы это влияние было приемлемым для Пользователя.

5. **Ограниченный Контент.** Пользователь не должен предоставлять «Лаборатории Касперского» какой-либо Контент, который: (a) Пользователь не имеет права предоставлять «Лаборатории Касперского»; (b) представляет собой любую медицинскую информацию; (c) содержит финансовую информацию любого лица; или (d) иным образом запрещена законом или подзаконными актами.
6. «Лаборатория Касперского» предоставляет поддержку добросовестно в соответствии с общепринятыми отраслевыми стандартами и использует соответствующий квалифицированный персонал.
7. Для оказания услуг «Лаборатории Касперского» вправе использовать аффилированных лиц и субподрядчиков.
8. Пользователь подтверждает свое участие в исследовании отзывов Пользователей по просьбе «Лаборатории Касперского».
9. «Лаборатория Касперского» несёт ограниченную ответственность за ущерб, причинённый умышленными действиями и грубой небрежностью и в случае невыполнения «Лабораторией Касперского» своих обязательств, она по своему выбору:
   (i) устранит такое нарушение и/или
   (ii) прекратит оказание услуг и вернет ту часть любых полученных средств, которая соответствует такому невыполнению.

СТОРОНЫ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ КОСВЕННЫЕ УБЫТКИ (ВКЛЮЧАЯ, В ЧАСТНОСТИ, ПОТЕРЮ ПРИБЫЛИ, ДОХОДОВ, ДАННЫХ, ОПЕРАЦИОННЫЙ ПРОСТОЙ).

Настоящие Условия и любые споры или требования, возникающие из них или в связи с ними, их предметом или порядком заключения (включая внедоговорные споры или требования), регулируются и толкуются в соответствии с материальным правом России. Каждая из сторон безоговорочно соглашается с тем, что арбитражный суд г. Москвы обладает исключительной юрисдикцией в отношении любых споров или претензий, возникающих из настоящего договора или в связи с ним, его предмета или порядка формирования (включая внедоговорные споры или претензии).

Приложение

Уровни критичности инцидентов, относящихся к продукту

«Уровень критичности 1» (критический) означает критическую проблему с Продуктом, влияющую на непрерывность бизнеса Пользователя посредством прерывания работоспособности Продукта или операционных систем Пользователя, или вызывающую потерю данных, установку стандартных настроек Пользователя в небезопасный режим или возникновение других проблем с безопасностью, при этом обходное решение отсутствует.

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

- вся локальная сеть (или критичная часть сети) не работает, что прерывает основные бизнес-процессы.

«Уровень критичности 2» (высокий) означает проблему высокого уровня критичности, вызывающую воздействие на функциональность Продукта, но не вызывающую повреждение/ потерю данных или прерывание 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:

- продукт полностью выведен из строя, но непрерывность основных бизнес-процессов не нарушается.

«Уровень критичности 3» (средний) означает некритичную проблему или запрос на обслуживание, не затрагивающие функциональность Продукта.

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

- продукт частично выведен из строя (работает несоответствующим образом), но другое программное обеспечение Пользователя не выведено из строя в результате работы Продукта.

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

Уровни критичности вирусных инцидентов

«Уровень критичности 1» (критический) означает вирусную эпидемию, влияющую на непрерывность бизнеса Пользователя посредством прерывания работоспособности Продукта или операционных систем Пользователя, или вызывающую потерю данных, при этом обходное решение отсутствует.

Перечень инцидентов, связанных с вредоносным программным обеспечением и соответствующих Уровню критичности 1, включает в себя (но не ограничивается) следующие инциденты:

- вся локальная сеть (или критичная часть сети) не работает;
- вирусная эпидемия;
- ложная тревога для файлов, входящих в критичные для бизнеса системы.

«Уровень критичности 2» (средний) означает проблему среднего уровня критичности, не вызывающую повреждение/ потерю данных или прерывание работоспособности программного обеспечения. Уровень критичности 1 рассматривается, как Уровень критичности 2, когда известно обходное решение.

Перечень инцидентов, связанных с вредоносным программным обеспечением и соответствующих Уровню критичности 2, включает в себя (но не ограничивается) следующие инциденты:

- инфицирование нескольких некритичных узлов сети;
- ложная тревога для файлов, входящих в некритичные для бизнеса системы.

kaspersky

www.kaspersky.ru/