

kaspersky

**Правила оказания
технической поддержки
для продуктов линейки
Kaspersky Industrial
CyberSecurity Enterprise**

Программа технической поддержки

1. Общие условия

Настоящая программа поддержки определяет перечень и порядок оказания услуг технической поддержки владельцу лицензии продуктовой линейки Kaspersky Industrial CyberSecurity Enterprise.

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 продуктов линейки Kaspersky Industrial CyberSecurity Enterprise.

«Инцидент» – 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.

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

«Ошибка продукта» – 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 технологического процесса 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 или технологического процесса 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.

«Ложная тревога» – ситуация, когда Продукт ошибочно воспринимает неинфицированный файл, как инфицированный.

3. Описание программы технической поддержки

Техническое консультирование по вопросам эксплуатации Kaspersky Industrial CyberSecurity и приём запросов на устранение негативных последствий инцидентов посредством:

- Предоставления доступа Пользователю к Интернет-Порталу технической поддержки АО «Лаборатория Касперского» с возможностью размещения запросов в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни)
- Приёма запросов по телефону приоритетной выделенной линии в режиме:
 - 24x7x365 для запросов уровня критичности 1-2;
 - по рабочим дням с 10:00 по 18:30 (время Московское) для запросов уровня срочности 3-4.
- Приёма запросов по электронной почте 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 «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

«Лаборатория Касперского» гарантирует время реакции на обращения Пользователя в соответствии с временными рамками, соответствующими уровням срочности инцидента:

Уровень критичности	Время реакции
Уровень критичности 1	30 минут*

Уровень критичности 2	4 часа*
Уровень критичности 3	6 рабочих часов
Уровень критичности 4	8 рабочих часов

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

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 1.

Контроль решения инцидентов

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

Инцидент считается находящимся в работе у Пользователя, когда «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 клиента не должно превышать 1 месяца. В случае превышения этого показателя, текущий инцидент автоматически закрывается.

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

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

При 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 владельцев лицензии Kaspersky Industrial Cybersecurity Enterprise.
- Информированию Пользователя о промежуточных результатах.

Предоставление кодов программных коррекций (patches) продукта

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

При обнаружении нестандартной проблемы, 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 на выпуск кодов частных коррекций выделенной группой инженеров, закрепленной за запросами Пользователей продуктовой линейки Kaspersky Industrial Cybersecurity Enterprise.
- Информирования Пользователя о промежуточных результатах

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

Дополнительные условия поддержки

Пользователь имеет право назначить до 8 (восьми) контактных лиц, имеющих право открывать заявки на оказание услуг технической поддержки. Список контактных лиц со стороны Пользователя должен быть определен дополнительно. 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 обновленную информацию.

Пользователь может зарегистрировать неограниченное количество инцидентов за весь срок действия лицензии.

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».

«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 технической поддержки

Программа поддержки продуктовой линейки Kaspersky Industrial CyberSecurity Enterprise не включает в себя следующие пункты:

- Разработку нового функционала продукта по запросу Пользователя.
- Улучшение производительности и конфигурирование устройства Пользователя.

- Лечение компьютеров, зараженных вредоносными программами (включая устранение последствий такого заражения).
- Запросы на описание вредоносных программ.
- Выездную поддержку.
- Сеансы удаленной поддержки.
- Поддержку в нерабочее время за исключением инцидентов уровня критичности 1 и 2.
- Вопросы о работе сторонних приложений и/или операционных систем.
- Применение сторонних патчей к операционным системам и приложениям для устранения уязвимостей.
- Интеграцию продуктов Лаборатории Касперского со сторонним программным обеспечением.
- Конфигурирование Продуктов силами специалиста технической поддержки.
- Советы по общей настройке информационной безопасности.
- Обучение работе с Продуктами.
- Демонстрацию, развертывание Продуктов.
- Изменение настроек и проверку работоспособности Продуктов.

Некоторые сервисы, не входящие программу поддержки, могут предлагаться как отдельные платные услуги.

Услуги, входящие в программу технической поддержки, 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, список 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.

4. Приложения

Приложение 1. Уровни критичности инцидентов, относящихся к продукту.

«Уровень критичности 1» (критический) означает критическую проблему с Продуктом, влияющую на непрерывность технологического процесса 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 технологические 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 технологических 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 Заказчика 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 технологического процесса Заказчика посредством прерывания работоспособности Продукта или операционных систем Заказчика, 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 производства 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 системы, некритичные для производства.