

**kaspersky**

**Расширенная программа  
технической поддержки  
«Плюс»**

MSA Plus

## 1. Общие условия

Настоящая программа поддержки определяет перечень и порядок оказания услуг технической поддержки владельцу данного Сертификата Расширенной Технической Поддержки уровня «Плюс» (MSA Plus).

Настоящая программа поддержки направлена на предоставление Пользователю расширенного перечня услуг, а также на предоставление повышенного качества обслуживания по сравнению с условиями стандартной поддержки, оказываемой в рамках Лицензионного соглашения АО «Лаборатория Касперского», определяющего условия использования программного Продукта Пользователем.

## 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.

**«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. 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.

**«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 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.

**«Услуга(и)»** – мероприятия и деятельность по сопровождению, технической поддержке и консультации, предоставляемые «Лабораторией Касперского» в рамках программы поддержки «Плюс».

**«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.

**«Модернизация»** – обновление Продукта, идентифицированное изменением номера версии 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 поддержки «Плюс»

### Техническое консультирование по вопросам эксплуатации продукта 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 выделенной приоритетной линии по рабочим дням с 10 до 18:30 (время Московское)
- 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	4 рабочих часа

Запросам Пользователей расширенной технической поддержки «Плюс» присваивается более высокий приоритет относительно стандартных запросов.

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 Пользователей расширенной технической поддержки «Плюс»

## Дополнительные условия поддержки

Пользователь имеет право назначить до 2(двух) контактных лиц, имеющих право открывать заявки на оказание услуг технической поддержки. Список контактных лиц со стороны Пользователя должен быть определен в сертификате на Расширенную Техническую поддержку. 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 версию сертификата Расширенной Технической поддержки.

Пользователь может зарегистрировать до 12 инцидентов за год в течение срока действия сертификата Расширенной Технической поддержки, если иное не указано в сертификате на Расширенную Техническую поддержку.

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 поддержки «Плюс»

Услуги, входящие в программу поддержки «Плюс», 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 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 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 бизнеса 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 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.