kaspersky

Расширенная программа технической поддержки для продуктов Technology Alliances (TA)

MSA for Technology Alliances (MSA for TA)

kaspersky

1. Общие условия

Настоящая программа поддержки определяет перечень и порядок оказания владельцу (Лицензиат) сертификата на услугу расширенной технической поддержки для продуктов Technology Alliances (MSA for TA) предоставляемой «Лабораторией Касперского» (Лицензиар).

Настоящая программа поддержки направлена на предоставление Лицензиату расширенного перечня услуг, а также на предоставление повышенного качества обслуживания по сравнению с условиями стандартной поддержки технологических продуктов.

2. Определения

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

«Лицензиар» - компания «Лаборатория Касперского».

«Лицензиат» - владелец сертификата Расширенной технической поддержки для продуктов Technology Alliances (MSA for TA).

«Инцидент» – любое событие, сообщенное Лицензиатом, 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 Лицензиата на предоставление технической поддержки, информации, совета или документации в случаях, не касающихся некорректного функционирования или прерывания нормальной работы Продукта.

«Конечный пользователь» – клиент, непосредственно использующий ПО Лицензиата, содержащее в своем составе Продукт.

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

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

«Время реакции» – время, прошедшее с момента получения Лицензиаром информации о любом инциденте до момента предоставления Лицензиату квалифицированного ответа.

«Обновление» – выпуск Лицензиаром базы данных с новыми сигнатурами для определения зловредного ПО или другими модификациями Продукта, обеспечивающей улучшение функциональности или производительности Продукта и/или содержащей новую функциональность или улучшения Продукта.

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

kaspersky

3. Поддержка конечных пользователей (первая линия поддержки)

Лицензиат самостоятельно организует и осуществляет поддержку конечных пользователей (первая линия поддержки), которая включает в себя:

- Консультации конечных пользователей по вопросам установки и использования Продукта.
- Консультации конечных пользователей по вопросам обновления баз и программных модулей Продукта.
- Диагностику и устранение проблем, которые могут быть решены самостоятельно.
- Диагностику и устранение известных проблем, решение которых описано в документации к продукту и онлайн ресурсах.
- Диагностику и устранение проблем аналогичных уже решенным ранее.
- Первоначальное исследование проблем, которые не могут быть решены самостоятельно.
- Получение информации, запрошенной второй линией поддержки.
- Внедрение решений, предложенных второй линией поддержки, на стороне конечного пользователя.
- Установку обновлений Продукта на стороне конечного пользователя.

4. Поддержка Лицензиата (вторая линия поддержки)

Лицензиар предоставляет Лицензиату техническую поддержку (вторая линия поддержки), которая включает диагностику и решение проблем, возникающих при корректном использовании Продукта в соответствии с документацией, которые не могут быть самостоятельно решены первой линией поддержки.

Поддержка оказывается по следующим каналам связи в круглосуточном режиме (включая выходные и праздничные дни):

- через интернет-портал Company Account (https://companyaccount.kaspersky.com),
- по электронной почте,
- по телефону (выделенная приоритетная линия).

При эскалации инцидента на вторую линию Лицензиат предоставляет Лицензиару следующую информацию:

- наименование и версию используемого Продукта,
- подробное описание проблемы,
- шаги для воспроизведения проблемы,
- конфигурационные файлы Продукта (при наличии),
- логи Продукта (при наличии).

Некоторые инциденты могут потребовать воссоздания условий возникновения с целью проведения тестирования и верификации проблемного сценария. В таком случае Лицензиат обязан предоставить Лицензиару всю необходимую информацию и специфическое программное или аппаратное обеспечение, необходимое для воспроизведения условий возникновения инцидента.

Лицензиар 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 Лицензиат обязан предоставить сотрудникам Лицензиара удаленный доступ к системам, где наблюдается проблема.

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, Лицензиар имеет право отказать в дальнейших работах по решению инцидента.

kaspersky

Ограничения второй линии поддержки

Вторая линия поддержки не оказываются для перечисленных ниже инцидентов:

- инциденты, решенные ранее или аналогичные таковым;
- инциденты, вызванные неполадками аппаратного обеспечения конечного пользователя;
- инциденты, возникшие на неподдерживаемых версиях программных платформ (например, на бета-версиях программных платформ, версиях новых пакетов обновлений или дополнений, не одобренных Лицензиаром в качестве совместимых с Продуктом);
- инциденты, вызванные установкой и запуском сторонних приложений (включая, но не ограничиваясь, списком неподдерживаемого или несовместимого программного обеспечения, указанного в документации или на сайте Лицензиара);
- инциденты, о которых Лицензиат не может предоставить точную информацию, обоснованно запрошенную Лицензиаром с целью воспроизведения, расследования и решения инцидента;
- инциденты, возникшие в результате неприменения или неправильного применения инструкций или документации Лицензиара, в случае правильного использования которых возникновение инцидента было бы невозможно.

5. Время реакции на инциденты

Лицензиар гарантирует время реакции на обращения Лицензиата в соответствии с временными рамками, соответствующими уровням критичности 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

*Время реакции гарантировано при дополнительном обращении Лицензиата по телефону.

6. Персональный технический менеджер (ПТМ)

Персональный технический менеджер (ПТМ) назначается Лицензиаром с целью организации единого канала взаимодействия с Лицензиатом. ПТМ является сотрудником Лицензиара и управляет обработкой всех инцидентов Лицензиата.

В обязанности технического менеджера входит:

- организация работ по технической поддержке специалистами Лицензиара для решения технических инцидентов;
- информирование Лицензиата о текущем состоянии решения запросов, предоставление ежеквартальной отчётности;
- контроль выполнения задач и обеспечение своевременных эскалаций при обработке инцидентов в процессе оказания услуг;

- поддержка ИТ-департамента Лицензиата в понимании и правильном использовании рекомендаций, предоставленных в процессе оказания услуг;
- проведение совместно с Лицензиатом регулярного анализа и согласование действий необходимых для решения технических и операционных инцидентов.

Лицензиат должен сообщить Лицензиару имена и контактную информацию сотрудников, назначенных для взаимодействия с ПТМ и предоставить его контактную информацию (в частности, адрес электронной почты и номер телефона), посредством которой с контактным лицом или полномочным представителем данного лица можно взаимодействовать во время работ над инцидентами.

Также Лицензиату доступна круглосуточная выделенная линия технической поддержки.

7. Управление качеством

Эскалация инцидентов и управление претензиями

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

Уровень эскалации	
1	Персональный технический менеджер
2	Руководитель группы поддержки технологических продуктов
3	Менеджер по работе с корпоративными клиентами (бизнес-контакт)

Предоставление отчетов по открытым инцидентам

В процессе решения инцидентов Лицензиар сделает все возможное для своевременного предоставления информации о статусе открытых инцидентов Лицензиату 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	

8. Дополнительные условия поддержки

Лицензиат имеет право назначить до 8 (восьми) контактных лиц, имеющих право открывать заявки на оказание услуг технической поддержки. Список контактных лиц со стороны Лицензиата должен быть определен в сертификате на Расширенную Техническую поддержку, предоставляемом Лицензиаром. Для изменения списка контактных лиц Лицензиат должен оформить запрос через Company Account. В ответ на запрос об изменении списка контактных лиц, Лицензиар предоставит пользователю обновленную версию сертификата Расширенной Технической поддержки.

Пользователь может зарегистрировать неограниченное количество инцидентов за весь срок действия сертификата Расширенной Технической поддержки.

9. Уровни критичности инцидентов

Уровень критичности инцидента определяется на основании описания проблемы, предоставленного Лицензиатом при эскалации на вторую линию поддержки. Лицензиар имеет право впоследствии пересмотреть уровень критичности инцидента, если его описание будет соответствовать другому уровню.

Запросы, полученные в рамках расширенной программы поддержки, рассматриваются с более высоким приоритетом, чем стандартные запросы.

«Уровень критичности 1» (критический) означает критическую проблему с Продуктом, влияющую на непрерывность бизнеса Лицензиата посредством прерывания работоспособности Продукта или операционных систем конечного пользователя, или вызывающую потерю данных, установку стандартных настроек в небезопасный режим или возникновение других проблем с безопасностью, при отсутствии обходного решения.
Сюда также входят следующие вирусные инциденты:

- Вся локальная сеть (или критичная часть сети) не работает.
- Вирусная эпидемия, влияющая на непрерывность бизнеса конечного клиента посредством прерывания работоспособности Продукта или операционных систем конечного клиента, или вызывающую потерю данных, при этом обходное решение отсутствует.
- Ложная тревога для файлов, входящих в критичные для бизнеса системы.

Уровень критичности 1 рассматривается как уровень критичности 2, когда известно обходное решение.

«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.
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 конечного пользователя не выведено из строя в результате работы Продукта;
- инфицирование нескольких некритичных узлов сети;
- ложная тревога для файлов, входящих в некритичные для бизнеса системы.

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