Соглашение об уровне обслуживания Kaspersky DDoS Protection (LLC ShieldMode)

Определения

Заказчик – юридическое лицо, имеющее действующий сертификат на оказание Услуги в соответствии с уровнями обслуживания, описанными в настоящем соглашении.

Система – программно-аппаратный комплекс «Kaspersky DDoS Protection» (далее KDP) и/или программно-аппаратный комплекс «Kaspersky DDoS Protection for Networks» и подключенные к нему внешние каналы связи, предназначенные для обнаружения Аномалий и Атак, Фильтрации трафика, и доставки очищенного Трафика до Защищаемого ресурса.

Исполнитель – ООО «Модель защиты» при использовании Системы

Услуга – Фильтрация Трафика Защищаемого ресурса с целью недопущения отказа Защищаемого ресурса в случае фиксирования Атаки на Защищаемый ресурс, а также обнаружение Атак на Защищаемый ресурс.

Анализ – анализ Трафика защищаемого ресурса с целью изучения и выявления в нем последовательностей и закономерностей, оценки его содержимого и адресов источников/получателей.

Параметры Анализа – индивидуальные граничные значения параметров Трафика Защищаемого ресурса (значения пиковой и средней нагрузки, распределения трафика по источнику и времени суток и др.), используемые при анализе Трафика Защищаемого ресурса

Аномалия – отклонение реальных значений измеряемого параметра Трафика Защищаемого ресурса более чем на 50% от установленного значения Профиля трафика, которое продолжается более 30 минут и свидетельствует о возможной Атаке.

Атака - распределенная атака на вычислительную систему, выполняемая с целью довести вычислительную систему до отказа, то есть создание повышенной нагрузки на вычислительную систему или ее компоненты, в результате которой легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен.

Защищаемый ресурс – сетевой сервис Заказчика, определяемый IP адресом или IP адресом и доменным именем (если ресурс имеет несколько доменных имен), в отношении которого оказывается Услуга, а также любые **Bypass ресурсы**

Объект защиты - специфичные атрибуты Защищаемого ресурса (порт, домен)

Bypass ресурс – определяемый IP адресом сетевой сервис Заказчика, Трафик которого проходит через Центры Очистки,

> **Защищаемый Bypass -** в отношении которого Услуга не оказывается, но к Трафику которого может применяться Фильтрация.
>
> **Незарегистрированный Bypass -** Bypass-ресурс без описания защищаемых объектов, в отношении которого Услуга не оказывается, но к Трафику которого может применяться Фильтрация

Инцидент – любое событие, связанное с Атакой на Защищаемый ресурс, вызванное проблемами в работе Системы или действиями Исполнителя, которое негативно влияет на доступность Защищаемого ресурса из сети Интернет. Выделяются следующие виды Инцидентов:

Критический инцидент – Инцидент, который приводит к полной недоступности Защищаемого ресурса из сети Интернет на 5 и более минут.

Существенный инцидент – Инцидент, который приводит к частичной недоступности Защищаемого ресурса из сети Интернет на 15 и более минут.

Некритичный Инцидент – все остальные Инциденты, которые не оказывают существенного негативного влияния на работоспособность Защищаемого ресурса.

Время реакции на Инцидент – период времени, в течение которого будет начата выработка решения нивелирующего влияние Инцидента на работу Защищаемых ресурсов.

Время реакции на обращение – период времени, в течение которого будет начата обработка обращения, для получения технической поддержки.

Время решения – период времени, в течение которого будет найдено постоянное или временное решение, нивелирующее влияние Инцидента на работу Защищаемых ресурсов.

Контактные лица Заказчика – сотрудники Заказчика, указанные в Списке Контактных лиц Заказчика, уникальными идентификаторами которых является e-mail

Легитимный трафик – Трафик, передаваемый в сторону Защищаемого ресурса, который получен от пользователей, предполагающих использовать Защищаемый ресурс по его назначению (например, от пользователей системы Интернет-банкинга, посетителей информационного сайта).

Личный кабинет – компонент Системы, представляющий собой web-интерфейс, принадлежащий АО «Лаборатории Касперского». Предназначен для управления Списком контактных лиц Заказчика, а также для предоставления Контактным лицам Заказчика информации о состоянии Трафика Защищаемых ресурсов.

Режим Always-On – режим постоянного прохождения Трафика Защищаемого ресурса через Центр очистки после Перенаправления трафика.

Режим On-Demand – режим, когда Трафик Защищаемого ресурса направляется Заказчиком через Центр очистки по факту обнаружения атаки.

Перенаправление трафика – комплекс действий по изменению сетевого маршрута доставки Трафика защищаемого Ресурса через Центры очистки, в соответствии со Схемой подключения.

Площадка Заказчика – совокупность оборудования, обеспечивающего работоспособность Защищаемых ресурсов, определенная Схемой подключения

Профиль трафика – совокупность значений измеряемых параметров Трафика Защищаемого ресурса, описывающая нормальный Трафик Защищаемого ресурса в виде набора статистических параметров за единицу времени.

Сенсор – программный компонент Системы, который передается Заказчику в случае, если необходимость установки Сенсора на Площадке Заказчика определена в Схеме подключения.

Устанавливается на принадлежащем Заказчику сервере, который должен быть подключен к сетевому оборудованию, обеспечивающему маршрутизацию Трафика Защищаемого ресурса. Осуществляет сбор статистики по Трафику Защищаемого ресурса, необходимой для обнаружения Аномалией и Атак, и передает такую статистику в Центры очистки.

Служба технической поддержки KDP – технический персонал ООО «Модель защиты» непосредственно работающий с системой Kaspersky DDoS Protection, занятый в подключении новых Защищаемых ресурсов и обслуживании существующих, отражении Атак и их аналитикой, приеме, регистрации и обработке обращений Заказчика.

Список контактных лиц Заказчика – список Контактных лиц Заказчика, которые оповещаются в случае Аномалий и Атак, а также имеют право на обращение за технической поддержкой и право на получение доступа в Личный кабинет. Список должен поддерживаться Заказчиком через Личный кабинет, там же должна содержаться информация о времени доступности Контактного лица заказчика и приоритета оповещений. Заказчик должен гарантировать круглосуточную доступность хотя бы одного из Контактных лиц Заказчика.

Схема подключения – документ, описывающий все аспекты подключения Услуги, такие как список Защищаемых ресурсов, список Площадок Заказчика, список Bypass ресурсов, способ Перенаправления трафика, необходимость установки Сенсора, место установки Сенсора, параметры доставки очищенного Трафика, временная зона клиента.

Трафик – сетевые пакеты, передаваемые по каналам передачи данных.

Фильтрация – выявление в Трафике Защищаемого ресурса Трафика, не являющегося Легитимным трафиком, и его удаление.

Центр очистки – компонент Системы, который осуществляет Анализ и Фильтрацию проходящего через него Трафика Защищаемого ресурса, а также сбор, анализ и хранение статистической информации о Трафике Защищаемого ресурса.

Сертификат домена – электронный документ, подтверждающий принадлежность домена владельцу Закрытого ключа.

Закрытый ключ – криптографический ключ, использующийся для аутентификации сервера владельца и шифрования передаваемых данных.

Удостоверяющий центр – организация, обеспечивающая выпуск и управление Сертификатами доменов.

1. Определение услуги

Услуга оказывается с использованием Системы в режиме Always On.

В рамках оказания услуги:

1. Заказчик обеспечивает:
   1.1 Перенаправление Трафика Защищаемого ресурса в соответствии со Схемой подключения.
   1.2 Возможности получения очищенного Трафика Защищаемых Ресурсов из Центра очистки на Площадке в соответствии со Схемой подключения.
   1.3 Актуальность Списка контактных лиц через Личный кабинет.
2. Исполнитель обеспечивает:
   2.1 Определение Профиля Трафика.
   2.2 Круглосуточное осуществление Анализа Трафика Защищаемого ресурса на предмет наличия Аномалий и Атак.
   2.3 Круглосуточное предоставление Заказчику результатов Анализа Трафика Защищаемого ресурса через Личный кабинет Заказчика.
   2.4 В случаях, определенных в разделе Уровни Сервисного обслуживания, оповещение Заказчика о наличии Аномалий и предполагаемых Атак в Трафике Защищаемого ресурса при их обнаружении.
   2.5 Фильтрацию Трафика Защищаемого ресурса.
   2.6 Доступ к Личному кабинету.
   2.7 В случаях, определенных в разделе Уровни Сервисного обслуживания, предоставление Заказчику в виде стандартизованных отчетов предустановленной формы результаты анализа Трафика Защищаемого ресурса
3. Если Схемой подключения предусмотрена установка Сенсора:
   3.1 Заказчик обеспечивает установку и настройку оборудования Сенсора, и предоставление доступа к нему службе технической поддержки KDP, согласно Схеме подключения.
   3.2 Исполнитель обеспечивает настройку сетевого взаимодействия Сенсора и Системы.

2. Условия работоспособности

1 Система «Kaspersky DDoS Protection» в части Фильтрации Трафика Защищаемого ресурса является работоспособной только при условии, что Схема подключения согласована со Службой технической поддержки KDP и реализована на Площадке заказчика и в Центре очистки, работоспособность реализованной Схемы подключения проверена и подтверждена Заказчиком и Исполнителем, а Заказчик поддерживает работоспособность подтвержденной Схемы подключения на своей стороне, в том числе обеспечивает:

1.1 Режим Always On Трафика Защищаемого ресурса на Центры очистки в соответствии со Схемой подключения. При этом через Центры очистки должен проходить весь Трафик Защищаемого ресурса, как входящий, так и исходящий.

1.2 Для Схемы подключения с маршрутизацией трафика - работоспособность одного или более GRE-туннелей, или выделенных каналов, с активными BGP-сессиями до каждой Площадки Заказчика.

Для Схемы Подключения с доставкой трафика с помощью Обратного Прокси – доступность для Системы Защищаемых ресурсов.

2 Если Схемой подключения предусмотрена установка Сенсора на Площадке Заказчика, то Заказчик обеспечивает:

2.1 Наличие не менее одного Сенсора на каждой Площадке Заказчика, на который поступает полная копия неизмененного Трафика Защищаемого ресурса. При этом оборудование, используемое Заказчиком для размещения Сенсора, должно соответствовать требованиям спецификации, предоставленной Технической поддержкой KDP.

2.2 Доступность Сенсора из сети Интернет и актуальность сетевых доступов к Сенсору из Центров Очистки.

3 Если Защищаемый ресурс работает по протоколу HTTPS, для обеспечения Параметров Фильтрации трафика, гарантируемых настоящим Соглашением, должно выполняться одно из следующих условий:

- Если Схемой подключения предусмотрена доставка трафика с помощью Обратного прокси, Заказчик обеспечивает возможность расшифровки запросов путем предоставления Исполнителю доступа к Сертификату домена Защищаемого Ресурса и соответствующего ему Закрытого ключа.
- Если Схемой подключения предусмотрена установка Сенсора на Площадке Заказчика, на Сенсоре должен присутствовать дополнительный сетевой интерфейс, на который перенаправляется полная копия расшифрованного Трафика Защищаемого ресурса.

4 Если схемой подключения предусмотрена доставка трафика с помощью Обратного прокси и предоставление Исполнителю доступа к Сертификату домена Защищаемого ресурса и соответствующего ему Закрытого ключа, то оказание Услуги не может быть обеспечено в случае отзыва Сертификата домена Защищаемого ресурса.

3. Описание процесса взаимодействия

3.1. Основной процесс

Процесс взаимодействия между Заказчиком и Исполнителем в рамках оказания Услуги включает следующие основные этапы:

1. Выполняется подключение к Системе, в ходе которого Заказчиком и Службой технической поддержки KDP согласовывается Схема подключения, согласно которой настраивается оборудование на стороне Заказчика и Исполнителя для Перенаправления Трафика Защищаемого ресурса на Центр Очистки. Если Схемой подключения предусмотрена установка Сенсора на Площадке Заказчика, то так же производится настройка оборудования, на котором размещен Сенсор. После успешного прохождения тестов настройки оборудования должны поддерживаться в том состоянии, в котором они были зафиксированы в Схеме подключения.
2. В течение двух недель с момента начала поступления Трафика Защищаемого ресурса в Центр очистки или начала поступления полной копии Трафика Защищаемых ресурсов на Сенсор (если Схемой подключения предусмотрена установка Сенсора на Площадке Заказчика) производится сбор статистических данных по Трафику Защищаемых ресурсов и строятся Профили трафика. В случае если Схемой подключения предусмотрена установка Сенсора на Площадке заказчика, то

отсутствие Сенсора или отсутствие копии Трафика Защищаемых ресурсов в неизмененном виде на Сенсоре в течение 2 недель не позволяет гарантировать эффективность мониторинга и Фильтрации Трафика.

3. Проводится тестовое Перенаправление трафика, в ходе которого проверяется корректность согласованной Схемы подключения и произведенных настроек оборудования.
4. После успешного тестового Перенаправления Трафика Защищаемого ресурса на Центр очистки прохождение Трафика Защищаемых ресурсов переводится в режим Always On.
5. Система переводится в режим постоянного мониторинга Аномалий и Атак в Трафике Защищаемого ресурса.
6. Заказчик обязан оповещать Службу технической поддержки KDP о производимых изменениях, влияющих на Схему подключения. Любое изменение в Схеме подключения должно в обязательном порядке согласовываться с Службой технической поддержки KDP, фиксироваться в новой Схеме подключения, а работоспособность новой Схемы подключения должна быть проверена и подтверждена Заказчиком и Исполнителем. В противном случае эффективность Анализа и Фильтрации Трафика Защищаемого ресурса не гарантируется.
7. В случае обнаружения Системой существенного отклонения реальных значений измеряемых параметров Трафика Защищаемого ресурса от Профиля трафика, свидетельствующего о возможной Атаке на Защищаемый ресурс, Служба эксплуатации KDP оповещает Контактных лиц Заказчика о наличии Аномалий или Атак в соответствии с параметрами оповещений, определенными в разделе Оповещения.
8. Служба технической поддержки KDP обеспечивает Фильтрацию и контроль степени очистки Трафика.
9. После регистрации Системой завершения Атаки Служба технической поддержки KDP оповещает об этом Контактных лиц Заказчика.
10. После завершения Атаки В Личном кабинете Заказчику становится доступен отчет об Атаке.

3.2. Дополнения к процессу при работе с зашифрованным трафиком

Процесс взаимодействия между Заказчиком и Исполнителем в рамках оказания Услуги при работе с зашифрованным трафиком Защищаемых ресурсов может включать дополнительные аспекты:

1. Предоставление Заказчиком Исполнителю доступа к Сертификату домена Защищаемого ресурса и соответствующего ему Закрытого ключа.

   Если схемой подключения предусмотрена доставка Трафика с помощью Обратного прокси, Заказчик имеет возможность:

   - передать оригинальный Сертификат домена и соответствующий ему Закрытый ключ Службе технической поддержке KDP защищенным способом;
   - передать дублирующий сертификат домена и соответствующий ему Закрытый ключ Службе технической поддержке KDP защищенным способом.
   - поручить Исполнителю выпуск дублирующего Сертификата домена; выпуск дублирующего Сертификата должен быть подтвержден Заказчиком по запросу партнера Исполнителя, который является аккредитованным Удостоверяющим центром.
2. Хранение Закрытого ключа и соответствующего ему Сертификата домена Защищаемого ресурса.

   Хранение Закрытого ключа и соответствующего Сертификата домена осуществляется Исполнителем с использованием изолированных модулей хранения и обеспечения безопасности.

Закрытый ключ соответствующего Сертификата домена хранится только в зашифрованном виде. В ходе обработки зашифрованного трафика Закрытый ключ не покидает периметра изолированных модулей хранения. Доступ к расшифрованному Закрытому ключу соответствующего Сертификата домена имеют выделенные сотрудники Исполнителя; параметры этого доступа регламентированы внутренними процедурами.

3. Отзыв сертификата домена защищаемого ресурса.

3.1. В случае отзыва Заказчиком оригинального или дублирующего сертификата домена Защищаемого ресурса, выпущенного Удостоверяющим центром по запросу Заказчика и переданного Службе технической поддержки KDP:

- Заказчик обязан уведомить Службу технической поддержки KDP о факте, причине и дате отзыва Сертификата домена;
- Заказчик обязан уведомить Службу технической поддержки KDP о сроках выпуска нового сертификата и его передачи.

3.2. В случае отзыва Заказчиком дублирующего сертификата домена Защищаемого ресурса, выпущенного Удостоверяющим центром по запросу Исполнителя:

- Заказчик обязан уведомить Службу технической поддержки KDP о факте, причине и дате отзыва Сертификата домена;
- Заказчик имеет возможность поручить Исполнителю повторный выпуск дублирующего Сертификата домена, который должен быть подтвержден Заказчиком по запросу партнера Исполнителя.
- Исполнитель, по поручению Заказчика, обязан инициировать выпуск дублирующего Сертификата домена и сообщить Заказчику информацию о предполагаемых сроках его выпуска.

3.3. В случае отзыва Исполнителем, в связи с подозрением на компрометацию, дублирующего сертификата домена Защищаемого ресурса, выпущенного Удостоверяющим центром по запросу Исполнителя:

- Исполнитель обязан уведомить Заказчика о факте и дате отзыва Сертификата домена;
- Заказчик имеет возможность поручить Исполнителю повторный выпуск дублирующего Сертификата домена, выпуск которого должен быть подтвержден Заказчиком по запросу партнера Исполнителя;
- Исполнитель, по поручению Заказчика, обязан инициировать выпуск дублирующего Сертификата домена и сообщить Заказчику информацию о предполагаемых сроках его выпуска.

3.4. В случае отзыва Удостоверяющим центром оригинального или дублирующего сертификата домена Защищаемого ресурса, выпущенного Удостоверяющим центром по запросу Заказчика и переданного Службе технической поддержки KDP:

- Исполнитель, при наличии достоверных сведений об отзыве Сертификата домена Удостоверяющим центром, обязан уведомить Заказчика о факте, причине и дате отзыва Сертификата домена;
- Заказчик, при наличии достоверных сведений об отзыве Сертификата домена Удостоверяющим центром, обязан уведомить Службу технической поддержки KDP о факте, причине и дате отзыва Сертификата домена;
- Заказчик обязан уведомить Службу технической поддержки KDP о сроках выпуска нового Сертификата домена и его передачи.

3.5. В случае отзыва Удостоверяющим центром дублирующего Сертификата домена Защищаемого ресурса, выпущенного Удостоверяющим центром по запросу Исполнителя:

- Исполнитель, при наличии достоверных сведений об отзыве Сертификата домена Удостоверяющим центром, обязан уведомить Заказчика о факте, причине и дате отзыва сертификата;
- Заказчик, при наличии достоверных сведений об отзыве Сертификата домена Удостоверяющим центром, обязан уведомить Службу технической поддержки KDP о факте, причине и дате отзыва сертификата;
- Заказчик имеет возможность поручить Исполнителю повторный выпуск дублирующего Сертификата домена, который должен быть подтвержден Заказчиком по запросу партнера Исполнителя;
- Исполнитель, по поручению Заказчика, обязан инициировать запрос на выпуск дублирующего сертификата домена и сообщить Заказчику информацию о предполагаемых сроках его выпуска.

3.6. В случае прекращения оказания Услуги Исполнитель имеет право инициировать запрос на отзыв Сертификата домена Защищаемого ресурса, выпущенного Удостоверяющим центром по запросу Исполнителя.

4. Распределение ответственности между Исполнителем и Заказчиком

Сферы ответственности исполнителя и Заказчика в ходе оказания Услуги определены в Таблице 1.

Таблица 1

Сфера ответственности	Исполнитель	Заказчик
Обеспечение Перенаправления трафика Защищаемого ресурса на Центр очистки		+
Работоспособность Площадки Заказчика		+
Отслеживание Аномалий и Атак в Трафике защищаемого Ресурса	+	
Оповещение сотрудников Заказчика о предполагаемых Атаках на Защищаемый ресурс	+	
Оповещение сотрудников Заказчика о завершении Атаки	+	
Контроль качества работы Системы	+	
Поддержание и использование согласованной и протестированной Схемы подключения на стороне Центров очистки в работоспособном состоянии, оповещение о производимых изменениях	+	
Поддержание и использование согласованной и протестированной схемы переключения на стороне Заказчика в работоспособном состоянии, оповещение о производимых изменениях		+
Работоспособность Bypass ресурсов		+

В случае, если Схемой подключения предусмотрена установка Сенсора на Площадке Заказчика, то в сферу ответственности Исполнителя и Заказчика так же входит:

Таблица 2

Сфера ответственности	Исполнитель	Заказчик
Работоспособность программного обеспечения Сенсора	+	
Работоспособность оборудования, на котором размещен Сенсор		+
Доступность Сенсора для Системы через сеть Интернет		+
Наличие копии Трафика Защищаемого ресурса на Сенсоре		+

В случае, если схемой подключения предусмотрена доставка трафика с помощью Обратного прокси и передача Сертификата домена Защищаемого ресурса Заказчиком Исполнителю, то в сферу ответственности Исполнителя и Заказчика так же входит:

Сфера ответственности	Исполнитель	Заказчик
Риск компрометации сертификата при передаче сертификата и соответствующего ему Закрытого ключа Заказчиком Исполнителю		+
Риск компрометации сертификата при выпуске дублирующего сертификата Партнером Исполнителя	+	
Контроль истечения срока действия оригинального сертификата, переданного Заказчиком Исполнителю		+
Контроль истечения срока действия дублирующего сертификата, выпущенного партнером исполнителя.	+	

5. Техническая поддержка

5.1 Объем технической поддержки

Служба технической поддержки KDP обеспечивает Анализ и Фильтрацию Трафика Защищаемого Ресурса, оповещение Контактных лиц и обработку их запросов.

Уровни сервисного обслуживания, включающие в себя доступность Технической поддержки, каналов коммуникаций, время решения инцидентов, время обработки обращений и т.д. определены в разделе Уровни сервисного обслуживания.

Техническая поддержка KDP включает в себя следующие действия:

1. отслеживание Аномалий и Атак в Трафике Защищаемого ресурса в соответствии с параметрами, определенными в разделе Уровни сервисного обслуживания.
2. уведомление Контактных лиц Заказчика об Аномалиях и предполагаемых Атаках в Трафике Защищаемых ресурсов в соответствии с параметрами оповещения, определенными в разделе Оповещения.
3. Контроль Фильтрации Трафика Защищаемого ресурса в случае подтверждения Атаки.
4. Уведомление Контактных лиц Заказчика в соответствии с параметрами, определенными в разделе Оповещение, о возврате характеристик Трафика Защищаемого ресурса к норме, свидетельствующем о завершении Атаки.
5. уведомление Контактных лиц Заказчика о регистрации Инцидента в случае его возникновения в соответствии с параметрами, определенными в разделе Время реакции на Инциденты.
6. решение Инцидента в соответствии с параметрами, определенными в разделе Время решения Инцидентов.

7. уведомление Контактных лиц Заказчика о решении Инцидента, в соответствии с параметрами, определенными в разделе Оповещения.
8. Прием и регистрацию обращений Контактных лиц Заказчика, в соответствии с параметрами, определенными в разделе Уровни сервисного обслуживания.
9. контроль за ходом выполнения работ по обращениям, закрытие запроса в соответствии с параметрами, определенными в разделе Время реакции на обращения.
10. информирование Контактных лиц Заказчика по Инцидентам/проблемам/работам массового характера, проводимым изменениям и технологическим работам, в случае если они могут повлиять на качество оказания Услуги.

Коммуникации между Контактными лицами Заказчика и Технической поддержкой возможны по телефону и электронной почте.

Служба технической поддержки KDP имеет право отказать Заказчику в выполнении запросов, превышающих объем Услуги, предусмотренный в настоящем соглашении. В случае отказа в выполнении запросов Заказчика, Контактные лица Заказчика имеют право обратиться за дополнительной информацией по адресу электронной почты KDPcomplaints@kaspersky.com.

5.2 Уровни Сервисного обслуживания

В рамках оказания Технической поддержки Услуги доступны несколько уровней сервисного обслуживания:

Сравнительные характеристики уровней сервисного обслуживания приведены в Таблице 3:

Уровень обслуживания/ параметр	**Platinum**	**Gold**	**Business**	**Standart**	**Standart WEB**	**Insured**
Объем фильтрации атаки, Гб/с	20,0	10,0	7,5	5,0	1,0	5,0
Включенный легитимный трафик, Мб/с	10,0	10,0	10,0	10,0	10,0	10,0
Время атаки, сутки	unlim	unlim	12	6	6	2
Схема включения для L7-ресурсов	all	dns	dns	dns	dns	all
SLA по доступности	99,5%	99,3%	99,0%	98,5%	98,5%	99,0%
SLA по реакции (п.5.6.)	**Premium**	**Base**	**Base**	**Light**	**Light**	**Base**
Портов на IP/подсеть	10	5	5	5	-	5
Доменов на 1 IP	10	5	5	5	1	5
Экспертная поддержка (см. п.5.8.)	24*7	24*7	8*5	8*5	-	8*5
Экстренная поддержка (см. п.5.6.)	24*7	24*7	24*7	24*7	24*7	24*7
Черно-белые списки	100	50	10	10	10	10
Балансировка трафика (серверов на IP)	10	3	3	2	1	2

5.3 Взаимодействие по электронной почте

Электронная почта является основным средством связи со Службой технической поддержки KDP. Обращения Контактных лиц Заказчика принимаются на адрес kdp@kaspersky.com. В тексте обращения необходимо указать название и IP-адрес Защищаемого ресурса, в отношении которого делается запрос, а также подробное описание проблемы или вопроса.

При обращении по электронной почте необходимо использовать адрес электронной почты, указанный в Списке контактных лиц Заказчика для конкретного Контактного лица Заказчика. Список Контактных лиц Заказчика и их адресов электронной почты должен соответствовать списку пользователей Личного кабинета и поддерживаться в актуальном состоянии через Личный кабинет. В случае использования адресов электронной почты незарегистрированных в Списке контактных лиц Заказчика Исполнитель оставляет за собой право не обрабатывать поступившие обращения.

5.4 Взаимодействие по телефону

Взаимодействие по телефону является экстренным средством связи, предназначенным для информирования Службы технической поддержки KDP о возникновении Критических Инцидентов и информирования Контактных лиц Заказчика об Атаках и Инцидентах.

Обращения Заказчика принимаются по телефону +7 (495)363-93-38 только от Контактных лиц заказчика. При обращении по телефону необходимо сообщить:

1. название компании;
2. свои ФИО;
3. название и IP-адрес Защищаемого ресурса, в отношении которого делается запрос;
4. подробное описание проблемы;

Исполнитель оставляет за собой право прервать разговор и связаться с обратившимся по телефону, указанному в Списке контактных лиц Заказчика для данного Контактного лица заказчика, для дополнительной проверки правомерности обращения.

Исполнитель оставляет за собой право производить запись отдельных звонков для обеспечения контроля качества.

5.5 Взаимодействие с использованием Личного кабинета

Личный кабинет Системы расположен по адресу «portal.kdp.kaspersky.ru» и предназначен для управления Списком контактных лиц Заказчика, а также для предоставления Контактным лицам заказчика информации о Трафике Защищаемых ресурсов.

Используя Личный кабинет, Контактные лица Заказчика имеют возможность:

1. анализировать статистику по Трафику Защищаемых ресурсов;

2. анализировать состояние Трафика Защищаемых ресурсов во время Атак;
3. настраивать механизмы автоматического оповещения;
4. редактировать «белые списки» и «черные списки», влияющие на параметры Фильтрации;
5. заказывать отчет о списках адресов и отчет об Атаке;

5.6 Время реакции на обращения

Время реакции на обращения Контактных лиц Заказчика, которое обеспечивает Служба технической поддержки KDP в рамках оказания Услуги, зависит от типа обращения, уровня сервисного обслуживания и временной зоны Клиента, зафиксированной в Схеме подключения и определено в Таблице 4.

Таблица 4

Тип обращения	Light	Base	Premium
Подозрение на Атаку на Защищаемые ресурсы	1 час (24x7x365)	30 мин (24x7x365)	15 мин (24x7x365)
Вопросы (по работе Системы, использованию Личного кабинета и пр.)	8 часов (8x5)	4 часа (8x5)	1 час (24x7x365)
Запросы на изменения (состава Защищаемых ресурсов, Схемы подключения и пр.)	12 часов (8x5)	8 часов (8x5)	2 часа (8x5)
Способ коммуникации	E-mail	E-mail	E-mail, телефон

5.7 Оповещения

Оповещение Контактных лиц Заказчика о выявленных Аномалиях и Атаках в Трафике Защищаемых ресурсов и возникающих Инцидентах производится Технической поддержкой KDP в соответствии с параметрами, определенными в Таблице 5.

Таблица 5

Событие	Light	Base	Premium
Аномалия	Недоступно	Недоступно	30 минут по электронной почте*
Атака на Защищаемый ресурс	Недоступно	Недоступно	30 минут по электронной почте
Завершение Атаки	Недоступно	Недоступно	30 минут по электронной почте

Возникновение Инцидента	Недоступно	2 часа по электронной почте	30 минут по электронной почте
Решение Инцидента	Недоступно	2 часа по электронной почте	15 минут по электронной почте

*Автоматическое оповещение обо всех Аномалиях в Трафике Защищаемых ресурсов может быть настроено через Личный кабинет.

5.8 Время реакции на Инциденты

Время реакции на Инциденты, которое обеспечивает Техническая поддержка KDP, зависит от степени критичности Инцидента, временной зоны клиента, зафиксированной в Схеме подключения и уровней сервисного обслуживания и определено в Таблице 6.

Таблица 6

Степень критичности Инцидента	Light	Base	Premium
Некритичный	24 часа (8x5)	8 часов (8x5)	4 часа (24x7x365)
Существенный	12 часов (8x5)	4 часа (24x7x365)	2 часа (24x7x365)
Критический	4 часов (24x7x365)	2 часа (24x7x365)	15 минут (24x7x365)

5.9 Время решения Инцидентов

Время решения Инцидентов, которое обеспечивает Техническая поддержка KDP, зависит от степени критичности Инцидента, уровней сервисного обслуживания, и временной зоны Клиента, зафиксированной в Схеме подключения и определено в Таблице 7.

Таблица 7

Степень критичности Инцидента	Light	Base	Premium
Некритичный	48 часов (8x5)	36 часа (8x5)	24 часов (24x7x365)
Существенный	36 часов (8x5)	24 часа (24x7x365)	12 часов (24x7x365)
Критический	24 часа (24x7x365)	12 часов (24x7x365)	8 часов (24x7x365)

В ходе решения некоторых Инцидентов требуется предоставление заказчиком дополнительной информации или непосредственное участие Заказчика. Заявленное Время решения Инцидентов обеспечивается Службой технической поддержки KDP только при условии выполнения Заказчиком своих обязательств по участию в решении Инцидентов, в соответствии с условиями, определенными в разделе Обязательства Заказчика по участию в решении Инцидентов.

5.10 Ограничения технической поддержки

В техническую поддержку Системы не входит:

1. реагирование на обращения, не связанные с защитой от Атак, в том числе вопросы, связанные с временем отклика ресурса или его доступностью из сети Интернет;

2. реагирование на обращения, касающиеся работы ресурсов, не входящих состав Защищаемых ресурсов;
3. реагирование на обращения, связанные с утечкой секретного ключа Сертификата домена;
4. реагирование на обращения, касающиеся работы любых программно-аппаратных комплексов, не входящих в состав Системы;
5. решение Инцидентов, по которым Заказчик не выполняет свои обязательства по участию в решении Инцидентов, в соответствии с условиями, определенными в разделе Обязательства Заказчика по участию в решении Инцидентов;
6. решение Инцидентов, условия возникновения которых не могут быть воспроизведены ни Заказчиком, ни Технической поддержкой KDP;
7. решение Инцидентов, являющихся следствием превышения Легитимным трафиком Заказчика выделенной полосы пропускания, определенной в разделе Закрепление выделенной полосы пропускания;

В рамках оказания Услуги и обеспечения работоспособности Системы Служба технической поддержки KDP не осуществляет:

1. Анализ безопасности и производительности программно-аппаратных комплексов Заказчика, а также консультации Контактных лиц Заказчика по связанным вопросам;
2. Конфигурирование и администрирование программно-аппаратных комплексов Заказчика, за исключением Сенсора, установленного на Площадке Заказчика, а также консультации Контактных лиц Заказчика по связанным вопросам;
3. Администрирование оборудования интернет-провайдера, услугами которого пользуется Заказчик, а также консультации Контактных лиц Заказчика по связанным вопросам;
4. Взаимодействие с персоналом интернет-провайдера, услугами которого пользуется Заказчик, а также консультации Контактных лиц Заказчика по связанным вопросам;
5. Проведение ремонтно-восстановительных работ на программно-аппаратных комплексах Заказчика, за исключением Сенсора, размещенного на Площадке Заказчика, а также консультации Контактных лиц Заказчика по связанным вопросам;
6. Для Схемы Подключения с доставкой трафика с помощью Обратного Прокси не осуществляется настройка параметров проксирования, в том числе кэширования, балансировки между несколькими адресами Защищаемого ресурса и иных параметров, обеспечивающих контроль за сетевым обменом ресурса.
7. Проведение других работ, не связанных непосредственно с работой Системы и ее компонентов.

В случае детектирования Службой Технической поддержки KDP отсутствия Трафика Защищаемого ресурса на Центре очистки, происходит оповещение Контактных лиц Заказчика. При повторном перенаправлении Трафика Защищаемого ресурса Клиент согласовывает со Службой Технической поддержки KDP факт перенаправления Трафика на Центры очистки.

В случае отключения перенаправления Заказчиком Трафика Защищаемого ресурса на Центры очистки, Система не обеспечивает Анализ и Фильтрацию Трафика.

6. Параметры функционирования Системы

6.1 Параметры Фильтрации Трафика

В процессе Фильтрации Трафика Защищаемых ресурсов Перенаправленного в режиме Always On, Исполнитель, гарантирует, что Система:

1. будет пропускать Трафик между Защищаемыми ресурсами и IP-адресами, помещенными Заказчиком в «белые списки»;
2. будет блокировать Трафик между Защищаемыми ресурсами и IP-адресами, помещенными Заказчиком в «черные списки»;
3. обеспечит очистку Трафика Защищаемых ресурсов в 98%[1] случаев на основе следующего алгоритма:
   3.1 если IP адрес является вредоносным, то вероятность его классификации в качестве нелегитимного равна указанному проценту по прошествии 5 минут после того, как IP адрес начал атаковать Защищаемый ресурс;
   3.2 если IP адрес является адресом легитимного пользователя, то вероятность его классификации в качестве легитимного равна указанному проценту по прошествии 5 минут после того как IP адрес начал обращаться к Защищаемому ресурсу.
4. обеспечит очистку Трафика в 98% случаев при условии, что емкость Атаки, направленной на Защищаемые ресурсы, не превышает лимиты, определенные в Таблице 8.

Таблица 8

Тип Атаки	Максимальная емкость Атаки*
Атаки, основанные на использовании протоколов UDP и ICMP (с большим размером пакетов)	1500 Гбит/с
Атаки на основе протоколов TCP, IPSEC, GRE и др.	40 Гбит/с или 50 млн пакетов/с

* В случае если емкость Атаки превысит указанные лимиты, Система не обрабатывает (полностью блокирует) Трафик, перенаправленный Заказчиком на Центры очистки.

6.2 Ограничение полосы фильтрации

Исполнитель закрепляет за Заказчиком полосу фильтрации Легитимного трафика, ограниченную на входе в Центров очистки, в объеме, не более предусмотренного тарифным планом и указанном в таблице 3.

В случае если объем проходящего через центры очистки легитимного Трафика Заказчика превысит выделенную полосу пропускания, доставка Трафика, превышающего объем выделенной полосы пропускания, не гарантируется.

[1] Исключением является очистка Трафика Защищаемых ресурсов, работающих по протоколу HTTPS, в отношении которых Заказчик не выполняет условия, определенные в п.3 раздела Условия работоспособности – в этом случае очистка Трафика Защищаемых ресурсов обеспечивается в 80% случаев.

6.3 Предоставление отчетов

Отчеты доступны Контактным лицам заказчика через Личный кабинет и формируются Системой автоматически. Состав отчетов, включенных в уровни сервисного обслуживания, определен в Таблице 10.

Таблица 10

Тип отчета	Light	Base	Premium
Отчет о списках адресов	-	-	+
Отчет об атаке	Не более 2 в год	+	+
Отчет о ресурсе	-	-	+

Отчет о списках адресов представляет собой актуальный на момент формирования отчета список «белых» и/или «черных» адресов Защищаемого ресурса, помещенных Контактными лицами заказчика в одноименный список через Личный кабинет, Трафик от этих адресов, соответственно, всегда пропускается или всегда блокируется Системой в ходе Фильтрации.

Отчет об атаке формируется для каждого атакованного Защищаемого ресурса и содержит описание основных характеристик Атаки, графики измеряемых параметров Защищаемого ресурса и прочее.

Отчет о ресурсе формируется за календарный месяц для каждого Защищаемого ресурса и содержит список Атак и иных значимых событий, диаграммы на основе реальных значений Трафика и прочее.

6.4 Время хранения информации в Системе

Информация об Аномалиях в Трафике Защищаемых ресурсов хранится в течение 2 календарных месяцев с момента возникновения и доступна Контактным лицам Заказчика через Личный кабинет. Информация об Атаках хранится в течение срока оказания Услуги и доступна Контактным лицам Заказчика в форме отчетов, формируемых по заявке из Личного кабинета.

6.5 Согласованные перерывы в функционировании Системы

Исполнитель имеет право прерывать функционирование Системы для проведения технологических работ по обслуживанию оборудования и каналов связи, а также для проведения экстренного обслуживания. Такие перерывы классифицируются как функционирование Системы в штатном режиме. Служба технической поддержки KDP уведомляет Контактных лиц Заказчика о перерывах в функционировании Системы в соответствии с параметрами, определенными в Таблице 11

Таблица 11

Тип работ	Продолжительность	Уведомления
Проведение плановых технологических работ	не более 2 часов подряд, не более 24 часов в календарный год	не менее чем за 1 календарный день до начала перерыва
Проведение экстренных (внеплановых) технологических работ	не более 12 часов в календарный год	непосредственно перед началом работ

7. Исключения

Заказчик и Исполнитель соглашаются квалифицировать ситуации, в которых могут наблюдаться сбои в работе Системы, как не являющиеся Инцидентом, если такие сбои явились следствием:

1. изменений Заказчиком Схемы подключения или других настроек, прямо или косвенно влияющих на работоспособность находящихся в зоны ответственности Исполнителя компонентов Системы и произведенных без согласования с Технической поддержкой KDP;
2. планового технического обслуживания Системы, заранее согласованного с Заказчиком, или связанного с модернизацией Системы по запросу Заказчика;
3. невыполнения Заказчиком своих обязательств по участию в решении Инцидентов, в соответствии с условиями, определенными в разделе Обязательства Заказчика по участию в решении Инцидентов;
4. обстоятельств, препятствующих работе Системы, возникших по вине Заказчика;
5. вмешательства Заказчика или третьей стороны в работу оборудования или программного обеспечения, находящегося на территории Заказчика, обеспечивающего работу Системы, без согласования со Технической поддержкой KDP;
6. Перенаправления трафика Защищаемого ресурса без согласования со Службой технической поддержки KDP;
7. отказа оборудования Заказчика или Интернет-провайдера, услугами которого пользуется Заказчик;
8. блокировки каналов поставщиком телекоммуникационных услуг связи на участке сетевого маршрута между Площадкой Заказчика и Центром очистки;
9. перерыва в работоспособности Системы, причиной которого являются обстоятельства непреодолимой силы, предусмотренные применимым законодательством.

8. Обязательства Заказчика по участию в решении Инцидентов

Некоторые Инциденты, связанные с работоспособностью Системы или с взаимодействием компонентов Системы с оборудованием Заказчика, требуют моделирования условий возникновения Инцидента с целью его локализации и поиска причин.

В ходе взаимодействия со Службой технической поддержки KDP по решению Инцидента, Заказчик обязан предоставить всю запрашиваемую Службой технической поддержки KDP информацию, необходимую для решения Инцидента, которой он располагает, и оказывать содействие в получении Службой технической поддержки KDP информации, необходимой для решения Инцидента.

В случае возникновения Инцидента с компонентами, размещенными на территории Заказчика, Заказчик обязан предоставить Службе технической поддержки KDP доступ к указанным компонентам по запросу Исполнителя, если все другие средства диагностики оказались неэффективными.