2022

Сертификат качества на программное обеспечение «Kaspersky DDoS Prevention+»

ПРЕДЕЛЬНЫЕ УСЛОВИЯ ФУНКЦИОНИРОВАНИЯ ПО ПРИОБРЕТЕННЫМ ЛИЗЕНЗИЯМ И ОПИСАНИЕ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Оглавление

Определения

Система – программное обеспечение «Kaspersky DDoS Prevention+» (KDP+), предназначенное для обнаружения Аномалий и Атак, Фильтрации трафика, и доставки очищенного Трафика до Защищаемого ресурса.

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 Лицензиата, определяемый IP адресом или IP адресом и доменным именем или группой доменов с одинаковыми настройками проксирования.

> **Ресурс с ограниченной защитой** – определяемый IP адресом или группой IP-адресов сетевой сервис Лицензиата, Трафик которого проходит через Центры Очистки, ресурс без спецификации защищаемых объектов, но к Трафику которого может применяться **Фильтрация** на основании превышения нормальных для **Ресурс с ограниченной защитой** объемов Трафика

Инцидент – любое событие, связанное с Атакой на Защищаемый ресурс, вызванное проблемами в работе Системы или действиями Лицензиата, 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.
>
> Реакция и решение которых описывается следующими характеристиками:
>
> **Время реакции на обращение** – период времени, в течение которого будет начата обработка обращения, для получения технической поддержки.
>
> **Время реакции на Инцидент** – период времени, в течение которого будет начата выработка решения нивелирующего влияние Инцидента на работу Защищаемых ресурсов.

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

Контактные лица Лицензиата – сотрудники Лицензиата, указанные в Списке Контактных лиц Лицензиата, 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 и предназначен для управления Списком контактных лиц Лицензиата, а также предоставления Контактным лицам Лицензиата информации о состоянии Защищаемых ресурсов.

API Системы - компонент Системы, представляющий собой интерфейс для автоматизированного взаимодействия с Системой

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

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

Always-On IPT – режим постоянного прохождения Трафика Защищаемого ресурса через Центр очистки после Перенаправления трафика без сохранения симметрии трафика.

Reverse-Proxy – режим постоянного прохождения Трафика Защищаемого ресурса через Центр очистки, с использованием технологии Reverse-Proxy

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

Площадка Лицензиата – 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 Лицензиату в случае, если необходимость установки Сенсора на Площадке Лицензиата определена в Схеме подключения. Устанавливается на принадлежащем Лицензиату 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 (KDP ERT) – технический персонал ООО «Модель защита» непосредственно работающий с системой Kaspersky DDoS Prevention+, занятый в подключении новых Защищаемых ресурсов и обслуживании существующих, отражении Атак и их аналитикой, приеме, регистрации и обработке обращений Лицензиата.

Расширенная техническая поддержка KDP (KDP AMT) – совместно – ERT и инженерный персонал ООО «Модель защита» непосредственно занятый в разработке и эксплуатации системы Kaspersky DDoS Prevention+ и осуществляющий изменения по заявкам типа RFC.

RFC (Request for changes) - заявка на изменение действующей конфигурации Системы, недоступные из интерфейса Личного кабинета или API Системы.

Список контактных лиц Лицензиата – список Контактных лиц Лицензиата, 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 Лицензиатом через Личный кабинет, там же должна содержаться информация о времени доступности Контактного лица Лицензиата и приоритета оповещений. Лицензиат должен гарантировать круглосуточную доступность хотя бы одного из Контактных лиц Лицензиата.

Схема подключения – документ (переписка по e-mail), описывающий все аспекты подключения/обеспечения доступности ПО для Лицензиата, такие как список Защищаемых ресурсов, список Площадок Лицензиата, список Bypass ресурсов, способ Перенаправления трафика, необходимость установки Сенсора, место установки Сенсора, параметры доставки очищенного Трафика, временная зона клиента другие применимые характеристики

Трафик – сетевые пакеты, передаваемые по каналам передачи данных.

Фильтрация – удаление Трафика не являющегося Легитимным по отношению к Защищаемому ресурсу

Центр очистки (или ЦО) – 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. Располагается на площадке Лицензиара.

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. Описание Системы

Kaspersky DDoS Prevention+ – решение, которое позволяет защитить ресурсы Клиента от DDoS-атак путем перенаправления пользовательского трафика на Центры очистки Исполнителя.

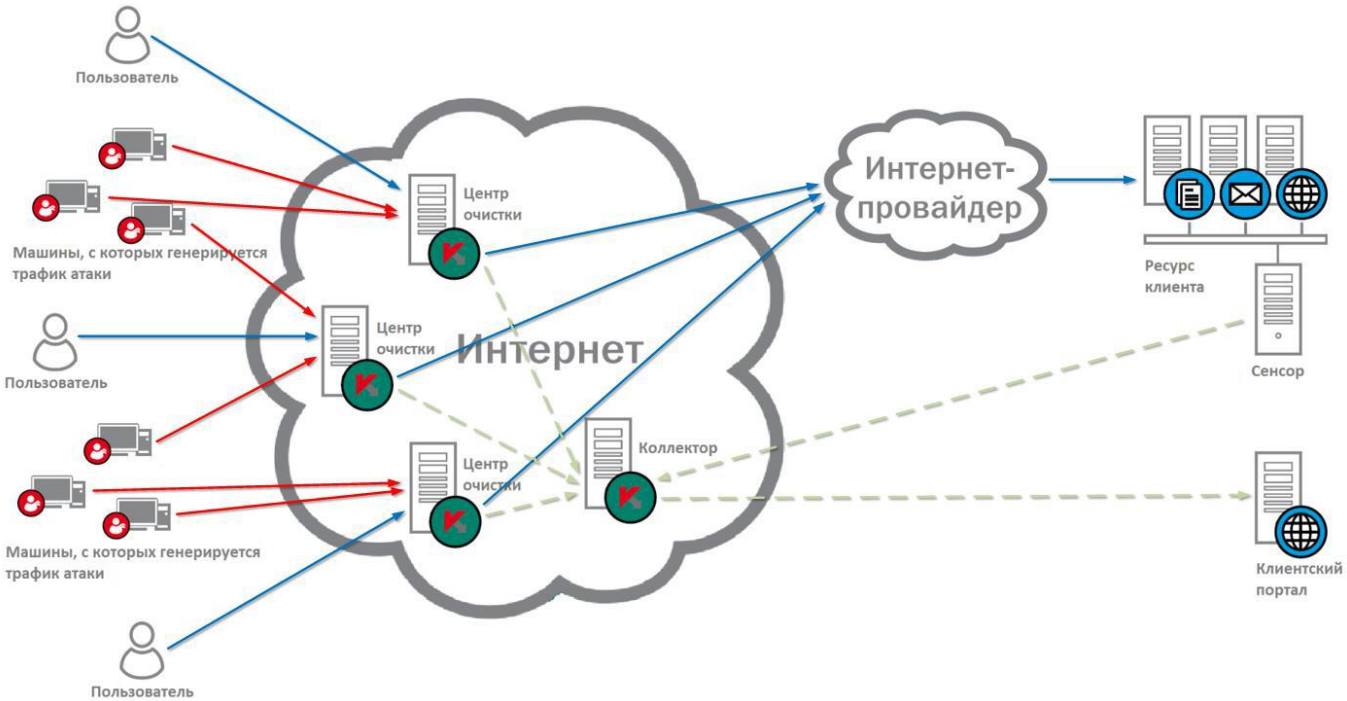
Назначение Системы — обнаружение DDoS-атак, а также очистка (фильтрация) трафика путем выявления и блокирования паразитного трафика, результатом чего является снижение нагрузки на атакуемый ресурс.

В ходе работы Система выполняет следующие функции:

- Собирает статистические параметры трафика Защищаемых ресурсов;
- Осуществляет построение профилей легитимного трафика Защищаемых ресурсов и вырабатывает на их основе правила обнаружения аномалий и атак;
- Производит мониторинг возникновения аномалий и атак в трафике Защищаемых ресурсов;
- Осуществляет фильтрацию трафика Защищаемых ресурсов, перенаправленного через Центр очистки, от паразитной составляющей;

Выполняет вспомогательные задачи, обеспечивающие работу перечисленных функций.

Схема работы Системы



2. Условия работоспособности

1 Система в части Фильтрации Трафика Защищаемого ресурса является работоспособной только при условии, что Схема подключения согласована со Службой технической поддержки KDP и реализована на Площадке Лицензиата и в Центре очистки, работоспособность реализованной Схемы подключения проверена и подтверждена Лицензиатом и Исполнителем, а Лицензиат

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.

1.1.1. Режим Always-On-IPT Трафика Защищаемого ресурса на Центры очистки в соответствии со Схемой подключения. При этом через Центры очистки должен проходить входящий Трафик Защищаемого ресурса.

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

1.3 Для Схемы Подключения с доставкой трафика с помощью Reverse-Proxy – доступность для Системы Защищаемых ресурсов.

2 Если Схемой подключения предусмотрена установка Сенсора на Площадке Лицензиата, то Лицензиат обеспечивает:

2.1 Наличие не менее одного Сенсора на каждой Площадке Лицензиата, на который поступает полная копия неизмененного Трафика Защищаемого ресурса. При этом оборудование, используемое Лицензиатом 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 Reverse-Proxy, Лицензиат 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 Лицензиата, 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 Reverse-Proxy и предоставление Исполнителю доступа к Сертификату домена Защищаемого ресурса и соответствующего ему Закрытого ключа, то функционирование Системы в отношении Защищаемого ресурса не может быть обеспечено в случае отзыва Сертификата домена Защищаемого ресурса.

3. Описание процесса взаимодействия

3.1. Основной процесс

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

1. Выполняется подключение к Системе, в ходе которого Лицензиатом и Службой технической поддержки KDP согласовывается Схема подключения, согласно которой настраивается оборудование на стороне Лицензиата и Исполнителя для Перенаправления Трафика Защищаемого ресурса на Центр Очистки.

1.1. Если Схемой подключения предусмотрена установка Сенсора на Площадке Лицензиата, 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. Проводится Перенаправление трафика с соответствие со схемой Схема подключения в ходе которого проверяется корректность согласованной Схемы подключения и произведенных настроек оборудования.

   2.1. При использовании режима On-demand трафик возвращается на Площадку Лицензиата без прохождения Центра Очистки.

   2.2. Любое изменение в Схеме подключения должно в обязательном порядке согласовываться с KDP ERT, фиксироваться в новой Схеме подключения, а работоспособность новой Схемы подключения должна быть проверена и подтверждена KDP ERT. В противном случае эффективность Анализа и Фильтрации Трафика Защищаемого ресурса не гарантируется.
3. Система переводится в режим мониторинга Аномалий и Атак в Трафике Защищаемого ресурса.
4. В течение периода от двух часов до двух недель с момента начала поступления Трафика Защищаемого ресурса в Центр очистки или начала поступления Трафика на Сенсор (если установка Сенсора предусмотрена) производится сбор статистических данных по Трафику Защищаемых ресурсов, достаточных для построения Профилей трафика.
5. 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 Лицензиата о наличии Аномалий или Атак в соответствии с параметрами оповещений, определенными в разделе Оповещения.
6. Служба технической поддержки KDP обеспечивает Фильтрацию и контроль степени очистки Трафика.
7. После регистрации Системой завершения Атаки Служба технической поддержки KDP оповещает об этом Контактных лиц Лицензиата.
8. После завершения Атаки в Личном кабинете Лицензиату становится доступен отчет об Атаке.

3.2. Процессы при работе с зашифрованным трафиком

Процесс взаимодействия при схеме доставки Трафика с помощью Reverse-Proxy, Лицензиат включает дополнительные аспекты:

1. Предоставление Лицензиатом доступа к Сертификату домена Защищаемого ресурса и соответствующего ему Закрытого ключа:
   - 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.
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 Лицензиатом оригинального или дублирующего сертификата домена Защищаемого ресурса, выпущенного Удостоверяющим центром по запросу Лицензиата и переданного Службе технической поддержки KDP:

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

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

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

4. Распределение ответственности между Исполнителем и Лицензиатом

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

Таблица 1

Сфера ответственности	Исполнитель	Лицензиат
Обеспечение Перенаправления трафика Защищаемого ресурса на Центр очистки		+
Работоспособность Площадки Лицензиата		+
Отслеживание Аномалий и Атак в Трафике защищаемого Ресурса	+	
Оповещение сотрудников Лицензиата о предполагаемых Атаках на Защищаемый ресурс	+	
Оповещение сотрудников Лицензиата 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 Лицензиата в работоспособном состоянии, оповещение о производимых изменениях		+

Работоспособность Bypass ресурсов		+

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

Таблица 2

Сфера ответственности	Исполнитель	Лицензиат
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 Reverse-Proxy и передача Сертификата домена Защищаемого ресурса Лицензиатом Исполнителю, то в сферу ответственности Исполнителя и Лицензиата так же входит:

Таблица 3

Сфера ответственности	Исполнитель	Лицензиат
Риск компрометации сертификата при передаче сертификата и соответствующего ему Закрытого ключа Лицензиатом Исполнителю		+
Риск компрометации сертификата при выпуске дублирующего сертификата Партнером Исполнителя	+	
Контроль истечения срока действия оригинального сертификата, переданного Лицензиатом 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 технической поддержки.

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 технической поддержки.
2. Уведомление Контактных лиц Лицензиата 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 Лицензиата в соответствии с параметрами, определенными в разделе Оповещение, о возврате характеристик Трафика Защищаемого ресурса к норме, свидетельствующем о завершении Атаки.
5. Уведомление Контактных лиц Лицензиата 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 Лицензиата о решении Инцидента, в соответствии с параметрами, определенными в разделе Оповещения.
8. Прием и регистрацию обращений Контактных лиц Лицензиата, в соответствии с параметрами, определенными в разделе Уровни технической поддержки.
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 Лицензиата 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 Лицензиата и Технической поддержкой возможны по телефону и электронной почте.

5.2 Уровни технической поддержки

В рамках оказания Технической поддержки Услуги доступны несколько уровней сервисного обслуживания соответствии с Лицензией. Сравнительные характеристики уровней сервисного обслуживания приведены в Таблице 4:

Таблица 4

SLA план технической поддержки	Light	Base	Standard	Advanced
Анализ и защита трафика	24x7	24x7	24x7	24x7
Экстренная техническая поддержка (ERT - Emergency Response Team)				
Режим работы ERT	24x7	24x7	24x7	24x7
Каналы связи с ERT				
e-mail	да	да	да	да
чат-бот	да	да	да	да
телефон	x	x	да	да
Время реакции на обращения в ERT	до 30 минут	до 30 минут	до 20 минут	до 10 минут
Реакция на обращение: Инцидент				
Критический	до 1 час	до 1 часа	до 30 минут	до 15 минут

Существенный	до 4 часов	до 2 часов	до 1 часа	до 30 минут
Некритичный	до 12 часов	до 12 часов	до 4 часов	до 2 часов
Расширенная техническая поддержка (AMT - Advanced Maintenance Team)				
Режим работы расширенной технической поддержки	5x8	5x8	24x7*	24x7*
Реакция на обращение: RFC	до 24 часов	до 12 часов	до 4 часов	до 1 часа
Персональный технический менеджер	x	x	да	да
Экспертная верификация отчетов об Атаках	нет	нет	да	да
Экспертная верификация отчетов об Ресурсе	нет	нет	да	да
Live-митинги с инженерами 3й линии	x	x	x	да

*- работы за рамками 8x5 проводятся в согласованное с Техническим менеджером время

5.3 Взаимодействие по электронной почте

Электронная почта является основным средством связи со Службой технической поддержки KDP. Обращения Контактных лиц Лицензиата принимаются на адрес support@kdp.zone . 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 Лицензиата для конкретного Контактного лица Лицензиата. Список Контактных лиц Лицензиата 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 Лицензиата 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 Лицензиата об Атаках и Инцидентах.

Обращения Лицензиата принимаются по телефону +7 (495)363-93-38 только от Контактных лиц Лицензиата. 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 Лицензиата для данного Контактного лица Лицензиата, 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 «kdp.kaspersky.com» и предназначен для управления Списком контактных лиц Лицензиата, а также для предоставления Контактным лицам Лицензиата информации о Трафике Защищаемых ресурсов.

Используя Личный кабинет, Контактные лица Лицензиата 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 Оповещения

Автоматическое оповещение обо всех Аномалиях и Атаках в Трафике Защищаемых ресурсов настраивается через Личный кабинет.

Дополнительное оповещение Контактных лиц Лицензиата по телефону о выявленных Атаках в Трафике Защищаемых ресурсов для клиентов в режиме On-Demand, в течении 15 минут с момента начала атаки.

Оповещения об Инцидентах производится Технической поддержкой KDP в соответствии с параметрами, определенными в Таблице 5.

Таблица 5

Событие	Light	Base	Standard	Advanced
Возникновение Инцидента	2 часа по электронной почте	2 часа по электронной почте	1 час по электронной почте	15 минут по электронной почте
Решение Инцидента	2 часа по электронной почте	2 часа по электронной почте	1 час по электронной почте	15 минут по электронной почте

5.7 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 X.

5.8 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 X.

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

5.9 Время реакции и решения RFC

Время реакции на RFC специфицировано в Таблице 4, время решения RFC планируется на следующий временной слот для внесения Изменений в Систему, обозначенный в ответе на RFC (не менее 2 слотов с 8 до 19 в рабочие дни). Если RFC не является стандартной процедурой согласно Описанию системы, время предоставления решения по RCF не регламентируется.

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 Лицензиат не выполняет свои обязательства по участию в решении Инцидентов, в соответствии с условиями, определенными в разделе Обязательства Лицензиата по участию в решении Инцидентов;
6. решение Инцидентов, условия возникновения которых не могут быть воспроизведены ни Лицензиатом, ни Технической поддержкой KDP;
7. решение Инцидентов, являющихся следствием превышения Легитимным трафиком Лицензиата выделенной полосы пропускания, определенной в Лицензии$

В рамках обеспечения работоспособности Защищаемого ресурса KDP ERT не осуществляет:

1. Анализ безопасности и производительности программно-аппаратных комплексов Лицензиата, а также консультации Контактных лиц Лицензиата по связанным вопросам;
2. Конфигурирование и администрирование программно-аппаратных комплексов Лицензиата, за исключением Сенсора, установленного на Площадке Лицензиата, а также консультации Контактных лиц Лицензиата по связанным вопросам;
3. Администрирование оборудования интернет-провайдера, услугами которого пользуется Лицензиат, а также консультации Контактных лиц Лицензиата по связанным вопросам;
4. Взаимодействие с персоналом интернет-провайдера, услугами которого пользуется Лицензиат, а также консультации Контактных лиц Лицензиата по связанным вопросам;

5. Проведение ремонтно-восстановительных работ на программно-аппаратных комплексах Лицензиата, за исключением Сенсора, размещенного на Площадке Лицензиата, а также консультации Контактных лиц Лицензиата по связанным вопросам;
6. Для Схемы Подключения с доставкой трафика с помощью Reverse-Proxy 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 Лицензиата. При повторном перенаправлении Трафика Защищаемого ресурса Клиент согласовывает со Службой Технической поддержки KDP факт перенаправления Трафика на Центры очистки.

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

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

6. Параметры функционирования Системы

6.1 Параметры Фильтрации Трафика

В процессе Фильтрации Трафика Защищаемых ресурсов Перенаправленного на ЦО, Исполнитель, гарантирует, что Система:

1. будет пропускать Трафик между Защищаемыми ресурсами и IP-адресами, помещенными Лицензиатом в «белые списки»;
2. будет блокировать Трафик между Защищаемыми ресурсами и IP-адресами, помещенными Лицензиатом в «черные списки»;
3. обеспечит очистку Трафика Защищаемых ресурсов в 98%[1] случаев на основе следующего алгоритма:

[1] Исключением является очистка Трафика Защищаемых ресурсов, работающих по протоколу HTTPS, в отношении которых Лицензиат не выполняет условия, определенные в п.3 раздела Описание Системы

Kaspersky DDoS Prevention+ – решение, которое позволяет защитить ресурсы Клиента от DDoS-атак путем перенаправления пользовательского трафика на Центры очистки Исполнителя.

Назначение Системы — обнаружение DDoS-атак, а также очистка (фильтрация) трафика путем выявления и блокирования паразитного трафика, результатом чего является снижение нагрузки на атакуемый ресурс.

В ходе работы Система выполняет следующие функции:

- Собирает статистические параметры трафика Защищаемых ресурсов;
- Осуществляет построение профилей легитимного трафика Защищаемых ресурсов и вырабатывает на их основе правила обнаружения аномалий и атак;
- Производит мониторинг возникновения аномалий и атак в трафике Защищаемых ресурсов;
- Осуществляет фильтрацию трафика Защищаемых ресурсов, перенаправленного через Центр очистки, от паразитной составляющей;

Выполняет вспомогательные задачи, обеспечивающие работу перечисленных функций.

Схема работы Системы

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 4:

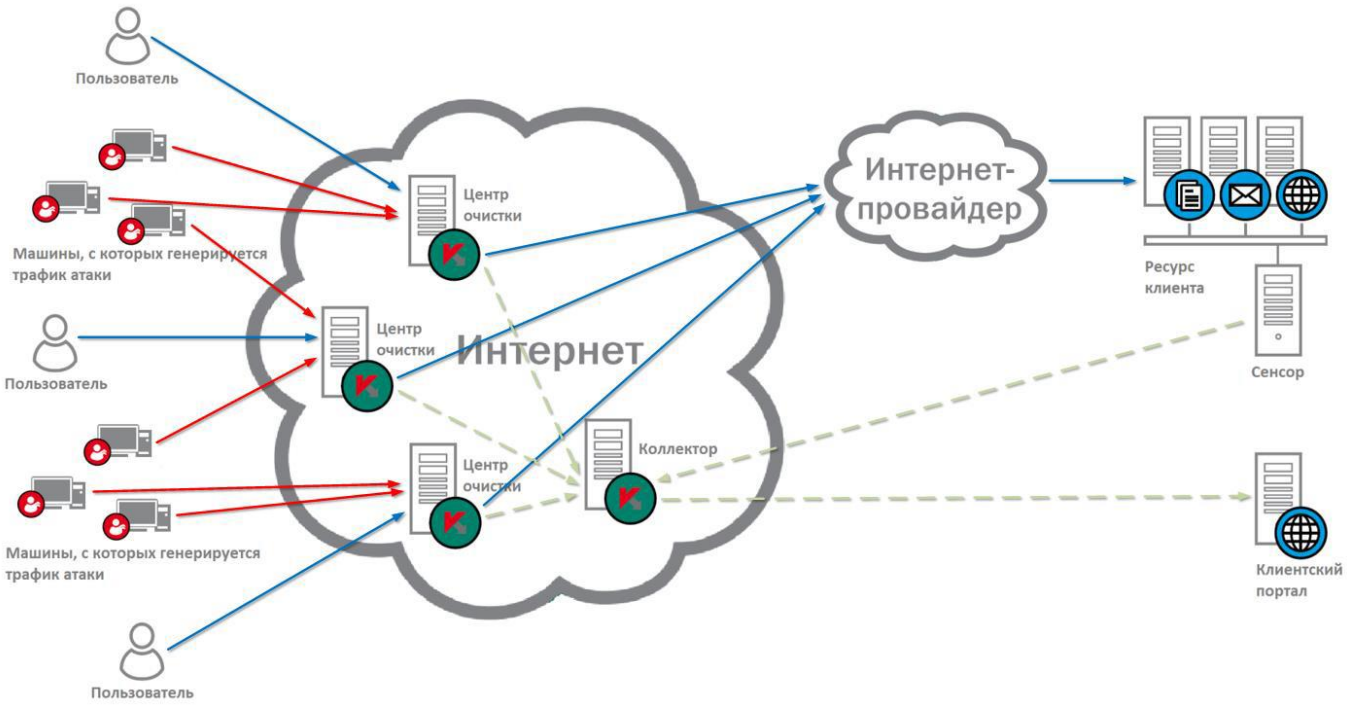
Таблица 4

Тип Атаки, параметр фильтрации/ Тип Лицензии	**KDP Standard**	**KDP Ultimate**	**KDP Ultimate+**
Атаки, основанные на использовании протоколов UDP и ICMP (с большим размером пакетов)	500 Гбит/с	1500 Гбит/с	2500 Гбит/с
Атаки на основе транспортных протоколов TCP, IPSEC, GRE и др.	3 Гбит/с или 5 млн пакетов/с	10 Гбит/с или 15 млн пакетов/с	20 Гбит/с или 25 млн пакетов/
Атаки на основе прикладных протоколов HTTP, HTTPS и др.	до 3000 RPS	до 10000 RPS	до 30000 RPS

* В случае если емкость Атаки превысит указанные лимиты, Система может ввести ограничения к Трафику (полностью блокирует или ограничивает), перенаправленному Лицензиатом на Центры очистки.

6.2 Ограничение полосы фильтрации

Исполнитель закрепляет за Лицензиатом полосу фильтрации Легитимного трафика, ограниченную на входе в Центров очистки, в объеме, не более предусмотренного Лицензией.



Условия работоспособности – в этом случае очистка Трафика Защищаемых ресурсов обеспечивается в 80% случаев.

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

6.3 Предоставление отчетов

Отчеты доступны Контактным лицам Лицензиата через Личный кабинет и формируются Системой автоматически. Состав отчетов, включенных в уровни техничкой поддержки, определен в Таблице 10

Таблица 10

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

Отчет о списках адресов представляет собой актуальный на момент формирования отчета список «белых» и/или «черных» адресов Защищаемого ресурса, помещенных Контактными лицами Лицензиата 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 Лицензиата через Личный кабинет. Информация об Атаках хранится в течение срока оказания Услуги и доступна Контактным лицам Лицензиата 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 Лицензиата 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

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

1. изменений Лицензиатом 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 Лицензиатом, или связанного с модернизацией Системы по запросу Лицензиата;
3. невыполнения Лицензиатом своих обязательств по участию в решении Инцидентов, в соответствии с условиями, определенными в разделе Обязательства Лицензиата по участию в решении Инцидентов;
4. обстоятельств, препятствующих работе Системы, возникших по вине Лицензиата;
5. вмешательства Лицензиата или третьей стороны в работу оборудования или программного обеспечения, находящегося на территории Лицензиата, обеспечивающего работу Системы, без согласования со Технической поддержкой KDP;
6. Перенаправления трафика Защищаемого ресурса без согласования со Службой технической поддержки KDP;
7. отказа оборудования Лицензиата или Интернет-провайдера, услугами которого пользуется Лицензиат;
8. блокировки каналов поставщиком телекоммуникационных услуг связи на участке сетевого маршрута между Площадкой Лицензиата и Центром очистки;
9. перерыва в работоспособности Системы, причиной которого являются обстоятельства непреодолимой силы, предусмотренные применимым законодательством.

8. Обязательства Лицензиата по участию в решении Инцидентов

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

В ходе взаимодействия со Службой технической поддержки KDP по решению Инцидента, Лицензиат 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 Лицензиата, Лицензиат обязан предоставить Службе технической поддержки KDP доступ к указанным компонентам по запросу Исполнителя, если все другие средства диагностики оказались неэффективными.