2024

Сертификат качества на программное обеспечение «Kaspersky DDoS Prevention +»

ПРЕДЕЛЬНЫЕ УСЛОВИЯ ФУНКЦИОНИРОВАНИЯ ПО ПРИОБРЕТЕННЫМ ЛИЗЕНЗИЯМ И ОПИСАНИЕ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Оглавление

Определения

Система – программно-аппаратный комплекс Kaspersky DDoS Prevention+, предназначенный для обнаружения и фильтрации DDoS-атак.

Анализ – анализ данных о Трафике 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 трафика от статистических. Наличие Аномалии не является гарантированным признаком Атаки – только подробный анализ трафика позволяет сделать вывод об Атаке.

Атака – распределенная атака на вычислительную систему, которая выполняется одновременно с большого числа компьютеров. Атака доводит вычислительную систему до отказа, то есть создает такие условия, при которых легитимные (правомерные) пользователи не могут получить доступ к ресурсам, либо доступ затруднен.

Защищаемый ресурс – сетевой сервис Лицензиата, находящийся под защитой Системы. Защищаемый ресурс определяется IP-адресом или IP-адресами и доменным именем или доменными именами.

> **Ресурс с ограниченной защитой** – определяемый IP-адресом или группой IP-адресов, входящих в одну подсеть, сетевой сервис Лицензиата, Трафик которого проходит через Центры Очистки. Ресурс без спецификации Защищаемых объектов, к Трафику которого может применяться Фильтрация на основании превышения нормальных для Ресурса 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, уникальным идентификатором которых является адрес электронной почты.

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.

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).

Лицензиат – лицо, владеющее лицензией на право использования программного обеспечения Kaspersky DDoS Prevention+.

Личный кабинет – компонент Системы, представляющий собой веб-интерфейс и предназначенный 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 Symmetric – режим постоянного прохождения Трафика Защищаемого ресурса через Центр очистки после Перенаправления трафика с сохранением симметрии Трафика.

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

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

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

Площадка Лицензиата – определяемая Схемой подключения совокупность оборудования Лицензиата, обеспечивающая работоспособность Защищаемых ресурсов и находящаяся в зоне ответственности Лицензиата.

Профиль фильтрации – набор значений параметров, с помощью которых измеряется трафик ресурса. Он характеризует обычное состояние трафика и представлен в виде статистических данных за определенный период времени.

Сенсор – компонент Системы, который получает информацию о трафике и преобразует ее в статистические данные.

Служба технической поддержки KDP – персонал, занятый в обслуживании и поддержке Системы Kaspersky DDoS Prevention+ и работающий с любыми запросами и проблемами Клиентов.

Emergency Response Team (KDP ERT) – технический персонал ООО «Модель защиты», работающий с Системой Kaspersky DDoS Prevention+, занятый в подключении новых Защищаемых ресурсов и обслуживании существующих, отражении Атак и их аналитике, приеме, регистрации и обработке обращений Лицензиата.

Advanced Maintenance Team (KDP AMT) –инженерный персонал ООО «Модель защиты», 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, недоступная из интерфейса Личного кабинета или API Системы.

Премиум RFC – экстренная заявка на изменение действующей конфигурации Системы, которая выполняется специалистами KDP AMT. По запросу Лицензиата любой стандартный запрос, обрабатываемый KDP ERT, может быть классифицирован как Премиум RFC и обработан с наивысшим приоритетом.

Схема подключения – документ (в минимальном виде письмо по электронной почте, согласованное всеми заинтересованными сторонами), описывающий все аспекты подключения/обеспечения доступности Системы 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 Лицензиата другие применимые характеристики.

Трафик – сетевые пакеты, передаваемые по каналам передачи данных.

Тестовое переключение – комплекс мер, осуществляемых для проверки корректности Схемы подключения. В ходе Тестового переключения Исполнителем и Лицензиатом производится Перенаправление трафика и оценивается корректность функционирования Защищаемых ресурсов под защитой. Подключение к Системе считается завершённым только после проведения Тестового переключения и подтверждения корректности работы Защищаемых ресурсов и Системы со стороны Исполнителя и Лицензиата.

Фильтрация – очистка Трафика, не являющегося Легитимным по отношению к Защищаемому ресурсу.

GEO-фильтрация – очистка Трафика, не входящего в Списки разрешенных или запрещенных стран для каждого профиля фильтрации, по определенным географическим зонам.

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. Располагается на площадке Исполнителя.

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

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

Центр сертификации – организация, обеспечивающая выпуск и управление Сертификатами доменов.

1. Описание Системы

Общее описание системы, которое опубликовано в онлайн-справке. Оно применимо к любой действующей Лицензии независимо от срока ее приобретения.

2. Условия работоспособности

1 Система Kaspersky DDoS Prevention+ в части Фильтрации Трафика Защищаемого ресурса считается 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 в ходе Тестового переключения и подтверждена Лицензиатом и Службой технической поддержки KDP. Лицензиат поддерживает работоспособность подтвержденной Схемы подключения на своей стороне, в том числе обеспечивает:

- Для Схемы подключения Always-On Symmetric – симметричное прохождение входящего и исходящего Трафика Защищаемого ресурса на Центры очистки в соответствии со Схемой подключения, а также работоспособность одного или более GRE-туннелей или выделенных каналов с активными BGP-сессиями до каждой Площадки Лицензиата.
- Для Схемы подключения Always-On Asymmetric – прохождение Трафика Защищаемого ресурса через Центры очистки в соответствии со Схемой подключения, а также работоспособность одного и более GRE-туннелей или выделенных каналов с активными BGP-сессиями до каждой Площадки Лицензиата.
- Для Схемы Подключения с доставкой трафика с помощью Обратного проксирования – доступность Защищаемых ресурсов для Системы.

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

2.1 Наличие на каждой Площадке Лицензиата не менее одного Сенсора, на который поступает полная копия неочищенного Трафика Защищаемого ресурса. При этом оборудование, используемое Лицензиатом для размещения Сенсора, должно соответствовать требованиям спецификации, предоставленной Службой технической поддержки 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 проксирования, Лицензиат обеспечивает возможность расшифровки запросов путем предоставления Службе технической поддержки KDP 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 Лицензиат перенаправляет полная копия расшифрованного Трафика (access-log) Защищаемого ресурса по протоколу Syslog в формате, согласованном в Схеме подключения.

4 Если схемой подключения предусмотрена доставка Трафика с помощью Обратного проксирования и предоставление Службе технической поддержки KDP 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.

5 Для Схем подключения, в условиях которых передача копии Трафика Защищаемого ресурса невозможна, со стороны Лицензиата должна быть организована передача данных о Трафике Защищаемого ресурса на Сенсор в формате *Flow (sFlow, NetFlow, jFlow). Формате передачи flow-потока определяется Схемой подключения.

3. Описание процесса взаимодействия

3.1. Основной процесс

Процесс взаимодействия между Лицензиатом и Службой технической поддержки KDP 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 Схеме подключения настраивается оборудование на стороне Лицензиата и Исполнителя для Перенаправления Трафика Защищаемого ресурса на Центр Очистки.
   - Если Схемой подключения предусмотрена установка Сенсора на Площадке Лицензиата, то также 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 в соответствии со Схемой подключения, в ходе которого проверяется корректность согласованной Схемы подключения и произведенных настроек оборудования.
   - При использовании режима On-demand трафик возвращается на Площадку Лицензиата без прохождения Центра очистки.
   - Любое изменение в Схеме подключения должно в обязательном порядке согласовываться со Службой технической поддержки KDP, фиксироваться в новой Схеме подключения, а работоспособность новой Схемы подключения должна быть проверена и подтверждена Службой технической поддержки KDP. 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 фильтрации.
5. В случае обнаружения Системой существенного отклонения реальных значений измеряемых параметров Трафика Защищаемого ресурса от Профиля фильтрации, которое свидетельствует 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

При использовании Схемы подключения с доставкой Трафика с помощью Обратного проксирования процесс работы Лицензиата включает дополнительные аспекты:

1. Предоставление Лицензиатом доступа к Сертификату домена Защищаемого ресурса и соответствующего ему Закрытого ключа путем выполнения следующих действий:
   1.1 Передать оригинальный Сертификат домена и соответствующий ему Закрытый ключ Службе технической поддержки KDP защищенным способом.
   1.2 Передать дублирующий сертификат домена и соответствующий ему Закрытый ключ Службе технической поддержки KDP защищенным способом.
2. 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 Центром сертификации по запросу Лицензиата и переданного Службе технической поддержки KDP, Лицензиат обязан предоставить Службе технической поддержки KDP следующую информацию:
      - причина и дата отзыва Сертификата домена;
      - сроки выпуска нового Сертификата и его передачи.
   3.2. В случае отзыва Центром сертификации оригинального или дублирующего Сертификата домена Защищаемого ресурса, выпущенного Центром сертификации по запросу Лицензиата и переданного Службе технической поддержки KDP:
      - Служба технической поддержки KDP при наличии достоверных сведений об отзыве Сертификата домена Центром сертификации обязана уведомить Лицензиата о факте, причине и дате отзыва Сертификата домена.
      - Лицензиат при наличии достоверных сведений об отзыве Сертификата домена Центром сертификации 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. Определение сферы ответственности

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 также входит:

Таблица 2. Определение сферы ответственности (Сенсор)

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		+
Наличие копии access-лога веб-сервера Защищаемого ресурса на Сенсоре		+

В случае, если Схемой подключения предусмотрена доставка Трафика с помощью Обратного проксирования и передача Сертификата домена Защищаемого ресурса Лицензиатом Исполнителю, то в сферу ответственности Исполнителя и Лицензиата также входит:

Таблица 3. Определение сферы ответственности (Сертификат)

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 Службы технической поддержки KDP, каналов коммуникаций, время решения Инцидентов, время обработки обращений и т.д. определены в разделе Уровни технической поддержки.

В обязанности Службы технической поддержки KDP входят следующие действия:

- Отслеживание Аномалий и Атак в Трафике Защищаемого ресурса в соответствии с параметрами, определенными в разделе Уровни технической поддержки.
- Уведомление Контактных лиц Лицензиата об Аномалиях и предполагаемых Атаках в Трафике Защищаемых ресурсов в соответствии с параметрами оповещения, определенными в разделе Оповещения.
- Контроль Фильтрации Трафика Защищаемого ресурса в случае подтверждения Атаки.
- Уведомление Контактных лиц Лицензиата в соответствии с параметрами, определенными в разделе Оповещения о возврате характеристик Трафика Защищаемого ресурса к норме, свидетельствующем о завершении Атаки.
- Уведомление Контактных лиц Лицензиата о регистрации Инцидента в случае его возникновения в соответствии с параметрами, определенными в разделе Время реакции на Инциденты.
- Решение Инцидента в соответствии с параметрами, определенными в разделе Время решения Инцидентов.
- Уведомление Контактных лиц Лицензиата о решении Инцидента, в соответствии с параметрами, определенными в разделе Оповещения.

- Прием и регистрация обращений Контактных лиц Лицензиата, в соответствии с параметрами, определенными в разделе Уровни технической поддержки.
- Контроль за ходом выполнения работ по обращениям, закрытие запроса в соответствии с параметрами, определенными в разделе Время реакции на обращения.
- Информирование Контактных лиц Лицензиата по Инцидентам/проблемам/работам массового характера, проводимым технологическим работам и внесенным изменениям, в случае если они могут повлиять на качество оказания Услуги.

Коммуникации между Контактными лицами Лицензиата и Службой технической поддержки KDP возможны по телефону и электронной почте.

5.2 Уровни технической поддержки

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

Таблица 4. Сравнительная характеристика уровней сервисного обслуживания

SLA план технической поддержки	Standart	Business	Enterprise	Advanced
Анализ и защита трафика	24x7	24x7	24x7	24x7
Служба технической поддержки KDP (ERT – Emergency Response Team)				
Режим работы ERT	24x7	24x7	24x7	24x7
Каналы связи с ERT				
e-mail	да	да	да	да
Telegram-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
Реакция на обращение: RFC	до 24 часов	до 12 часов	до 4 часов	до 1 часа
Служба технической поддержки KDP (AMT – Advanced Maintenance Team)				
Режим работы расширенной технической поддержки	5x8	24x7*	24x7*	24x7*
Экспертная верификация отчетов об Атаках	x	x	да	да
Экспертная верификация отчетов об Ресурсе	x	x	да	да
Обзор инцидентов	x	x	x	да

*- работы за рамками 8x5 проводятся в согласованное с Техническим менеджером время в рамках Премиум RFC.

В рамках Услуги предусмотрена возможность по запросу Лицензиата любой стандартный запрос, обрабатываемый KDP ERT, классифицировать как Премиум RFC. Запрос принимается в работу и выполняется специалистами KDP AMT с наивысшим приоритетом. Сравнительные характеристики уровней сервисного обслуживания приведены в Таблице 5.

Таблица 5. Сравнительная характеристика уровней сервисного обслуживания (Премиум RFC)

SLA план технической поддержки	Standart	Business	Enterprise	Advanced
Премиум RFC, в месяц	1	2	6	12
Премиум RFC, в год	4	8	16	36
Время реакции на обращение	до 15 минут	до 15 минут	до 15 минут	до 15 минут

5.3 Взаимодействие по электронной почте

Электронная почта является основным средством связи со Службой технической поддержки KDP. Обращения Контактных лиц Лицензиата принимаются на адрес электронной почты kdp@kaspersky.com. В тексте обращения необходимо указать:

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

При обращении Службы технической поддержки KDP к Контактному лицу Лицензиата 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, не зарегистрированных в Списке контактных лиц Лицензиата, Исполнитель оставляет за собой право не обрабатывать поступившие обращения.

5.4 Взаимодействие по телефону

Телефон 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:

- название компании;
- ФИО;
- название и IP-адрес Защищаемого ресурса, в отношении которого делается запрос;
- 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, чтобы дополнительно проверить правомерность обращения.

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

5.5 Взаимодействие с использованием Личного кабинета

Личный кабинет Системы доступен по адресу https://portal.kdp.global/ 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:

- анализировать статистику по Трафику Защищаемых ресурсов;
- анализировать состояние Трафика Защищаемых ресурсов во время Атак;
- настраивать механизмы автоматического оповещения;
- редактировать Списки разрешенных IP-адресов и Списки запрещенных IP-адресов, влияющие на параметры Фильтрации;
- 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. Через Личный кабинет возможно настроить уведомления по прочим событиям Системы.

Дополнительное оповещение Контактных лиц Лицензиата по телефону о выявленных Атаках в Трафике Защищаемых ресурсов осуществляется 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 6.

Таблица 6. Время оповещения об Инцидентах

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 Служба технической поддержки KDP, зависит от степени критичности Инцидента, временной зоны Лицензиата, зафиксированной в Схеме подключения и уровней сервисного обслуживания и определено в Таблице 6.

5.8 Время решения Инцидентов

Время решения Инцидентов, которое обеспечивает Служба технической поддержки KDP, зависит от степени критичности Инцидента, уровней сервисного обслуживания, и временной зоны Лицензиата, зафиксированной в Схеме подключения и определено в Таблице 6.

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 Описании Системы. Если RFC не является стандартной процедурой согласно Описанию системы, время предоставления решения по RCF не регламентируется.

5.10 Ограничения технической поддержки

В обязанности Службы технической поддержки KDP не входят следующие действия:

- Реагирование на обращения, не связанные с защитой от Атак, в том числе вопросы, связанные с временем отклика ресурса или его доступностью из сети Интернет.
- Реагирование на обращения, касающиеся работы ресурсов, не входящих состав Защищаемых ресурсов.
- Реагирование на обращения, связанные с утечкой секретного ключа Сертификата домена.
- Реагирование на обращения, касающиеся работы любых программно-аппаратных комплексов, не входящих в состав Системы.
- 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.
- Решение Инцидентов, условия возникновения которых не могут быть воспроизведены ни Лицензиатом, ни Службой технической поддержки KDP.
- Решение Инцидентов, являющихся следствием превышения Легитимным трафиком Лицензиата выделенной полосы пропускания, определенной в разделе Закрепление выделенной полосы пропускания.

В рамках обеспечения работоспособности Защищаемого ресурса в обязанности Службы технической поддержки KDP не входят следующие действия:

- Анализ безопасности и производительности программно-аппаратных комплексов Лицензиата, а также консультация Контактных лиц Лицензиата по связанным вопросам.
- Конфигурирование и администрирование программно-аппаратных комплексов Лицензиата, за исключением Сенсора, установленного на Площадке Лицензиата, а также консультация Контактных лиц Лицензиата по связанным вопросам.
- Администрирование оборудования интернет-провайдера, услугами которого пользуется Лицензиат, а также консультация Контактных лиц Лицензиата по связанным вопросам.

- Взаимодействие с персоналом интернет-провайдера, услугами которого пользуется Лицензиат, а также консультация Контактных лиц Лицензиата по связанным вопросам.
- Проведение ремонтно-восстановительных работ на программно-аппаратных комплексах Лицензиата, за исключением Сенсора, размещенного на Площадке Лицензиата, а также консультация Контактных лиц Лицензиата по связанным вопросам.
- Для Схемы Подключения с доставкой трафика с помощью Обратного проксирования – настройка параметров проксирования, в том числе кэширования, балансировки между несколькими адресами Защищаемого ресурса и иных параметров, обеспечивающих контроль за сетевым обменом Защищаемого ресурса.
- Проведение других работ, не связанных непосредственно с работой Системы и ее компонентов.

В случае обнаружения Службой технической поддержки KDP отсутствия Трафика Защищаемого ресурса на Центре очистки, производится 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@kaspersky.com.

6. Параметры функционирования Системы

6.1 Параметры Фильтрации Трафика

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

- будет пропускать Трафик между Защищаемыми ресурсами и IP-адресами, помещенными Лицензиатом в Списки разрешенных IP-адресов;
- будет блокировать Трафик между Защищаемыми ресурсами и IP-адресами, помещенными Лицензиатом в Списки запрещенных IP-адресов;
- обеспечит очистку Трафика Защищаемых ресурсов в 98%[1] случаев на основе следующего алгоритма:
  - 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;
  - 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.
- обеспечит фильтрацию Трафика в 98% случаев при условии, что емкость Атаки, направленной на Защищаемые ресурсы, не превышает лимиты*, определенные в Таблице 7.

Таблица 7. Предельные лимиты фильтрации DDoS-атак

Тип Лицензии/ Тип Атаки, параметр фильтрации	Kaspersky DDoS Prevention+, WebIP 25 Мб/с	Kaspersky DDoS Prevention+, WebIP 75 Мб/с	Kaspersky DDoS Prevention+, Bundle 200 Мб/с	Kaspersky DDoS Prevention+, Bundle 500 Мб/с	Kaspersky DDoS Prevention+, Bundle 1,25 Гб/с	Kaspersky DDoS Prevention+, Bundle 3,00 Гб/с
Атаки, основанные на использовании протоколов UDP и ICMP	1000 Гбит/с	1500 Гбит/с	2000 Гбит/с	2500 Гбит/с	Без лимита	Без лимита
Атаки на основе транспортных протоколов TCP, IPSEC, GRE и др.	5 Гбит/с или 10 млн пакетов/с	10 Гбит/с или 15 млн пакетов/с	15 Гбит/с или 20 млн пакетов/	50 Гбит/с или 25 млн пакетов/	80 Гбит/с или 35 млн пакетов/	100 Гбит/с или 50 млн пакетов/
Атаки на основе прикладных протоколов	2500 RPS	50000 RPS	100000 RPS	100000 RPS	150000 RPS	250000 RPS

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

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

6.2 Ограничение полосы фильтрации

Исполнитель закрепляет за Лицензиатом полосу фильтрации Легитимного трафика, ограниченную на входе в Центр очистки, в объеме, не более предусмотренного Лицензией и указанного в Таблице 8.

Таблица 8. Описание параметров лицензии KDP

Параметры лицензии KDP+	Kaspersky DDoS Prevention+, WebIP 25 Мб/с	Kaspersky DDoS Prevention+, WebIP 75 Мб/с	Kaspersky DDoS Prevention+, Bundle 200 Мб/с	Kaspersky DDoS Prevention+, Bundle 500 Мб/с	Kaspersky DDoS Prevention+, Bundle 1,25 Гб/с	Kaspersky DDoS Prevention+, Bundle 3,00 Гб/с
Общий объем легитимного трафика под защитой, Мб/с*	25	75	200	500	1280	3072
в том числе в режиме Обратного проксирования, Мб/с**	25	75	100	200	400	800
превышение объема легитимного трафика	допускается не более чем на 2 месяца подряд**					
Гарантированная доступность ресурса в месяц, %	97,5%	99,0%	99,5%	99,5%	99,5%	99,9%
Допустимое превышение атак, суток в год/в месяц	30/15	45/15	45/15	45/31	90/31	90/31
Доступ к API	x	x	да	да	да	да
Бесплатный сертификат от Let’s Encrypt	да	да	да	да	да	да
Активная проверка доступности	x	да	да	да	да	да
Балансировка трафика (апстримов на IP)	2	3	3	10	10	10
Количество правил в списках, шт. на IP	10	25	50	50	100	100
GEO-фильтрация	да	да	да	да	да	да
Применимый SLA для технической поддержки	Standard	Business	Enterprise	Enterprise	Advanced	Advanced
Возможность обработки запроса инженерами KDP AMT	x	x	да	да	да	да
Персональный технический менеджер	x	x	x	x	да	да
Проведение удаленных аудио-совещаний с KDP AMT	x	x	x	x	x	да

* - по данным с Сенсора Лицензиата, учитывается превалирующий Трафик

** - В случае превышения объема трафика 2 месяца подряд, Лицензиат обязуется повысить уровень лицензии

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 9.

Таблица 9. Отчеты, включенные в уровни технической поддержки

Тип отчета	Standard	Business	Enterprise	Advanced
Отчет о списках адресов	-	-	-	+
Отчет об атаке	+	+	+	+
Отчет о ресурсе	-	-	+	+

Отчет о списках адресов представляет собой актуальный на момент формирования отчета Список разрешенных и/или запрещенных 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 10.

Таблица 10. Время проведения работ на инфраструктуре KDP

Тип работ	Продолжительность	Уведомления
Проведение плановых технологических работ	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:

- изменений Лицензиатом Схемы подключения или других настроек, прямо или косвенно влияющих на работоспособность находящихся в зоны ответственности Исполнителя компонентов Системы и произведенных без согласования со Службой технической поддержки KDP;
- планового технического обслуживания Системы, заранее согласованного с Лицензиатом или связанного с модернизацией Системы по запросу Лицензиата;
- невыполнения Лицензиатом своих обязательств по участию в решении Инцидентов, в соответствии с условиями, определенными в разделе Обязательства Лицензиата по участию в решении Инцидентов;
- обстоятельств, препятствующих работе Системы, возникших по вине Лицензиата;
- вмешательства Лицензиата или третьей стороны в работу оборудования или программного обеспечения, находящегося на территории Лицензиата, обеспечивающего работу Системы, без согласования со Службой технической поддержки KDP;
- Перенаправления трафика Защищаемого ресурса без согласования со Службой технической поддержки KDP;
- отказа оборудования Лицензиата или Интернет-провайдера, услугами которого пользуется Лицензиат;
- блокировки каналов поставщиком телекоммуникационных услуг связи на участке сетевого маршрута между Площадкой Лицензиата и Центром очистки;
- 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.

9. Метрики измерения доступности Защищаемых ресурсов

Метрикой доступности Защищаемых ресурсов являются процент успешных проверок внешней системы мониторинга. В случаях со Схемой подключения с Обратным проксированием возможна оценка доступности по успешным кодам ответов веб-сервера (200).

Если трафик всех Защищаемых ресурсов Клиента не проходит через Систему, то показателем доступности Системы является Личный кабинет Kaspersky DDoS Prevention+ (https://portal.kdp.global/). В показателе доступности Системы и Защищаемых ресурсов учитываются только проблемы связанные с качеством Фильтрации DDoS-атак и проблемы в работе Системы. Иные Инциденты, которые привели к недоступности Защищаемых ресурсов не учитываются при расчете выполнения Соглашения об уровне обслуживания (SLA), а также ситуации описанные в разделе Исключения.