Сертификат качества

на программное обеспечение

Kaspersky DDoS Prevention

Содержание

Содержание 1
Определения 2
1. Условия работоспособности 4
2. Общее описание процесса взаимодействия 5
3. Распределение ответственности между АО «Лаборатория Касперского» и Лицензиатом 7
4. Техническая поддержка 8
4.1. Объем технической поддержки 8
4.2. Взаимодействие по электронной почте 8
4.3. Взаимодействие по телефону 9
4.4. Взаимодействие с использованием Личного кабинета 9
4.5. Время реакции на обращения 9
4.6. Оповещения 10
4.7. Время реакции на Инциденты 10
4.8. Время решения Инцидентов 10
4.9. Ограничения технической поддержки 10
5. Параметры функционирования Системы 12
5.1. Общие параметры функционирования 12
5.2. Параметры Фильтрации Трафика 12
5.3. Положение о принципах работы с шифрованным трафиком 13
5.4. Закрепление выделенной полосы пропускания 13
5.5. Предоставление отчетов 14
5.6. Время хранения информации в Системе 14
5.7. Согласованные перерывы в функционировании Системы 14
6. Исключения 16
7. Обязательства Лицензиата по участию в решении Инцидентов 17

Определения

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

Аномалия - отклонение реальных значений измеряемого параметра Трафика Защищаемого ресурса более чем на 50% от установленного значения Профиля трафика, длящееся более чем 30 минут и свидетельствующее о возможной Атаке.

Атака - распределённая, атака на вычислительную систему, выполняемая одновременно с большого числа компьютеров с целью довести вычислительную систему до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен.

Время реакции – период времени, в течение которого будет начата обработка обращения для получения технической поддержки или обращения по Инциденту.

Время решения - период времени (с момента окончания Времени реакции), в течение которого будет найдено постоянное или временное решение, нивелирующее влияние Инцидента на работу Защищаемых ресурсов.

Защищаемый ресурс – сетевой сервис Лицензиата, определяемый IP адресом.

Инцидент – любое событие, связанное с Атакой на Защищаемый ресурс, вызванное проблемами в работе Системы или действиями Службы эксплуатации KDP, 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 в течение 5 и более минут.
>
> **Существенный инцидент** – Инцидент, который приводит к частичной недоступности Защищаемого ресурса из сети Интернет в течение 15 и более минут.
>
> **Некритичный** Инцидент – все остальные Инциденты, которые не оказывают существенного негативного влияния на работоспособность Защищаемого ресурса.

Контактные лица Лицензиата – сотрудники Лицензиата, ответственные за переключение Трафика на Центры очистки.

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

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

Перенаправление трафика – комплекс действий по изменению сетевого маршрута доставки Трафика защищаемого Ресурса к Центру очистки. Перенаправление трафика выполняется Лицензиатом в случае подтверждения наличия Атаки Службой эксплуатации KDP. Возможно Перенаправление трафика по инициативе Лицензиата в условиях отсутствия Атаки по согласованию со Службой эксплуатации KDP.

Площадка Лицензиата - физическая площадка (здания, помещения), на которой размещены Защищаемые ресурсы.

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

Сенсор - компонент Системы, который передается Лицензиату. Устанавливается на сервере, принадлежащем Лицензиату, 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. Также является объектом лицензирования.

Служба эксплуатации KDP - технический персонал АО «Лаборатория Касперского», непосредственно работающий с системой Kaspersky DDoS Prevention, занятый в подключении новых Защищаемых ресурсов и обслуживании существующих, отражении Атак и их аналитикой.

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, включая информацию о времени доступности Контактного лица Лицензиата и приоритета оповещений. Лицензиат должен гарантировать круглосуточную доступность хотя бы одного из Контактных лиц Лицензиата.

Схема подключения - документ, описывающий все аспекты подключения, такие как список Защищаемых ресурсов, список Площадок Лицензиата, список незащищаемых ресурсов (Трафик которых проходит через Центры Очистки во время Атак), способ Перенаправления трафика, место установки Сенсора, точки терминации виртуальных туннелей.

Трафик - сетевые пакеты, передаваемые по каналам передачи данных сети Интернет.

Фильтрация – выявление и удаление в Трафике сетевых пакетов не являющихся легитимными.

Центр очистки - компонент Системы, который осуществляет анализ и Фильтрацию проходящего через него Трафика, а также сбор, анализ и хранение статистической информации о Трафике, поступающей с Сенсоров. Располагается на независимой, физически удаленной от оборудования Лицензиата площадке, принадлежащей АО «Лаборатории Касперского».

Bypass ресурс - сетевой сервис Заказчика, определяемый IP адресом, Трафик которого проходит через Центры Очистки, в отношении которого Услуга не оказывается, но к Трафику, которого может применяться Фильтрация.

1. Условия работоспособности

Система «Kaspersky DDoS Prevention» в части Фильтрации Трафика может эффективно работать только при условии, что со Службой эксплуатации KDP согласована Схема подключения и успешно проведено тестовое Перенаправление Трафика в соответствии со Схемой подключения, а Лицензиат поддерживает актуальность Схемы подключения на своей стороне, в том числе обеспечивает:

- Наличие не менее одного Сенсора на каждой Площадке Лицензиата, на который поступает полная копия неизмененного Трафика Защищаемого ресурса[1]. При этом оборудование, используемое Лицензиатом для размещения Сенсора, должно соответствовать требованиям спецификации, предоставленной Службой эксплуатации KDP.
- Доступность Сенсора из сети Интернет и актуальность сетевых доступов к Сенсору из Центров Очистки.
- Перенаправление трафика Лицензиатом на Центры очистки в момент Атаки в соответствии со Схемой подключения. При этом через Центры очистки должен проходить весь Трафик, как входящий, так и исходящий.
- Превентивное Перенаправление трафика Лицензиатом на Центры очистки, согласованное со Службой эксплуатации KDP, в соответствии со Схемой подключения. При этом через Центры очистки должен проходить весь Трафик, как входящий, так и исходящий.
- Для Схемы подключения с маршрутизацией трафика - работоспособность не менее двух 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.
- Поддержание в актуальном состоянии списка протоколов и портов на Защищаемом ресурсе, в отношении которых должна осуществляться Фильтрация.
- Поддержание в актуальном состоянии Списка контактных лиц Лицензиата и доступность хотя бы одного из Контактных лиц круглосуточно.

[1] В случае, если Защищаемый ресурс работает по протоколу HTTPS, на Сенсоре должен присутствовать дополнительный сетевой интерфейс, на котором присутствует расшифрованная копия Трафика.

2. Общее описание процесса взаимодействия

Общий процесс взаимодействия между Лицензиатом и АО «Лаборатория Касперского», в ходе эксплуатации Системы включает следующие основные этапы:

- Выполняется подключение к Системе, в ходе которого Лицензиатом и Службой эксплуатации KDP согласовывается Схема подключения, согласно которой настраивается оборудование на стороне Лицензиата и АО «Лаборатория Касперского».
- Лицензиат предоставляет Службе эксплуатации KDP список протоколов и портов на Защищаемом ресурсе, в отношении которых должна осуществляться Фильтрация.
- В течение двух недель с момента начала поступления Трафика на Сенсор, производится сбор статистических данных по Трафику Защищаемых ресурсов и строятся Профили трафика. При отсутствии Сенсора или копии Трафика Защищаемых ресурсов в неизмененном виде на Сенсоре, эффективность мониторинга и Фильтрации Трафика не гарантируются.
- Проводится тестовое Перенаправление трафика, в ходе которого проверяется корректность согласованной Схемы подключения и произведенных настроек оборудования, включая настройки оборудования, на котором размещен Сенсор. После успешного прохождения тестов, настройки оборудования должны поддерживаться в том состоянии, в котором они были зафиксированы в Схеме подключения.
- Лицензиат обязан оповещать Службу эксплуатации KDP о производимых изменениях, влияющих на Схему подключения. Любое изменение в Схеме подключения должно в обязательном порядке сопровождаться повторным тестовым Перенаправлением трафика и фиксированием новой Схемы подключения. В противном случае эффективность мониторинга и Фильтрации Трафика не гарантируется.
- Система переводится в режим мониторинга Аномалий и Атак в Трафике Защищаемых ресурсов.
- На свое усмотрение Контактные лица Лицензиата, по согласованию со Службой эксплуатации KDP, могут принять решение о Перенаправлении трафика, и производят действия по его перенаправлению на Центры очистки.
- В случае обнаружения Системой существенного отклонения реальных значений измеряемых параметров Трафика Защищаемого ресурса от Профиля трафика, Служба эксплуатации KDP оповещает Контактных лиц Лицензиата о наличии Аномалий или Атак в соответствии с параметрами оповещения, определенных в разделе Оповещения.
- Контактные лица Лицензиата принимают решение о Перенаправлении трафика.
- Контактные лица Лицензиата производят комплекс действий по Перенаправлению трафика, в соответствии со Схемой подключения.
- Служба эксплуатации KDP обеспечивает Фильтрацию и контроль степени очистки Трафика.
- После регистрации Системой завершения Атаки, Служба эксплуатации KDP оповещает об этом Контактных лиц Лицензиата.
- Контактные лица Лицензиата принимают решение о завершении нахождения под защитой и, после оповещения об окончании атаки от Службы эксплуатации KDP, выполняют действия по возврату Трафика на оригинальный маршрут. По инициативе Лицензиата срок

нахождения под защитой может быть продлен, но только при условии согласования со Службой эксплуатации KDP.

- Лицензиар вправе в любое время в одностороннем порядке вносить в настоящий Сертификат изменения, не связанные с ухудшением характеристик и параметров ПО, при условии, что любая новая редакция Сертификата будет размещена на Интернет-ресурсе Лицензиара www.kaspersky.ru за 30 дней до даты внесения таких изменений.

3. Распределение ответственности между АО «Лаборатория Касперского» и Лицензиатом

Сферы ответственности АО «Лаборатории Касперского» и Лицензиата в ходе эксплуатации Системы определены в Таблице 1.

Таблица 1

Сфера ответственности	АО «Лаборатория Касперского»	Лицензиат
Работоспособность программного обеспечения Сенсора	+	
Работоспособность Площадки Лицензиата, в том числе работоспособность оборудования, на котором размещен Сенсор		+
Отслеживание Аномалий и Атак в Трафике защищаемого Ресурса	+	
Оповещение сотрудников Лицензиата о предполагаемых Атаках на Защищаемый ресурс	+	
Оповещение сотрудников Лицензиата о завершении Атаки	+	
Принятие решения о Перенаправлении трафика и возврате Трафика на оригинальный маршрут		+
Перенаправление трафика во время Атаки, по инициативе Лицензиата или в ходе тестового переключения		+
Контроль качества работы системы очистки при включенном режиме Фильтрации	+	
Управление учетными записями защищаемых Ресурсов (DNS-записи) или маршрутизацией (BGP)		+
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, в том числе в составе протоколов и портов на Защищаемом ресурсе, в отношении которых должна осуществляться Фильтрация		+
Работоспособность незащищаемых ресурсов, Трафик которых идет через Центры очистки (переключение по BGP)[2]		+

[2] Трафик незащищаемых ресурсов пропускается через Центры очистки в соответствии с условиями, определенными в разделе Закрепление выделенной полосы пропускания

4. Техническая поддержка

4.1. Объем технической поддержки

Служба эксплуатации KDP обеспечивает коммуникации между Лицензиатом и АО «Лаборатория Касперского» и отвечает за прием и обработку запросов Контактных лиц Лицензиата. Техническая поддержка предоставляется ежедневно и круглосуточно. Параметры предоставления технической поддержки, не оговоренные в настоящем Сертификате, определяются в Регламенте Сопровождения, который предоставляется Лицензиату по запросу.

Техническая поддержка включает в себя следующие действия:

- уведомление Контактных лиц Лицензиата об Аномалиях и Атаках в Трафике Защищаемых ресурсов в соответствии с параметрами оповещения, определенными в разделе Оповещения;
- уведомление Контактных лиц Лицензиата о возврате характеристик Трафика к норме, свидетельствующем о завершении Атаки в соответствии с параметрами оповещения, определенными в разделе Оповещения;
- прием запросов Контактных лиц Лицензиата, их регистрация, классификация и, при необходимости, маршрутизация на следующие уровни поддержки;
- контроль хода выполнения работ по запросу, эскалация в случае возникновения проблем с исполнением запроса, информирование Контактных лиц Лицензиата о ходе выполнения работ, закрытие запроса;
- информирование Контактных лиц Лицензиата по Инцидентам/проблемам/работам массового характера, проводимым изменениям и технологическим работам.

Служба технической поддержки KDP имеет право отказать Лицензиату в выполнении запросов, превышающих объем технической поддержки, описанный 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.

4.2. Взаимодействие по электронной почте

Электронная почта является основным средством связи со Службой эксплуатации KDP. Обращения Контактных лиц Лицензиата 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 ящик, указанный в Списке контактных лиц Лицензиата для конкретного Контактного лица Лицензиата. В случае использования незарегистрированных в Списке контактных лиц лицензиата адресов электронной почты АО «Лаборатория Касперского» оставляет за собой право связаться с обратившимся Контактным лицом для дополнительной проверки правомерности обращения.

4.3. Взаимодействие по телефону

Взаимодействие по телефону является экстренным средством связи, предназначенным для информирования Службы эксплуатации KDP о возникновении Критических Инцидентов и информирования Контактных лиц Лицензиата об Атаках.

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

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

АО «Лаборатория Касперского» 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.

АО «Лаборатория Касперского» оставляет за собой право производить запись отдельных звонков для обеспечения контроля качества.

4.4. Взаимодействие с использованием Личного кабинета

Личный кабинет Системы расположен по адресу https://kdp.kaspersky.com и предназначен для управления Списком контактных лиц Лицензиата, а также 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 «белые списки» и «черные списки», влияющие на параметры Фильтрации;
- заказывать отчет о списках адресов и отчет об Атаке.

4.5. Время реакции на обращения

Время реакции на обращения Контактных лиц Лицензиата, которое обеспечивает Служба эксплуатации KDP в рамках оказания технической поддержки, зависит от типа обращения и определено в Таблице 2.

Таблица 2

Тип обращения	Время реакции
Подозрение на Атаку на Защищаемые ресурсы	15 минут
Вопросы (по работе Системы, использованию Личного кабинета и пр.)	1 час
Запросы на изменения (состава Защищаемых ресурсов, Схемы подключения и пр.)	2 часа

Информация об Инциденте	определено в разделе 4.7

4.6. Оповещения

Оповещение Контактных лиц Лицензиата о выявленных Аномалиях и Атаках в Трафике Защищаемых ресурсов производится Службой эксплуатации KDP в соответствии с параметрами, определенными в Таблице 3 и зависит от того, проходит ли Трафик Защищаемых ресурсов через Центры очистки.

Таблица 3

Событие	**Время и способ оповещения**	
	Трафик Защищаемых ресурсов **проходит** через Центры очистки	Трафик Защищаемых ресурсов **НЕ** проходит через Центры очистки
Аномалия	30 минут по электронной почте	30 минут по электронной почте
Атака на Защищаемый ресурс	30 минут по электронной почте	15 минут по телефону
		30 минут по электронной почте
Завершение Атаки	30 минут по электронной почте	30 минут по электронной почте

4.7. Время реакции на Инциденты

Время реакции на Инциденты, которое обеспечивает Служба эксплуатации KDP, зависит от степени критичности Инцидента и определено в Таблице 4.

Таблица 4

Степень критичности Инцидента	**Время реакции**
Некритичный	4 часа
Существенный	2 часа
Критический	15 минут

4.8. Время решения Инцидентов

Время решения Инцидентов, которое обеспечивает Служба эксплуатации KDP, зависит от степени критичности Инцидента и определено в Таблице 5.

Таблица 5

Степень критичности Инцидента	**Время решения**
Некритичный	24 часа
Существенный	12 часов
Критический	8 часов

В ходе решения некоторых Инцидентов требуется предоставление Лицензиатом дополнительной информации или непосредственное участие Лицензиата. Заявленное Время решения Инцидентов обеспечивается Службой эксплуатации 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.

4.9. Ограничения технической поддержки

В техническую поддержку Системы не входит:

- 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 в 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 ЛК 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 Технической поддержкой KDP;
- решение Инцидентов, являющихся следствием превышения Легитимным трафиком Лицензиата выделенной полосы пропускания, определенной в разделе Закрепление выделенной полосы пропускания;
- обработка запросов касающихся последствий решенного инцидента.

В рамках технической поддержки и обеспечения работоспособности Системы, Служба эксплуатации KDP не осуществляет:

- Анализ безопасности и производительности программно-аппаратных комплексов Лицензиата, а также консультации Контактных лиц Лицензиата по связанным вопросам;
- Конфигурирование и администрирование программно-аппаратных комплексов Лицензиата, за исключением Сенсора, установленного на Площадке Лицензиата, а также консультации Контактных лиц Лицензиата по связанным вопросам;
- Администрирование оборудования интернет-провайдера, услугами которого пользуется Лицензиат, а также консультации Контактных лиц Лицензиата по связанным вопросам;
- Взаимодействие с персоналом интернет-провайдера, услугами которого пользуется Лицензиат, а также консультации Контактных лиц Лицензиата по связанным вопросам;
- 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;
- 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.
- Проведение других работ, не связанных непосредственно с работой Системы и ее компонентов.

5. Параметры функционирования Системы

5.1. Общие параметры функционирования

Общие параметры функционирования Системы определены в Таблице 6. Параметры функционирования Системы, не оговоренные в настоящем Сертификате, определяются в Регламенте Сопровождения, который предоставляется Лицензиату по запросу.

Таблица 6

Параметр	Время	Язык
Отслеживание Аномалий и Атак	24x7x365	-
Фильтрация Трафика	24x7x365	-
Техническая поддержка	24x7x365	русский

5.2. Параметры Фильтрации Трафика

В процессе Фильтрации Трафика Защищаемых ресурсов, АО «Лаборатория Касперского», гарантирует[3], что Система:

- будет пропускать Трафик между Защищаемыми ресурсами и IP-адресами, помещенными Лицензиатом в «белые списки»;
- будет блокировать Трафик между Защищаемыми ресурсами и IP-адресами, помещенными Лицензиатом в «черные списки»;
- обеспечит очистку Трафика Защищаемых ресурсов в 98% случаев[4] на основе следующего алгоритма:
    - если IP адрес является вредоносным, то вероятность его блокировки 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 прохождения равна указанному проценту по прошествии 5 минут после того как IP адрес начал обращаться к Защищаемому ресурсу.
- обеспечит очистку Трафика в 98% случаев при условии, что емкость Атаки, направленной на Защищаемые ресурсы, не превышает лимиты, определенные в Таблице 7.

3 Исключением является ситуация, когда Лицензиат предоставил некорректную информацию о составе протоколов и портов на Защищаемом ресурсе, в отношении которых должна осуществляться Фильтрация.
4 Исключением является очистка Трафика Защищаемых ресурсов, работающих по протоколу HTTPS в отношении которых Лицензиатом не предоставляется расшифрованная копия Трафика на Сенсоре или не был предоставлен доступ к сертификату домена защищаемого ресурса при обработке трафика методом проксирования - этом случае эффективность фильтрации гарантируется на уровне 80%.

Таблица 7

Тип Атаки	Максимальная емкость Атаки*
Атаки, основанные на использовании протоколов UDP и ICMP (с большим размером пакетов)	500 Гбит/с
Атаки на основе протоколов TCP, IPSEC, GRE и др.	20 Гбит/с или 25 млн пакетов/с

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

5.3. Положение о принципах работы с шифрованным трафиком

При обработке Центром Очистки HTTPS Трафика методом проксирования, Лицензиат обязан обеспечить возможность расшифровки содержимого пакета путем предоставления доступа к сертификату домена Защищаемого Ресурса. Лицензиат имеет возможность передать оригинальный сертификат домена в Центр Очистки или авторизировать выпуск дополнительного сертификата домена партнером Исполнителя. Со стороны Исполнителя доступ к расшифрованному сертификату домена есть у одного уполномоченного лица. Обслуживающий персонал Kaspersky DDoS Prevention не имеет доступа к расшифрованному сертификату домена. В период обслуживания, при поступлении шифрованного трафика на Центр Очистки, производится его дешифрация, проверка дешифрованных пакетов на наличие следов Атаки, шифрация пакета и передача шифрованного пакета в сторону Лицензиата. При необходимости отзыва дубликата сертификата домена, Лицензиат должен обратиться с соответствующей заявкой в Службу Эксплуатации KDP.

5.4. Закрепление выделенной полосы пропускания

АО «Лаборатория Касперского» обязуется закрепить за Лицензиатом полосу пропускания Легитимного трафика, ограниченную на выходе из Центров очистки, в объеме не более предусмотренного типом лицензии, определенном в Таблице 8.

Таблица 8

Тип лицензии	Закрепленная полоса пропускания*
KDP Standard	до 100 Мбит/сек
KDP Ultimate	до 300 Мбит/сек
KDP Ultimate+	до 2 Гбит/сек

* Полоса пропускания закрепляется не за каждым Защищаемым ресурсом в отдельности, а под весь Трафик, перенаправляемый Лицензиатом на Центры очистки.

В случае если полоса пропускания, занимаемая Легитимным трафиком Лицензиата, проходящим через Центры очистки, превысит выделенную полосу пропускания, доставка объема Трафика, составляющего превышение выделенной полосы пропускания, не гарантируется.

По запросу Лицензиата в отношении Bypass ресурсов возможно применение Фильтрации, исходя из следующего алгоритма: блокируется трафик от IP-адресов, обращающихся к Bypass ресурсам, которые создают наибольшую нагрузку в момент превышения закрепленной за Лицензиатом полосы пропускания.

5.5. Предоставление отчетов

Отчеты доступны Контактным лицам Лицензиата через Личный кабинет и формируются Системой автоматически. Состав отчетов, включенных в лицензию, определен в Таблице 9.

Таблица 9

Тип лицензии	Отчет о списках адресов	Отчет об атаке	Отчет о ресурсе
KDP Standard	+	+	-
KDP Ultimate	+	+	+
KDP Ultimate+	+	+	+

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 которых, соответственно, всегда пропускается или всегда блокируется Системой в ходе Фильтрации.

Отчет об атаке формируется для каждого атакованного Защищаемого ресурса и содержит описание основных событий Атаки, графики измеряемых параметров Защищаемого ресурса, диаграммы соотношения протоколов и географического распределения Трафика.

Отчет о ресурсе формируется для каждого Защищаемого ресурса и содержит список Атак, список наиболее заметных Аномалий, диаграммы на основе реальных значений Трафика за календарный месяц.

5.6. 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 действия лицензии и доступна Контактным лицам Лицензиата в форме отчетов, формируемых по заявке из Личного кабинета.

5.7. Согласованные перерывы в функционировании Системы

АО «Лаборатория Касперского» 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 эксплуатации KDP уведомляет Контактных лиц Лицензиата о перерывах в функционировании Системы в соответствии с параметрами, определенными в Таблице 10.

Таблица 10

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 2 часов в календарный год	непосредственно перед началом работ

Таким образом показатель доступности Системы составляет 99,95%.

6. Исключения

Стороны соглашаются квалифицировать следующие 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 компонентов Системы, находящихся в зоны ответственности АО «Лаборатория Касперского», и произведенных без согласования с Службой эксплуатации 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 эксплуатации KDP;
- Перенаправления трафика без согласования со Службой эксплуатации KDP;
- отказа оборудования Лицензиата или интернет-провайдера, услугами которого пользуется Лицензиат;
- блокировки каналов поставщиком телекоммуникационных услуг связи между Площадкой Лицензиата и Центром очистки;
- перерыва в работоспособности Системы, причиной которого являются обстоятельства непреодолимой силы, предусмотренные применимым законодательством.

7. 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 эксплуатации KDP по решению Инцидента, Лицензиат обязан предоставить всю запрашиваемую Службой эксплуатации KDP информацию, необходимую для решения Инцидента, которой он обладает, и оказывать содействие в получении Службой эксплуатации KDP информации, необходимой для решения Инцидента.

В случае возникновения Инцидента с компонентами, размещенными на территории Лицензиата, Лицензиат обязан предоставить Службе эксплуатации KDP доступ к указанным компонентам.