

СЕРТИФИКАТ КАЧЕСТВА

НА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
KASPERSKY DDOS PREVENTION

Содержание

1.	Определения.....	3
1.	Условия работоспособности ПО	4
2.	Общее взаимодействие в рамках сервиса Kaspersky DDoS Prevention	4
3.	Распределение ответственности между ЗАО «Лаборатория Касперского» и Лицензиатом.....	5
4.	Ограничения технической поддержки	5
5.	Обстоятельства непреодолимой силы	6
6.	Параметры работы.....	6
6.1	Общие параметры работы ПО и службы технической поддержки	6
6.2	Оповещение о выявленных аномалиях и приведение системы в готовность к фильтрации	7
6.3	Закрепление выделенной полосы фильтрации	7
6.4	Время фильтрации трафика, включенное в тариф	7
6.5	Время реакции на инциденты	8
6.6	Время решения инцидентов	8
6.7	Время реакции на обращения	8
6.8	Параметры фильтрации трафика	8
6.9	Непрерывность работы ПО	9
6.10	Время хранения информации об атаках в Системе	10
6.11	Контроль решения инцидентов и аномалий	10
6.12	Мониторинг качества обслуживания	10
6.13	Оцениваемые критерии качества работы ПО	11
7.	МЕТОДИКА ОЦЕНКИ КАЧЕСТВА РАБОТЫ ПО И ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ	11
7.1	Время оповещения о аномалиях	11
7.2	Параметры фильтрации трафика	12
7.3	Непрерывность работоспособности ПО	12
8.	Согласованные перерывы в предоставлении ПО	12
9.	Служба технической поддержки	13
10.	Обязательства Лицензиата по участию в решении инцидентов	13
11.	Порядок Взаимодействия в рамках работы ПО	14
11.1	Телефон	14
11.2	Электронная почта	14
11.3	Портал Системы	15
11.4	Условия проведения работ на объекте Лицензиата	15

1. Определения

«**Система**», «**Программа**» – компоненты, процессы и обслуживающий персонал «Kaspersky DDoS Prevention».

«**Атака**» – действие, целью которого является попытка дестабилизации работоспособности ресурса, либо отказ в обслуживании, либо отвлечение внимания администратора от попытки захвата контроля (повышение прав) над удалённой/локальной вычислительной системой.

«**DoS-атака**» - от англ. Denial of Service, отказ в обслуживании. Атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легитимные (правомерные) Пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверами), либо этот доступ затруднён. Отказ системы может быть как самоцелью (например, сделать недоступным популярный Интернет-сайт), так и одним из шагов к овладению системой (если во внештатной ситуации Программное обеспечение выдаёт какую-либо критическую информацию — например, версию, часть программного кода и т.д.). Если атака выполняется одновременно с большого числа компьютеров, говорят о **DDoS-атаке** (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»).

«**Трафик**» - объём информации, передаваемой по каналам связи за определенный период времени.

«**Легитимный трафик**» – трафик к вычислительной системе, который идет от пользователей, которые предполагают использовать вычислительную систему по ее назначению (например, пользователь системы Интернет-банкинга, посетитель информационного сайта).

«**Паразитный трафик**» – трафик, не соответствующий выявленным и утвержденным статистическим критериям легитимного трафика.

«**Фильтрация трафика**», «**Очистка трафика**» – выделение в трафике защищаемого Ресурса Паразитного трафика и его удаление.

«**Аномалия**» - отклонение статистических характеристик трафика, направленного на ресурс от расчетных.

«**Ресурс**» – сетевой сервис Лицензиата, определяемый доменным именем или IP адресом.

«**Коллектор**», «**Центр очистки**», «**Фильтрующий Маршрутизатор**», «**Прокси-сервер**», «**Сенсор**» – компоненты системы «Kaspersky DDoS Prevention».

«**Перенаправление трафика**» – процесс доставки трафика защищаемого Ресурса к Центру очистки.

«**Туннель**» – способ доставки трафика от Центра очистки до защищаемого Ресурса, заключающийся в организации преобразования адресов (при необходимости такого преобразования) и инкапсуляции трафика на стороне Центра очистки, перенаправлении инкапсулированного трафика в сторону защищаемого Ресурса, снятие инкапсуляции и (при необходимости) повторного преобразования адресов на стороне защищаемого Ресурса.

«**Обращение**» – электронное письмо или звонок с проблемой уполномоченного представителя Лицензиата ЗАО «Лаборатория Касперского».

«**Инцидент**» – любое событие, связанное с системой и персоналом «Kaspersky DDoS Prevention», которое негативно влияет или может повлиять в дальнейшем на функционирование Ресурса.

«**Проблема**» – основная неизвестная причина инцидента.

«**Существенный инцидент**» – инцидент, который существенно сказывается на работе Ресурса.

«**Критический инцидент**» – инцидент, который делает Ресурс Лицензиата полностью неработоспособной или приводит к существенному ухудшению его работоспособности.

«**Некритичный инцидент**» – все остальные инциденты, которые не оказывают существенного негативного влияния на работоспособность Ресурса.

«Время регистрации» - период времени, который проходит от Обращения до подтверждения представителями ЗАО «Лаборатория Касперского» факта принятия Инцидента к рассмотрению.

«Время реакции» – период времени (начиная с момента регистрации инцидента), в течение которого будет начата обработка инцидента. Продолжительность времени реакции напрямую зависит от критичности инцидента.

«Время решения» - период времени (с момента окончания времени реакции), в течение которого будет найдено постоянное или временное решение инцидента.

«Качество обслуживания» – выражение работоспособности Системы в определенных и измеряемых критериях.

«Объект Лицензиата» – объекты (здания, помещения), где расположены программно-аппаратные комплексы Ресурса ЗАО «Лаборатория Касперского»а.

«Код активации» - генерируемый ЗАО «Лаборатория Касперского»ом уникальный буквенно-цифровой код, позволяющий Лицензиату использовать Систему.

«Активация Программы», «Активация Системы» - ввод кода активации в интерфейс Системы, соответствующий моменту начала использования Системы Лицензиатом.

1. Условия работоспособности ПО

Система «Kaspersky DDoS Prevention» в части фильтрации трафика может эффективно работать только при условии, что

- Лицензиат обеспечивает возможность подключения к Ресурсам Сенсоров, для мониторинга аномалий и построения статистического профиля Ресурсов одним из следующих методов (оптимальный метод определяется специалистами ЗАО «Лаборатория Касперского» после обследования сетевой инфраструктуры Ресурса Лицензиата):
 - размещение оборудования компонента Сенсора в непосредственной близости от Ресурса;
 - Зеркалирование трафика с Ресурса на Сенсор;
 - Направление агрегированной информации о трафике на Сетевой сенсор (NetFlow).
- Лицензиат имеет возможность оперативно администрировать DNS-записи своих Ресурсов и/или управлять анонсированием автономных систем (блоками провайдеро-независимых адресов).

2. Общее взаимодействие в рамках сервиса Kaspersky DDoS Prevention

- Сотрудники ЗАО «Лаборатория Касперского»а мониторят наличие аномалий в трафике защищаемых Ресурсов.
- Сотрудники ЗАО «Лаборатория Касперского» оповещают ответственных сотрудников Лицензиата о наличии устойчивых аномалий в трафике
- Ответственные сотрудники Лицензиата оценивают загруженность своих ресурсов и принимают решение о начале фильтрации
- Ответственные сотрудники Лицензиата производят комплекс действий по переключению трафика защищаемых ресурсов на систему очистки
- Сотрудники ЗАО «Лаборатория Касперского» обеспечивают запуск фильтрации и контроль степени очистки трафика, при необходимости корректируя настройки системы.

- В случае, когда атака прекращается, специалисты ЗАО «Лаборатория Касперского» информируют об ответственных сотрудников Лицензиата.
- Ответственные сотрудники Лицензиата принимают решение о прекращении фильтрации и выполняют действия по приведению маршрутов прохождения трафика к защищаемым ресурсам в исходное состояние.

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

Таблица 1

Сфера ответственности	ЗАО «Лаборатория Касперского»	Лицензиат
Работоспособность Сервиса Kaspersky DDoS Prevention, в том числе – работоспособность программной части сенсора	+	
Работоспособность инфраструктуры защищаемых ресурсов, в том числе – работоспособность аппаратной части сенсора		+
Поддержание работоспособности работы сервиса через распределенную систему фильтрации	+	+
Мониторинг аномалий в трафике защищаемого ресурса	+	
Оповещение сотрудников Лицензиата о аномалиях в трафике защищаемого ресурса	+	
Оповещение сотрудников Лицензиата о возможности приостановления фильтрации	+	
Принятие решения о начале/завершении процесса фильтрации		+
Контроль качества работы системы очистки при включенном режиме фильтрации	+	+
Управление учетными записями защищаемых ресурсов (DNS - записи) или маршрутизацией (BGP)		+

4. Ограничения технической поддержки

В техническую поддержку ПО «Kaspersky DDoS Prevention» не входит решение:

- инцидентов, связанных с неработоспособностью любых программно-аппаратных комплексов, не входящих в состав оборудования Системы;
- инцидентов, при решении которых Лицензиат не выполняет [«Обязательства Лицензиата по участию в решении инцидентов»](#) (см. соответствующий раздел);
- инцидентов, условия возникновения которых не могут быть воспроизведены ни Лицензиатом, ни ЗАО «Лаборатория Касперского»;
- инцидентов, не являющихся последствиями или составляющими DDoS атак.

В рамках поддержки и сопровождения ПО «Kaspersky DDoS Prevention» ЗАО «Лаборатория Касперского» не производит:

- анализ безопасности и производительности программно-аппаратных комплексов Лицензиата;
- конфигурирование и администрирование программно-аппаратных комплексов Лицензиата;
- администрирование оборудования провайдеров Интернет услуг, которыми пользуется Лицензиат;

- взаимодействие с персоналом провайдеров Интернет услуг, которыми пользуется Лицензиат;
- проведение ремонтно-восстановительных работ на программно-аппаратных комплексах Лицензиата;
- проведение других работ, не связанных непосредственно с работой ПО и его компонент.

5. Обстоятельства непреодолимой силы

Стороны соглашаются квалифицировать следующие ситуации, в которых могут наблюдаться сбои в работе ПО как штатные, если такие сбои явились следствием:

- изменений Лицензиатом настроек, прямо или косвенно влияющих на компоненты ПО, находящихся в зоне ответственности ЗАО «Лаборатория Касперского», производимых без согласования с ЗАО «Лаборатория Касперского»;
- перерыв в работе ПО, возникший при плановом техническом обслуживании оборудования, заранее согласованном с Лицензиатом, или связанным с модернизацией ПО, по запросу Лицензиата;
- перерыв в работе ПО, вызванный несоблюдением Лицензиатом [«Обязательства Лицензиата по участию в решении инцидентов»](#) (см. соответствующий раздел);
- перерыв в работе ПО, возникший при устранении обстоятельств, препятствующих работе ПО, возникших по вине Лицензиата;
- вмешательство Лицензиата или третьей стороны в работу оборудования и программного обеспечения, находящегося на территории Лицензиата, обеспечивающего работу Системы, без согласования с ЗАО «Лаборатория Касперского».
- перенаправление трафика на подсистему очистки без согласования с техническими специалистами ЗАО «Лаборатория Касперского».
- отказы оборудования Лицензиата или Провайдера интернет-услуг Лицензиата, находящегося за пределами зоны ответственности ЗАО «Лаборатория Касперского»;
- работа каналов связи между компонентами инфраструктур Лицензиата и ЗАО «Лаборатория Касперского» заблокирована поставщиком телекоммуникационных услуг
- внештатной ситуации. Под внештатной ситуацией понимается возникновение перерыва в работоспособности ПО в штатном режиме в течение более 8 часов, причиной которого является одно из ниже перечисленных событий:
 - Отказ компонентов инфраструктур провайдеров Интернет-услуг ЗАО «Лаборатория Касперского» на срок более 8 часов, по причинам, на которые ЗАО «Лаборатория Касперского» не имеет влияния.
 - Частичное разрушение, пожар или затопление помещения Дата-Центра, в котором размещено оборудование ЗАО «Лаборатория Касперского».
 При возникновении внештатной ситуации ЗАО «Лаборатория Касперского» обязуется восстановить функции сервиса в минимальном объеме в течение 4 часов.
- Иных обстоятельств непреодолимой силы (в соответствии с условиями договора).

6. Параметры работы

6.1 Общие параметры работы ПО и службы технической поддержки

Общие параметры работы ПО и службы технической поддержки представлены в Таблице 2.

Таблица 2

	Время, GMT+3	Язык
Мониторинг аномалий и фильтрация	24x7	Русский
Техническая поддержка и сопровождению	24x7	Русский

6.2 Оповещение о выявленных аномалиях и приведение системы в готовность к фильтрации

Указанные показатели представлены в Таблице 3.

Таблица 3

	Время оповещения о аномалиях и приведения системы в готовность (способ оповещения об аномалиях)	% своевременного выполнения
Отклонения от статистических параметров	2 рабочих часа (по электронной почте)	80%
Значительное превышение статистических параметров (не более чем на 50%)	30 минут (по электронной почте или телефону)	80%
Существенное превышение статистических параметров	15 минут (по телефону)	80%

6.3 Закрепление выделенной полосы фильтрации

ЗАО «Лаборатория Касперского» обязуется закрепить за Лицензиатом полосу входящего трафика в объеме не более предусмотренным выбранным тарифным планом, соответствующие показатели представлены в Таблице 4:

Таблица 4

Тарифный план	Ограничение (логика ИЛИ)	
	Объем данных	Количество пакетов в секунду
Basic Edition	0	0
Basic Edition (при условии приобретения доп. лицензии)	2 Гбит/сек	300 000
Standard Edition	2 Гбит/сек	300 000
Advanced Edition	5 Гбит/сек	600 000
Ultimate Edition	5 Гбит/сек	600 000

В случае, если на систему фильтрации поступает трафик, превышающий указанные характеристики, ЗАО «Лаборатория Касперского» вправе не обрабатывать тот объем трафика, который составляет превышение.

6.4 Время фильтрации трафика, включенное в тариф

ЗАО «Лаборатория Касперского» обязуется фильтровать атаки, направленные на ресурс Лицензиата в течении временного отрезка, предусмотренного выбранным тарифным планом. Время фильтрации трафика, включенного в тариф представлено в Таблице 5:

Таблица 5

Тарифный план	Время защиты (дней в календарный месяц)
Basic Edition	0
Standard Edition	3
Advanced Edition	3
Ultimate Edition	Без ограничений
Kaspersky DDoS Prevention	1 день

Service, Extended Cover Option [1 день]	
--	--

В случае, если атака (несколько атак) превышают по длительности указанный лимит времени, ЗАО «Лаборатория Касперского» обязуется оплатить объем дополнительного трафика по счету Лицензиата.

6.5 *Время реакции на инциденты*

Время реакции на инциденты представлено в Таблице 6

Таблица 6

	Время реакции	% своевременного выполнения
Некритичный	4 рабочих часа	80%
Существенный	2 рабочих часа	90%
Критический	1 рабочий час	95%

6.6 *Время решения инцидентов*

Показатели времени решения инцидентов представлено в Таблице 7.

Таблица 7

	Время решения	% своевременного выполнения
Некритичный	В течении 3-х рабочих дней	80%
Существенный	В течении 1-го рабочего дня	80%
Критический	В течении 12 часов	80%

6.7 *Время реакции на обращения*

Время реакции на обращения представлено в Таблице 8.

Таблица 8

	Время реакции	% своевременного выполнения
Некритичный	4 рабочих часа	80%
Существенный	2 рабочих часа	90%
Критический	1 рабочий час	95%

6.8 *Параметры фильтрации трафика*

В процессе фильтрации трафика во время Атаки, ЗАО «Лаборатория Касперского», гарантирует, что ПО:

- будет пропускать трафик от адресатов, помещенных Лицензиатом в «белые листы»
- будет блокировать трафик от адресатов, помещенных Лицензиатом в «черные листы»
- обеспечит очистку трафика от паразитной составляющей на уровне, представленному в таблице 9.

▪ Таблица 9

п/п	Тип Атаки	Средний % очистки*	Средний % прохождения легитимных запросов**
1.	нелегитимный трафик на невостребованный протокол и/или порт (пример — UDP Flood, ICMP Flood)	98%	98%

2.	инициация соединения по протоколу TCP (SYN-Flood) со случайной подменой IP-адреса отправителя данных (IP-Spoof)	98%	98%
3.	установка полноценного TCP-соединения и с его дальнейшим сбрасыванием без обмена данными внутри сокета (TCP Connect Flood)	98%	98%
4.	отказ в обслуживании сервиса/ресурса атакой по протоколу HTTP/1.0 или HTTP/1.1 путем отправки данных: 1. вне спецификации протокола; 2. по спецификации протокола без дальнейшего следования инструкциям перенаправления (HTTP Redirect, JavaScript Redirect); 3. по спецификации протокола с дальнейшим следованием инструкциям перенаправления против защиты на уровне теста Тьюринга (captcha).	98%	98%
5.	отказ в обслуживании сервиса/ресурса по протоколу HTTPS в случае наличия криптографического сертификата на фильтрующих ресурсах	98%	98%
6.	отказ в обслуживании сервиса/ресурса по протоколу HTTPS в случае отсутствия сертификата на фильтрующих ресурсах	80%	80%
7.	фильтрация трафика в условиях наличия большого количества легитимных пользователей ресурса с генерацией трафика разных характеристик	80%	80%
8.	атака по протоколу DNS с генерацией легитимных запросов	80%	80%
9.	Иные типы атак	75%	75%

* Указанный процент очистки рассчитан на основе следующего алгоритма: если IP адрес является вредоносным, то вероятность его блокировки равна указанному в таблице проценту по прошествии 10 минут после того, как IP адрес начал атаковать защищаемый Ресурс.

** Указанный процент прохождения легитимных запросов рассчитан на основе следующего алгоритма: если IP адрес является адресом легитимного пользователя ресурса, то вероятность его прохождения равна указанному в таблице проценту по прошествии 10 минут после того как IP адрес начал обращаться к защищаемому Ресурсу во время Атаки.

6.9 Непрерывность работы ПО

ЗАО «Лаборатория Касперского» обязуется обеспечить непрерывную работоспособность ПО в течение всего срока действия договора.

В качестве подтверждения непрерывности работы ПО, ЗАО «Лаборатория Касперского» предоставляет Лицензиату журналы регистрации, в которых с интервалом не менее чем в 5 минут представлены характеристики входящего - исходящего трафика, параметров отклика ресурса и т.п.

ЗАО «Лаборатория Касперского» оставляет за собой право использовать собственные технические методы контроля непрерывности работы ПО.

Отсутствие информации в указанных выше журналах регистрации за период, превышающий 15 минут может восприниматься Лицензиатом как нарушение непрерывности работы ПО.

В случае, если потеря указанной информации стала следствием технических причин и не повлекла нарушения непрерывности работы ПО, ЗАО «Лаборатория Касперского» обязан уведомить об этом Лицензиата в течение 30 минут после обнаружения сбоя.

6.10 *Время хранения информации об атаках в Системе*

Время хранения информации об атаках в Системе представлено в Таблице 10.

Таблица 10

Тарифный план	Ординарной информации	Информация об атаках
Basic Edition	2 месяца	-
Basic Edition (при условии приобретения доп. лицензии)	2 месяца	-
Standard Edition	2 месяца	-
Advanced Edition	2 месяца	1 год
Ultimate Edition	2 месяца	3 года
Kaspersky DDoS Prevention Service, Logs Option, 1 year	-	1 год
Kaspersky DDoS Prevention Service, Logs Option, 3 years	-	3 года

6.11 *Контроль решения инцидентов и аномалий*

Инцидент может быть как в работе у Лицензиата (т.е. Лицензиат предпринимает действия, способствующие решению инцидента ЗАО «Лаборатория Касперского»), так и в работе ЗАО «Лаборатория Касперского».

Инцидент считается находящимся в работе у Лицензиата, когда ЗАО «Лаборатория Касперского» производит запрос дополнительной информации у Лицензиата, или, например, ожидает от Лицензиата действий по перенаправлению трафика на Центры очистки. После того, как Лицензиат предоставляет запрошенную информацию или выполняет необходимые технические действия, уведомив специалистов ЗАО «Лаборатория Касперского», инцидент считается переданным в работу ЗАО «Лаборатория Касперского».

ЗАО «Лаборатория Касперского» несет ответственность только за время, в течение которого инцидент или аномалия находились в работе у ЗАО «Лаборатория Касперского».

В процессе решения инцидентов ЗАО «Лаборатория Касперского» сделает все возможное для своевременного предоставления информации о статусе инцидентов, находящихся в работе, Лицензиату в соответствии с графиком, указанным в Таблице 11

Таблица 11

	График предоставления отчетов
Некритичный	Ежедневно (по электронной почте)
Существенный	Каждые 4 часа (по электронной почте или телефону)
Критический	Ежечасно (по телефону)

6.12 *Мониторинг качества обслуживания*

ЗАО «Лаборатория Касперского» производит хранение следующей информации о зарегистрированных инцидентах, находящихся в работе, и закрытых инцидентах:

- Общее количество закрытых инцидентов;
- Общее количество инцидентов «в работе»;
- Порядковый номер инцидента и описание;
- Уровень срочности инцидента;
- Статус инцидента;
- Дата и время регистрации инцидента у ЗАО «Лаборатория Касперского»;
- Время реакции относительно заданного уровня обслуживания;

- Время, в течение которого инцидент находился в работе у Лицензиата;
- Время, в течение которого инцидент находился в работе у ЗАО «Лаборатория Касперского»;
- Сторону, у которой в текущий момент инцидент находится в работе (ЗАО «Лаборатория Касперского» / Лицензиат);
- ФИО ответственного технического специалиста со стороны ЗАО «Лаборатория Касперского»;
- Дата и время фактического решения инцидента.

ЗАО «Лаборатория Касперского» представляет Лицензиату отчеты о закрытых инцидентах на ежемесячной основе.

6.13 Оцениваемые критерии качества работы ПО

К оцениваемым параметрам качества работы ПО относятся показатели, представленные в Таблице 12:

Таблица 12

Параметр	Критерии оценки качества
Выявление факта начала Атаки	Своевременность информирования о выявленных аномалиях
Качество фильтрации трафика	Процентное соотношение входящего и исходящего трафика
Непрерывность работы ПО	Время работоспособности сервиса, в т.ч. полнота предоставленной ЗАО «Лаборатория Касперского» информации о статистике трафика на контролируемом ресурсе, степени очистки трафика и т.п. информации.
Техническая поддержка	Своевременное реагирование на обращения Лицензиата и своевременное решение возникших инцидентов.

7. МЕТОДИКА ОЦЕНКИ КАЧЕСТВА РАБОТЫ ПО И ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

7.1 Время оповещения о аномалиях

По факту обнаружения Программным обеспечением аномалий в трафике Лицензиата, ЗАО «Лаборатория Касперского» обязуется уведомить уполномоченных лиц Лицензиата в течение 15 минут с момента обнаружения устойчивых признаков атаки.

Факт начала атаки может быть рассчитан Лицензиатом по публикуемым ЗАО «Лаборатория Касперского» журналам регистрации.

Различают следующие степени нарушения качества по данному параметру, представленные в Таблице 13:

Таблица 13

Нарушенный параметр ПО	Степень нарушения	Численная характеристика
Своевременность обнаружения факта атаки	легкая	От 30 минут до 1 часа
	средняя	От 1 часа до 3-х часов
	грубая	Свыше 3-х часов

В случае, если ЗАО «Лаборатория Касперского» не обеспечил доступность уполномоченных лиц, ответственных за получение информации, он не в праве выставлять претензии по нарушению данного параметра качества.

7.2 Параметры фильтрации трафика

Различают следующие степени нарушения качества по данному параметру

- Не обеспечен пропуск трафика от адресатов, помещенных Лицензиатом в «белые листы»
- Не обеспечено блокирование трафика от адресатов, помещенных Лицензиатом в «черные листы»
- Параметры очистки трафика от паразитной составляющей отличаются от заявленных на величину более чем на 20% (в сторону ухудшения характеристик)

7.3 Непрерывность работоспособности ПО

Базовым интервалом для расчета непрерывности работы ПО считается интервал в 5 минут.

В случае, если в ходе Атаки такие показатели очистки трафика, как:

- Параметры очистки
- Пропуск/блокировка трафика из белых/черных списков
- Готовность ЗАО «Лаборатория Касперского» обрабатывать трафик (прохождение трафика через центры очистки)

превышают заявленные в течении более чем 15 минут, то различают следующие степени нарушения качества по данному параметру, представленные в Таблице 14:

Таблица 14

Нарушенный параметр ПО	Степень нарушения	Численная характеристика
Непрерывность работоспособности ПО	легкая	От 15 минут до 30 минут
	средняя	От 30 минут до 1 часа
	грубая	Свыше 1 часа

8. Согласованные перерывы в предоставлении ПО

ЗАО «Лаборатория Касперского» имеет право по согласованию с Лицензиатом прерывать предоставление ПО для проведения технологических работ по обслуживанию оборудования и каналов связи, а также для проведения экстренного обслуживания. Стороны соглашаются квалифицировать данные перерывы, представленные в Таблице 15, как работу ПО в штатном режиме и не включать их во время недоступности при расчете показателей работы ПО.

Таблица 15

№ п/п	Позиция	Показатели	Уведомление Лицензиата	Дополнительные условия
-------	---------	------------	------------------------	------------------------

№ п/п	Позиция	Показатели	Уведомление Лицензиата	Дополнительные условия
1.	Проведение технологических работ	Суммарная продолжительность перерывов - не более 16 часов в год Интервалы между перерывами - не менее 30 календарных дней.	Не менее чем за 2 календарных дня до начала перерыва	Время проведения работ согласовывается с Лицензиатом
2.	Проведение экстренного связанного с установкой выпускаемых производителем обновлений (upgrades) и/или корректирующих заплаток (patches) имеющих критическое значение для работоспособности, производительности, безопасности ПО	Время перерыва равно фактическому времени установки обновлений (upgrades), корректирующих заплаток (patches) и тестирования	Непосредственно перед началом работ	Предполагаемая продолжительность проведения работ сообщается Лицензиату

9. Служба технической поддержки

Служба технической поддержки ЗАО «Лаборатория Касперского» обеспечивает коммуникации между Лицензиатом и ЗАО «Лаборатория Касперского» и отвечает за прием и обработку запросов Лицензиата.

Приём и обработка запросов включает в себя следующие действия:

- приём запросов Лицензиата, их регистрация, классификация и маршрутизация на следующие уровни поддержки;
- контроль хода выполнения работ по запросу, эскалация в случае возникновения проблем с исполнением запроса, информирование Лицензиата о ходе выполнения работ, закрытие запроса;
- уведомление Лицензиата об обнаруженных аномалиях и прочих инцидентах;
- информирование Лицензиата о типе атаки и выдача рекомендаций по противодействию (при возможности);
- информирование Лицензиата по инцидентам/проблемам/работам массового характера, проводимым изменениям и технологическим работам.

10. Обязательства Лицензиата по участию в решении инцидентов

Лицензиат обязан:

- предоставить ЗАО «Лаборатория Касперского» список лиц (включающий контактную информацию), обладающих квалификацией, достаточной для обеспечения Перенаправления и приема трафика на стороне Лицензиата и создания копии трафика и доставки его на Сенсор, и ответственных за выполнение обязательств Лицензиата, согласно настоящего Соглашения.
В случае отсутствия лиц, обладающих достаточной квалификацией, Лицензиат обязан предоставить ЗАО «Лаборатория Касперского» необходимую для организации Перенаправления и приема трафика информацию, а также предоставить доступ к обеспечивающему прием трафика оборудованию с уровнем

- привилегий, достаточным для осуществления конфигурации необходимого для приема трафика программного обеспечения;
- предоставить ЗАО «Лаборатория Касперского» список лиц (включающий контактную информацию), уполномоченных инициировать от имени Лицензиата заявки и запросы в адрес ЗАО «Лаборатория Касперского», реагировать на запросы ЗАО «Лаборатория Касперского» и принимать необходимые решения в экстренной ситуации;
 - предоставить ЗАО «Лаборатория Касперского» список лиц (включающий контактную информацию), уполномоченных обращаться за технической поддержкой;
 - Держать в актуализированном виде список принадлежащих ЗАО «Лаборатория Касперского» Ресурсов, в соответствии с Договором
 - обеспечить размещение Сенсора на площадке Лицензиата или зеркальный отвод трафика с Ресурса Лицензиата на Сенсор, или выдачу Flow-информации в адрес ЗАО «Лаборатория Касперского»;
 - обеспечить доступ к оборудованию, обеспечивающему оказание ПО, размещенному на территории Лицензиата (Сенсор). Порядок предоставления доступа к оборудованию уточняется вместе с Лицензиатом, в зависимости от топологии сети, принятых политик безопасности и т.д.
 - создать условия, необходимые для Перенаправления трафика, подлежащего Фильтрации, и обеспечить Перенаправление такого трафика на Центры очистки в случае атак;
 - обеспечить прием очищенного трафика на своих ресурсах.

Кроме того, некоторые инциденты, связанные с работоспособностью Системы или с взаимодействием компонент Системы с оборудованием Лицензиата, требуют моделирования условий возникновения инцидента с целью локализации и поиска причин.

Лицензиат обязан предоставить всю необходимую для проведения работ информацию и оказывать содействие сотрудникам ЗАО «Лаборатория Касперского», вовлеченным в процесс решения инцидента, в получении необходимой для проведения работ информации, а также в получении объекта исследования и программного и/или аппаратного обеспечения, необходимого для моделирования условий возникновения инцидента в случае, если необходимое программное и/или аппаратное обеспечение отсутствует у ЗАО «Лаборатория Касперского».

В случае возникновения инцидента с компонентами, размещенными на территории Лицензиата, Лицензиат обязан предоставить доступ сотрудникам ЗАО «Лаборатория Касперского» к указанным компонентам непосредственно на объекте Лицензиата.

11. Порядок Взаимодействия в рамках работы ПО

11.1 Телефон

Взаимодействие по телефону является экстренным средством связи, предназначенным для информирования ЗАО «Лаборатория Касперского» о возникновении критических инцидентов.

Обращения Лицензиата принимаются по телефону +7 (800) 700-88-11. При обращении по телефону необходимо сообщить тип запроса: «DDoS Prevention».

По телефону Лицензиат имеет возможность:

- Получать экстренные консультации по действиям в случае возникновения критических инцидентов.

11.2 Электронная почта

Электронная почта является вторым основным средством связи с ЗАО «Лаборатория Касперского», предназначенным для регистрации инцидентов авторизованными сотрудниками Лицензиата.

Обращения Лицензиата принимаются на адрес ddosprevention@kaspersky.com.

Посредством *электронной почты* Лицензиат имеет возможность:

- Регистрировать инциденты; производить мониторинг зарегистрированных инцидентов;

- Получать рекомендации по организации мероприятий активного противодействия.

11.3 Портал Системы

Портал Системы «Kaspersky DDoS Prevention», расположенный по адресу www.ddosprevention.ru предназначен для предоставления специалистам Лицензиата информации о работоспособности сервиса и статистике происходящих событий.

Пользуясь порталом, Лицензиат может

- Отслеживать Работоспособность компонент системы
- Анализировать статистику загрузки Ресурса
- Контролировать аномалии
- Настраивать механизмы сигнализации о достижении уровней аномальности
- Уведомлять персонал ЗАО «Лаборатория Касперского» о принятии решения о переключении трафика
- Редактировать списки черных/белых адресов фильтрации

11.4 Условия проведения работ на объекте Лицензиата

ЗАО «Лаборатория Касперского» производит часть работ, связанных с использованием ПО, непосредственно на объекте Лицензиата в случае регистрации критического инцидента, связанного с оборудованием, расположенным на территории Лицензиата.

Способ проведения работ (*непосредственно на объекте Лицензиата или удаленно*), определяется:

- ЗАО «Лаборатория Касперского» в случае, если зарегистрирован критический инцидент;
- Лицензиатом в иных случаях.