ОБЩИЕ УСЛОВИЯ ОКАЗАНИЯ УСЛУГИ

«ЗАЩИТА ОТ DDOS-АТАК»

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1.	Информация	Сведения (данные) независимо от формы их представления.
1.2.	Интернет (Публичный или Глобальный Интернет)	Международное объединение независимых сетей связи общего пользования с коммутацией пакетов, являющихся совокупностью промежуточных и конечных систем, взаимодействующих через открытые протоколы и процедуры на базе протоколов семейства TCP/IP.
1.3.	Публичный IP-адрес (сетевой адрес)	Уникальный идентификатор в сети передачи данных, присваиваемый узлу промежуточной или конечной системы публичной сети Интернет.
1.4.	Доменное имя (Domain Name)	Обозначение символами, предназначенное для адресации сайтов в сети Интернет в целях обеспечения доступа к информации, размещенной в сети Интернет.
1.5.	DNS (Domain Name System)	Иерархичная система (база данных) доменных имён, поддерживаемая на размещенных в Глобальной сети Интернет DNS-серверах, взаимодействующих по определённому протоколу.
1.6.	Трафик	Объём информации, передаваемой по каналам связи за определенный период времени.
1.7.	Промежуточная система	Система, осуществляющая выбор пути передачи пакетов и передачу их по выбранному пути к следующей Промежуточной или Конечной системе.
1.8.	Автономная система (AS)	Это группа IP сетей, управляемых оператором связи (или несколькими операторами связи), имеющими единую политику маршрутизации. AS имеет уникальный номер (ASN), необходимый для обмена информацией о маршрутах с другими AS, который осуществляется по протоколу межсетевой маршрутизации (BGP-4).
1.9.	Конечная система	Специализированное или универсальное вычислительное устройство, подключенное к Интернет.
1.10.	СПД Оператора	Сеть Передачи Данных (СПД) Оператора на основе системы протоколов TCP/IP, с единой политикой маршрутизации и администрирования, определяемых Оператором, и взаимодействующая с Глобальной сетью

		Интернет. СПД Оператора является Промежуточной системой в Глобальной сети Интернет.
1.11.	Граничный маршрутизатор (Border Gateway)	Аппаратный маршрутизатор Оператора, используемый для сопряжения СПД Оператора с Глобальной сетью Интернет с использованием Протокола BGP.
1.12.	Протокол BGP, Border Gateway Protocol (BGP-4), Протокол граничного шлюза	Основной протокол динамической маршрутизации в Интернете. Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами (AS). Передаваемая информация включает в себя список AS, к которым имеется доступ через данную систему. Выбор наилучших маршрутов осуществляет Border Gateway (Граничный маршрутизатор) исходя из правил, принятых в сети.
1.13.	Порт доступа	Порт на устройстве доступа СПД Оператора для подключения оборудования Клиента к СПД Оператора.
1.14.	Сетевые ресурсы	Технологические ресурсы Промежуточных систем Интернет сетей (каналы связи, сетевые устройства, маршрутизаторы), обеспечивающие функционирование Промежуточных систем, а именно, передачу трафика. Недостаток или нарушение работоспособности сетевых ресурсов промежуточных систем может приводить, например, к задержкам в передаче или даже к потерям пакетов в таких системах.
1.15.	Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
1.16.	Ресурс сети Интернет (далее Ресурс)	Сетевые ресурсы и Конечные системы, в т.ч. Информационные системы.
1.17.	Сайт в сети Интернет	Совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством сети Интернет по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет"
1.18.	Пользователь Глобальной сети Интернет (далее Пользователь)	Лицо, использующее в своих целях Ресурсы сети Интернет, посредством Конечной системы.
1.19.	Администратор информационной системы	Физическое или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее

	(Администратор Ресурса)	базах данных, в частности определяющие политику взаимодействия информационной системы с Глобальным Интернет и права других Пользователей по отношению к информационной системе.
1.20.	Контактное лицо Клиента	Представитель Клиента или квалифицированный технический сотрудник компании Клиента (список лиц представлен в Заказе, на оказание Услуги, не более 3 человек), уполномоченный Клиентом выполнять следующие действия от имени Клиента: • инициировать Обращения в адрес Службы технической поддержки Оператора; • реагировать на запросы со стороны Оператора и принимать необходимые решения в экстренных ситуациях.
1.21.	Электронное сообщение	Информация, переданная от одного Пользователя Глобального Интернет к другому посредством систем обмена сообщениями (электронная почта, мессенджер и т.п.).
1.22.	Несанкционированный доступ	Действия Пользователя, направленные на получение несанкционированного доступа к Ресурсу, последующее использование такого доступа, а также уничтожение, или модификация программного обеспечения или информации (данных), не принадлежащих Пользователю и без согласования с Администратором этого Ресурса, Под несанкционированным доступом к Ресурсу понимается доступ любым способом, отличным от разрешенного или предполагавшегося Администратором данного Ресурса.
1.23.	Сетевая атака	Действия Пользователя сети Интернет, направленные на нарушение нормального функционирования Ресурсов. К таким действиям относится, но этим не ограничивается, передача на Ресурсы бессмысленной или бесполезной информации (паразитный трафик), создающей паразитную нагрузку на эти Ресурсы, а также каналы связи сети Интернет, в объемах, превышающих минимально необходимые для проверки связности сетей и доступности отдельных Ресурсов.
1.24.	DoS-атака (Denial of Service)	Разновидность сетевых атак на компьютерные системы, сети связи, связанные с большим количеством запросов (в виде IP-пакетов), направленных на IP-адреса, используемых Клиентом. DoS-атака имеет своей целью отказ в работе атакуемой системы из-за исчерпания ресурсов оборудования, либо ресурсов каналов связи..
1.25.	DDoS-атака (Distributed Denial of	DoS-атака, выполнение которой осуществляется одновременно с большого числа компьютеров,

	Service)	подключенных к Интернет.
1.26.	Аудит трафика	Анализ Трафика в направлении Объекта с целью изучения и выявления статистическими методами закономерностей в Трафике, IP-адресов источников/получателей и других значений Параметров Анализа.
1.27.	Объект мониторинга (Объект)	Ресурс Клиента, имеющий публичные IP-адреса (маска подсети), Трафик, в направлении которого, анализируется Оператором в рамках оказания услуги «Защита от DDoS-атак». Для каждого Объекта мониторинга Оператор применяет соответствующие Параметры анализа.
1.28.	Параметры Анализа	Индивидуальные граничные значения параметров Трафика в сторону Объекта (значения пиковой и средней нагрузки, различные распределения значений параметров трафика по источнику, времени суток и т.д.), используемые при анализе Трафика Клиента Оператором.
1.29.	Легитимный Трафик	Трафик в направлении Объекта, который направляется от Пользователей, предполагающих использовать Объект по его назначению (например, Трафик от легальных пользователей системы интернет-банкинга или сайта в сети Интернет).
1.30.	Нежелательный Трафик (Нелегитимный Трафик)	Трафик, не соответствующий выявленным статистическим критериям Легитимного трафика, поступающий в направлении Объекта.
1.31.	Система анализа	Программно-аппаратный комплекс, состоящий из сетевого оборудования и оборудования DDoS-защиты компании Arbor Networks, выполняющий с помощью вероятностных методов Аудит Трафика, поступающего в сторону Объекта, на предмет наличия в нем Нелегитимного трафика.
1.32.	Устройство Очистки	Программно-аппаратный комплекс, состоящий из сетевого оборудования и оборудования DDoS-защиты компании Arbor Networks, выполняющий с помощью вероятностных методов очистку Трафика, поступающего в сторону Объекта, от Нежелательного трафика.
1.33.	WEB-интерфейс Услуги	Программно-аппаратный комплекс, состоящий из сетевого оборудования и оборудования DDoS-защиты компании Arbor Networks, обеспечивающий Клиенту возможность просмотра статистики по Трафику, поступающего в сторону Объекта Клиента.
1.34.	Очистка Трафика	Удаление входящего Нежелательного Трафика DDoS-

	(Фильтрация Трафика)	атаки с целью сокращения его влияния на Объект, в направлении которого он направлен.
1.35.	Baseline	В заданный момент времени среднее из значений параметра Трафика Клиента за предыдущие тридцать минут и значений данного параметра, имевших место в то же время, в те же дни недели периода оказания Услуги. При усреднении перечисленного множества значений учитываются только те значения, которые характеризуют нормальное прохождение Трафика, т.е. подсчитанные во время отсутствия Нежелательного Трафика.
1.36.	Параметры Фильтрации	Набор параметров входящего на Ресурс Клиента Трафика: • диапазон IP-адресов отправителя; • диапазон адресов портов отправителя; • диапазон IP-адресов получателя; • диапазон адресов портов получателя; • наименование и параметр (TCP Flags и т.д.) протокола.
1.37.	Договор	Договор на оказание услуг на базе облачной платформы (Оферта о заключении договора на оказание услуг на базе облачной платформы)

Термины и определения, используемые в настоящих Общих условиях имеют значения, аналогичные указанным в Договоре, «Регламенте технической поддержки».

Настоящие Общие условия оказания услуги «Защита от DDos-атак» являются неотъемлемой частью Договора. При заключении Договора Клиент подтверждает, что ознакомился с Общими условиями и обязуется их исполнять в соответствии с условиями Договора.

2. ОПИСАНИЕ УСЛУГИ

Услуга «Защита от DDoS-атак» (далее Услуга) – совокупность действий Оператора, направленных на противодействие атакам типа DoS/DDoS (посредством обнаружения и фильтрации нежелательного трафика), нацеленных на переполнение Нежелательным Трафиком каналов доступа к сети Интернет, предоставленных Оператором Клиенту. При этом, пропуск трафика Клиента осуществляется Оператором через сеть ПАО «Ростелеком».

2.1. Кому может быть предоставлена Услуга.

Услуга «Защита от DDoS-атак» является сопутствующей и предоставляется только для Клиентов, которые используют услугу «Резервированный доступ в Интернет», при этом, пропуск трафика Клиента осуществляется Оператором через сеть ПАО «Ростелеком». В случае если Клиент использует услугу «Резервированный доступ в Интернет», применяя динамическую маршрутизацию по протоколу BGP-4, то Оператор рекомендует Клиенту настроить политику маршрутизации на своей сети таким образом, чтобы весь трафик в сторону Ресурсов Клиента шел только через сеть Оператора. В противном случае трафик атаки может достигать Ресурсов Клиента через сети других операторов, минуя Устройство очистки Оператора.

2.2. Состав Услуги.

В рамках Услуги осуществляется:

- подготовка Оператором Системы анализа Трафика, используемой для выявления Нежелательного Трафика, входящего на Объект Клиента из сети Интернет;
- Аудит Трафика в направлении Объекта Клиента в целях определения параметров нормального прохождения Трафика (при отсутствии Нежелательного трафика) и формирования соответствующих ему Параметров Анализа;
- круглосуточный анализ Трафика в направлении Объекта на предмет его соответствия Параметрам Анализа;
- круглосуточное предоставление Клиенту через WEB-интерфейс Услуги результатов анализа Трафика в графическом виде посредством демонстрации графиков или таблиц через WEB-интерфейс Услуги;
- предоставление Клиенту в виде предустановленной формы в формате PDF стандартизованных отчетов по результатам анализа Трафика в сторону Объекта;
- оповещение Клиента о наличии Нежелательного Трафика при его появлении;
- перенаправление (в автоматическом режиме или по запросу Клиента) входящего в сторону Объекта Трафика Клиента на Устройство Очистки в целях фильтрации Нежелательного Трафика.

3. ОСОБЕННОСТИ ОКАЗАНИЯ УСЛУГИ

3.1. Параметры анализа и виды Аудит трафика

3.1.1. Аудит Трафика Клиента проводится Оператором по следующим параметрам:

- качественные характеристики трафика (распределение по протоколам);
- количество пакетов Трафика в секунду (PPS);
- количество байт Трафика в секунду (BPS).

3.1.2. Оператор осуществляет динамический анализ Трафика Клиента. Динамический анализ осуществляется на основании одновременного сравнения фактических значений PPS и BPS Трафика Клиента с Baseline значениями данных параметров, и одновременно с соответствующими значениями Параметров Анализа. Данный вид анализа служит для выявлений отклонений реальных значений прохождения всего Трафика Клиента от статистически обычных значений.

3.2. Типы предупреждений

3.2.1. При превышении фактическими параметрами Трафика Клиента пороговых значений Параметров Анализа или Baseline, а так же определении наличия в трафике сигнатур потенциально опасного трафика, Система анализа Оператора делает вывод о вероятном наличии Нежелательного трафика в составе Трафика Клиента и производит предупреждения об этом, формируя записи в WEB-интерфейсе Услуги. В соответствии с установленными производителем характеристиками системы существует несколько Типов предупреждений, отличающихся по степени отклонения от значений Параметров анализа или от Baseline:

- «Красное» – критическое превышение, вероятность наличия Нежелательного Интернет-трафика велика;
- «Желтое» – умеренное превышение, вероятность наличия Нежелательного Интернет-трафика средняя;
- «Зеленое» – небольшое превышение, вероятность наличия Нежелательного Интернет-трафика малая.

3.3. Инсталляция Услуги

В рамках инсталляции услуги Оператор:

3.3.1. устанавливает в Системе анализа Трафика Параметры Анализа Трафика, поступающего в сторону Объекта Клиента;

3.3.2. настраивает WEB-интерфейс Услуги для отображения результатов анализа Трафика и предоставляет Клиенту доступ к этому WEB-интерфейсу Услуги.

3.4. Аудит трафика

3.4.1. По соглашению с Клиентом Оператор в течение 14 календарных дней с момента подключения Услуги проводит анализ Трафика Клиента статистическими методами (Аудит трафика) в целях определения параметров Трафика в сторону Объекта, которые характеризуют индивидуальные признаки нормального прохождения Трафика Клиента. Для проведения Аудита трафика действий Клиента не требуется.

3.4.2. По результатам Аудита трафика, в случае если со стороны Клиента течение 5-ти рабочих дней отсутствуют замечания, предоставленные в письменном виде или по электронной почте, Оператор устанавливает полученные в ходе Аудита трафика индивидуальные Параметры Анализа для каждого Объекта. В случае наличия замечаний Клиента, процесс Аудита трафика (п. 3.4.1) повторяется до момента отсутствия замечаний от Клиента.

3.5. Информирование о Нежелательном трафике

3.5.1. Оператор считает возникновение «Красных» или «Желтых» предупреждений при анализе Трафика Клиента признаком наличия Нежелательного Трафика в сторону Объекта Клиента.

3.5.2. В случае возникновения «Красных» или «Желтых» предупреждений, либо при изменении типа ранее зарегистрированных предупреждений, Оператор информирует Клиента о данных событиях путем уведомления в виде моментального графического отображения данных событий в WEB-интерфейсе Услуги.

3.6. Фильтрация и очистка Трафика.

3.6.1. Оператор может инициировать и производить на своем оборудовании пропуск Трафика Клиента через Устройство Очистки с автоматически сформированными Параметрами Фильтрации. В этом случае Трафик Клиента перенаправляется на Устройство Очистки и далее, после интеллектуальной обработки на Устройстве Очистки Оператора, Легитимный Трафик Клиента направляется на Ресурс Клиента с IP-адресом, на который он был послан изначально.

3.6.2. Пропуск Трафика Клиента через Устройство Очистки может быть осуществлен двумя способами:

- в автоматическом режиме (устанавливается по умолчанию), при возникновении «Красных» или «Желтых» предупреждений при анализе Трафика Клиента;
- по запросу от Контактных лиц Клиента (Клиент анализирует информацию о Нежелательном трафике и, в случае необходимости, обращается к Оператору) через Службу технической поддержки через Личный кабинет Клиента или на электронный адрес Оператора, указанный в разделе «Реквизиты» Договора.

3.7. WEB-интерфейс Услуги и Отчеты

3.7.1. Оператор предоставляет Клиенту доступ к WEB-интерфейсу Услуги, в котором Клиент может в on-line режиме наблюдать статистику по Услуге.

3.7.2. В WEB-интерфейсе Услуги Клиент получает от Оператора доступ к WEB-отчетам о результатах анализа Трафика в сторону Объекта Клиента.

3.7.3. Доступ Клиента к WEB-интерфейсу Услуги осуществляется по протоколу SSL посредством web-браузера, установленного на компьютере Клиента. Доменное имя WEB-интерфейса Услуги указывается Оператором в Заказе на Услугу. Доступ к WEB-интерфейса Услуги осуществляется после ввода учетной информации однозначно идентифицирующей Клиента (логин и пароль). Данные реквизиты передаются Клиенту Оператором и отражаются в Заказе на Услугу.

3.7.4. Клиент обязуется обеспечивать конфиденциальность всей своей учетной информации (логины и пароли). На Клиенте в полном объеме лежит риск последствий утраты учетной информации и/или последствия ее разглашения. .

3.7.5. Доступ к WEB-интерфейсу Услуги может быть осуществлен с оборудования, имеющего оговоренный в Заказе на Услугу диапазон IP-адресов (не более 3-х IP-адресов).

4. ОГРАНИЧЕНИЯ УСЛУГИ

4.1. Количество Объектов

Клиенту предоставляется возможность использовать в рамках Услуги как минимум 1 (один) Объект, включающий в себя 1 (один) IP-адрес или 1 (один) диапазон IP-адресов (маска подсети), для которых Оператором осуществляется Аудит Трафика.

При возникновении у Клиента необходимости в организации дополнительных Объектов мониторинга, Клиент может запросить у Оператора такую возможность. Количество дополнительных Объектов указывается путем формирования Клиентом нового Заказа на оказание Услуги.

Предоставление Клиенту возможности в организации дополнительных Объектов мониторинга, оплачивается Клиентом дополнительно к стоимости Услуги согласно тарифу. Максимальное количество дополнительных Объектов 5 (пять) штук.

4.2. Используемый протокол Трафика

Услуга обеспечивает фильтрацию Трафика только для сегмента сети Интернет, использующего протокол IPv4.

4.3. Пиковые нагрузки на сеть Оператора

Оператор вправе отказать в перенаправлении Трафика Объекта Клиента на Устройство Очистки в том случае, если это может повлечь отрицательные последствия для функционирования сети Оператора и его подрядчиков, и так же Ресурсов/оборудования других клиентов Оператора. К таким случаям относятся, но не ограничиваются, случаи превышения допустимой пиковой нагрузки на Устройство Очистки, перегрузки магистральных каналов подключения Устройства Очистки, другие технологические особенности оказания услуг.

4.4. Вероятностный характер используемых методик защиты от DDoS-атак

Клиент извещен о том, что Устройство Очистки функционирует на основании анализа параметров состоявшихся ранее DDoS-атак или поступившего ранее Нежелательного Трафика. Данные параметры с точки зрения профилактики нежелательных событий носят вероятностный характер. В этой связи Оператор не гарантирует, что пропуск Трафика

Клиента через Устройство Очистки обеспечит ожидаемый Клиентом уровень защиты от DDoS-атак.

5. СОСТАВ И МОДИФИКАЦИЯ УСЛУГИ

5.1. Состав Услуги

Конкретный состав, условия и параметры Услуги определяются в соответствии с Заказом на оказание Услуги.

5.2. Изменения параметров Услуги

Клиент вправе потребовать изменения параметров оказываемой Услуги, направив Оператору в письменном виде или по электронной почте подробный запрос с указанием сути изменений и желаемые сроки выполнения таких работ. Оператор в течение 10 (десять) рабочих дней с даты получения запроса должен сообщить о возможности изменений и при её наличии ориентировочную стоимость и срок выполнения этих работ.

6. ЭКСПЛУАТАЦИОННЫЕ ХАРАКТЕРИСТИКИ УСЛУГИ

6.1. Режим оказания Услуги.

Услуга предоставляется 24 часа в сутки 7 дней в неделю, 365 (366) дней в году.

6.2. Время перенаправления трафика на Устройство Очистки.

При организации пропуска Трафика Клиента через Устройство Очистки по запросу Клиента, период времени от момента регистрации заявки Клиента в Службе технической поддержки на перенаправление трафика на Устройство Очистки до момента начала осуществления очистки не превышает 20-ти минут.

6.3. Производительность Устройства Очистки.

Максимальный объем направляемого на Устройство Очистки Интернет-трафика – 160 Гбит/с (пиковое суммарное значение для всех абонентов Услуги). В случае превышения данных значений потока входящего трафика, Система Очистки обрабатывает входящую информацию по принципу сброса избыточной нагрузки.

7. ПЛАТЕЖИ

Клиент обязан производить следующие платежи за Услугу в соответствии с Договором и тарифами, указанным в Заказе на оказание Услуги.

7.1. Периодические платежи.

7.1.1. Периодические платежи в течение срока действия Заказа за предоставление услуги «Защиты от DDoS-атак» включают оплату неограниченного количества активаций/деактиваций перенаправления Трафика Клиента на Устройство Очистки в течение расчетного периода.

7.1.2. Периодические платежи в течение срока действия Заказа за предоставление дополнительных Объектов.

7.1.3. В случае предоставления Услуги неполный календарный месяц, расчёт периодических платежей за данный месяц производится по количеству дней фактически оказываемых услуг. При этом суточная плата определяется путём деления платы, установленной за месяц на 30 (среднее количество дней месяце). Дни подключения или отключения Услуги считаются целыми днями предоставления Услуги (24 часа).

8. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

8.1. Устранение неисправностей Оператором.

Оператор предпринимает меры для устранения неисправностей, перерывов или ухудшения качества оказываемой Услуги. При возникновении Инцидентов, Клиент и Служба технической поддержки Клиента действуют в соответствии с «Регламентом технической поддержки» к Договору.

8.2. Сообщения необходимости технического обслуживания.

Клиент незамедлительно сообщает о необходимости технического обслуживания в службу технической поддержки Оператора. Оператор фиксирует время обращения Клиента, выясняет причину возникновения проблемы и предпримет необходимые меры для устранения повреждений. Оператор также уведомляет Клиента о предпринятых мерах по устранению повреждений Услуги по его запросу.