

ПРИЛОЖЕНИЕ № 2.CRS.3.

к Договору

СОГЛАШЕНИЕ ОБ УРОВНЕ ПРЕДОСТАВЛЕНИЯ УСЛУГ «ЗАЩИТА ОТ DDOS-АТАК (STORMWALL)», «ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ (STORMWALL)»

1. ПРЕДМЕТ СОГЛАШЕНИЯ

- 1.1. Настоящее Соглашение об уровне предоставления услуг (далее – Соглашение) является документом, фиксирующим Доступность Услуги, а также целевые количественные и качественные характеристики предоставления Услуги.
- 1.2. Услуги предоставляются Заказчику Исполнителем совместно с партнером ООО «СТОРМ ЛАБС» (бренд StormWall, далее – Партнер). Заказчик уведомлен и согласен с тем, что в рамках предоставления Услуги трафик будет проходить в том числе и через сеть Партнера.
- 1.3. Исполнитель гарантирует работу сети в рамках своей зоны ответственности и не несет ответственность за возможные неполадки в сетях за пределами зоны ответственности Исполнителя.

2. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА УСЛУГИ И ПРОЦЕДУРА ВЗАИМОДЕЙСТВИЯ СТОРОН

- 2.1. При возникновении у Заказчика технической или иной проблемы при потреблении Услуги, проведении Исполнителем Регламентных или Аварийно-восстановительных работ, представитель Заказчика и Исполнитель взаимодействуют в соответствии с условиями Общего соглашения об уровне предоставления Услуги.
- 2.2. При обнаружении атаки Исполнитель обеспечивает блокирование атаки и уведомляет Заказчика об обнаружении атаки, посредством электронной почты и уведомления в личном кабинете.
- 2.3. При окончании атаки Исполнитель включает штатный режим работы системы защиты и уведомляет Заказчика об окончании атаки посредством электронной почты и уведомления в личном кабинете.
- 2.4. При изменении режима работы системы защиты (например, при обнаружении подозрительной активности) Исполнитель уведомляет Заказчика посредством электронной почты.
- 2.5. При необходимости проведения профилактических работ Исполнитель уведомляет Заказчика не менее чем за сутки до времени работ. В момент выполнения работ не должны быть нарушены требования к качеству предоставления Услуги.
- 2.6. При обнаружении влияния Услуги на доступность сервисов Заказчика обеспечивается возможность быстрого отключения защиты для разбора ситуации, а также быстрого включения защиты Заказчиком самостоятельно посредством панели управления в личном кабинете Услуги.
- 2.7. Режим технической поддержки, установленный Таблицей 2 Общего соглашения об уровне предоставления Услуги, составляет 24x7 в отношении любого типа Инцидента по Услуге.

3. ЦЕЛЕВЫЕ ЗНАЧЕНИЯ ПОКАЗАТЕЛЕЙ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

- 3.1. Согласно п. 5.1. Общего соглашения об уровне предоставления Услуги устанавливаются особые целевые значения показателей технической поддержки для Услуги (Таблица 1):

Табл. 1. Целевые значения показателей технической поддержки

Параметры устанавливаемых целевых значений	Наименование тарифного плана		
	Защита сети – тарифы Standard	Защита сайта от DDoS – тарифы Business ONE, Business 100 Защита сети – тариф Business Защита сервисов – тариф Business	Защита сайта от DDoS – тарифы Enterprise ONE, Enterprise 100, Private ONE, Private 100 Защита сети – тариф Enterprise, Private Защита сервисов – тариф Enterprise, Private
Время реакции 1-й линии поддержки, предоставляемой Исполнителем, не более	15 мин	15 мин	15 мин

Время реакции 2-й, 3-й линии поддержки, предоставляемой Партнером, не более	60 мин	30 мин	15 мин
---	--------	--------	--------

- 3.2. С учетом положений п. 1.2. Приложения 1.CRS.3. целевые значения показателей технической поддержки в отношении Услуги «Защита веб-приложений (StormWall)» отдельно не устанавливаются.

4. ПРОВЕДЕНИЕ РЕГЛАМЕНТНЫХ И АВАРИЙНО-ВОССТАНОВИТЕЛЬНЫХ РАБОТ

- 4.1. Условия проведения Регламентных и Аварийно-восстановительных работ в отношении Услуг приведены в Таблице 2:

Табл. 2. Условия проведения Регламентных и Аварийно-восстановительных работ

Наименование работ	Продолжительность и интервалы между перерывами	Уведомление Заказчика
Регламентные работы	Время проведения Регламентных / Аварийно-восстановительных работ не ухудшает установленные для тарифного плана показатели гарантированной Доступности защищаемого ресурса	Не менее чем за 2 (два) рабочих дня до начала перерыва
Аварийно-восстановительные работы	Заказчика, приведенные в Таблице 3	Не менее чем за 2 (два) часа до начала перерыва

5. ПАРАМЕТРЫ ДОСТУПНОСТИ, РЕАЛИЗУЕМЫЕ УСЛУГОЙ

- 5.1. Целевые (гарантированные) значения Доступности защищаемого сервиса Заказчика, приведены в Таблице 3:

Табл. 3. Показатели Доступности защищаемого ресурса Заказчика

Показатель Доступности защищаемого сервиса Заказчика	Наименование тарифного плана		
	Защита сайта от DDoS – тарифы Business ONE, Business 100	Защита сайта от DDoS – тарифы Enterprise ONE, Enterprise 100	Защита сайта от DDoS – тарифы – Private ONE, Private 100
	Защита сети – тарифы Standard	Защита сети – тариф Business	Защита сети – тариф Enterprise, Private
	Защита сервисов – тариф Standard	Защита сервисов – тариф Business	Защита сервисов – тариф Enterprise, Private
Гарантированная доступность защищаемого сервиса Заказчика при условии отсутствия причин недоступности Услуги 24x7x365 (24 часа в сутки, 7 дней в неделю, 365 дней в году)	не менее 99,2%	не менее 99,5%	не менее 99,9%

- 5.2. С учетом положений п. 1.2. Приложения № 1.CRS.3., целевые (гарантированные) значения Доступности защищаемого сервиса Заказчика в отношении Услуги «Защита веб-приложений (StormWall)» отдельно не устанавливаются.
- 5.3. Доступность защищаемого сервиса Заказчика, реализуемые Услугой, определяется следующим образом: вычитая из общего времени в отчетном периоде (календарном месяце) совокупности времени Недоступности защищаемого сервиса Заказчика, деленное на общее время в текущем календарном месяце.
- 5.4. Время недоступности защищаемого сервиса Заказчика начинает течь с момента подачи Заказчиком Обращения на устранение неисправности. Заказчик должен сообщить о прекращении Доступности защищаемого сервиса через личный кабинет портала <https://stormwall.pro/my/>. Время Недоступности защищаемого сервиса Заказчика истекает в момент устранения неисправности.
- 5.5. После устранения неисправности поданное Обращение может временно оставаться открытым для дальнейшего выяснения случившегося, и закрыта Заказчиком после выполнения всех относящихся к тому административных работ.
- 5.6. Общее время Недоступности защищаемого сервиса Заказчика по причине ряда периодически возникающих сбоев с одинаковыми причинно-следственными связями в отношении одного и того же защищаемого сервиса Заказчика, является совокупностью времени Недоступности Услуги в соответствии с Заявкой на устранение неисправности и не включает в себя время Доступности Услуги между периодически возникающими сбоями.

6. КОМПЕНСАЦИЯ ЗА НАРУШЕНИЕ СОГЛАШЕНИЯ

- 6.1. Если Доступность защищаемого сервиса Заказчика за один календарный месяц не соответствует п. 5.1. Соглашения, Исполнитель осуществляет компенсацию в следующем порядке:

Табл. 4. Компенсации за нарушение целевых показателей Доступности Услуги

Наименование тарифного плана	Гарантированная Доступность защищаемого сервиса Заказчика в месяц	Время недоступности защищаемого сервиса Заказчика	Размер компенсации, в %
Защита сайта от DDoS – тарифы Business ONE, Business 100 Защита сети – тарифы Standard Защита сервисов – тариф Standard	не менее 99,2%	Более 5 часов 50 минут	0,05% месячной стоимости Услуги (тарифа) за каждую минуту простоя сверх указанного времени, но не больше стоимости Услуги за один расчетный период (месяц)
Защита сайта от DDoS – тарифы Enterprise ONE, Enterprise 100 Защита сети – тариф Business Защита сервисов – тариф Business	не менее 99,5%	Более 3 часа 39 минут	
Защита сайта от DDoS – тарифы – Private ONE, Private 100 Защита сети – тариф Enterprise, Private Защита сервисов – тариф Enterprise, Private	не менее 99,9%	Более 44 минут	

- 6.2. В подсчете Времени недоступности не учитываются интервалы недоступности, связанные с:
- сбоями у Интернет-провайдеров в цепочке между конечным клиентом и сетью Исполнителя, а также сетью Исполнителя и сетью Заказчика;
 - автоматическим обнаружением неисправности по протоколу BGP (BGP dead timer);
 - перестроением маршрутов по протоколу BGP в обход сбойного соединения;
 - процессом реагирования DDoS-сенсора на возникшую DDoS-атаку;
 - рисками, связанными с принудительным отключением защиты Заказчиком или по согласованию с Заказчиком.
- 6.3. Компенсация выражается в предоставлении Заказчику соответствующего количества дней ~ бесплатного оказания Услуги, вплоть до 1 (одного) календарного месяца. Размер компенсации определяется исходя из суммы платежа за Услугу за 1 (один) календарный месяц и установленного процента компенсации. Полученная сумма переводится Исполнителем из процентов в количество дней ~ бесплатного оказания Услуги.
- 6.4. Компенсация за Недоступность защищаемого сервиса Заказчика по вине Исполнителя выражается исключительно в предоставлении бесплатных дней оказания услуги. Максимальный размер компенсации – 1 (один) календарный месяц бесплатного оказания Услуги. Компенсация не может выражаться в выплате денежных средств или зачисляться на счет Заказчика.
- 6.5. Для получения компенсации Заказчик после окончания месяца, в котором Услуга была недоступна, направляет Исполнителю заявление на предоставление компенсации. Заявление заполняется Заказчиком на официальном бланке Заказчика и подписывается уполномоченным лицом Заказчика, с обязательным указанием номера Обращения, в котором сообщалось о Недоступности Услуги, времени недоступности Услуги и даты недоступности Услуги.
- 6.6. На основании заявления Заказчика о предоставлении компенсации, Исполнитель в течение 30 (тридцати) календарных дней делает расчет компенсации, а именно рассчитывает количество дней ~ бесплатного оказания Услуги, или принимает решение об отказе в предоставлении компенсации, если неработоспособность Услуги наступила по причине, не зависящей от Исполнителя, или была запланирована Исполнителем, о чем Заказчик был уведомлен.
- 6.7. После принятия решения о предоставлении компенсации или об отказе, Исполнитель уведомляет об этом Заказчика в соответствии с условиями Общего соглашения об уровне предоставления Услуг.

7. ОТЧЕТНОСТЬ И ОГРАНИЧЕНИЯ

- 7.1. Подключая Услуги, Заказчик получает доступ в личный кабинет портала <https://stormwall.pro/my/>, в котором ему доступны подробная статистика по трафику и ежемесячные отчеты об инцидентах в формате PDF.
- 7.2. Технические аспекты работы системы фильтрации трафика, за несоблюдение которых Исполнитель не отвечает, и при несоблюдении которых Исполнитель не может гарантировать обеспечение заявленного уровня качества услуг по фильтрации трафика:
- для целей фильтрации трафика предполагается, что данные из сети Интернет передаются не непосредственно на IP-адрес сервера или виртуальной машины Заказчика, а на адрес, имеющий FQDN сервера или виртуальной машины Заказчика;

- в случае, если сервер или виртуальная машина Заказчика, для обеспечения стабильности и бесперебойности работы которого подключены услуги по фильтрации трафика, будет способен принимать входящий трафик от любых серверов в сети Интернет, Исполнитель не может гарантировать оказание услуги по фильтрации трафика в запрашиваемом объеме до момента полного обновления DNS-записей об адресах серверов защищаемых доменов во всей сети Интернет;
- для исключения ситуации обработки сервером Заказчика вредоносного входящего трафика на сервере или в тенанте Заказчика должен быть включен или развернут межсетевой экран (firewall), блокирующий любой входящий трафик, кроме входящего трафика с конкретного сервера Исполнителя;¹
- для снижения количества вредоносного трафика, блокируемого межсетевым экраном (firewall) Заказчика, а соответственно, для снижения нагрузки на сервер или виртуальную машину Заказчика, Заказчик обязан предпринять меры по сокрытию (неразглашению) фактических IP адресов серверов и виртуальных машин, для которых осуществляется фильтрация трафика.

¹ В случае защиты виртуальной машины, размещаемой в тенанте Заказчика на базе Инфраструктуры, в качестве соответствующего межсетевого экрана (firewall) может быть использован и соответствующим образом настроен Edge Gateway.