

ПРИЛОЖЕНИЕ № 1.5.
к ДоговоруОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ
«SBERCLOUD ANTI-DDOS», «SBERCLOUD ANTI-DDOS+WAF»

1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГ

- 1.1. **Услуга SberCloud Anti-DDoS** – услуга фильтрации трафика от атак отказа в обслуживании или DDoS-атак в целях обеспечения стабильности и бесперебойности работы размещаемых у Исполнителя сервисов¹ Заказчика, доступных по протоколам HTTP, HTTPS или иным прикладным протоколам, подверженным DDoS-атакам.
- 1.2. **Услуга SberCloud Anti-DDoS+WAF** – услуга фильтрации трафика от DDoS-атак, расширенная опцией защиты размещаемых у Исполнителя сервисов от полного спектра современных атак, направленных на эксплуатацию уязвимостей WEB-приложений (функция Web Application Firewall, WAF).
- 1.3. Услуги предоставляются в сотрудничестве с ООО «Эйч-эль-эль» (Qrator Labs, далее – Партнер).
- 1.4. Услуги предоставляются на базе облачного решения Партнера по защите от DDoS-атак и атак, направленных на эксплуатацию уязвимостей WEB-приложений, реализованного с помощью отдельной инфраструктуры облачной платформы Партнера, включающей более десяти центров обработки данных (ЦОД) по всему миру, в том числе три ЦОД в России (далее – облако Партнера). Сеть облака Партнера спроектирована и построена в расчете на работу под постоянным воздействием большого числа DDoS-атак. Узлы фильтрации облака Партнера подключены к каналам крупнейших магистральных Интернет-провайдеров США, России, Западной и Восточной Европы, Юго-восточной Азии. Таким образом, в отличие от сетей операторов хостинга (особенно, виртуального), сеть облака Партнера спроектирована в расчете на экстремальные нагрузки, и атака на один из ресурсов, защищаемых облаком Партнера, никак не влияет на работоспособность других защищаемых ресурсов (сайтов, WEB-приложений). В рамках Услуги SberCloud Anti-DDoS+WAF облако Партнера обеспечивает, как противодействие DDoS-атакам, так и защиту от хакерских атак, направленных на эксплуатации уязвимостей сервисов (сайтов) Заказчика.
- 1.5. Услуги по фильтрации трафика заключаются в объявлении сервером (или виртуальной машиной) Заказчика фильтрующего облака Партнера путем внесения соответствующих записей в описание DNS-зоны, к которой принадлежит сервер (или виртуальная машина) Заказчика. На фильтрующем облаке Партнера происходит последовательное выполнение следующих операций с данными, передаваемыми на сервер с FQDN сервера Заказчика:
- прием передаваемых на FQDN сервера (или виртуальной машины) Заказчика, на котором функционирует его защищаемый сервис, запросов (прием входящего трафика);
 - анализ структуры запросов (анализ входящего трафика) на предмет наличия последовательностей данных, способных повлечь некорректное функционирование защищаемого сервиса Заказчика;
 - отсеечение запросов, содержащих последовательности данных, нарушающие корректное функционирование защищаемого сервиса Заказчика (очистка входящего трафика от вредоносной составляющей);
 - перенаправление входящего трафика очищенного от вредоносной составляющей (легитимного трафика) на реальный IP-адрес сервера (или виртуальной машины) Заказчика, на котором функционирует его защищаемый сервис.
- 1.6. После подключения Услуги трафик Заказчика постоянно, вне зависимости от наличия атаки, поступает в сеть облака Партнера и анализируется им. Легитимный («очищенный») трафик перенаправляется на защищаемый сервис (сайт) Заказчика, размещаемый в инфраструктуре облачной платформы Исполнителя. Такая схема работы позволяет узлам фильтрации Партнера сформировать профиль трафика, который является нормой для каждого сервиса (сайта) Заказчика в отдельности, и в случае любых отклонений реагировать на это.
- 1.7. Все узлы фильтрации сети инфраструктуры облачной платформы Партнера работают независимо друг от друга и, в случае выхода из строя одного из них, трафик защищаемого сервиса Заказчика не потеряется, а автоматически будет перенаправлен на другой ближайший узел фильтрации облака Партнера.

¹ Здесь и далее по тексту настоящего документа под сервисами Заказчика подразумеваются любые сервисы, доступные по протоколу HTTP, HTTPS или иным прикладным протоколам, подверженным DDoS-атакам, в том числе, но не ограничиваясь WEB-сайтами, Интернет-магазинами и прочими WEB-сервисами Заказчика.

- 1.8. Передача легитимного («очищенного») трафика от облака Партнера до инфраструктуры облачной платформы Исполнителя осуществляется с использованием выделенного оптического канала связи, организуемого и поддерживаемого силами Исполнителя и Партнера. Указанный канал изолирован от сети Интернет и построен на базе резервированных, оптических линий связи.
- 1.9. Общая архитектура решения Услуги SberCloud Anti-DDoS приведена ниже на Рис.1:

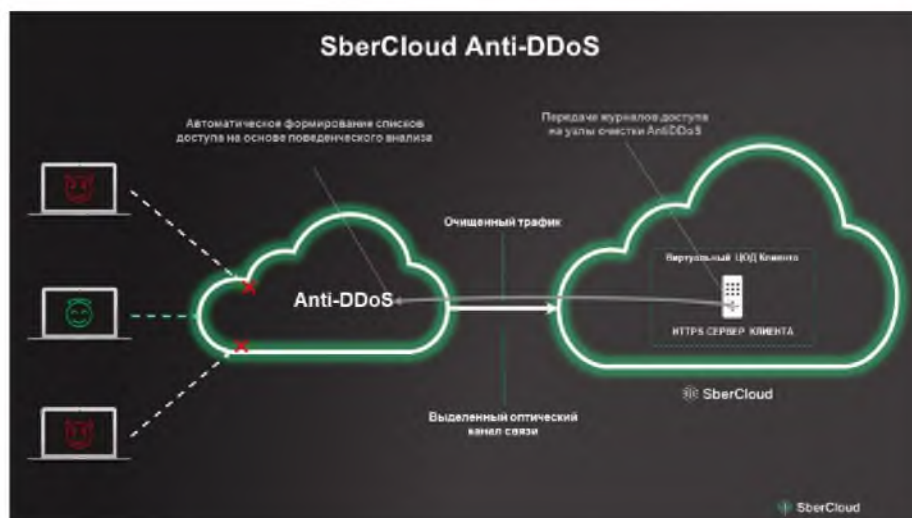


Рис.1. Общая архитектура решения Услуги SberCloud Anti-DDoS

- 1.10. **Базовая функциональность Услуги SberCloud Anti-DDoS включает:**
- 1.10.1. противодействие атакам класса «отказ в обслуживании», в том числе
- DDoS-атаки, направленные на исчерпание канальной емкости;
 - DDoS-атаки на сетевую инфраструктуру;
 - DDoS-атаки транспортного уровня;
 - DDoS-атаки, основанные на протоколах SSL/TLS;
 - DDoS-атаки уровня приложений.
- 1.11. **Базовая функциональность Услуги SberCloud Anti-DDoS+WAF включает:**
- 1.11.1. противодействие атакам класса «отказ в обслуживании» (пункт 1.10 настоящего документа);
- 1.11.2. выявление и блокирование современных атак на сервисы Заказчика, в том числе, но не ограничиваясь противодействием следующим угрозам безопасности уровня приложений:
- Injection;
 - Broken Authentication;
 - Sensitive data exposure;
 - XML External Entities (XXE);
 - Broken Access control;
 - Security misconfigurations;
 - Cross-Site Scripting (XSS);
 - Insecure Deserialization;
 - Using Components with Known Vulnerabilities;
 - Insufficient Logging and Monitoring.
- 1.12. В составе Услуги SberCloud Anti-DDoS осуществляется²:
- подключение к услуге;
 - фильтрация трафика от DDoS-атак на всех уровнях;
 - фильтрация HTTPS-трафика от DDoS-атак на прикладном уровне при условии предоставления (раскрытия) Заказчиком закрытых ключей шифрования SSL/TLS для их загрузки в облако Партнера;
 - перевод сервиса (сайта) Заказчика на использование протокола HTTPS³ с использованием бесплатных закрытых ключей шифрования SSL/TLS от Let's Encrypt, загружаемых в облако Партнера;
 - передача «очищенного» трафика от облака Партнера до размещаемого у Исполнителя сервиса Заказчика с использованием выделенного оптического канала связи;
 - балансировка трафика сервиса Заказчика между узлами облака Партнера, а далее – распределение трафика между сервисами Заказчика, функционирующими в инфраструктуре облачной платформы Исполнителя, по определенному алгоритму;

² Входит во все тарифные планы Услуги (без самостоятельной тарификации).

³ В случае если ранее для доступа к защищаемому сервису (сайту) Заказчика использовался протокол HTTP.

- мониторинг производительности защищаемого сервиса (сайта) Заказчика с оповещением по электронной почте о возникающих проблемах в его работе;
 - предоставление доступа к системе мониторинга трафика в режиме реального времени посредством Личного кабинета);
 - сбор и отображение подробной статистики по трафику сервиса Заказчика в Личном кабинете Заказчика;
 - предоставление ежемесячных подробных отчетов об инцидентах в формате PDF.
- 1.13. В составе Услуги SberCloud Anti-DDoS+WAF осуществляется (без самостоятельной тарификации):
- предоставление услуг, изложенных в пункте 1.7. настоящего документа;
 - активное сканирование сайта Заказчика на наличие уязвимостей уровня приложений, которые могут привести к его «взлому»;
 - предоставление отчетов об обнаруженных уязвимостях уровня приложений сайта Заказчика с рекомендациями по их устранению;
 - предоставление услуги «Virtual Patching» в отношении сайта Заказчика с автоматическим отслеживанием состояния уязвимости до момента ее устранения и контролем качества устранения уязвимостей;
 - защита сайта Заказчика от атак-перебора (брутфорс паролей и т.д., включается по запросу Заказчика);
 - осуществление активной проверки угроз из трафика на сайты Заказчика;
 - формирование периодических отчетов.
- 1.14. В рамках предоставляемого в составе услуги SberCloud Anti-DDoS+WAF сервиса WAF осуществляются:
- блокирование большей части атак на веб-приложения при работе с большим потоком трафика;
 - выявление существующих ошибок безопасности веб-приложений;
 - защита приложений сайта от попыток эксплуатации неисправленных уязвимостей путем обнаружений и блокировки попыток атак и вторжений в режиме on-line, что позволяет не приостанавливать работу сайта (не предоставляется на этапе тестовой эксплуатации);
 - автоматическое отслеживание состояния уязвимости до момента ее устранения;
 - контроль устранения уязвимостей.
- 1.15. Для обеспечения возможности работы WAF в составе услуги SberCloud Anti-DDoS+WAF необходима передача и загрузка в облако Партнера закрытых ключей шифрования SSL/TLS, используемых Заказчиком для организации защищенного доступа к их сайтам с использованием протокола HTTPS.
- 1.16. **Технические характеристики облака Партнера:**
- более 1000 Гбит/с пассивной полосы пропускания - детерминированная обработка IP-пакетов без установления TCP-соединения;
 - более 500 Гбит/с активной полосы пропускания - каждое входящее TCP-соединение обрабатывается и анализируется;
 - менее 5% ложных срабатываний в процессе отражения DDoS-атаки;
 - время обучения сети от момента подключения нового Заказчика - менее 2 часов:
 - в 33% случаев - до 4 минут;
 - в 60% случаев - от 5 минут до 1 часа;
 - время старта фильтрации атаки на «обученном» трафике – в 80% случаев до 2 минут от начала атаки;
 - добавленное время задержки при проксировании трафика - от 0 до 100 мс. В случае проксирования HTTP-трафика в силу использования persistent HTTP-соединений с защищаемым сервисом возможен прирост скорости работы защищаемого сервиса;
 - опциональная балансировка очищенного трафика между экземплярами сервиса Заказчика на основе алгоритмов: primary-backup, round-robin, iphash, а также в фиксированных пропорциях;
 - количество защищаемых сервисов Заказчика - неограниченно.
- 1.17. Для подключения к Услуге Заказчику необходимо самостоятельно:
- изменить А-запись, соответствующую доменному имени защищаемого сервиса, в своей DNS-зоне, чтобы она указывала на выделенный этому сервису IP-адрес в облаке Партнера (Qrator-IP);
 - настроить межсетевой экран (firewall) для запрета хождения трафика на IP адрес защищаемого ресурса с любых внешних адресов кроме узлов Qrator Labs;
 - настроить сертификаты для очистки зашифрованного трафика.
- 1.18. Услуги доступны только для сервисов Заказчика, функционирующих в инфраструктуре облачной платформы Исполнителя.

2. ОГРАНИЧЕНИЯ

- 2.1. 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 «Организации» (тенанте) Заказчика должен быть включен или развернут межсетевой экран (firewall), блокирующий любой входящий трафик, кроме входящего трафика с конкретного сервера Исполнителя;⁴
 - 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.

3. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГАМ

3.1. Возможные виды подключения / изменения / отключения Услуг:

3.1.1. посредством подписания Заказа.

3.2. Возможность проведения тестирования Услуг:

3.2.1. При заказе Услуг возможно проведение предварительного тестирования до начала проведения расчетов по Услугам. При этом период тестирования по услугам составляет:

- 2 (Две) недели бесплатного тестирования для услуги SberCloud Anti-DDoS вне зависимости от количества защищаемых сервисов Заказчика. В период тестирования Услуги SberCloud Anti-DDoS защита выполняется в полном объеме без каких-либо функциональных ограничений.
- 1 (Один) месяц бесплатного тестирования для услуги SberCloud Anti-DDoS вне зависимости от количества защищаемых сервисов Заказчика. В период тестирования Услуги SberCloud Anti-DDoS + WAF защита выполняется в полном объеме без каких-либо функциональных ограничений. При этом защита с использованием WAF выполняется в режиме мониторинга в течение периода обучения WAF на трафике защищаемого сервиса Заказчика, составляющего примерно 2 недели, и может быть переведена в режим блокировки по решению Заказчика после завершения периода обучения WAF.

3.2.2. Если оплата пользования Услугой SberCloud Anti-DDoS уже выполняется в соответствии с выставляемыми Исполнителем счетами, проведение тестирования дополнительных защищаемых с использованием Услуги сервисов Заказчика невозможно.

3.2.3. Если оплата пользования Услугой SberCloud Anti-DDoS + WAF еще не выполнялась Заказчиком ранее, то возможно проведение тестирования Услуги SberCloud Anti-DDoS + WAF после начала оплаты в соответствии с выставляемыми Исполнителем счетами за пользование Услугой SberCloud Anti-DDoS.

3.2.4. Если оплата пользования Услугой SberCloud Anti-DDoS + WAF уже выполняется в соответствии с выставляемыми Исполнителем счетами, проведение тестирования дополнительных защищаемых с использованием Услуги сервисов Заказчика невозможно.

3.2.5. Если по результатам проведения тестирования Услуг Заказчик принимает решение об отказе от пользования любой из тестируемых Услуг, то данная услуга не подключается и оплата по ней не производится.

3.3. Возможный порядок расчётов по Услугам:

3.3.1. постоплата.

3.4. Возможные способы оплаты / порядок пополнения баланса:

3.4.1. оплата в безналичном порядке на основании выставленного Исполнителем счёта.

⁴ В случае защиты виртуальной машины, размещаемой в «Организации» (тенанте) Заказчика на базе инфраструктуры облачной платформы Исполнителя, в качестве соответствующего межсетевого экрана (firewall) может быть использован и соответствующим образом настроен VMWare NSX Edge.