

ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ «ЗАЩИТА ОТ DDoS-АТАК (STORMWALL)», «ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ (STORMWALL)»

1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГ

- 1.1. Услуга «Защита от DDoS-атак (StormWall)» – услуга по защите от атак отказа в обслуживании или DDoS-атак сервисов¹ Заказчика, доступных по протоколам HTTP, HTTPS или иным прикладным протоколам, подверженным DDoS-атакам.
- 1.2. Услуга «Защита веб-приложений (StormWall)» – услуга по фильтрации веб-трафика для защиты от атак, направленных на эксплуатацию уязвимостей WEB-приложений (функция Web Application Firewall, WAF). Услуга «Защита веб-приложений (StormWall)» предоставляется Заказчикам только совместно с услугой «Защита от DDoS-атак (StormWall)».
- 1.3. Услуги предоставляются в сотрудничестве с ООО «СТОПМ СИСТЕМС» (бренд StormWall, далее – Партнер) и на базе его облачного решения² по защите от DDoS-атак и атак, направленных на эксплуатацию уязвимостей WEB-приложений.

2. ОПИСАНИЕ УСЛУГИ «ЗАЩИТА ОТ DDoS-АТАК (STORMWALL)»

- 2.1. Общие характеристики Услуги:
 - 2.1.1. предоставляется посредством изменения DNS-записей интернет-сервисов Заказчика с целью направления всех запросов на оборудование Исполнителя.
 - 2.1.2. при срабатывании защиты реализована отправка E-Mail-уведомлений о начавшейся и прекратившейся атаке.
 - 2.1.3. Услуга обеспечивает:
 - сквозную передачу на оборудование Заказчика IP-адресов источников запросов;
 - возможность прохождения протокола WebSocket с настройкой соответствующих портов;
 - беспрепятственную работу легальных поисковых ботов и не оказывает влияния на показания Яндекс- и Google-метрик в части источников перехода даже в режиме фильтрации атаки. При этом полностью исключено влияние защиты на такие показатели, как число внутренних переходов, число отказов и продолжительность сессии;
 - не менее 5 точек очистки трафика по миру в США, Европе, Российской Федерации, Центральной Азии и в Китае.
 - 2.1.4. Включение режима блокировки атаки и очистки трафика осуществляется автоматически при обнаружении системой мониторинга Исполнителя атаки, направленной на Интернет-ресурсы Заказчика, а также при поступившей заявке от Заказчика.
 - 2.1.5. поддерживает автоматическую установку бесплатных Let's Encrypt SSL сертификатов, предоставляемых Исполнителем.
- 2.2. Технические характеристики Услуги:
 - 2.2.1. Защита от следующих типов атак:
 - TCP-флуд (включая SYN ACK reflecton flood, TCP ACK flood, TCP fragmented attack);
 - SYN-флуд (включая Spoofed SYN flood);
 - UDP-флуд (включая DNS/NTP/SSDP amplification, UDP fragment flood);
 - HTTP/S-флуд (POST/GET bot attack, SlowLoris);
 - ICMP-флуд (включая Smurf attack, Ping of Death);
 - Флуд другими протоколами (GRE flood etc.);
 - Заполнение полосы пропускания (volumetric flood).
 - 2.2.2. Услуга обеспечивает:
 - фильтрацию как HTTP, так и HTTPS трафика с раскрытием приватных ключей SSL;
 - поддержку протокола HTTP/2 без переключения клиентов с поддержкой протокола HTTP/2 на более старые версии протокола;
 - балансировку нагрузки между пулом основных и резервных бэкендов;
 - кэширование для необходимых расширений файлов;
 - 2.2.3. Защита на уровне оборудования Исполнителя:

¹ Здесь и далее по тексту 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, доменными именами, Интернет-магазинами и прочими WEB-сервисами Заказчика.

² Т.е. без необходимости установки программного обеспечения на серверы Заказчика.

- обеспечивается защита от атак, имеет техническую возможность подавления (грубой очистки) атаки емкостью не менее 3,5 Тбит/сек;
- обеспечивается тонкая пакетная фильтрация трафика со скоростью не менее 1,6 Тбит/с.

3. ПОРЯДОК ДОСТУПА К УСЛУГЕ «ЗАЩИТА ОТ DDOS-АТАК (STORMWALL)»

- 3.1. Заказчику предоставляется личный кабинет и API для управления услугой с возможностью изменения защиты (в том числе ее отключения), порогов ее срабатывания, бэкендов, параметров проверки доступности бэкендов, сертификатов и приватных ключей, черных и белых списков, исключения по типам файлов, исключения по локациям.
- 3.2. Личный кабинет Услуги предоставляет Заказчику следующие функциональные возможности:
- 3.2.1. управление порогами (лимитами) для обнаружения атак:
- По количеству запросов в секунду;
 - По % соотношению запросов, завершенных с ошибками на подзащитном сервисе;
 - По скорости увеличения входящего трафика;
 - Возможность настройки индивидуальных порогов для блокировки IP-адресов по количеству заблокированных запросов и запросов в определенных области web-приложения (Location);
 - Возможность настройки максимальной продолжительности атаки, а также управление условиями завершения (обратного перехода из режима активной фильтрации в режим обнаружения).
- 3.2.2. В личном кабинете Услуги присутствуют следующие возможности:
- Выбор определенного домена/поддомена и персональная настройка для каждого сайта
 - Возможность построения различных графиков:
 - o запросов к сайту с возможностью выбора типа отображаемых запросов: общее количество запросов, разрешенные запросы, из кэша, в белом списке, всего заблокированных запросов, ошибки;
 - o объема трафика с возможностью просмотра информации за диапазон в 5 минут;
 - o Графики времени ответа и кодов ответа с возможностью просмотра информации за диапазон в 5 минут с шагом 0-50 ms, 51-100 ms, 201-600 ms, 601-1000 ms, 1001-4000 ms;
 - o График кодов ответа с возможностью просмотра информации за диапазон в 5 минут;
 - Возможность масштабирования графиков за период 5 минут, 15 минут, 1 час, 3 часа, 6 часов, 24 часа, 3 дня, неделя, месяц;
 - Тепловая карта запросов;
 - Информация о городах и странах, откуда были запросы. Отображение в виде списка и в виде круговой (секторной) диаграммы;
 - Список и круговая (секторная) диаграмма основной локацией запросов с отображением процента;
 - Возможность скачать лог запросов;
 - Возможность управления функциями black и whitelist для определенного домена/поддомена, а именно просмотр и добавления/удаления IP адресов;
 - Возможность просмотра истории атак для определенного домена/поддомена с выбором конкретных дат и формированием PDF-отчета в реальном времени. По каждой атаке должна быть возможность просмотреть подробную информацию по цели атаки, по уровню атаки, по времени начала и конца атаки, мощность атаки, протокол и значение на момент атаки в gbps / bps / cps с подробным графиком. В деталях трафика должна быть информация по запросам на сайт, объему трафика, времени ответа, кода ответа и тепловая карта с указанием топ локаций;
 - Возможность просмотра заблокированных IP адресов и истории блокировок за определенный период с указанием времени и причины блокировки;
 - Возможность смены IP backend адреса сервера/хостинга;
 - Возможность добавления субаккаунтов с настройками прав управления под каждый аккаунт отдельно;
 - Возможность смены имени домена/поддомена без дополнительных плат или обращений;
 - Возможность ручной настройки редиректов с одного домена на другой.
 - Возможность добавления Websocket
 - Возможность добавление e-mail адресов для получения рассылок об атаках
 - Возможность активации проактивной защиты для проверки новых клиентов по методам location, keepalive соединения, использованию User Agent и лимитам RPS
- 3.2.3. В личном кабинете обеспечивается возможность ознакомления со списком атак за указанный временной интервал. По каждой атаке существует возможность просмотреть подробную информацию по цели атаки, по уровню атаки, по времени начала и конца атаки, мощность атаки, протокол и значение на момент атаки в gbps / bps / cps с подробным графиком. В деталях трафика предоставляется информация по запросам на сайт, объему трафика, времени ответа, кода ответа и тепловая карта с указанием топ локаций.

3.2.4. Используемые режимы Услуги:

- Полностью выключена в этом режиме защита полностью выключена. Ни при каких обстоятельствах защита не будет переключена ни каким из автоматов
- Выключена/авто для запросов с обычных IP защита выключена. Но если IP находится в грейлисте, то уровень защиты автоматически повысится до редиректа. Если IP находится в дарклисте, то защита будет повышена до максимальной(капча). Если IP находится в блэклисте, то соединение закроется с 418 статусом.
- Редирект/авто для запросов с обычных IP применяется редирект. Но если IP находится в грейлисте, то уровень защиты автоматически повысится до JS валидации. Если IP находится в дарклисте, то защита будет повышена до максимальной(капча). Если IP находится в блэклисте, то соединение закроется с 418 статусом.
- JS/авто для запросов с обычных IP применяется JS валидация. Для IP грейлиста/дарклиста применяется JSA. Если IP находится в блэклисте, то соединение закроется с 418 статусом.
- JSA/авто для запросов с обычных IP применяется JSA валидация. Для IP грейлиста/дарклиста применяется капча. Если IP находится в блэклисте, то соединение закроется с 418 статусом.
- Капча/авто для всех запросов применяется капча
- Редирект (Redirect) для всех запросов применяется редирект.
- JS для всех запросов применяется JS валидация.
- JSA для всех запросов применяется JS валидация.

3.3. Заказчику предоставляется доступ ко всем запросам, проходящим через систему Anti-DDoS, в режиме реального времени через личный кабинет и через API, с возможностью поиска и выборки запросов, построения графиков по заданной выборке, с интервалом хранения запросов не меньше 1 недели.

4. ОПИСАНИЕ УСЛУГИ «ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ (STORMWALL)»

4.1. Общие характеристики Услуги:

- 4.1.1. поддерживает режимы блокировки («в разрыв») обратный прокси-сервер (reverse proxy);
- 4.1.2. предоставляет режим блокировки («в разрыв») допускает возможность частичного или полного отключения блокировки на время настройки Услуги или регламентных работ;
- 4.1.3. имеет возможность терминирования защищенного SSL/TLS – трафика (SSL/TLS-offload), в том числе с размещением нескольких поддерживающих HTTPS WEB приложений (сайтов) на одном IP адресе, а затем упаковки обратно в SSL/TLS соединение;
- 4.1.4. Может автоматически определять статический контент в трафике приложений, а также отдельный режим его обработки для обеспечения оптимальной производительности и повышения эффективности анализа данных в подсистеме управления и мониторинга;
- 4.1.5. Может обрабатывать массовые однотипные блокируемые запросы в специальном режиме непосредственно в подсистеме захвата трафика, без передачи в подсистему анализа трафика, для обеспечения оптимальной производительности при защите от бот-активности и DDoS атак;
- 4.1.6. обеспечивает возможность контроля использования защищаемого приложения легитимными пользователями;
- 4.1.7. поддерживает схемы работы «разрешено все, что не запрещено явно», «запрещено все, что не разрешено явно», а также комбинации обеих схем, в зависимости от рассматриваемой модели угроз и критичности защищаемых приложений;
- 4.1.8. обеспечивает своевременное обнаружение факторов компрометации и возможность последующего расследования инцидентов;
- 4.1.9. Возможность разделения запросов к статическому и динамическому контенту для экономии системных ресурсов, а также ресурсов, требуемых аналитику для разбора событий (запросы к статическим ресурсам не должны отображаться в консоли мониторинга);
- 4.1.10. предоставляет возможность управления правилами принятия решений (создание, удаление, перегруппировка) с помощью графического конфигуратора через интерфейс управления.
- 4.1.11. Для всех запросов применяется капча.
- 4.1.12. поддерживает гибкие механизмы автоматического обучения для снижения затрат времени и ресурсов на настройку при внедрении и обслуживании в условиях частых изменений функционала защищаемых приложений, а также в условиях активного цикла разработки (см. подробнее ниже).

4.2. Технические характеристики Услуги:

- 4.2.1. Поддержка следующих ключевых возможностей:
 - поддерживает протокол WebSocket, приложения, использующие NTLM-аутентификацию;
 - Работа с использованием сигнатурных методов обнаружения аномалий³;
- 4.2.2. Защита от следующих видов атак:
 - основных видов атак на веб-приложения из перечня OWASP Top 10;

³ В том числе наличие базового набора встроенных сигнатур в комплекте поставки для защиты от угроз OWASP top 10; поддержка распространенного открытого формата веб-сигнатур ModSecurity;

- на протокол HTTP, включая атаки на переполнение буфера; синтаксических в т.ч. различных атак класса injection (внедрение команд в передаваемые данные SQL Injection, Code Injection, OS Command Injection, LDAP Injection, Path Traversal и др.);
 - «методом грубой силы», в т.ч. переборных атак и атак класса «умный DoS»;
 - логических на приложения, в том числе от атак на механизмы аутентификации и контроля сессий и атак на бизнес-логику;
 - «внутри» передаваемых данных с произвольным уровнем вложенности (атаки на бэкэнд, механизмы сериализации/десериализации и т.п.);
 - на клиенты веб-приложений (CSRF, XSS);
 - 0-day и 1-day атак;
 - нежелательной активности с применением средств автоматизации (защита от ботов).
- 4.2.3. Возможность гибкой настройки различных типов моделей для каждого из защищаемых приложений, в том числе:
- определения и фильтрации статического контента;
 - валидации протокола HTTP, включая контроль заголовков, cookie и др.;
 - рекурсивной модели синтаксического анализа запросов и ответов с поддержкой различных видов сжатия, кодирования и способов передачи данных с произвольным уровнем вложенности данных (в частности, XML, JSON, BASE64, GZIP, SOAP);
 - источников – определение характеристик источника на основе параметров запроса;
 - определения логических действий (бизнес-действий) в приложении, параметров логических действий и их значений, последовательностей действий, проверки успешности действий;
 - идентификации, аутентификации и контроля сессий в приложении;
 - защиты от переборных атак и атак типа «умный DoS» на уровне отдельных логических действий и произвольных параметров действия;
 - Наличие готовых моделей валидации протокола HTTP и синтаксического анализа запросов для типового веб-приложения в комплекте поставки;
 - Возможность ручной тонкой настройки моделей отдельно для каждого из логических действий и параметров, в частности настройка сигнатурного анализа, моделей параметров, конфигураций модуля защиты от переборных атак;
- 4.2.4. Возможность обнаружения следующих видов аномалий:
- аномалий или значимых данных как в HTTP-запросах, так и в HTTP-ответах; в работе приложения на основе настроенных позитивных моделей приложения (совпадение с моделью или наоборот – отклонение от нее);
 - работы приложения на основе сопоставления значений параметров HTTP запросов/ответов с сигнатурами атак;
 - аномалий и значимых параметров непосредственно внутри вложенных данных, передаваемых по протоколу HTTP без ограничений на количество уровней вложенности; в процессе работы механизмов идентификации, аутентификации, авторизации пользователей и контроля пользовательских сессий;
 - аномалий, свидетельствующих о возможных попытках атак, осуществляемых «методом грубой силы» (bruteforce);
 - нарушение бизнес-логики приложения или контроля выполнения бизнес-логики путем использования соответствующей позитивной модели работы приложения;
- 4.2.5. Механизмы подавления ложных срабатываний, доступные Заказчику:
- предварительного ("раннего") подавления, чтобы исключить возможность их влияния на сформированные правила принятия решений, а также чтобы предотвратить их попадание в интерфейс мониторинга;
- упрощенного ("быстрого") подавления Исполнителем непосредственно при просмотре описания выявленной аномалии;
 - возможность тонкой настройки различных механизмов определения аномалий в привязке к отдельным параметрам запроса/ответа или логическим действиям в приложении.
- 4.2.6. Возможности работы с HTTP-транзакциями:
- Наличие настраиваемого модуля принятия решений, позволяющего выделять значимые события информационной безопасности и принимать решения относительно дальнейших действий в отношении HTTP-транзакций (запрос/ответ);
 - Управление правилами принятия решений на основе данных об источнике (ip-адрес, пользователь, id сессии) и цели HTTP-транзакции (приложение, логическое (бизнес)-действие), а также обнаруженных в ней аномалиях или значимых данных;
 - Поддержка следующих возможных решений: заблокировать HTTP-транзакцию, пропустить HTTP-транзакцию, пометить HTTP-транзакцию, модифицировать ответ;
- 4.2.7. Услуга обладает следующими возможностями автоматического обучения:
- определение и описание статического контента на основе анализа статистики запросов к защищаемым приложениям;

- построение рекурсивной модели синтаксического анализа данных запросов и ответов с поддержкой различных видов сжатия, кодирования и способов передачи данных с произвольным уровнем вложенности (в частности, XML, JSON, BASE64, GZIP, SOAP);
 - выявление сигнатурных правил с высоким уровнем ложных срабатываний (автоматическое подавление ложных срабатываний);
 - построение модели маршрутизации запросов для веб-приложения;
 - построение моделей логических действий в приложении и моделей параметров этих действий, а также последовательностей (цепочек) логических действий;
 - Оценка отклонения параметров логических действий в веб-приложении от статистической нормы;
- 4.2.8. Возможности по выполнению автоматического обучения:
- непрерывное обучение в процессе функционирования;
 - периодический запуск заданий по обучению по установленному расписанию;
 - ручной однократный запуск заданий по обучению;
 - инкрементное (только для изменений, произошедших с момента предыдущего обучения), а также частичная ручная корректировка результатов обучения для отдельных статических ресурсов, ложных срабатываний, логических действий и т.п. без необходимости проводить обучение заново.
- 4.2.9. Результаты автоматического обучения полностью интерпретируемы и корректируемы Исполнителем.

5. СОСТАВ, УСЛОВИЯ И ПОРЯДОК ОКАЗАНИЯ УСЛУГИ

- 5.1. Услуги доступны для заказа как для сервисов Заказчика, функционирующих как в Облаке Cloud.ru, так и в сторонней инфраструктуре Заказчика.
- 5.2. Пользуясь Услугами, Заказчик подтверждает, что доменные имена, для которых подключаются Услуги, принадлежат ему на законном основании, либо он действует от имени и по поручению законных владельцев этих доменных имен.
- 5.3. Для подключения Услуг «Защита от DDoS-атак (StormWall)» и «Защита Веб-приложений (StormWall)»:
- 5.3.1. Заказчик выбирает тарифный план на основании предполагаемой полосы легитимного трафика, гарантированной доступности защищаемых сервисов и необходимой дополнительной функциональности из Таблицы № 1;
- 5.3.2. Исходя из выбранных параметров Услуг (см. п. 5.1.1.), заполняет форму Заказа Услуги, представленную в приложении № 1.CRS.3.A. и направляет её Исполнителю на адрес электронной почты уполномоченного лица;
- 5.3.3. В течение 3 (трех) рабочих дней Исполнитель обязуется согласовать предоставление Услуг Заказчику либо предоставить мотивированный отказ, при этом Стороны признают, что т.к. Услуга является партнёрской, отказ в её предоставлении может быть связан с действиями партнёра; В случае согласования предоставления Услуги, Исполнитель передает уполномоченному лицу Заказчика логина и пароль от личного кабинета Услуги, размещенной на сайте партнера.

Табл.1. Тарифные планы Услуги «Защита от DDoS-атак (StormWall)»

| Наименование тарифа | Диапазон на выбор, включенного в тариф легитимного трафика (после очистки, без учета трафика атак) | Набор опций, входящих в абонентскую плату по тарифу |
|--|--|--|
| Защита сайта от DDoS – тариф Business ONE | 50 Мбит/с | <ul style="list-style-type: none"> • Защита 1 домена 2-го уровня и до 100 его поддоменов; • Защита от атак на уровнях L3-L7 модели OSI; • Балансировка нагрузки между бэкендами; • Защищенный DNS для защищаемых объектов; • HyperCache CDN (кэширование статических объектов в оперативной памяти фильтров) и оптимизация загрузки сайта (путем применения протокола HTTP/2); • Личный кабинет (аналитика, отчеты, настройки защиты); • Просмотр/управление списками заблокированных адресов и историей блокировок; • Поддержка HTTPS и HTTP/2; • API для управления сервисом; • GeoIP (проверки, блокировки); • До 500 Black/White/Grey-листов; • Поддержка Websocket. |
| | 100 Мбит/с | |
| | 200 Мбит/с | |
| | 300 Мбит/с | |
| | 400 Мбит/с | |
| | 500 Мбит/с | |
| | 1000 Мбит/с | |
| | 1500 Мбит/с | |
| | 2000 Мбит/с | |
| | 2500 Мбит/с | |

| | | |
|---|--------------|--|
| | 3000 Мбит/с | |
| | 3500 Мбит/с | |
| | 4000 Мбит/с | |
| | 4500 Мбит/с | |
| | 5000 Мбит/с | |
| | 6000 Мбит/с | |
| | 7000 Мбит/с | |
| | 8000 Мбит/с | |
| | 9000 Мбит/с | |
| | 10000 Мбит/с | |
| Защита сайта от DDoS – тариф Enterprise ONE | 50 Мбит/с | <ul style="list-style-type: none"> • Защита 1 домена 2-го уровня и до 100 его поддоменов; • Защита от атак на уровнях L3-L7 модели OSI; • Балансировка нагрузки между бэкендами; • Защищенный DNS для защищаемых объектов; • HyperCache CDN (кэширование статических объектов в оперативной памяти фильтров) и оптимизация загрузки сайта (путем применения протокола HTTP/2); • 1 выделенный IP-адрес; • Экспертная поддержка AntiDDoS (чат в приложении Slack или Telegram); • Возможность подключения защиты L7 без раскрытия частных ключей SSL/TLS; • Возможность реализации нестандартных методов подключения (через физический стык или L2-канал); • Личный кабинет (аналитика, отчеты, настройки защиты); • Ролевая модель доступа к личному кабинету и логирование действий пользователей; • Просмотр/управление списками заблокированных адресов и историей блокировок; • Поддержка HTTPS и HTTP/2; • API для управления сервисом; • GeoIP (проверки, блокировки); • До 1000 Black/White/Grey-листов; • Поддержка Websocket; • Проактивный мониторинг; • Управление защитой от ботов (цепочки правил HTTP); • Поддержка ГОСТ-шифрования и сертификатов; • Персонализация страниц ошибок; • Доступ к Graylog. |
| | 100 Мбит/с | |
| | 200 Мбит/с | |
| | 300 Мбит/с | |
| | 400 Мбит/с | |
| | 500 Мбит/с | |
| | 1000 Мбит/с | |
| | 1500 Мбит/с | |
| | 2000 Мбит/с | |
| | 2500 Мбит/с | |
| | 3000 Мбит/с | |
| | 3500 Мбит/с | |
| | 4000 Мбит/с | |
| | 4500 Мбит/с | |
| | 5000 Мбит/с | |
| | 6000 Мбит/с | |
| | 7000 Мбит/с | |
| | 8000 Мбит/с | |
| | 9000 Мбит/с | |
| | 10000 Мбит/с | |
| Защита сайта от DDoS – тариф Business UNL | 50 Мбит/с | <ul style="list-style-type: none"> • Защита 100 доменов 2-го уровня и до 100 поддоменов на каждый домен; • Защита от атак на уровнях L3-L7 модели OSI; • Балансировка нагрузки между бэкендами; • Защищенный DNS для защищаемых объектов; • HyperCache CDN (кэширование статических объектов в оперативной памяти фильтров) и оптимизация загрузки сайта (путем применения протокола HTTP/2); • Личный кабинет (аналитика, отчеты, настройки защиты); • Просмотр/управление списками заблокированных адресов и историей блокировок; • Поддержка HTTPS и HTTP/2; • API для управления сервисом; • GeoIP (проверки, блокировки); • До 500 Black/White/Grey-листов; • Поддержка Websocket. |
| | 100 Мбит/с | |
| | 200 Мбит/с | |
| | 300 Мбит/с | |
| | 400 Мбит/с | |
| | 500 Мбит/с | |
| | 1000 Мбит/с | |
| | 1500 Мбит/с | |
| | 2000 Мбит/с | |
| | 2500 Мбит/с | |
| | 3000 Мбит/с | |

| | | |
|---|--------------|---|
| | 3500 Мбит/с | |
| | 4000 Мбит/с | |
| | 4500 Мбит/с | |
| | 5000 Мбит/с | |
| | 6000 Мбит/с | |
| | 7000 Мбит/с | |
| | 8000 Мбит/с | |
| | 9000 Мбит/с | |
| | 10000 Мбит/с | |
| | | |
| Защита сайта от DDoS – тариф Enterprise UNL | 50 Мбит/с | <ul style="list-style-type: none"> • Защита 100 доменов 2-го уровня и до 100 поддоменов на каждый домен; • Защита от атак на уровнях L3-L7 модели OSI; • Балансировка нагрузки между бэкендами; • Защищенный DNS для защищаемых объектов; • HyperCache CDN (кэширование статических объектов в оперативной памяти фильтров) и оптимизация загрузки сайта (путем применения протокола HTTP/2); • 1 выделенный IP-адрес; • Экспертная поддержка AntiDDoS (чат в приложении Slack или Telegram); • Возможность подключения защиты L7 без раскрытия приватных ключей SSL/TLS; • Возможность реализации нестандартных методов подключения (через физический стык или L2-канал); • Личный кабинет (аналитика, отчеты, настройки защиты); • Ролевая модель доступа к личному кабинету и логирование действий пользователей; • Просмотр/управление списками заблокированных адресов и историей блокировок; • Поддержка HTTPS и HTTP/2; • API для управления сервисом; • GeoIP (проверки, блокировки); • До 1000 Black/White/Grey-листов; • Поддержка Websocket; • Проактивный мониторинг; • Управление защитой от ботов (цепочки правил HTTP); • Поддержка ГОСТ-шифрования и сертификатов; • Персонализация страниц ошибок; • Доступ к Graylog. |
| | 100 Мбит/с | |
| | 200 Мбит/с | |
| | 300 Мбит/с | |
| | 400 Мбит/с | |
| | 500 Мбит/с | |
| | 1000 Мбит/с | |
| | 1500 Мбит/с | |
| | 2000 Мбит/с | |
| | 2500 Мбит/с | |
| | 3000 Мбит/с | |
| | 3500 Мбит/с | |
| | 4000 Мбит/с | |
| | 4500 Мбит/с | |
| | 5000 Мбит/с | |
| | 6000 Мбит/с | |
| | 7000 Мбит/с | |
| | 8000 Мбит/с | |
| | 9000 Мбит/с | |
| | 10000 Мбит/с | |
| Защита серверов и сетей – тариф Standard | 50 Мбит/с | <ul style="list-style-type: none"> • 1 ASN; • 1 туннель/подключение; • 10 префиксов; • Защита от атак на уровнях L3-L5 модели OSI; • Типы подключения: Физическое подключение на MMTC-9, GRE-туннель, MPLS; • Нет поддержки в чате (только тикеты); • Нет DDoS-сенсора; • Нет индивидуальных профилей защиты; • Защита от атак до 600 Гбит/с. |
| | 100 Мбит/с | |
| | 200 Мбит/с | |
| | 300 Мбит/с | |
| | 400 Мбит/с | |
| | 500 Мбит/с | |
| | 600 Мбит/с | |
| | 700 Мбит/с | |
| | 800 Мбит/с | |
| | 900 Мбит/с | |
| | 1000 Мбит/с | |
| | 1500 Мбит/с | |
| | | |

| | | |
|--|--------------|---|
| | 2000 Мбит/с | |
| | 3000 Мбит/с | |
| | 4000 Мбит/с | |
| | 5000 Мбит/с | |
| | 6000 Мбит/с | |
| | 7000 Мбит/с | |
| | 8000 Мбит/с | |
| | 9000 Мбит/с | |
| | 10000 Мбит/с | |
| | 15000 Мбит/с | |
| | 20000 Мбит/с | |
| | 30000 Мбит/с | |
| | 40000 Мбит/с | |
| | 50000 Мбит/с | |
| | 60000 Мбит/с | |
| | 70000 Мбит/с | |
| Защита серверов и сетей – тариф Business | 50 Мбит/с | <ul style="list-style-type: none"> • 1 ASN; • 1 туннель/подключение; • 10 префиксов; • Защита от атак на уровнях L3-L5 модели OSI; • Типы подключения: Физическое подключение на MMTC-9, GRE-туннель, MPLS; • Нет поддержки в чате (только тикеты); • Нет DDoS-сенсора; • Нет индивидуальных профилей защиты; • Защита от атак до 600 Гбит/с. |
| | 100 Мбит/с | |
| | 200 Мбит/с | |
| | 300 Мбит/с | |
| | 400 Мбит/с | |
| | 500 Мбит/с | |
| Защита серверов и сетей – тариф Enterprise | 600 Мбит/с | <ul style="list-style-type: none"> • До 10 ASN (собственных или транзит); • До 10 туннелей/подключений; • До 100 префиксов; • Защита от атак на уровнях L3-L5 модели OSI; • Типы подключения: Физическое подключение на MMTC-9, GRE-туннель, MPLS; • Поддержка в чате Slack/Telegram; • DDoS-сенсор; • Индивидуальные профили защиты; • Защита от атак без ограничений по емкости. |
| | 700 Мбит/с | |
| | 800 Мбит/с | |
| | 900 Мбит/с | |
| | 1000 Мбит/с | |
| | 1500 Мбит/с | |
| | 2000 Мбит/с | |
| | 3000 Мбит/с | |
| | 4000 Мбит/с | |
| | 5000 Мбит/с | |
| | 6000 Мбит/с | |
| | 7000 Мбит/с | |
| | 8000 Мбит/с | |
| | 9000 Мбит/с | |
| | 10000 Мбит/с | |
| | 15000 Мбит/с | |
| | 20000 Мбит/с | |
| | 30000 Мбит/с | |

| | | |
|---|--------------|---|
| | 40000 Мбит/с | |
| | 50000 Мбит/с | |
| | 60000 Мбит/с | |
| | 70000 Мбит/с | |
| Защита сайта от хакерских атак с помощью WAF – тариф Т1 (доступна только при заказе Услуги Защиты от DDoS-атак) | 100 RPS | <ul style="list-style-type: none"> • Защита 1 веб-приложения; • Валидация протокола HTTP (типы запросов, заголовки и их параметры и т.п.); • Автоматическая фильтрация статических ресурсов: отдельный режим обработки статических ресурсов (обеспечивает оптимальную производительность анализа данных в подсистеме управления и мониторинга); • Анализ запросов и ответов с использованием набора сигнатур, определяющих атаки OWASP Top 10; • Блокировка источника при обнаружении множественных аномалий в запросах от него (Last Recent BlockedCache); • Ограничение частоты запросов от одного источника (Rate Limiting) для приложения в целом; • Предварительное подавление ложных срабатываний при подключении (на основе машинного обучения и с привлечением аналитиков); • Подавление ложных срабатываний при обращении в службу поддержки; • Доступ с правами "на чтение" к расширенному личному кабинету WAF, который отображает текущие модели и правила защиты; • Отправка уведомлений о критичных событиях ИБ по электронной почте (настраивается по запросу в службу поддержки); • Хранение событий безопасности; • Хранение аномальных транзакции; • Отправка регулярных отчетов о работе WAF (настраивается по запросу Партнера в службу поддержки). |
| | 300 RPS | |
| | 500 RPS | |
| | 700 RPS | |
| | 1000 RPS | |
| | 1500 RPS | |
| | 2000 RPS | |
| | 3000 RPS | |
| | 5000 RPS | |
| | 7000 RPS | |
| | 10000 RPS | |
| | 10000 RPS | |
| Защита сайта от хакерских атак с помощью WAF – тариф Т2 (доступна только при заказе Услуги Защиты от DDoS-атак) | 100 RPS | <p>Функционал согласно тарифу Защита сайта от хакерских атак с помощью WAF – тариф Т1 и дополнительно к нему:</p> <ul style="list-style-type: none"> • Автоматическое определение выполняемых логических действий и проверка их параметров на соответствие установленным моделям. Модель бизнес-логики может строится вручную или с помощью машинного обучения (результаты машинного обучения являются полностью интерпретируемыми или корректируемыми). Для логических действий и параметров могут быть установлены названия, соответствующие их реальным функциям в приложении (с целью упрощения анализа запросов и событий безопасности) ; • Определение успешности выполняемых действий на основе анализа ответов, в том числе - вложенных данных; • Определение источников - произвольных параметров логических действий, которые характеризуют источник запроса (IP-адрес, идентификатор сессии, имя пользователя, определенная cookie и т.п.) ; • Контроль пользователей и сессий, которая определяет ключевые параметры сессии, а также логические действия, в рамках которых эти параметры; устанавливаются, контролируются и инвалидируются). • Контроль авторизации пользователей на уровне сессий и выполняемых логических действий (соответствующие правила могут задаваться на WAF) ; • Контроль количества запросов к отдельным логическим действиям в зависимости от параметров источника запроса и других параметров (Rate Limiting) ; • Хранение данных транзакций без аномалий с использованием сэмплирования в выделенном |
| | 300 RPS | |
| | 500 RPS | |
| | 700 RPS | |
| | 1000 RPS | |
| | 1500 RPS | |
| | 2000 RPS | |
| | 3000 RPS | |
| | 5000 RPS | |
| | 7000 RPS | |
| | 10000 RPS | |
| | 10000 RPS | |

| | | |
|---|------------|---|
| | | <p>хранилище "теплых" данных (warm data) для последующего ретроспективного анализа, в т.ч. борьбы с ботами;</p> <ul style="list-style-type: none"> • Возможность формирования кастомизированных автоматических отчетов (настройка отчетов выполняется в рамках услуг расширенного сопровождения - профессиональных сервисов); • Возможность отправки данных в SIEM-систему Партнера с использованием унифицированного интерфейса API (настраивается по запросу Партнера в службу поддержки). |
| Защита сайта от хакерских атак с помощью WAF – тариф Т3 (доступна только при заказе Услуги Защиты от DDoS-атак) | 100 RPS | <p>Функционал согласно тарифу Защита сайта от хакерских атак с помощью WAF – тариф Т2 и дополнительно к нему:</p> <ul style="list-style-type: none"> • Возможность гибкой настройки передаваемых данных (сырые запросы, деревья разбора, логические действия, события безопасности и т.п.); • Предоставление выделенных узлов анализа для повышения гибкости конфигурации и оптимизации производительности; • Предоставление выделенной инсталляции для еще большей гибкости конфигурации и оптимизации производительности для высоконагруженных ресурсов. |
| | 300 RPS | |
| | 500 RPS | |
| | 700 RPS | |
| | 1000 RPS | |
| | 1500 RPS | |
| | 2000 RPS | |
| | 3000 RPS | |
| | 5000 RPS | |
| | 7000 RPS | |
| | 10000 RPS | |
| Cloud Application Firewall (uC-WAF) | 100 RPS | <p>Описание методов очистки трафика:</p> <ul style="list-style-type: none"> • Реагирования на угрозы, описанные в OWASP Top Ten. • Инспектирование запросов и ответов в соответствии с политикой безопасности, журналирование событий предотвращения утечки данных – инспекция ответов сервера на наличие критичных данных. • Применение как позитивной, так и негативной модели безопасности инспектирование всего содержимого веб-страниц, включая HTML, DHTML и CSS, а также нижележащих протоколов доставки содержимого (HTTP/HTTPS) • Инспектирование сообщений веб-сервиса, если веб-сервис подключен к интернету (SOAP, XML). • Инспектирование любого протокола или конструкции данных, использующихся для передачи данных веб-приложения вне зависимости от того, является ли он проприетарным или стандартизованным (как для входящих, так и исходящих потоков данных). <p>Описание функциональных возможностей модуля WAF:</p> <ul style="list-style-type: none"> • Функции анализа и обработки данных <p>Обработка трафика на внешнем агенте в режиме обратного прокси-сервера (reverse proxy) – соединение в разрыв, выступая в качестве прокси-сервера между клиентом и защищаемым веб-приложением (с помощью внешних агентов, расположенных в ИТ-инфраструктуре). Поддержка HTTP 1.0, 1.1, WebSocket (ws, wss), XML. Анализ данных в нотации XML, JSON, GraphQL.</p> <p>Функции реагирования:</p> <p>"Наборы правил обработки трафика, настроенные на защиту объектов (ресурсов) на базе технологий:</p> <ul style="list-style-type: none"> • Apache Struts – включает только те правила, которые предназначены для защиты веб-приложений, разработанных на фреймворке Apache Struts; • http://ASP.NET – включает только те правила, которые предназначены для защиты веб-приложений, созданных на платформе http://ASP.NET; |
| | 300 RPS | |
| | 500 RPS | |
| | 750 RPS | |
| | 1 000 RPS | |
| | 2 000 RPS | |
| | 3 000 RPS | |
| | 4 000 RPS | |
| | 5 000 RPS | |
| | 10 000 RPS | |

| | | |
|---|---|---|
| | | <ul style="list-style-type: none"> • Java — включает только те правила, которые предназначены для защиты веб-приложений, разработанных на языке Java; • Joomla CMS — включает только те правила, которые предназначены для защиты веб-приложений, основанных на системе управления контентом Joomla; • LAMP (PHP, Apache, MySQL) — включает только те правила, которые предназначены для защиты веб-приложений, разработанных при помощи инструментов PHP, Apache или MySQL; • Microsoft Exchange — включает только те правила, которые предназначены для защиты сервера Microsoft Exchange; • Node.js — включает только те правила, которые предназначены для защиты веб-приложений, созданных на платформе Node.js; • PHP — включает только те правила, которые предназначены для защиты веб-приложений, разработанных на языке PHP; • Default template (стандартный шаблон) — включает правила всех остальных системных наборов." <p>Функции передачи данных:</p> <ul style="list-style-type: none"> • Программные интерфейсы (REST API) для автоматизации задач по управлению системой с помощью внешних программных средств. • Функции хранения данных <p>"Хранение данных:</p> <ul style="list-style-type: none"> • события безопасности; • параметры безопасности и данных о конфигурации." <p>• Функции управления:</p> <p>" • Управление защищаемыми приложениями, и связанных с ними событий безопасности и политик безопасности.</p> <ul style="list-style-type: none"> • Возможность управления функциями Услуги через веб-интерфейс (HTTPS). • Обеспечение управления Услугой через любой из интерфейсов должна предоставляться только авторизованным (уполномоченным) пользователям. • Обеспечение реализации ролевой модели управления доступом к функциям Услуги, доступным через веб-интерфейс. • Регистрация событий, связанных с действиями пользователей системы и системными операциями (журнал аудита). • Визуализация данных о событиях безопасности в виде таблиц и гистограмм на ленте событий. • Возможность указания временного периода, за который отображаются события безопасности. • Возможность обновления данных о событиях безопасности в автоматическом и «ручном» режимах. • Отслеживание статуса применения конфигурации на внешнем агенте. • Автоматизированное обновление баз знаний (правил защиты);" |
| Дополнительный домен на тарифах Business | - | - |
| Дополнительный IP-адрес на тарифах Business | - | - |
| Дополнительный домен на тарифах Enterprise | - | - |
| Дополнительный IP-адрес на тарифах Enterprise | | |
| Дополнительно 10 префиксов | | |

| | | |
|--|---|---|
| Дополнительно 1 AS | | |
| Дополнительно 1 туннель | | |
| DDoS сенсор | | |
| Поддержка в Slack/Telegram | | |
| Защита сайта от хакерских атак с помощью WAF дополнительного веб приложения на тарифе T1 | - | - |
| Защита сайта от хакерских атак с помощью WAF дополнительного веб приложения на тарифе T2 | - | - |
| Защита сайта от хакерских атак с WAF дополнительного веб приложения на тарифе T3 | - | - |

6. ТАРИФИКАЦИЯ УСЛУГИ

- 6.1. Расчетным периодом является календарный месяц.
- 6.2. Оплата за Услуги состоит из фиксированной оплаты по тарифу и переменной частей (за превышение легитимной пропускной способности и/или количество запросов в секунду (RPS)).
- 6.3. Размер фиксированной платы, определяется на основании выбранного тарифа.
- 6.4. Сумма оплаты за превышение легитимной пропускной способности и/или количество запросов в секунду (RPS) рассчитывается по следующей формуле:

Если $Y > R$

$$P = (T + F * (Y - R))$$

P - Ежемесячный платеж за Услугу.

T - Цена за 1 месяц пользования по тарифу.

F - Цена за 1 Мбит/с превышения и/или цена за 1 RPS превышения, указанная в Спецификации в Приложении 1 к Договору.

R - Легитимная пропускная способность, включенная в подписку.

Y - Фактически использованная легитимная пропускная способность по 95 перцентилю за расчетный период. Легитимная полоса пропускания, включенная в подписку, может быть превышена на 36 часов за каждый расчетный период (5% времени в месяц). Используемая полоса пропускания измеряется делением количества переданных данных на 5 минутный интервал. По окончании расчетного периода 5% от максимальных значений удаляются. Затем из оставшихся 95% выбирается максимальное число, которое используется для расчета.

- 6.5. При расчёте превышения Тарифа Cloud Application Firewall (uC-WAF) за основу берется фактически потребленная пропускная способность программ, определяемая по методу 95-й перцентиль (далее – «значение К»). Если значение К превысило Тариф на 15% и более для Тарифов до 750 RPS включительно или на 200 RPS и более для Тарифов от 1000 RPS, в Вознаграждение Исполнителя включается Сверхнормативный тариф, рассчитываемый в следующем порядке:

- 6.5.1. Для Тарифов до 750 RPS (запросов в секунду) включительно:

- Если значение К превысило Тариф в диапазоне от 15% до 59,99%, вознаграждение за превышение Тарифа рассчитывается по формуле: (следующий Тариф) – (текущий Тариф) * 0,7.
- Если значение К превысило Тариф на 60% и выше, Вознаграждение за превышение Тарифа рассчитывается по формуле: (необходимый для значения К Тариф) – (текущий Тариф).

Пример: Заказчик выбрал Тариф 300 RPS. Значение К в Отчетном периоде составило 547 RPS. Необходимый для значения К Тариф – 750 RPS. Расчёт Сверхнормативного тарифа производится путём вычитания из стоимости Тарифа 750 RPS стоимости Тарифа 300 RPS.

6.5.2. Для Тарифов 1000 RPS (запросов в секунду) и выше:

- Если значение К превысило Тариф в диапазоне от 200 RPS до 499 RPS, Вознаграждение за превышение Тарифа рассчитывается по формуле: (следующий Тариф) – (текущий Тариф) * 0,6.
- Если значение К превысило Тариф на 500 RPS и выше, Вознаграждение за превышение Тарифа рассчитывается по формуле: (необходимый для значения К Тариф) – (текущий Тариф).»

7. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГАМ

7.1. Возможные виды подключения / изменения / отключения Услуг:

7.1.1. Посредством подписания Заказа⁴.

7.2. Возможный порядок расчётов по Услугам:

7.2.1. Постоплата.

7.3. Возможные способы оплаты / порядок пополнения Баланса:

7.3.1. Оплата в безналичном порядке на основании выставленного Исполнителем счёта.

⁴ С учётом особенностей, изложенных в разделе 6 настоящего Приложения.