|  |  |
| --- | --- |
|  | **Утверждено:**  Начальник Управления по информационной безопасности  ООО «ЕвроСибЭнерго-Гидрогенерация»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Афанасьев  (подпись)  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

**Техническое задание**

**Подписка на сервис MSSP** **WAF+AntiDDOS**

Иркутск

2023

**СОДЕРЖАНИЕ**

[1 НАИМЕНОВАНИЕ ЗАКУПАЕМОЙ ПРОДУКЦИИ (ТОВАРОВ, РАБОТ, УСЛУГ) 3](#_Toc147245838)

[1.1 НАИМЕНОВАНИЕ ЗАКУПАЕМОЙ ПРОДУКЦИИ 3](#_Toc147245839)

[1.2 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 3](#_Toc147245840)

[2 ЗАКАЗЧИК 3](#_Toc147245841)

[3 ЦЕЛИ ПРОЕКТА 3](#_Toc147245842)

[4 ЗАДАЧИ ПРОЕКТА 4](#_Toc147245843)

[5 ТРЕБОВАНИЯ К СЕРВИСУ WAF+ANTIDDOS 4](#_Toc147245844)

[5.1 КЛЮЧЕВЫЕ ПАРАМЕТРЫ СЕРВИСА 4](#_Toc147245845)

[5.2 ТРЕБОВАНИЯ К ПОДСИСТЕМЕ ANTIDDOS 5](#_Toc147245846)

[5.3 ТРЕБОВАНИЯ К ПОДСИСТЕМЕ WAF 5](#_Toc147245847)

[5.4 ТРЕБОВАНИЯ К ВЕБ-ПОРТАЛУ 8](#_Toc147245848)

[6 ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ 8](#_Toc147245849)

[6.1 ТРЕБОВАНИЯ К ПЕРСОНАЛУ 8](#_Toc147245850)

[6.2 ТРЕБОВАНИЯ К ОПЫТУ ВЫПОЛНЕНИЯ РАБОТ 8](#_Toc147245851)

# НАИМЕНОВАНИЕ ЗАКУПАЕМОЙ ПРОДУКЦИИ (ТОВАРОВ, РАБОТ, УСЛУГ)

## Наименование закупаемой продукции

Приобретение подписки на сервис MSSP WAF+AntiDDOS.

## Термины и определения

|  |  |
| --- | --- |
| **Термин** | **Определение** |
| Заказчик | ООО «ЕвроСибЭнерго-Гидрогенерация» |
| Исполнитель | Организация, осуществляющая предоставление сервиса MSSP WAF+AntiDDOS |
| WAF (Web Application Firewall) | Межсетевой экран уровня веб-приложений – программное обеспечение, предназначенное для обнаружения и блокирования сетевых атак на веб-приложение |
| AntiDDOS | Сервис защиты веб-приложений от DDOS атак |
| DDOS (Distributed Denial of Service) | Разновидность DoS-атаки, реализующая отказ системы в обслуживании посредством исчерпания тех или иных вычислительных ресурсов самой атакуемой системы или внешних сервисов, от функционирования которых зависит работа атакуемой системы (транзитные операторы связи, источники данных и т. д.). |
| Managed Security Service Provider (MSSP) | Управляемый поставщик услуг безопасности (компания, предоставляющая сервисы в области информационной безопасности) |
| Security information and event management (SIEM система) | Система, предназначенная для сбора и анализа (корреляции) информации о событиях безопасности с целью обнаружения инцидентов ИБ |
| Application Programming Interface (API) | Программный интерфейс приложения, предназначенный для обмена данными между системами, программами, приложениями. API определяет порядок взаимодействия, используя запросы и ответы. |

# ЗАКАЗЧИК

Заказчик – ООО «ЕвроСибЭнерго-Гидрогенерация»

# ЦЕЛИ ПРОЕКТА

Настоящее техническое задание определяет требования к сервису по защите веб-приложений от сетевых атак и атак типа «отказ в обслуживании» (далее – сервис или MSSP WAF+AntiDDOS).

Использование сервиса направлено на достижение следующих целей:

* Обеспечение комплексной защиты веб-приложений и ИТ-инфраструктуры Заказчика от DDoS-атак на всех уровнях модели OSI, до 7-го уровня (уровня приложения) включительно;
* Защита веб-приложений от атак OWASP TOP 10;
* Предотвращение бот-активности на веб-приложениях;
* Предотвращение подбора учетных записей (bruteforce) на порталах авторизации;
* Защита порталов авторизации от «атак переполнения»;
* Защита от атак credential stuffing;
* Создание виртуальных патчей для веб-приложений (создание динамических правил блокировки, основанных на результатах работы узла фильтрации);
* Фильтрация трафика по значениям полей заголовков.

# ЗАДАЧИ ПРОЕКТА

В рамках предоставления сервиса решаются следующие задачи:

* развертывание и настройка компонентов сервиса в облачной инфраструктуре Исполнителя;
* перенастройка DNS-записей защищаемых ресурсов Заказчика на облачную инфраструктуру Исполнителя;
* ограничение доступа к веб-приложениям Заказчика из сети Интернет;
* профилирование защищаемых ресурсов Заказчика;
* перевод трафика защищаемых ресурсов на центры очистки antiDDOS;
* перевод трафика защищаемых ресурсов на облачный WAF (в режим блокировки атак);
* осуществление непрерывного мониторинга атак в отношении защищаемых ресурсов с целью обнаружения инцидентов ИБ;
* отправка уведомлений по обнаруженным инцидентам в SIEM-систему Заказчика по API;
* обеспечение проактивной защиты веб-приложений.

# ТРЕБОВАНИЯ К сервису WAF+AntiDDOS

## Ключевые параметры сервиса

Срок действия подписки на сервис MSSP WAF+AntiDDOS – 5 лет (60 месяцев).

Подписка начинает действовать после завершения процесса настройки компонентов сервиса в инфраструктуре Исполнителя, перенастройки DNS-записей защищаемых ресурсов Заказчика на облачную инфраструктуру Исполнителя и окончания профилирования защищаемых ресурсов.

После завершения вышеописанных этапов Заказчик направляет уведомление Исполнителю, что инфраструктура Заказчика готова к переводу защищаемых ресурсов на работу через сервис MSSP WAF+AntiDDOS.

До момента получения уведомления от Заказчика работа WAF в режиме блокировки атак и фильтрация сетевого трафика через центры очистки antiDDOS со стороны Исполнителя не осуществляется.

Схема предоставления сервиса – «облачный» WAF+AntiDDOS (все компоненты сервиса располагаются в инфраструктуре Исполнителя).

Схема подключения AntiDDOS – изменение DNS А-записи защищаемого ресурса на центр очистки, проксирование трафика с раскрытием SSL при помощи промежуточного SSL сертификата.

Выпуск промежуточного SSL сертификата защищаемых ресурсов для прокси сервера должен входить в стоимость услуги. Использование wildcard-сертификатов не допускается.

Все компоненты сервиса приобретаются, настраиваются и обслуживаются за счет и силами Исполнителя.

Наличие возможности интеграции сервиса с SIEM-системой Заказчика по API.

Наличие веб-портала с доступом из сети Интернет для отображения информации об атаках, к которому предоставляется доступ представителям Заказчика.

Количество защищаемых ресурсов Заказчика (веб-приложений) – 60.

Максимальное количество запросов в секунду (суммарно по всем защищаемым ресурсам) – 200 RPS.

Легитимная полоса фильтрации превалирующего трафика – 100 Мбит/с.

Полоса фильтрации вредоносного (нежелательного) трафика – 500 Гбит/с.

Гарантированная доступность системы фильтрации трафика – не ниже 99,5%.

Сервис предоставляется в режиме 24х7х365 (366).

Реагирование на инциденты работоспособности сервиса осуществляется в режиме 24х7х365 (366).

В рамках предоставления сервиса Исполнителем на постоянной непрерывной основе должно проводиться:

* настройка и корректировка индивидуальных профилей защиты для защищаемых ресурсов;
* выявление ложноположительных срабатываний механизмов фильтрации;
* внесение изменений в конфигурацию защищаемых веб-приложений;
* настройка политик защиты для веб-приложений по требованию Заказчика;
* тонкая настройка всех модулей защиты для защищаемых приложений.

## Требования к подсистеме AntiDDOS

Сервис должен обеспечивать защиту от всего спектра атак вида «отказ в обслуживании», направленных как на исчерпание канальной емкости, так и на исчерпание ресурсов прикладной системы.

Сервис должен поддерживать функциональность мониторинга IP-сетей на предмет наличия серверов, уязвимых к атакам типа amplification.

Режим работы сервиса должен обеспечиваться изменением DNS А-записи защищаемого ресурса на центр очистки, проксированием трафика с раскрытием SSL при помощи промежуточного SSL сертификата.

Выпуск промежуточного SSL сертификата защищаемого ресурса для прокси сервера должен входить в стоимость услуги. Использование wildcard-сертификатов не допускается.

Сервис должен защищать подключаемые к системе очистке трафика корпоративные ресурсы от DDoS-aтaк всех типов, вплоть до уровня L7 модели OSI.

Перевод трафика защищаемых ресурсов на центры очистки должен выполняться на постоянной основе, а не только в момент DDOS атаки.

Легитимная полоса фильтрации превалирующего трафика – 100 Мбит/с.

Полоса фильтрации вредоносного (нежелательного) трафика – 500 Гбит/с.

Сервис должен обеспечивать передачу ІР-адреса источников сетевых пакетов в HTTP заголовке на защищаемый ресурс после прохождения прокси-серверов системы очистки трафика с возможностью отслеживания и мониторинга ір-адресов источников, обращающихся к защищаемым ресурсам.

Система очистки трафика должна иметь реализованный сбор статистики в реальном времени со средним (за неделю) интервалом не более 5 минут и предоставление ее в виде графиков в веб-портале.

Система очистки графика должна поддерживать размер файлов для загрузки пользователем на защищаемые ресурсы (upload) не менее 20 Мб.

Гарантированная доступность системы фильтрации трафика должна быть не ниже 99,5%.

## Требования к подсистеме WAF

Количество защищаемых ресурсов Заказчика (веб-приложений) – 60.

Максимальное количество запросов в секунду (суммарно по всем защищаемым ресурсам) – 200 RPS.

Среднее количество запросов в секунду (суммарно по всем защищаемым ресурсам) – 30 RPS.

Пиковые значения входящего трафика к веб-приложениям – 80 Мбит/сек.

Средние значения входящего трафика к веб-приложениям – 10 Мбит/сек.

Пиковые значения исходящего трафика к веб-приложениям – 30 Мбит/сек.

Средние значения исходящего трафика к веб-приложениям – 10 Мбит/сек.

Версия используемого HTTP – HTTP/1.1, HTTP/2.

Сервис должен поддерживать работу веб-приложений, использующих websocket.

Сервис должен поддерживать работу веб-приложений, использующих TLS 1.2, TLS 1.3.

Для всех веб-приложений должен быть настроен редирект с протокола http на протокол https (для всех разделов веб-сайта).

Задержка сетевых веб-запросов не должна превышать 100 ms.

Подсистема должна поддерживать следующий функционал:

* Возможность блокировки отдельного веб-запроса;
* Анализ трафика веб-приложений с помощью правил фильтрации;
* Обнаружение уязвимостей в веб-приложениях с помощью пассивного сканера;
* Внедрение безопасных HTTP-заголовков;
* Проверка параметров запросов к защищаемым веб-приложениям на предмет совпадений с сигнатурами кибератак для идентификации вредоносных запросов;
* Проверка HTTP-ответов с целью предотвращения утечки данных и обеспечения дополнительной защиты с помощью специальных HTTP-заголовков;
* Предотвращение кибератак на веб-приложения с использованием следующего ПО: Acunetix, Burp Suite, OWASP ZAP, XSSER, w9scan, Wapiti, Arachni, Paros, Tenable, Nessus, sqlmap, Nikto, WPScan, Vega, WebInspect, WebCruiser, Dirsearch, Dirbuster;
* Извлечение аутентификационной информации из запроса с целью отслеживания попыток входа в систему и контроля доступа к ресурсам для пользователей веб-приложений или групп пользователей при помощи списка правил, определяющих права доступа субъектов (пользователь, группа) к ресурсам веб-приложения;
* Фильтрация на основе технологий «черный список» и «белый список»;
* Защита от ботнет-активности (при помощи проверок Bot Mitigation, JS Challenge, reCAPTCHA v2 и v3, Проверка DNS, Fingerprinting, Определение сигнатур ботнет-устройств);
* Защита от DoS атак на уровне приложений (при помощи технологии Rate Limiting);
* Создание виртуальных патчей для веб-приложений (создание динамических правил блокировки, основанных на результатах работы узла фильтрации).

Подсистема должна включать в себя защиту от следующих классов атак (но не ограничиваться ими):

* Подделка межсайтовых запросов (CSRF).
* SQL- и NoSQL-инъекции (Blind SQL Injection, NoSQL Injection, Classic SQL Injection, Error-based SQL Injection).
* Межсайтовый скриптинг (Reflected XSS, Stored XSS, DOM-based XSS).
* Удаленное выполнение произвольного кода (RCE).
* Выход за пределы рабочей директории веб-сервера (Path Traversal).
* Внедрение внешней сущности XML (XXE).
* Атаки подбором учетных данных (BruteForce).
* Инъекция шаблона на стороне веб-сервера (SSTI).
* Информационная XML-бомба.
* Небезопасное перенаправление (open redirect).
* Подделка запросов на стороне веб-сервера (SSRF).
* Принудительный просмотр ресурсов веб-приложения (Directory/File/User/Password enumeration, IDOR, MFLAC).
* Раскрытие информации (Information Exposure / InfoLeak).
* Выполнение удаленных/локальных файлов на стороне веб-сервера (RFI/LFI).
* CRLF-инъекция.
* LDAP-инъекция.
* Атака вида HTTP Response Splitting.
* Внедрение веб-шелла.
* Перехват пользовательской сессии (session hijacking).
* Кража личных данных пользователей.
* Выполнение удаленных команд на стороне веб-сервера (OS Command).
* Атаки credential stuffing.

Подсистема должна реализовывать следующие методы обнаружения ботов:

* Анализ заголовков запросов, тела запросов и контекста сессий прикладного трафика на предмет аномалий, характерных для автоматизированных инструментов;
* Сбор отпечатка клиентского веб-браузера с использованием инъекции JavaScript-кода на отдельной странице, демонстрируемой пользователю, и передача данного отпечатка в подсистему для анализа и выявления аномалий в параметрах браузера и устройства пользователя;
* Поиск наличия компонентов, характерных для автоматизированных headless-браузеров в данных отпечатка клиентского веб-браузера;
* Поведенческий анализ одиночных пользователей и групп пользователей на предмет активности, нехарактерной для общей пользовательской базы.

Подсистема должна поддерживать возможность передачи IP-адресов выявленных вредоносных ботов подсистеме antiDDOS атак для их блокировки на распределенном периметре защиты.

Подсистема должна поддерживать возможность работы как для всего веб-приложения, так и для отдельных локаций (URL), содержащихся в нем, включая различные их подмножества.

## Требования к веб-порталу

Исполнителем предоставляются персонифицированные учетные записи для работников Заказчика (не менее 20 шт.) для доступа к веб-порталу сервиса.

Доступ к веб-порталу должен быть организован с применением механизмов шифрования (TLS) и двухфакторной аутентификацией (логин/пароль + СМС/одноразовый код).

Веб-портал должен предоставлять статистику по заблокированным кибератакам и индикаторам атак (ip-адреса источника, паттерны ботов, тип атаки и ее показатели и пр.).

Веб-портал должен поддерживать возможность импорта информации о подозрительных IP-адресах, подлежащих блокировке.

Веб-портал должен поддерживать возможность блокировки подозрительного IP-адреса по HTTP-коду ответа сервера.

# требования к Исполнителю

## Требования к персоналу

В штате исполнителя должен быть следующий персонал:

* Инженеры по настройке компонентов сервиса – не менее 5 человек;
* Выделенный и закрепленный за Заказчиком сервис-менеджер – не менее 1 человека;

Все вышеуказанные специалисты должны иметь профильное образование по направлению информационных технологий или информационной безопасности, а также документы, подтверждающие повышение квалификации в соответствии со специализацией.

Инженеры по настройке должны быть доступны 24 часа в сутки 7 дней в неделю.

Сервис-менеджер должен быть доступен в рабочие дни в период с 8:00 до 18:00 по часовому поясу UTC+7 или UTC+8.

## Требования к опыту выполнения работ

Исполнитель должен иметь опыт выполнения работ по защите веб-приложений от сетевых атак и атак типа «отказ в обслуживании» не менее 3 лет, что подтверждается договорами на выполнение работ/оказание услуг по защите веб-приложений от сетевых атак и атак типа «отказ в обслуживании».