**Техническое задание**

**на** **оказание услуг по обеспечению защиты Интернет-ресурсов АО ИД «Республика Башкортостан» от DDoS-атак**

1. **Термины и определения, используемые в настоящем Техническом задании (далее – ТЗ):**

**Заказчик** – Акционерное общество Издательский дом «Республика Башкортостан».

**Исполнитель** – участник процедуры закупки, признанный победителем процедуры закупки/единственным участником процедуры закупки.

**DDoS-атаки** – разновидности атак на компьютерные системы, сети связи, связанные с большим количеством запросов (в виде IP-пакетов и HTTP-запросов), направленных на веб-сайты и/или IP-адреса оборудования Заказчика. Имеют своей целью и приводят к отказу в работе системы из-за исчерпания ресурсов Заказчика — ресурсов оборудования либо ресурсов каналов связи. Если атака производится одновременно с большого количества IP-адресов, то в этом случае она называется распределённой атакой на отказ в обслуживании (DDoS). Если атака производится одного IP-адреса, то она называется атакой на отказ в обслуживании (DOS). Целью этих атак является создание таких условий, при которых легитимные (правомерные) пользователи Заказчика не могут получить доступ к предоставляемым им ресурсам либо этот доступ затруднён. В последующем в Техническом задании рассматриваются DDoS-атаки (т.к. DoS-атаки являются упрощенным (предельным) случаем DDoS-атак).

**Трафик (сетевой трафик (интернет-трафик))** – объём информации, передаваемой через компьютерную сеть за определённый период времени.

**Эталонная модель взаимодействия открытых систем (ЭМBOC)** – модель, разработанная Международной организацией стандартизации, содержащая семь уровней (слоев) протоколов и предназначенная для коммуникации между устройствами в сети. Уровни ЭМВОС: физический (L1), канальный (L2), сетевой (L3), транспортный (L4), сеансовый (L5), представительский (L6), прикладной (L7).

**HTTP** –протокол передачи данных прикладного уровня ЭМВОС, изначально — в виде гипертекстовых документов в формате языка HTML, в настоящее время используется для передачи произвольных данных.

**HTTPS** – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов TLS или устаревшего SSL.

**WebSocket** — протокол связи поверх транспортного уровня (TCP-соединения), предназначенный для обмена сообщениями между браузером пользователя и веб-сервером в режиме реального времени.

1. **Предмет закупки:** оказание услуг по обеспечению защиты Интернет-ресурсов АО ИД «Республика Башкортостан» от DDoS-атак (далее – услуги).
2. **Назначение услуг:** обеспечение защиты от DDoS-атак на уровне сети и приложений для трафика HTTP(S)/Websocket, поступающего на интернет-сервисы
АО ИД «Республика Башкортостан»в режиме реального времени, посредством обнаружения и фильтрации системой защиты от DDoS-атак.
3. **Сроки оказания услуг:**

4.1. Срок защиты доменов и сервисов Заказчика от DDoS-атак: 01.08.2025 г. по 31.07.2026 г. (включительно).

1. **Место оказания услуг:** услуги оказываютсяпо местонахождению Исполнителяпосредством аппаратно-программного комплекса системы, обеспечивающего защиту от атак (далее – Система), т.е. без установки программного обеспечения, осуществляющего очистку трафика, на серверы Заказчика.
2. **Общие требования к оказанию Услуг**
	1. Исполнитель в рамках предоставляемых услуг обеспечивает:
		1. Проведение стресс-тестирования объектов Заказчика, указанных в пункте 7 настоящего ТЗ, для выявления устойчивости к DDoS-атакам существующей системы защиты Заказчика в сроки, установленные в п. 4.1. настоящего ТЗ.

В течение 1 (Одного) рабочего дня с даты проведения стресс-тестирования Исполнитель передает ответственному представителю Заказчика Отчет о проведении стресс-тестирования (далее – Отчет) в бумажном формате подписанный, уполномоченным лицом со стороны Исполнителя. Отчет составляется в свободной форме и должен содержать дату проведения тестирования, список объектов тестирования, описание используемой методики тестирования, средства тестирования, типы нагрузки и схемы изменения нагрузки, анализ реакции оцениваемых объектов на нагрузку, выводы об эффективности существующей системы защиты Заказчика.

* + 1. Круглосуточную защиту от DDoS-атак от неограниченного числа источников с помощью телекоммуникационного оборудования Исполнителя с возможностью идентификации аномалий (отклонение от повседневной эксплуатации) и сетевых атак и активации противодействия атаке (изменение схемы маршрутизации трафика, с переводом на устройство Очистки Исполнителя, перенаправление легитимного трафика от устройства Очистки Исполнителя, либо после деактивации Заказчиком защиты с web-портала – восстановление обычной оптимальной маршрутизации трафика).
	1. Заказчик не предоставляет Исполнителю оборудование, необходимое для организации обеспечения доступа к сети Интернет, предоставления каналов связи.
	2. Исполнитель должен своими силами обеспечить мониторинг защищаемых ресурсов внешними сервисами, не зависящими от инфраструктуры Исполнителя.
	3. Исполнитель использует собственное телекоммуникационное оборудование для фильтрации трафика.
	4. Система Исполнителя, обеспечивающая защиту от атак, должна иметь техническую возможность подавления атаки, направленной на ресурсы Заказчика, емкостью не менее 5000 Гбит/сек.
	5. Исполнитель должен обеспечить не менее 8 (Восьми) точек очистки трафика по миру, в том числе в регионах:
* Российская Федерация;
* Европа;
* Юго-восточная Европа;
* Центральная Азия;
* Китай;
* Сингапур;
* ОАЭ;
* США.
	1. Услуга защиты от DDoS-атак должна предоставляться посредством изменения DNS-записей интернет-сервисов Заказчика с целью направления всех запросов на оборудование Исполнителя.
	2. Исполнитель предоставляет Заказчику доступ к Системе защиты от DDoS-атак через личный кабинет и через API, с возможностью управления списком и параметрами защищаемых ресурсов, просмотра списка заблокированных IP-адресов, выгрузки списка заблокированных IP-адресов в формате csv и разблокировки выбранных IP-адресов, поиска и выборки информации об атаках, запросов, построения графиков по заданной выборке, с интервалом хранения запросов не меньше 1 (Одной) недели.
	3. Система защиты должна поддерживать необходимые параметры скорости передачи данных в сети Исполнителя для обеспечения гарантированной пропускной способности, установленной в пункте 7 настоящего ТЗ.
	4. Интернет-ресурсы, используемые Исполнителем для предоставления услуг, не должны фигурировать в Едином реестре доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено, размещенном на официальном сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (https://eais.rkn.gov.ru/).
1. **Требования к объему предоставляемой Услуги:**

Исполнитель должен обеспечить защиту следующих объектов Заказчика:

* + - не менее 200 (двести) доменов 2 (второго) уровня и не менее 1000 (тысячи) доменов 3-го (третьего) уровня, зарегистрированных Заказчиком, на уровнях с L3 (сетевого) по L7 (прикладной) ЭМ ВОС;
		- сервисов Заказчика с суммарной средней пропускной способностью не менее 100 (сто) Мбит/с, с возможностью кратковременного повышения на срок до 36 (Тридцати шести) часов в течение 1 (Одного) месячного периода.
1. **Требования к Системе, обеспечивающей защиту от атак:**
	1. Система должна обеспечивать защиту 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 и т.п.);
		* Заполнение полосы пропускания (volumetric flood).
	2. Система должна обеспечивать фильтрацию как HTTP, так и HTTPS трафика.
	3. Система должна обеспечивать фильтрацию с раскрытием приватных ключей SSL. В случае обеспечение защиты без раскрытия приватных ключей SSL Исполнитель должен отражать атаки на уровнях с L3 (сетевого) по L7 (прикладной) ЭМ ВОС путем анализа UDP-потока логов запросов с веб-серверов или балансировщиков Заказчика.
	4. Система должна обеспечивать поддержку протокола HTTP/2 без переключения клиентов с поддержкой протокола HTTP/2 на более старые версии протокола.
	5. При оказании услуг Системой должна осуществляться автоматическая балансировка нагрузки между пулом основных и резервных бэкендов.
	6. Система должна осуществлять кэширование для необходимых расширений файлов.
	7. Система должна обеспечивать возможность беспрепятственной загрузки на ресурсы Заказчика медиафайлов размером до 8ГБ (Восьми гигабайт) с возможностью оперативного увеличения указанного ограничения до 40ГБ (Сорока гигабайт) по запросу Заказчика.
	8. Система должна поддерживать автоматический выпуск, продление и установку бесплатных Let’s Encrypt SSL сертификатов, предоставляемых Заказчиком.
	9. Система должна поддерживать установку и одновременное использование SSL ГОСТ и RSA сертификатов.
	10. Система должна обладать функционалом по обнаружению ботов на основе анализа аномальной активности при работе с сайтами Заказчика.
	11. Система должна обеспечивать сквозную передачу на оборудование Заказчика IP-адресов источников запросов.
	12. Система должна обеспечивать сквозную передачу на оборудование Заказчика JA3-отпечаток в отдельном заголовке.
	13. Система должна обеспечивать возможность прохождения протокола WebSocket с настройкой соответствующих портов, отличных от стандартных портов HTTP(S).
	14. Система должна обеспечивать беспрепятственную работу легальных поисковых ботов и не должна влиять на показания Яндекс- и Google-метрик в части источников перехода, в том числе в режиме фильтрации атаки. При этом должно быть полностью исключено влияние защиты на такие показатели, как число внутренних переходов, число отказов и продолжительность сессии.
	15. Услуга должна вносить минимальную задержку для клиентов при обращении к защищаемым сервисам, в пределах 50мс.
	16. 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, в случае если ресурс, на который направлена атака, не был настроен в Личном кабинете Заказчика. Вышеуказанные Заявки могут быть направлены Исполнителю любым способом, указанным в п. 10.10 Технического задания.
	17. В случае применения Исполнителем автоматизированных проверок доступности ресурсов Заказчика по коду HTTP-ответа с подстановкой промежуточной веб-страницы, должна быть предусмотрена возможность выбора кода HTTP-ответа для отдачи такой страницы.
	18. Система должна обеспечивать возможность как ручной, так и автоматизированной интеллектуальной настройки порогов обнаружения атаки на основе исторических данных индивидуально для разных групп хостов в сети Заказчика.
	19. Для интеграции с системами Заказчика должно быть предусмотрено взаимодействие посредством API. Минимальный набор функционала, обеспечиваемого API, должен включать:
		1. Чтение списка и настроек защищаемых ресурсов, включая, как минимум следующее: список и веса бэкендов, настройки SSL, черные и белые списки защиты;
		2. Добавление/удаление/изменение настроек защищаемых ресурсов, включая как минимум: список и веса основных и резервных бекендов, настройки SSL, черные и белые списки защиты;
		3. Выгрузка информации об атаках за произвольный период времени, включая как минимум следующие данные: мощность, протокол, тип, цель, время начала и окончания;
		4. Получение информации о заблокированных IP-адресах клиентов для выбранного домена, возможность выгрузки списка заблокированных IP-адресов в формате csv, а также разблокировка выбранных IP-адресов и просмотр истории блокировок за период не менее 1 месяца с указанием их причины.
	20. Система должна незамедлительно обеспечивать отправку E-Mail-уведомлений, Telegram сообщений, Webhook о начавшейся и прекратившейся атаке и иметь возможность самостоятельной настройки уведомлений об атаках в личном кабинете.
2. **Требования к Личному кабинету:**
	1. В течение 1 (Одного) рабочего дня с даты начала оказания услуг Исполнитель должен предоставить Заказчику личный кабинет (ЛК) для управления услугой и API для автоматизированного взаимодействия с Системой защиты со следующими базовыми возможностями:
		1. Выбор режима защиты (в том числе ее отключения) из минимального набора вариантов, указанных в пункте 9.2 настоящего ТЗ.
		2. Управление порогами (лимитами) срабатывания защиты согласно пункту 9.3 настоящего ТЗ.
		3. Управление адресами бэкендов Заказчика согласно пункту 9.4 настоящего ТЗ.
		4. Настройка сертификатов, необходимых для обеспечения шифрования трафика между пользователем и сайтом, и приватных ключей.
		5. Настройка черных и белых списков источников, в том числе с использованием информации о географической принадлежности адресов источников.
		6. Управление исключениями по типам файлов, по областям web-приложений (локациям) Заказчика.
	2. Перечень режимов защиты должен содержать следующий минимальный набор:
		1. Защита полностью выключена;
		2. Набор режимов с принудительным HTTP-редиректом, JS-валидацией, применением CAPTCHA для всех входящих запросов.
		3. Набор режимов с автоматическим включением HTTP-редиректа, JS-валидации, применения CAPTCHA в зависимости от «рейтинга» источника запросов, а также их географической принадлежности.
	3. Личный кабинет должен предоставлять следующие возможности управления порогами (лимитами) для обнаружения атак:
		1. Настройка порогов по количеству запросов в секунду.
		2. Настройка порогов по процентному соотношению запросов, завершенных с ошибками на подзащитном сервисе.
		3. Настройка порогов по скорости увеличения входящего трафика.
		4. Настройка индивидуальных порогов для блокировки IP-адресов по количеству заблокированных запросов и запросов в определенные локации.
		5. Настройка минимальной продолжительности атаки, т.е. минимального времени, в течение которого защита переходит из активного режима в режим наблюдения.
		6. Настройка условий завершения (обратного перехода из режима активной фильтрации в режим обнаружения).
	4. Личный кабинет должен предоставлять следующие возможности для управления бэкендами Заказчика:
		1. Добавление/удаление адресов бэкенд-серверов.
		2. Настройка весов для автоматической балансировки.
		3. Настройка типа бэкенда на балансировку в обычном режиме или использование его в качестве резервного, активизируемого только при недоступности основных бэкендов.
	5. Личный кабинет должен предоставлять следующие возможности для управления кэшированием:
		1. Включение/выключение кэширования;
		2. Настройка расширений файлов, которые будут попадать в кэш;
		3. Настройка времени (в минутах), после которого считается, что файл в кэше устарел;
		4. Принудительный сброс кэша.
	6. В личном кабинете должны присутствовать следующие дополнительные возможности:
		1. Возможность раздельного управления указанными настройками защиты для каждого защищаемого домена/поддомена.
		2. Отображение графиков запросов к защищаемому ресурсу с возможностью выбора типа отображаемых запросов: общее количество запросов, разрешенные запросы, запросы из кэша, в белом списке, всего заблокированных запросов, ошибки.
		3. Отображение графиков объема трафика с возможностью просмотра информации за заранее определенный диапазон.
		4. Отображение графиков времени ответа и кодов ответа с возможностью просмотра информации за заранее определенный диапазон с выбираемым шагом.
		5. Отображение графиков кодов ответа с возможностью просмотра информации за заранее определенный диапазон.
		6. Отображение тепловой карты запросов.
		7. Отображение информации о городах и странах, откуда были запросы, в виде списка и в виде круговой (секторной) диаграммы.
		8. Отображение списка и круговой (секторной) диаграммы основной локации запросов с отображением процента.
		9. Возможность масштабирования графиков со следующим минимальным набором интервалов отображения:
			1. Несколько интервалов в течение суток (от нескольких минут до нескольких часов);
			2. Сутки;
			3. Неделя;
			4. Месяц.
		10. Возможность просмотра фильтрации и скачивания журнала запросов.
		11. Возможность просмотра истории атак для определенного домена/поддомена с выбором конкретных дат и формированием отчета в формате PDF 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 RPS/BPS 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.
		12. Возможность просмотра заблокированных IP адресов и истории блокировок за определенный период с указанием времени и причины блокировки, а также разблокировки выбранных адресов.
		13. Возможность самостоятельного добавления Заказчиком учетных записей с настройками прав управления под каждый аккаунт отдельно.
		14. Возможность самостоятельной смены имени домена/поддомена без дополнительных плат или обращений;
		15. Возможность ручной настройки редиректов с одного домена на другой.
		16. Возможность добавления Websocket, с использованием портов, отличных от TCP80 и TCP443.
		17. Возможность добавления e-mail адресов, чат-бота в Telegram, Webhook URL для получения рассылок об атаках.
		18. Возможность включения проактивной защиты для проверки новых клиентов по методам location, keepalive соединения, использованию User Agent и лимитам RPS. При нарушениях, запросы с клиентского IP-адреса должны фильтроваться без переключения защиты всего сайта.
		19. Возможность создания фильтров по локациям с возможностью блокировки нарушителей при превышении числа запросов с заданным методом в заданную локацию за заданный промежуток времени.
		20. Возможность создания цепочек правил обработки HTTP-запросов, позволяющие разрешить, блокировать запросы, либо обрабатывать их в другой цепочке, на основании соответствия или не соответствия набору параметров с указанием числа запросов, времени анализа, методов, локаций и заголовков HTTP.
		21. Возможность создания списков JA3 отпечатков, позволяющих разрешить, блокировать запросы, либо обрабатывать их с принудительным HTTP-редиректом, JS-валидацией, применением CAPTCHA, в том числе с привязкой к IP-адресам источников.
3. **Порядок оказания услуг и взаимодействия с Заказчиком:**
	1. Все необходимые данные для оказания услуг, в том числе сведения о стандартных нагрузках на трафик, о пиковой нагрузке на трафик и т.д., Заказчик предоставляет Исполнителю в течение 2 (Двух) рабочих дней с даты подписания Договора сторонами.
	2. При обнаружении атаки Система должна незамедлительно блокировать атаку (время перехода защиты в активный режим должно быть в пределах от 1(Одной) до 120 (ста двадцати) секунд в зависимости от типа атаки) и уведомлять Заказчика об обнаружении атаки, посредством электронной почты ответственного представителя Заказчика и уведомления в личном кабинете.
	3. При окончании атаки Исполнитель включает штатный режим работы системы защиты и незамедлительно уведомляет Заказчика об окончании атаки посредством электронной почты ответственного представителя Заказчика и уведомления в личном кабинете.
	4. При изменении режима работы Системы защиты (например, при обнаружении подозрительной активности) Исполнитель незамедлительно уведомляет Заказчика посредством электронной почты.
	5. В целях разбора инцидентов Исполнитель предоставляет Заказчику доступ к журналам Системы защиты с временем хранения не менее 72 (Семидесяти двух) часов. Журналы системы должны содержать следующий минимальный набор полей: имя домена, на который был отправлен запрос; адрес клиента, отправившего запрос; статус и причина фильтрации запроса; заголовки User-Agent и Referer; адрес бэкенда для проксирования запроса, код ответа бэкенда.
	6. При оказании услуг должна быть предусмотрена возможность быстрого отключения защиты для разбора ситуации, а также быстрого включения защиты Заказчиком для каждого из защищаемых ресурсов самостоятельно посредством Личного кабинета в случае обнаружении неблагоприятного влияния на доступность сервисов Заказчика для пользователей.
	7. При необходимости проведения профилактических работ Исполнитель уведомляет Заказчика не позднее 2 (Двух) календарных дней до начала проведения таких работ.
	8. Недоступность услуги в связи с профилактическими (плановыми) работами не должна превышать 10 (Десяти) часов в календарный год. В момент выполнения профилактических работ не должны быть нарушены требования к качеству предоставления услуги.
	9. Исполнитель должен обеспечить круглосуточное 24 часа в сутки 7 дней в неделю сопровождение Заказчика с временем реакции на запрос не более 30 (Тридцати) минут в течение всего периода оказания Услуг посредством:
* системы ввода заявок (тикетов);
* электронной почты;
* телефонной связи.
	1. Исполнитель должен иметь возможность выделения Заказчику персонального менеджера в течение 3 (Трех) рабочих дней с даты получения соответствующего запроса от Заказчика.
	2. При осуществлении сопровождения и взаимодействия с Заказчиком Исполнитель должен оперативно по согласованию с Заказчиком осуществлять решение проблем с защитой, с выявленными атаками, с доступностью сервисов Заказчика.
	3. Исполнитель уведомляет Заказчика о проведении любых плановых ремонтных работ, включая профилактические работы, которые могут вызвать перерывы в работе услуги, минимум за сутки до начала проведения таких работ.
	4. Язык предоставления технической поддержки – русский.
	5. Техническая поддержка осуществляется Исполнителем своими силами и включена в цену оказания Услуг.
1. **Требования к качеству предоставляемых услуг:**
	1. Качество оказываемых услуг должно соответствовать условиям настоящего Технического задания и Договора, а при отсутствии в Договоре требований к качеству или при их недостаточности – требованиям, обычно предъявляемым к качеству услуг такого рода.
	2. Исполнитель гарантирует доступность интернет-сервисов Заказчика в течение всего срока оказания услуги.
	3. Доступность Услуги определяется как процент времени в течение отчетного периода, когда Услуга была доступна, без учета времени перерывов в оказании Услуги для планового обслуживания средств связи и оборудования.
	4. Доступность Услуги обеспечивается на уровне не менее 99,5% (Девяносто девять целых пять десятых процента) от суммарного времени за календарный месяц в часах.
	5. Если федеральными законами или в установленном в соответствии с ними порядке, в частности стандартами, предусмотрены обязательные требования к оказываемым услугам, Исполнитель должен оказать услугу, соответствующую этим требованиям.
	6. Если в процессе оказания услуг Исполнитель допустил отступления от условий Договора, ухудшившие качество оказываемых услуг, Исполнитель в течение 2 (Двух) календарных дней с даты обнаружения Заказчиком недостатков в услугах обязан безвозмездно устранить их за свой счет.
2. **Требования к безопасности оказываемых услуг:**
	1. Оказываемые услуги должны соответствовать требованиям качества, безопасности жизни и здоровья, а также иным требованиям сертификации, безопасности (нормам и правилам, государственным стандартам и т.п.), лицензирования, установленным действующим законодательством Российской Федерации.
	2. При оказании услуг Исполнитель несет ответственность за причинение какого-либо вреда здоровью, жизни или имуществу Заказчика, его представителям и иным лицам, задействованным или каким-либо образом, участвующим в мероприятиях, оказываемых Исполнителем.
	3. Во время подготовки и оказания услуг Заказчик не несет никакой ответственности за причинение какого-либо вреда здоровью, жизни или имуществу третьих лиц, а равно иным нематериальным благам гражданина, вызванных действиями или бездействиями Исполнителя, его работников или представителей.