ТОО «Интернет-компания PS»

Условия использования услуги

Защита от DDoS-атак: Pro

Версия от 15.12.2025

Целью данного документа является описание параметров предоставления услуги ТОО «Интернет-компания PS» «Защита от DDoS-атак: Pro» (далее — Услуга), для обеспечения согласованного уровня качества оказания услуги.

Настоящий документ Соглашение об уровне обслуживания или SLA («Соглашение»):

- описывает Услугу;
- устанавливает порядок предоставления Заказчику Услуги;
- является неотъемлемой частью Публичного договора, опубликованного по адресу: https://www.ps.kz/agreements/offer («Оферта»).

Предоставляемая Услуга в соответствии с НК РК 03–2019 «Общий классификатор видов экономической деятельности», введенном в действие Министерством индустрии и инфраструктурного развития Республики Казахстан с 1 января 2020 года, включена в подкласс 63.11.1.

Термины, которые используются, но не определены в Соглашениях, имеют значение, присвоенное им в Оферте и в разделе «Помощь» на Сайте Исполнителя: https://www.ps.kz/faq. Соглашение содержит пункты с активными гиперссылками на веб-страницы с более подробной информацией, которые являются неотъемлемой частью Соглашения.

Исполнитель вправе без какого-либо специального уведомления вносить изменения в Соглашение, в связи с чем, Заказчик обязуется регулярно отслеживать эти изменения. Действующая редакция Соглашения размещена по адресу: https://www.ps.kz/agreements/antiddos-pro-sla. Использование Заказчиком Услуги после изменения Соглашения является подтверждением его согласия с их новой редакцией.

Услуга оказывается: круглосуточно, без выходных.

1. Общие положения

1.1. Услуга предусматривает предоставление защиты каналов связи, сетевого оборудования, веб-сайтов, приложений от DDoS-атак, а также противодействие разным типам и методам DDoS-атак.

1.2. Термины и определения:

- **Анализ** — анализ данных о Трафике Защищаемого ресурса с целью изучения и выявления в нем последовательностей и закономерностей, оценки его содержимого и адресов источников/получателей;
- **Атака** — распределенная атака на вычислительную систему, выполняемая с целью довести вычислительную систему до отказа, то есть создание повышенной нагрузки на вычислительную систему или ее компоненты, в результате которой легитимные (правомерные) пользователи Системы не могут получить доступ к предоставляемым Системой ресурсам, либо этот доступ затруднен;
- **Доменное имя** — символьное (буквенно-цифровое) обозначение, сформированное в соответствии с правилами адресации Интернета, соответствующее определенному сетевому адресу и предназначенное для поименованного обращения к объекту Интернета;
- **Защита от DDoS-атак на уровне L3** — фильтрация и блокировка аномального трафика на сетевом уровне;
- **Защита от DDoS-атак на уровне L4** — анализ транспортного трафика (TCP/UDP), фильтрация и блокировка подозрительных соединений;
- **Защита от DDoS атак на уровне L7** — анализ и фильтрация прикладного трафика, включая HTTP- и DNS-атаки, а также иные виды прикладных атак, вызывающих отказ в обслуживании веб-сервисов;
- **Защищаемый ресурс** — сетевой сервис Заказчика, определяемый IP-адресом, группой IP-адресов, IP-адресом и доменным именем или группой доменов;
- **Легитимный трафик** — трафик, передаваемый в сторону Защищаемого ресурса, который получен от пользователей, предполагающих использовать Защищаемый ресурс по его назначению;
- **Система** — программное обеспечение, предназначенное для обнаружения Атак, Фильтрации Трафика и доставки очищенного Трафика до Защищаемого ресурса;
- **Панель управления Защищаемых ресурсов** — персонифицированный веб-интерфейс, предоставляемый Заказчику в рамках оказания Услуги, позволяющий получать информацию о состоянии Защищаемых ресурсов и управлять политиками фильтрации Трафика Защищаемых ресурсов;
- **Параметры Анализа** — индивидуальные граничные значения параметров Трафика Защищаемого ресурса (значения пиковой и средней нагрузки, распределения Трафика по источнику и времени суток и др.), используемые при анализе Трафика Защищаемого ресурса;
- **Трафик** — сетевые пакеты, передаваемые по каналам передачи данных;
- **Фильтрация** — очистка Трафика, не являющегося Легитимным по отношению к Защищаемому ресурсу;

- **Центр очистки** — компонент Системы, размещаемый у Исполнителя, который осуществляет Анализ и Фильтрацию проходящего через него Трафика Защищаемого ресурса, а также сбор, анализ и хранение статистической информации о Трафике Защищаемого ресурса;
- **GEO-фильтрация** — очистка Трафика, не входящего в списки разрешенных или запрещенных стран для каждого профиля фильтрации, по определенным географическим зонам;
- **IP-адрес** — уникальный числовой идентификатор устройства в Интернете или компьютерной сети, работающей по протоколу IP.

2. Состав Услуги

2.1. Услуга включает в себя:

- анализ трафика;
- защиту от DDoS-атак на уровне L3-L4, L7 (по выбору Заказчика);
- фильтрацию Трафика Защищаемого ресурса (блокировку нелегитимного, вредоносного трафика);
- техническую поддержку в рамках оказания Услуги;
- уведомление Заказчика и обработку его запросов по вопросам оказания Услуги;
- предоставление доступа к Панели управления Защищаемых ресурсов;
- настройку Списков разрешенных, запрещенных IP-адресов;
- предоставление информации о Трафике Защищаемых ресурсов и зафиксированных атаках;
- уведомление Заказчика об Атаках путём отправки уведомлений на электронные адреса Уполномоченных представителей Заказчика.

2.3. Заказчику при первичном подключении Услуги предоставляется Тестовый период оказания Услуги, в рамках которого Система, обеспечивая защиту ресурсов Заказчика, анализирует трафик Заказчика. По истечении Тестового периода Исполнитель направляет уведомление Заказчику об объеме Трафика Защищаемых ресурсов Заказчика и рекомендациями по тарифному плану и дальнейшей защите ресурсов.

2.4. В состав Услуги не входит:

- Реагирование на обращения, не связанные с защитой от Атак, в том числе вопросы, связанные с временем отклика Защищаемого ресурса или его доступностью из сети Интернет;
- реагирование на обращения, касающиеся работы ресурсов, не входящих в состав Защищаемых ресурсов;
- реагирование на обращения, связанные с безопасностью и сохранностью приватных ключей SSL/TLS-сертификатов Заказчика;
- реагирование на обращения, касающиеся работы любых программно-аппаратных комплексов, не входящих в состав Системы;
- решение Инцидентов, условия возникновения которых не могут быть воспроизведены ни Заказчиком, ни Исполнителем;
- решение Инцидентов, являющихся следствием превышения Легитимным трафиком Заказчика выделенной полосы пропускания;
- проведение других работ, не связанных непосредственно с работой Системы и ее компонентов.

3. Порядок оказания Услуги

3.1. Заказчик для получения Услуги в Консоли управления Заказчика (https://console.ps.kz/) или на сайте (https://www.ps.kz/):

- выбирает Услугу;
- выбирает Тарифный план;
- указывает ресурсы (IP-адрес(-а), домены, подсети), который(-ые) подлежит(-ат) защите;
- отправляет запрос на заказ Услуги;
- взаимодействует с Исполнителем по формированию состава, объема Услуги;
- использует Услугу в рамках бесплатного Тестового периода (14 календарных дней);
- по истечении Тестового периода взаимодействует с Исполнителем по оформлению окончательного заказа Услуги;
- формирует окончательную Заявку на Услугу;
- оплачивает счет на Услугу.

3.2. Оказание Услуги начинается после оплаты Заказчиком автоматически сформированного счета по завершении Тестового периода.

3.3. В рамках подключения Услуги Исполнитель предоставляет Заказчику доступ к Панели управления Защищаемых Ресурсов, через которую можно:

- получать информацию о Трафике Защищаемых ресурсов:
- анализировать статистику по Трафику Защищаемых ресурсов;
- анализировать состояние Трафика Защищаемых ресурсов во время Атак;
- настраивать механизмы автоматического оповещения;
- редактировать Список разрешенных IP-адресов и Список запрещенных IP-адресов, влияющих на параметры Фильтрации Трафика Защищаемых ресурсов;
- заказывать отчет об Атаке;
- настраивать автоматическое уведомление по событиям Системы.

4. Оплата Услуги

4.1. Стоимость Услуги определяется согласно тарифному плану Исполнителя, исходя из объема трафика Защищаемых ресурсов Заказчика, с использованием метода 91-го перцентиля.

4.2. Заказчику предоставляется Тестовый бесплатный период продолжительностью 14 календарных дней при первичном подключении Услуги, по итогам которого формируется окончательная стоимость Услуги для Заказчика.

4.3. Заказчик осуществляет предоплату очередного периода предоставления Услуги до его начала, в ином случае предоставление Услуги приостанавливается (отключается доступ к Услуге).

4.4. В случае отказа Заказчика от Услуги до истечения оплаченного периода, Услуга остается подключенной до конца оплаченного периода, и будет отключена по его завершению. Возврат Заказчику денежных средств в этом случае не производится.

5. Уровень оказания Услуги

5.1. Гарантированная доступность Услуги определяется в соответствии с выбранным Заказчиком тарифным планом.

Описание параметров тарифных планов Услуги

Тарифные планы	**Standard SLA**	**Business SLA**	**Gold SLA**	**Platinum SLA**
Общий объем Легитимного трафика под защитой, Мбит/с	Индивидуально	Индивидуально	Индивидуально	Индивидуально
Защита L3-L4	Да	Да	Да	Да
Защита L7	Да	Да	Да	Да
Гарантированная доступность ресурса в месяц, %	98,5%	98,5%	99,2%	99,5%
Фильтрация атак	До 5 Гбит/с	До 7,5 Гбит/с	До 10 Гбит/с	До 20 Гбит/с
Максимальное время атаки / Длительность атак, сутки	До 6 суток/мес	До 12 суток/мес	Без лимита	Без лимита
Количество подключаемых доменов на IP-адрес	До 5	До 5	До 10	Без лимита

Количество подключаемых IP-адресов/подсетей	До 5	До 5	До 10	Без лимита
Количество правил в списках, штук на IP	До 10	До 10	До 50	Без лимита
GEO-фильтрация	Да	Да	Да	Да

Если объем проходящего через Центры очистки Легитимного трафика Заказчика превысит выделенную полосу пропускания, доставка Трафика, превышающего объем выделенной полосы пропускания, не гарантируется.

Если емкость Атаки превысит указанные лимиты, Система может ввести ограничения к Трафику (полностью блокирует или ограничивает), перенаправленному Заказчиком на Центры очистки.

Исполнитель гарантирует, что в случае прохождения трафика через Центры очистки при отсутствии DDoS-атак, потери легитимных пакетов не могут превышать 0,5%.

Исполнитель закрепляет за Заказчиком полосу фильтрации Легитимного трафика, ограниченную на входе в Центр очистки, в объеме, не более предусмотренного Тарифным планом.

5.2. Гарантированная доступность Услуги определяется без учета времени простоя, вызванного проведением плановых работ. Исполнитель имеет право прерывать функционирование Системы для проведения технологических работ по обслуживанию оборудования и каналов связи, а также для проведения экстренного обслуживания. Такие перерывы классифицируются как функционирование Системы в штатном режиме.

Виды работ:

- **плановые работы** — организационные и технические мероприятия Исполнителя по мониторингу, настройке и обновлению IT-инфраструктуры, с регламентированными сроками и порядком проведения;
- **внеплановые работы** — нерегламентированные (экстренные) организационные и технические мероприятия Исполнителя с целью устранения сбоев и неполадок в IT-инфраструктуре.

Исполнитель уведомляет Уполномоченных представителей Заказчика о перерывах в функционировании Системы в соответствии с установленными параметрами:

Работы	**Уведомления**	**Время проведения**	**Продолжительность**
Плановые	не менее, чем за 24 часа до начала работ	в часы наименьшей нагрузки (с 00:30 до 06:30 GMT+5)	не более 24 часов в календарный год
Внеплановые	по факту перед началом работ	в любое время суток, по необходимости	не более 12 часов в календарный год

5.3. Во всех случаях Исполнитель будет стремиться к максимально быстрой реакции на обращения Заказчика. При проведении работ по обращениям Исполнитель руководствуется следующей системой приоритетов:

Приоритет	**Критичность**	**Время реагирования (часы)**	**Время разрешения (часы)**	**Период обслуживания**
Высокий	Периодические прерывания в предоставлении основных услуг, значительное ухудшение показателей их качества, отказ элементов IT-инфраструктуры	1	8	круглосуточно, 7 дней в неделю

Средний	Неполадки, не приводящие к полному прерыванию предоставления основных услуг, но влияющие на показатели их качества.	2	24	круглосуточно, 7 дней в неделю
Низкий	Неполадки, обращения, связанные с предоставлением технической и иной информации	4	72	в будние дни с 10:00 до 19:00

Время реагирования — период времени от фиксации обращения Заказчика (время создания обращения в Консоли управления или Тикет-системе), до момента, когда Исполнитель обязан начать процедуры и действия, необходимые для восстановления функционирования и/или разрешения проблем.

Время разрешения — время, за которое Исполнитель должен предоставить временное или постоянное решение проблемы, необходимое для восстановления нормального функционирования (начиная от времени создания обращения).

Время разрешения указывается без учета времени, затраченного на взаимодействие с Заказчиком в части уточнения, получения информации в обращении, ожидания ответа или действий Заказчика.

В ходе решения обращений Заказчика требуется предоставление Заказчиком дополнительной информации или непосредственное его участие. Заявленное время решения обращения обеспечивается только при условии выполнения Заказчиком своих обязательств по участию в решении/рассмотрении обстоятельств Обращения.

5.4. Обращение Заказчика автоматически регистрируется средствами Тикет-системы: фиксируется время поступления и присваивается номер.

Уведомление о регистрации обращения Заказчика отправляется на электронную почту Уполномоченного представителя Заказчика. Список Уполномоченных представителей Заказчика и их адресов электронной почты должен соответствовать списку пользователей Панели управления Защищаемых ресурсов и поддерживаться Заказчиком в актуальном состоянии. В случае использования Заказчиком адресов электронной почты, не зарегистрированных в Консоли управления Заказчика, Панели управления Защищаемых ресурсов, Исполнитель оставляет за собой право не обрабатывать поступившие обращения.

По номеру регистрации обращения Заказчику доступна в Консоли управления функция отслеживания статуса своего обращения.

5.5. Работоспособность сервисов в рамках Услуги обеспечивается следующими способами:

- путем консультирования по телефону Заказчика;
- с помощью функционала Консоли управления через Тикет-систему.

5.6. Техническая поддержка осуществляется круглосуточно путем обращения Заказчика через Консоль управления и обработкой Исполнителем обращения в Тикет-системе.

5.7. Консультационная, информационная поддержка обеспечивается путем обращения Заказчика по телефону, через Консоль управления, и обработкой Исполнителем обращения в Тикет-системе, в соответствии с контактами Заказчика и временными рамками, предусмотренными https://www.ps.kz/company/contacts.

6. Особые условия

6.1. Заказчик обязан:

6.1.1. предупредить Исполнителя об имеющейся, на момент оформления заказа Услуги, атаке на предоставляемый к защите ресурс;

6.1.2. предоставлять Исполнителю корректные данные ресурсов, подлежащих защите.

6.2. При использовании Услуги для осуществления деятельности, подлежащей в соответствии с законодательством РК сертификации и лицензированию, Заказчик должен иметь соответствующие лицензии, сертификаты и иные разрешительные документы.

6.3. Исполнитель гарантирует:

6.3.1. оказание Услуги в соответствии с ее техническими характеристиками и параметрами, установленными в настоящем Соглашении и Заявке Заказчика;

6.3.2. работу Системы в штатном режиме, включая мониторинг и автоматическую фильтрацию Трафика в соответствии с установленными профилями защиты;

6.3.3. соблюдение конфиденциальности информации, передаваемой в рамках оказания Услуги;

6.3.4. что Система в процессе Фильтрации Трафика Защищаемых ресурсов, перенаправленного на Центры Очистки:

1. будет пропускать Трафик между Защищаемыми ресурсами и IP-адресами, помещенными Заказчиком в Списки разрешенных IP-адресов;
2. будет блокировать Трафик между Защищаемыми ресурсами и IP-адресами, помещенными Заказчиком в Списки запрещенных IP-адресов;
3. обеспечит фильтрацию Трафика Защищаемых ресурсов в 98% случаев на основе следующего алгоритма:
    - если IP-адрес является вредоносным, то вероятность его классификации в качестве нелегитимного равна указанному проценту по прошествии 5 минут после того, как IP-адрес начал атаковать Защищаемый ресурс;
    - если IP-адрес является адресом легитимного пользователя, то вероятность его классификации в качестве легитимного равна указанному проценту по прошествии 5 минут после того, как IP-адрес начал обращаться к Защищаемому ресурсу.
4. обеспечит фильтрацию Трафика в 98% случаев при условии, что Общий объем Легитимного трафика под защитой не превышает установленные лимиты, предусмотренные в пункте 5.1 настоящего Соглашения.

6.4. Исполнитель не гарантирует:

6.4.1. обеспечение эффективной защиты ресурса, предоставленного к защите в процессе осуществления атаки на него, так как осуществление настройки модели защиты предусмотрено только в период стандартной работы сервиса Заказчика;

6.4.2. полное исключение рисков кратковременной потери доступности сервиса Заказчика по причине ранее неизвестных атак.

6.5. Информация о Трафике Защищаемых ресурсов хранится у Исполнителя в течение 2 календарных месяцев с момента ее возникновения и доступна Уполномоченным представителям Заказчика через Панель управления Защищаемых ресурсов. Информация об Атаках хранится в течение срока оказания Услуги и доступна Уполномоченным представителям Заказчика в форме отчетов, формируемых по заявке в Панели управления Защищаемых ресурсов.

6.6. Инциденты, связанные с работоспособностью Системы или с взаимодействием компонентов Системы с оборудованием Исполнителя, требуют моделирования условий возникновения Инцидента с целью его локализации и поиска причин.

В ходе взаимодействия с Исполнителем по решению Инцидента Заказчик обязан предоставить всю запрашиваемую Исполнителем информацию, необходимую для решения Инцидента, которой он располагает, и оказывать содействие в получении Исполнителем информации, необходимой для решения Инцидента.

В случае возникновения Инцидента с компонентами, размещенными на территории Заказчика, Заказчик обязан предоставить Исполнителю доступ к указанным компонентам по запросу Исполнителя, если все другие средства диагностики оказались неэффективными.

6.7. Метрикой доступности Защищаемых ресурсов является процент успешных проверок системы мониторинга. Если Трафик всех Защищаемых ресурсов Клиента не проходит через Систему, то показателем доступности Системы являются данные, отображаемые в Панели управления Защищаемых ресурсов. В показателе доступности Системы и Защищаемых ресурсов учитываются только проблемы, связанные с качеством Фильтрации DDoS-атак, и проблемы в работе Системы. При расчете выполнения настоящего Соглашения не учитываются:

6.7.1. Инциденты, которые привели к недоступности Защищаемых ресурсов;

6.7.2. сбои в работе Системы, не являющиеся Инцидентом, которые явились следствием:

- изменений Заказчиком настроек, прямо или косвенно влияющих на работоспособность находящихся в зоны ответственности Исполнителя компонентов Системы и произведенных без согласования с Исполнителем;
- планового технического обслуживания Системы, заранее согласованного с Заказчиком или связанного с модернизацией Системы по запросу Заказчика;
- невыполнения Заказчиком своих обязательств по участию в решении Инцидентов в соответствии с условиями, определенными в пункте 6.6. настоящего Соглашения;

- обстоятельств, препятствующих работе Системы, возникших по вине Заказчика;
- вмешательства Заказчика или третьей стороны в работу оборудования или программного обеспечения, находящегося на территории Заказчика, обеспечивающего работу Системы без согласования с Исполнителем;
- отказа оборудования Интернет-провайдера, услугами которого пользуется Заказчик;
- блокировки каналов поставщиком телекоммуникационных услуг связи на участке сетевого маршрута между Заказчиком и Центром очистки;
- перерыва в работоспособности Системы, причиной которого являются обстоятельства непреодолимой силы, предусмотренные применимым законодательством.

7. Условия компенсации

7.1. Вопросы недоступности Услуги по вине Исполнителя на основании соответствующего обращения Заказчика в Тикет-системе разрешаются в индивидуальном порядке путем переговоров сторон.

7.2. Если Исполнитель располагает собственными данными о времени простоя, он вправе использовать эти данные. Разногласия о времени простоя разрешаются путем переговоров сторон.

7.3. Компенсируется каждый час простоя в размере 1% от суммы ежемесячного платежа Заказчика за Услугу:

- **стоимость Услуги в месяц / 100 × количество часов**

при этом общая сумма компенсации не может превышать 100% стоимости Услуги в месяц. Компенсация начисляется на баланс аккаунта в Консоли управления Заказчика в виде бонусов.

Компенсация может выражаться в выплате денежных средств Заказчику только в случае его отказа от дальнейшего использования Услуги и проведения сверки взаиморасчетов.

7.4. Не подлежит компенсации простой:

- связанный с обстоятельствами непреодолимой силы и иными обстоятельствами, произошедшими не по вине Исполнителя;
- вызванный действиями (бездействием) Заказчика;
- произошедший по причине отказа ПО, разработанного третьими лицами или являющегося собственностью (либо арендуемого) Заказчиком;
- вызванный сбоями системы сетевых служб, находящимися за пределами прямого контроля Исполнителя, а также задержками распространения информации об обновлении DNS-записей;
- связанный с проведением плановых работ, согласно п. 5.2. настоящего Соглашения.