ОБЩИЕ УСЛОВИЯ ОКАЗАНИЯ УСЛУГИ
«ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ»

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1.	Сетевая Атака	Действие (последовательность Вредоносных запросов), осуществляемое по каналам связи, целью которого является захват управления (повышение прав) над целевой удалённой вычислительной системой, несанкционированная модификация содержания удалённых ресурсов, распространение вредоносного программного кода, доведения вычислительной системы до отказа в обслуживании, либо иная другая форма дестабилизации работы целевой удалённой вычислительной системы.
1.2.	Вредоносный запрос (Вредоносный Программный Код)	Специально сформированный запрос (набор данных), передаваемый по каналам связи и нацеленный на использование существующих Уязвимостей веб-приложения. Вредоносный запрос предназначен для получения несанкционированного доступа к вычислительным ресурсам целевой системы или к информации, хранимой на ней, с целью несанкционированного использования ресурсов системы или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу системы, и/или владельцу компьютерной сети, путем копирования, искажения, удаления или подмены информации, а также повышения привилегий доступа к целевой системе.
1.3.	Уязвимость веб-приложения (Уязвимость)	Недостаток веб-приложения, используя который, можно намеренно нарушить её целостность и вызвать неправильную работу. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, вирусов и других Вредоносных программ, скриптовых и SQL-инъекций. Некоторые Уязвимости известны только теоретически, другие же активно используются и имеют известные эксплойты.
1.4.	Публичный IP-адрес (внешний)	Уникальный сетевой адрес в публичной сети Интернет, построенной на основе протокола IP (межсетевой протокол передачи данных).
1.5.	Трафик	Объём информации, передаваемой по каналам связи за определенный период времени.
1.6.	Легитимный трафик	Трафик в направлении вычислительной системы, который направляется от пользователей, предполагающих использовать вычислительную систему по ее назначению (например, Трафик от пользователей системы интернет-банкинга или

		посетителей информационного сайта) и не содержащий Вредоносного Программного Кода.
1.7.	Паразитный Трафик (Нелегитимный Трафик)	Трафик, не соответствующий выявленным статистическим критериям Легитимного трафика или содержащий Вредоносный запрос или Вредоносный Программный Код.
1.8.	Ресурс	Веб-приложение, располагающееся в сети Интернет с использованием доменного имени, и требующее особого внимания при защите его от Сетевых атак. Ресурс описывается набором параметров: IP-адрес (обязательный параметр), доменное имя, тип сетевого протокола, тип клиентского сервиса.
1.9.	Фильтрация Трафика (Очистка Трафика)	Удаление (блокирование) Паразитного Трафика или Вредоносного Программного Кода из входящего на Ресурс Трафика с целью сокращения его влияния на Ресурсы Клиента.
1.10.	Web Application Firewall (Комплекс WAF)	Межсетевой экран для защиты веб-приложений (Ресурсов) представляет собой программно-аппаратный комплекс, состоящий из программного обеспечения «Валарм» (WALLARM), произведенного компанией ООО «ОНСЕК ИНК.», и Облачной платформы, образуя, таким образом, программно-аппаратный комплекс по Фильтрации Трафика. Основной задачей Комплекса WAF является защита Ресурсов Клиента от Сетевых атак путем проверки XML/SOAP семантики потокового Трафика, а также проверки HTTP Трафика с целью обнаружения и блокировки Сетевых атак на Ресурсы Клиента.
1.11.	Технический Представитель Клиента	квалифицированный технический сотрудник компании Клиента (список лиц представлен в п.1.1 Заказа, не более 3 человек), уполномоченный Клиентом выполнять следующие действия от имени Клиента: • инициировать Обращения в адрес службы технической поддержки Оператора; • реагировать на запросы со стороны Оператора и принимать необходимые решения в экстренных ситуациях.
1.12.	Договор	Договор на оказание услуг на базе облачной платформы (Оферта о заключении договора на оказание услуг на базе облачной платформы)
1.13.	Уровень доступности Услуги	Уровень доступности Услуги определяется в «Соглашении об уровне обслуживания для Услуги «Защита веб-приложений».

1.14.	Соглашение об уровне обслуживания для Услуги (SLA)	Документ, являющийся неотъемлемой частью Договора, описывающий Уровни доступности услуги «Защита веб-приложений».
1.15.	Сайт	Официальный веб-сайт Оператора (совокупность информации (электронные документы, программное обеспечение, базы данных), объединенная под одним адресом сайта в сети Интернет), являющийся частью Облачной Платформы, размещенный по адресу в сети Интернет https://ts-cloud.ru/.
1.16.	Личный кабинет	Специальный раздел Сайта, в котором Клиент может просматривать заказанные Услуги и оформлять Заявки на оказание Услуги.
1.17.	Панель управления (Dashboard)	Специальный раздел Сайта, с доступом через Личный кабинет Клиента, либо специализированная веб-страница, ссылка на которую содержится в Личном кабинете Клиента, и с помощью которой, Техническим Представителям Клиента предоставляется информация о работоспособности Услуги и статистики происходящих событий (Легитимный и Нелегитимный трафик, типы атак, параметры атак, объем отфильтрованного трафика, и т.п.).
1.18.	Аутентификационные данные Панели управления	Пара символьных наборов «логин» + «пароль», и/или иная аналогичная информация, предоставляемая Оператором, с использованием которой Клиент может получить удалённый доступ к Панели управления и начать полнофункциональное пользование Услугой на условиях Договора и настоящих Общих Условий.

Термины и определения, используемые в настоящих Общих условиях имеют значения, аналогичные указанным в Договоре, «Регламенте технической поддержки», «Соглашении об уровне обслуживания для услуги «Защита веб-приложений». Настоящие Общие условия оказания услуги «Защита веб-приложений» являются неотъемлемой частью Договора. При заключении Договора Клиент подтверждает, что ознакомился с Общими условиями и обязуется их исполнять в соответствии с условиями Договора.

2. ОПИСАНИЕ УСЛУГИ

2.1. Определение Услуги

«Защита веб-приложений» (далее Услуга) представляет собой совокупность работ и услуг, направленных на защиту веб-приложения (Ресурса) Клиента от Сетевых Атак с использованием комплекса Web Application Firewall (Комплекс WAF) Оператора.

2.2. Кому может быть предоставлена Услуга

Услуга «Защита веб-приложений» может быть предоставлена Клиенту для защиты Ресурсов от Сетевых атак, размещаемых не только на Облачной платформе Оператора, но и на любых других узловых точках сети Интернет.

2.3. Состав Услуги

Услуга включает в себя базовые и дополнительные компоненты Услуги. Состав Услуги, исчерпывающий перечень её параметров и их значения определяется в Заказе на Услугу.

В рамках Услуги осуществляется:

- подготовка Оператором Комплекса WAF;
- мониторинг входящего на Ресурс трафика, осуществляемый посредством Комплекса WAF, с целью распознавания трафика Сетевой Атаки;
- Фильтрация Трафика, осуществляемая посредством Комплекса WAF;
- базовая Техническая Поддержка Клиента;
- круглосуточное предоставление Клиенту результатов анализа Трафика в графическом или табличном виде через Панель управления;
- оповещение Клиента о наличии Сетевых Атак или Паразитного Трафика в направлении Ресурсов Клиента;
- предоставление Клиенту, по электронной почте, в виде предустановленной формы стандартизованных отчетов по результатам мониторинга Трафика в направлении Ресурсов Клиента.

2.4. Режимы предоставления Услуги

Услуга предоставляется в одном из трех режимах:

- режим «По умолчанию» – режим работы определяется настройками, заданными в конфигурационных файлах Комплекса WAF;
- режим «Мониторинг» – обрабатываются все запросы, но не фильтруются (не блокируются) никакие из них, даже если обнаружены вредоносные запросы;
- режим «Блокировка» – в этом режиме фильтруются (блокируются) все вредоносные запросы.

Выбор режима определяется Клиентом по необходимости, переключение режимов может быть осуществлено Клиентом через Панель управления.

После Фильтрации Трафика уже очищенный трафик направляется к Ресурсам Клиента. Все эти действия (мониторинг и Фильтрация Трафика) Комплекс WAF производит в автоматическом режиме.

2.5. Сведения, необходимые для предоставления Услуги

Клиент предоставляет Оператору следующую информацию:

- набор сетевых префиксов, составляющих защищаемые Ресурсы;
- описание защищаемых Ресурсов (заполненный Технический Опросник);
- SSL/TLS ключи для доменного имени защищаемого Ресурса (веб-приложения);
- электронный адрес для предоставления Клиенту регулярных отчетов о функционировании Услуги.

Клиенту необходимо поменять DNS запись защищаемого Ресурса (веб-приложения) на IP-адрес Комплекса WAF, а так же предоставить IP-адрес, на который будет передаваться Трафик после Фильтрации трафика.

2.6. Подготовка к предоставлению Услуги.

С целью подключения Клиента к Услуге выполняются следующие инсталляционные работы (услуги):

2.6.1. Регистрация защищаемых Ресурсов.

Защищаемые Ресурсы регистрируются в Комплексе WAF. В Комплексе WAF так же должны быть прописаны технические параметры Ресурсов, ключевых клиентских сервисов, для сбора более детальной статистики с целью повышения эффективности защиты Ресурсов от Сетевых атак.

Комплекс WAF начинает собирать данные о Трафике и рассчитывать статистические и поведенческие критерии Легитимного трафика сразу после завершения регистрации защищаемого Ресурса в Комплексе WAF и перенаправлении трафика на него. Эти данные станут доступны для просмотра через Панель управления и будут использоваться Комплексом WAF для противодействия Сетевым атакам.

2.6.2. Организация доступа к Панели управления Комплексом WAF.

Организовывается возможность on-line доступа Клиента к Панели управления для осуществления мониторинга функционирования Услуги. Доступ к Панели управления Комплекса WAF осуществляется через Личный кабинет. Реквизиты доступа к Панели управления высылаются Представителям Клиента на этапе инсталляции Услуги.

2.6.3. Организация предоставления регулярных отчетов.

Регулярные отчеты высылаются на адрес электронной почты учетной записи клиентского аккаунта, используемого при регистрации Клиента в Комплексе WAF. При необходимости, Клиент может изменить адрес электронной почты для доставки регулярных отчетов посредством отправки соответствующего Запроса в Службу Технической Поддержки Клиентов в процессе пользования Услугой.

2.7. Базовые компоненты Услуги (основные услуги)

Базовые компоненты Услуги заказываются и оплачиваются Клиентом на основании подписанного Клиентом Заказа.

2.7.1. Панель управления

Для доступа в Панель управления Оператор предоставляет Клиенту Аутентификационные данные Панели управления в течение 3 (трех) рабочих дней с момента реализации Оператором Заказа на оказание Услуги.

Панель управления в реальном времени отображает историю событий Комплекса WAF и текущее состояние защищаемых Ресурсов:

- Отображение в реальном времени информации о событиях, Сетевых Атаках и Вредоносных запросах: дата и время события, количество обнаруженных Сетевых Атак, количество произошедших Вредоносных запросов, примерная стоимость Сетевых Атак.
- Отображение в реальном времени информации об Уязвимостях веб-приложений: дата и время обнаружения Уязвимости, количество Уязвимостей высокого уровня опасности, количество Уязвимостей среднего уровня опасности, количество Уязвимостей низкого уровня опасности.
- Управление «черным списком» IP-адресов.
- Отображение статистики по отдельно выбранному веб-приложению.
- Отображение статистики по количеству запросов, фильтруемых в секунду, количество осуществляемых Сетевых атак в секунду.
- Раздел «Сканер» – отображение информации о сканировании Уязвимостей защищаемых веб-приложений: дата и время последнего сканирования, общее количество обнаруженных уязвимостей, количество уязвимостей каждого уровня риска.

- Раздел «События» содержит три подраздела для отображения информации о Сетевых Атаках, Вредоносных запросах и Уязвимостях. Подраздел «Атаки» содержит все группы связанных между собой Вредоносных запросов. Подраздел «Инциденты» содержит все Вредоносные запросы, нацеленные на использование существующих Уязвимостей. Подраздел «Уязвимости» содержит все обнаруженные ошибки, допущенные при проектировании, разработке или внедрении защищаемого веб-приложения, которые могут привести к реализации риска информационной безопасности.
- Раздел «Уязвимости» содержит информацию об Уязвимостях защищаемых веб-приложений. Комплекс WAF хранит историю всех Уязвимостей, периодически проверяя состояние каждой, включая закрытые Уязвимости. Если закрытая Уязвимость откроется вновь, Клиент получит уведомление. По умолчанию список отсортирован по времени обнаружения Уязвимости.

2.7.2. Базовые тарифные планы

Услуга предусматривает для Клиента возможность выбора одного из трех Базовых тарифных планов для защиты одного веб-приложения, в зависимости от Трафиковой нагрузки, оцениваемой в количестве запросов в секунду (Requests Per Second, RPS), поступающих в направлении защищаемого веб-приложения. Описание Базовых тарифных планов показано в таблице ниже:

Базовая Услуга	**Максимальная Трафиковая нагрузка, RPS**	**Краткое функциональное описание**
WAF-100	до 100 RPS	Комплекс WAF осуществляет непрерывный мониторинг и фильтрацию HTTP и HTTPS-трафика, поступающего к защищаемому веб-приложению, а также блокировку вредоносных запросов. Подсистема управления Комплекса WAF представляет данные о Сетевых атаках, уязвимостях защищаемого веб-приложения, инцидентах информационной безопасности, а также возможности для управления и настройки различных компонентов Комплекса WAF. Управление осуществляется через Панель управления. Доступ к Панели управления осуществляется по защищенному протоколу HTTPS. Комплекс WAF обеспечивает защиту от следующих угроз по классификации OWASP TOP-10: SQLi, XSS, XXE, Path traversal, Forced browsing, SSRF, CLRF, Memcached injection, key-value/NoSQL injection, и др. Комплекс WAF предоставляет возможность ручного создания правил обработки входящего трафика, а также виртуального патчинга (Virtual Patching).
WAF-500	до 500 RPS	
WAF-1000	до 1000 RPS	

Оператор осуществляет Фильтрацию Трафика при величине Трафиковой нагрузки не более той, что указана в таблице для соответствующего тарифного плана. В случае превышения Клиентом установленной для каждого тарифного плана величины максимальной Трафиковой нагрузки, Клиенту предлагается перейти на другой тарифный план, с величиной максимальной Трафиковой нагрузки, соответствующей фактически поступающей в сторону веб-приложения Клиента. В случае отказа Клиента от перехода на тарифный план соответствующий фактической Трафиковой нагрузке веб-приложения Клиента, Оператор вправе блокировать запросы, превышающие величину максимальной Трафиковой нагрузки, установленную для данного тарифного плана.

Для обеспечения защиты веб-приложения Клиента от Сетевых атак при Трафиковой нагрузке свыше 1000 RPS, Оператор готов предоставить Клиенту расширенный вариант

Услуги «Защита веб-приложений» в рамках отдельного технического решения и дополнительного соглашения на оказание такой услуги.

2.7.3. Предоставление регулярных отчетов по стандартной форме

В рамках Услуги Клиенту высылаются стандартные ежемесячные отчеты о предоставленной Услуге. Отчеты ежемесячно высылаются Клиенту по электронной почте с адреса noreply@ts-cloud.ru в автоматическом режиме по окончании отчетного периода на адрес, указанный в Заказе при подключении Услуги.

При необходимости со стороны Клиента в восстановлении ранее предоставленного ему регулярного стандартного ежемесячного отчета, Клиент может направить в службу технической поддержки Оператора Запрос на повторную отправку отчета с указанием календарного месяца, за который требуется повторный стандартный отчет. Отчет будет выслан Клиенту по электронной почте на электронный адрес, указанный Клиентом в Заказе на Услугу. Повторное предоставление стандартных ежемесячных отчетов может быть осуществлено за период не более чем 12 месяцев, предшествующих месяцу отправки Клиентом Запроса в службу технической поддержки Оператора.

2.7.4. Базовая Техническая Поддержка Клиента

Для передачи сообщений об Инцидентах и Запросах, Клиент может обращаться в Службу Технической Поддержки Клиента. Служба Технической Поддержки Клиентов работает круглосуточно 7 дней в неделю.

Клиент вправе потребовать модификацию, изменение состава или объема оказываемых Услуг, направив Оператору Заявку с подробным описанием и желаемые сроки выполнения таких работ. После получения письменного уведомления, Оператор сообщит ориентировочную стоимость и возможные сроки выполнения работ. Работы выполняются на основании отдельного Заказа.

Порядок оказания технической поддержки изложен в «Регламенте технической поддержки».

Заказывая Услугу «Защита веб-приложений», Клиент соглашается с настоящими Общими условиями и подтверждает, что он (сотрудники, подрядчики или иные представители Клиента, которым будет предоставлен доступ к Панели управления) обладает специальными знаниями и квалификацией, достаточной для управления защитой от атак на веб-приложения, а также гарантирует, что он обладает необходимыми навыками по администрированию выявленных уязвимостей защищаемых веб-приложений.

Оператор будет предпринимать для разрешения Инцидентов все разумные усилия.

2.8. Дополнительные компоненты Услуги (дополнительные услуги)

Дополнительные компоненты Услуги заказываются и оплачиваются Клиентом на основании подписанного Клиентом Заказа.

Стоимость Дополнительных компонентов не входит в стоимость Базовых компонентов услуги.

2.8.1. Дополнительные услуги к Базовым тарифным планам

В рамках каждого Базового тарифного плана, по запросу Клиента, могут быть предоставлены дополнительные услуги, функциональный состав которых показан в таблице ниже:

Дополнительная услуга	Описание дополнительной услуги
Сканирование уязвимостей	Осуществляется поиск узлов инфраструктуры, принадлежащих заданным пространствам доменных имен. Для формирования периметра используются данные, получаемые из прямых и обратных DNS запросов, протокола WHOIS, BGP, путем словарного перебора доменных имен и другие способы. Для найденных инфраструктурных компонентов модуль производит анализ публично доступных служб и сервисов (сканирование портов).
Перепроверка Сетевых атак	Поиск уязвимостей на защищаемом Ресурсе при помощи векторов атак из отфильтрованных вредоносных запросов, поступающих на модуль фильтрующего узла Комплекса WAF. Этот подход помогает выявлять индивидуальные уязвимости Ресурса, в том числе ZERO-day.
Защита от поведенческих Сетевых атак	Модуль Комплекса WAF защищает веб-приложение от поведенческих Сетевых атак типа BruteForce, Directory Busting, Credential Stuffing и других.
Защита дополнительного домена второго уровня	Защита от Сетевых атак для одного дополнительного домена второго уровня, используемого Клиентом в рамках защищаемого веб-приложения.

2.8.2. Расширенная Техническая Поддержка Клиента

Расширенный уровень платной Технической Поддержки Клиента включает в себя закрепление выделенного инженера и помощь в настройках и управлении режимами защиты веб-приложений Клиента.

3. СРОКИ ВЫПОЛНЕНИЯ ИНСТАЛЛЯЦИОННЫХ РАБОТ И ОКАЗАНИЯ УСЛУГИ

Плановый срок выполнения инсталляционных работ составляет 10 (десять) рабочих дней с даты подписания Сторонами Заказа по Услуге «Защита веб-приложений». Полный возможный перечень инсталляционных работ указан в п. 2.6 настоящего документа. Срок выполнения и состав инсталляционных работ, адаптированные в соответствии с условиями проекта, указываются в Заказе.

Услуга оказывается в течение срока действия Заказа.

4. ТАРИФИКАЦИЯ И ОПЛАТА УСЛУГИ

Оплата за оказание Услуги осуществляется посредством единовременных и ежемесячных платежей.

Тарифы устанавливаются Сторонами в Прайс-листе и Заказе на оказание Услуги.

4.1. Единовременные платежи

Единовременные платежи могут быть установлены за инсталляционные и дополнительные виды работ, осуществляемые Оператором.

Единовременный инсталляционный платеж – это стоимость выполнения следующих инсталляционных работ:

- конфигурирование на сети Оператора;
- регистрация защищаемых Ресурсов Клиента в Комплексе WAF;

- настройка клиентского доступа к Панели управления;
- настройка регулярных отчетов.

По требованию Клиента, Оператор может выполнить в интересах Клиента определенный набор дополнительных работ. В этом случае Услуга считается нестандартной и подлежит отдельной проработке на предмет определения технической возможности и стоимости нестандартной Услуги, а также ее сроков предоставления. При этом, срок предоставления нестандартной Услуги будет увеличен на срок дополнительного проектирования и подготовки выполнения дополнительных работ.

Оказание нестандартной Услуги, оплата Клиентом дополнительных работ осуществляется на основании отдельного Заказа.

4.2. Ежемесячные платежи за базовые компоненты Услуги

Стоимость Базового тарифного плана приведена из расчета за 1 (один) полный календарный месяц за 1 (одно) защищаемое веб-приложение (Ресурс, домен второго уровня).

4.3. Ежемесячные платежи за дополнительные компоненты Услуги

Стоимость дополнительных услуг приведена из расчета за 1 (один) полный календарный месяц за 1 (одно) защищаемое веб-приложение (Ресурс).

4.4. Ежемесячные платежи за расширенную Техническую Поддержку Клиента

Тариф приведен из расчета за 1 (один) полный календарный месяц за все защищаемые веб-приложения (Ресурсы) указанные в Заказе.

5. ТЕРРИТОРИЯ ОКАЗАНИЯ И ДОСТУПНОСТЬ УСЛУГИ

Услуга оказывается в Дата Центре Оператора, Услуга доступна пользователям на всей территории России.

6. СОБСТВЕННОСТЬ НА СРЕДСТВА ПРЕДОСТАВЛЕНИЯ УСЛУГИ

Клиент соглашается, что собственность на оборудование и исключительные права на программное обеспечение, используемые Оператором для обеспечения предоставления Услуги, сохраняются за Оператором, его субподрядчиками и лицензиарами. Клиент обязуется не нарушать и не создавать условий для нарушения имущественных прав на оборудование и исключительных прав на программное обеспечение Оператора и третьих лиц.

Собственность на Комплекс WAF, остается за Оператором или его субподрядчиками. Данное оборудование и программное обеспечение не продается и не передается в собственность Клиенту.

7. ТЕХНИЧЕСКИЕ ОГРАНИЧЕНИЯ

7.1. Клиент должен соблюдать все технические меры предосторожности, необходимые для использования Услуги и обеспечения совместимости его веб-сайта и/или Программных Приложений с Услугой, Виртуальными машинами, системными ресурсами, программным обеспечением и техническими ограничениями Облачной Платформы Оператора.

7.2. Клиент обязуется соблюдать рекомендации и условия Оператора при разработке своих информационных технологий. Оператор не несет ответственности за ненадлежащую

работу Услуги и/или потерю данных в результате несоблюдения условий использования Услуги.

7.3. Клиент обязуется не совершать никаких действий, которые могут повлиять на конфигурацию Комплекса WAF, его работоспособность и безопасность или оказать негативный эффект на производительность Комплекса WAF.

7.4. Клиент должен обеспечить отсутствие избыточной Трафиковой нагрузки на Комплекс WAF в период использования Услуги. В случае если суммарная интенсивность (Мбит/с) входящего Трафика (Легитимный Трафик плюс Паразитный Трафик) на защищаемый Ресурс превышает допустимую интенсивность, установленную Оператором в рамках услуги «Резервированный доступ в Интернет», Оператор оставляет за собой право блокировать частично или полностью Трафик, направляемый в сторону защищаемого Ресурса.

7.5. Оператор освобождается от ответственности в случае, если конфигурация Услуги, выбранная Клиентом, не является достаточной для удовлетворения потребностей Клиента в части требований и подключений или превышает предусмотренные Клиентом параметры.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Оператор не несет ответственности за нарушение работоспособности и выход из строя Ресурсов Клиента. Для исключения убытков Клиент самостоятельно должен обеспечить страхование своего Ресурса от рисков, связанных с нарушением работоспособности и/или выходом его из строя.

8.2. Оператор не несет ответственности за неправомерное использование Услуги, предоставленной Клиенту.

8.3. Оператор не несет ответственности за невозможность оказания Услуги, а также за какие-либо убытки, ущерб, вред, причиненные Клиенту, наступившие в результате действий или бездействия третьих лиц, в результате противоправных действий (бездействия) этих лиц.

8.4. Услуга предоставляется «как есть» (услуга предоставляется с использованием программного обеспечения WALLARM компании ООО «ОНСЕК ИНК.», https://wallarm.ru/, специфика и характер Фильтрации Трафика обусловлены производителем программного обеспечения WALLARM компании ООО «ОНСЕК ИНК.»), «со всеми ошибками» (в случае обнаружения ошибок программного обеспечения WALLARM при Фильтрации Трафика, подобные ошибки разрешаются в установленном производителем программного обеспечения порядке, в данном случае компанией ООО «ОНСЕК ИНК.»). Оператор отказывается от предоставления любых гарантий явно не предусмотренных Договором и настоящими Общими Условиями, в том числе, без ограничения, от подразумеваемых гарантий, включая гарантии товарной пригодности, пригодности для определенной цели, качества исполнения или предоставления и отсутствия нарушения прав иных правообладателей.

8.5. Клиент несет ответственность за действия Технического Представителя Клиента во время предоставления Услуги.