Условия предоставления права использования программного обеспечения
Программный комплекс «Solar Space»

1. Термины и определения

Паразитный трафик	Трафик, который из-за своих свойств, характера или объёма способен нарушить функционирование инфраструктуры Лицензиата.
ПО	Программное обеспечение «Программный комплекс «Solar Space», предназначенное для фильтрации веб-трафика и защиты интернет-ресурсов от DDoS-атак, вредоносных ботов и кибератак. ПО включено в Единый реестр российских программ для электронных вычислительных машин и баз данных (реестровая запись № 23679 от 29.08.2024). Карточка в реестре: https://reestr.digital.gov.ru/reestr/2623376/. Использование ПО осуществляется путем удаленного доступа через сеть Интернет посредством Личного кабинета без передачи экземпляра ПО Лицензиату.
Личный кабинет	Часть ПО, представляющая собой веб-интерфейс, размещенный по адресу в сети Интернет https://my.solarspace.pro/, посредством которого осуществляется удаленный доступ к ПО и его функциональным возможностям.
Лицензия	Право использования ПО, предоставляемое Лицензиату в соответствии с настоящим документом.
Иная договорная документация	Совокупность документов, оформляемых в рамках договорных отношений между сторонами, включая договоры, заказы, дополнительные соглашения и иные документы, определяющие условия, объем, порядок и особенности взаимодействия сторон.
DNS	Система доменных имен, компьютерная распределенная система для получения информации о доменах семейства TCP/IP.
A-запись	Тип записи в DNS, который сопоставляет доменное имя с его IP-адресом, позволяя браузерам и другим сервисам находить сервер, на котором размещен сайт или сервис.
TXT-запись	Тип записи в системе DNS, который хранит текстовую информацию, часто используется для подтверждения владения доменом.
Домен	Уникальное символьное имя, служащее для идентификации веб-ресурса в сети Интернет.
Интернет-ресурс	Совокупность электронных файлов в компьютерной сети, объединенных под одним доменным именем (сайт, веб-приложение, веб-ресурс).
IP-адрес	Уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.
Трафик	Объем информации, передаваемой по сети Интернет на веб-ресурс.
Запрос	Обращение к базе данных веб-ресурса, совершаемое пользователем и/или ботом, а также его метод.
Закон о персональных данных	Федеральный законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
Бот	Программа для ЭВМ, автоматически совершающая запросы с определенного IP-адреса, имитирующая признаки и поведение интернет-пользователя на публичном ресурсе Лицензиата и

	осуществляющая автоматизированный сбор данных, перебор паролей или иные вредоносные действия по отношению к этому ресурсу.
DDoS-атака или DDoS	Атака, связанная с большим количеством запросов к веб-ресурсу, имеющая своей целью и/или приводящая к отказу в работе системы из-за исчерпания ее ресурсов: процессора, памяти сервера либо каналов связи.
WAF Lite	Web Application Firewall – функциональный модуль ПО для обнаружения и блокирования вредоносных сетевых запросов, направленных на эксплуатацию уязвимостей веб-приложений.
RPS	Количество запросов к веб-приложению в секунду.
TLS	Протокол защиты транспортного уровня, обеспечивающий защищенную передачу данных между веб-приложениями и пользователями в сети Интернет.
SSL-протокол	Сетевой протокол, используемый для обеспечения конфиденциальности обмена трафиком между веб-приложениями и пользователями в сети Интернет.
SSL/TLS-сертификат	Цифровой сертификат, удостоверяющий подлинность веб-приложения, и позволяющий использовать зашифрованное соединение при передаче данных через сеть Интернет.
HTTPS	HyperText Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования SSL/TLS с целью повышения безопасности.
OWASP Top-10	Open Web Application Security Project (OWASP) – регулярно публикуемый в интернете рейтинг основных угроз безопасности веб-приложений.

2. Общие сведения

2.1. Наименование предмета

Лицензиар предоставляет Лицензиату на условиях простой (неисключительной) лицензии право использования ПО. Право использования реализуется путем удаленного доступа к ПО через сеть Интернет посредством Личного кабинета и не предполагает передачу экземпляра ПО, его скачивание или установку на устройства Лицензиата.

Право использования предоставляется на территории Российской Федерации на срок оплаченного периода, указанного в Иной договорной документации или в Личном кабинете, и в пределах выбранного тарифа, количества доменов, пропускной способности, RPS и иных согласованных параметров. Допустимый способ использования – удаленный доступ к функциональным возможностям ПО через Личный кабинет исключительно для защиты интернет-ресурсов Лицензиата и в пределах параметров Иной договорной документации.

Размер лицензионного вознаграждения, состав предоставляемой функциональности и срок действия Лицензии определяются Иной договорной документацией. Лицензиат не вправе воспроизводить, распространять, модифицировать, декомпилировать ПО, предоставлять сублицензии или иным образом использовать ПО за пределами прямо предоставленных прав, если иное не установлено в Иной договорной документации или письменно не согласовано с Лицензиаром.

2.2. Состав предоставляемого права использования

В рамках Лицензии Лицензиату может предоставляться доступ к следующим функциональным компонентам ПО и опциям (состав опредяется Иной договорной документацией и выбранным тарифом):

- Защита сайта от DDoS-атак (WEB AntiDDoS);
- Защита сайта от ботов (WEB Antibot);
- Защита сайта от кибератак (WAF Lite);
- Личный кабинет;
- Обеспечение работоспособности ПО в объеме, предусмотренном настоящими Условиями.

Дополнительная функциональность, доступная в рамках Лицензии за отдельную плату:

- Защита дополнительного домена
    - Защита дополнительного домена расширяет право использования ПО на дополнительный домен Лицензиата. Для дополнительного домена применяется тот же набор функциональных возможностей защиты, что и для основного домена, если иное не указано в Заказе.
    - Для подключения дополнительной функциональности выполняются подключение и настройка дополнительного домена в Личном кабинете, применение правил фильтрации трафика, мониторинг состояния защиты и формирование отчетности средствами ПО.

- Подключение защиты дополнительного домена не увеличивает общий объем включенного трафика и иные лимиты Лицензии (кроме количества защищаемых доменов), если иное прямо не согласовано Сторонами.

2.3. Назначение и цели использования ПО

ПО предназначено для повышения уровня защищенности информационных ресурсов Лицензиата путем выявления и блокирования атак на прикладном уровне, направленных на снижение или прекращение доступности интернет-ресурсов, а также для помощи в следующих задачах (в зависимости от приобретенного комплекта функциональных подсистем):

- Защита от DDoS-атак: предотвращение распределенных атак, направленных на перегрузку серверов и блокировку их работы;
- Защита от ботов: обнаружение и блокировка вредоносных ботов и автоматизированных средств, которые могут перегружать системы или пытаться получить несанкционированный доступ;
- Защита от кибератак (WAF Lite): обнаружение и блокировка попыток взлома веб-приложений, защита от уязвимостей и предотвращение утечек данных.

3. Основные условия исполнения обязательств

3.1. Способ и условия использования ПО

- ПО используется путем удаленного доступа через Личный кабинет в сети Интернет по модели SaaS;
- Лицензиат регистрируется в Личном кабинете самостоятельно. Для получения помощи с регистрацией Лицензиат вправе обратиться в службу поддержки Лицензиара;
- ПО функционирует с использованием технологии обратного прокси-сервера (Reverse Proxy). Лицензиат самостоятельно изменяет A-запись DNS доменного имени защищаемого интернет-ресурса. Функциональность ПО не распространяется на исходящие запросы от интернет-ресурсов;
- Лицензиар не предоставляет Лицензиату физического подключения к оборудованию Лицензиара, каналов связи или доступа к сети Интернет;
- Лицензиат самостоятельно несет ответственность за сохранность данных для входа в Личный кабинет и за последствия их утраты или разглашения.

3.2. Функциональные и технические характеристики ПО

(a) Защита сайта от DDoS-атак (WEB AntiDDoS)

Подсистема защиты сайта от DDoS-атак (WEB AntiDDoS) является базовой функциональностью и предназначена для предотвращения распределенных атак, направленных на блокировку работы интернет-ресурсов на уровне L7.

Функционал подсистемы WEB AntiDDoS включает в себя следующий набор возможностей:

- Подсистема обеспечивает фильтрацию HTTP/HTTPS-трафика;
- Подсистема обеспечивает фильтрацию с раскрытием приватных ключей SSL;
- Подсистема поддерживает протокол HTTP/2 без переключения Лицензиатов на более старые версии протокола;
- Подсистема автоматически осуществляет балансировку нагрузки между пулом основных и резервных бэкендов;
- Подсистема осуществляет кэширование для необходимых расширений файлов;
- Подсистема поддерживает автоматический выпуск, продление и установку бесплатных Let’s Encrypt SSL-сертификатов;
- Подсистема поддерживает установку и одновременное использование SSL ГОСТ и RSA сертификатов;
- Фильтрация веб-трафика производится путем перехвата TCP-пакетов на 80 и 443 портах и доменов без ограничения по количеству поддоменов;
- Подсистема поддерживает протоколы HTTP/0.9, HTTP/1.0, HTTP/1.1, HTTP/2.0, SPDY;
- Подсистема поддерживает SSL/TLS 1.2 и 1.3 шифрования;
- Подсистема поддерживает возможность осуществления HTTP-redirect;
- Подсистема поддерживает создание списков доверенных и запрещенных адресов или сетей (черные и белые списки);

- Подсистема обеспечивает сквозную передачу на оборудование Лицензиата IP-адресов источников запросов;
- Подсистема обеспечивает сквозную передачу на оборудование Лицензиата JA3-отпечатка в отдельном заголовке;
- Подсистема обеспечивает возможность прохождения протокола WebSocket с настройкой соответствующих портов, отличных от стандартных портов HTTP(S);
- Подсистема обеспечивает беспрепятственную работу легальных поисковых ботов и не влияет 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;
- Подсистема может вносить задержку для Лицензиатов при обращении к защищаемым сервисам в пределах 50 мс. Лицензиар не гарантирует задержку в рамках указанных лимитов, так как она зависит от качества подключения со стороны Лицензиата к сети Интернет.

Подсистема WEB AntiDDoS способствует защите от следующих типов атак:

- HTTP флуд (HTTP Flood, Excessive VERB);
- HTTP флуд одиночными запросами (Single Request HTTP Flood, Multiple VERB Single Request);
- HTTP флуд одиночными сессиями (Single Session HTTP Flood, Excessive VERB Single Session);
- Атака с целью отказа приложения (Faulty Application Attack);
- Атака фрагментированными HTTP-пакетами (Fragmented HTTP Flood, HTTP Fragmentation);
- Сессионная атака, атака медленными сессиями (Session Attack, SlowLoris);
- Рекурсивный HTTP GET флуд (Recursive HTTP GET Flood).

Подсистема обеспечивает защиту в пределах той ширины канала в Мбит/с, которая заказана и оплачена Лицензиатом, и только для тех доменов, которые включены Лицензиатом в Лицензию.

(б) Защита сайта от автоматических атак и ботов (WEB Antibot)

Подсистема WEB Antibot является дополнительной функциональностью и может быть подключена только вместе с подсистемой WEB AntiDDoS. Она предназначена для обнаружения и блокировки вредоносных ботов и автоматизированных средств, которые могут перегружать системы, похищать данные или пытаться получить несанкционированный доступ. Лицензиар не гарантирует полную блокировку вредоносных ботов.

Функционал подсистемы WEB Antibot включает в себя следующий набор возможностей:

- Подсистема обладает функционалом по обнаружению ботов на основе анализа аномальной активности при работе с сайтами Лицензиата;
- Подсистема может блокировать и размечать IP-адреса ботов-источников трафика, а также управлять блокировками размеченных источников в Личном кабинете;

- Подсистема передает вердикт по запросам в HTTP-заголовке: запрос сформирован автоматизированным средством (ботом) или реальным пользователем защищаемого сайта;
- Подсистема автоматически отслеживает запросы ботов следующих поисковых систем: Google, Yandex, Mail.ru, Rambler, Bing, Yahoo, Ask.com, Baidu, DuckDuckGo и не блокирует их вне зависимости от настроек защиты;
- Подсистема позволяет детектировать ботов с первого запроса и предоставлять информацию о статистике трафика, стране происхождения атаки и информации о векторе атаки;
- Максимальная задержка работы подсистемы при обработке трафика на уровне приложений составляет не более 5 мс.

Требования к размещению и функционированию:

- Подсистема размещается на единой аппаратной и программной платформе Лицензиара с подсистемой фильтрации трафика DDoS-атак и исключает дополнительное перенаправление трафика пользователей ресурса Лицензиата при своей работе;
- Функционирование осуществляется без размещения дополнительных аппаратных или программных компонентов на стороне инфраструктуры приложения Лицензиата.

Подсистема имеет режимы:

- Мониторинга, в котором активность ботов обнаруживается и сообщается, но не блокируется без вмешательства Лицензиата;
- Блокировки, в котором боты автоматически блокируются при обнаружении.

Режим определяется Лицензиатом (с использованием интерфейса Личного кабинета). Для каждого сайта может быть настроен отдельный режим.

Подсистема способствует распознаванию и предотвращению вредоносной активности ботов следующих видов:

- Перебор и скачивание содержимого сетевого ресурса (web scraping);
- Перебор логинов, паролей, промо-кодов в полях ввода и формах авторизации (brute-force attacks);
- Массовая подстановка значений в формы контактных данных, опросов, поисковых систем (credential stuffing);
- Атаки на заполнение корзины покупателя и исчерпание товарного каталога;
- Автоматизированная массовая скупка билетов, товаров, услуг на сетевых ресурсах, осуществляющих розничную онлайн-торговлю.

Методы обнаружения ботов, используемые Подсистемой:

- 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 и передача данного отпечатка в подсистему для анализа и выявления аномалий в параметрах браузера и устройства пользователя;
- Поиск 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, и оценка ее влияния на состояние публичного ресурса Лицензиата.

Лицензиар вправе использовать другие методы обнаружения ботов, но не гарантирует их наличие.

Варианты реагирования на обнаруженную угрозу:

- Запись в журнал;
- Разметка запроса особым заголовком и пропуск в сторону ресурса Лицензиата;
- Демонстрация страницы проверки с JavaScript-кодом для сбора отпечатка браузера;
- Отдача пользователю ответа с кодом ошибки;
- Блокировка IP-адреса пользователя на варьируемый временной интервал.

Варианты реагирования определяются Лицензиатом (с использованием интерфейса Личного кабинета). Варианты реагирования могут быть настроены вместе или по отдельности для каждого сайта.

Подсистема обеспечивает защиту в пределах той ширины канала в Мбит/с, которая заказана и оплачена Лицензиатом, и только для тех доменов, которые включены Лицензиатом в Лицензию.

(в) Защита сайта от кибератак (WAF Lite)

Подсистема защиты сайта от кибератак (WAF Lite) является дополнительной функциональностью и может быть подключена только совместно с подсистемами WEB AntiDDoS и WEB Antibot в совокупности.

WAF Lite – это облегченная версия WAF, представляющая собой специализированное программное решение для защиты веб-приложений от различных атак. Она анализирует входящий и исходящий HTTP/HTTPS-трафик, фильтрует его и блокирует вредоносные запросы, направленные на эксплуатацию уязвимостей в приложениях. WAF Lite обеспечивает защиту от наиболее распространенных атак, таких как SQL-инъекции, межсайтовый скриптинг (XSS), атаки на сессию и другие виды угроз, которые могут привести к компрометации данных или нарушению работы системы. Подсистема WAF Lite включает базовые правила для фильтрации трафика и предотвращения типичных угроз, однако не обладает продвинутыми возможностями настройки и мониторинга.

Функционал подсистемы WAF Lite включает в себя следующий набор возможностей:

- Проверка HTTP/HTTPS-запросов на уровне веб-приложений и на соответствие RFC;
- Обработка XML-документов и SOAP-запросов;

- Проверка параметров запросов к защищаемым веб-приложениям на предмет совпадений с предустановленными сигнатурами атак для идентификации вредоносных запросов;
- Проверка HTTP(S)-ответов с целью предотвращения утечки данных и обеспечения дополнительной защиты с помощью специальных HTTP-заголовков;
- Защита от атак типа межсайтовое выполнение сценариев (XSS);
- Обнаружение ботов и средств взлома (Acunetix, Burp Suite, ZAP) путем внедрения в защищаемую страницу JS-скрипта и мета-тегов для защиты от CSRF;
- Отслеживание пользовательских сессий для идентификации пользователей;
- Защита по принципу "черный список" IP-адресов;
- Самообучаемая позитивная модель безопасности ("белый список") приложения для выявления аномального поведения и защиты от атак нулевого дня (настраивается Лицензиатом с использованием интерфейса Личного кабинета);
- Автоматическая генерация сигнатур ("виртуальных патчей") на основе результатов анализа уязвимостей;
- Терминация SSL и/или TLS: расшифровка и проверка HTTPS-трафика перед отправкой к веб-приложению;
- Защита пользователей путем встраивания соответствующего JS-модуля в страницу, вызываемую пользователем.

Подсистема способствует защите от атак из списка OWASP Top 10:

- Обход правил доступа (Broken Access Control): защита от несанкционированного доступа к ресурсам и данным, управляемая строгими политиками контроля доступа;
- Ошибки криптографии (Cryptographic Failures): защита данных с использованием надежных криптографических методов, предотвращение утечек и нарушений целостности данных;
- Инъекции ненадежных данных (Injection): обнаружение и блокировка инъекционных атак, таких как SQL-инъекции, командные инъекции и XSS;
- Ошибки в проектировании (Insecure Design): реализация безопасных архитектур и проектных решений для предотвращения уязвимостей на этапе разработки;
- Ошибки в системе безопасности (Security Misconfiguration): автоматическое выявление и устранение ошибок конфигурации безопасности;
- Устаревшие и уязвимые компоненты (Vulnerable and Outdated Components): обнаружение и обновление уязвимых компонентов программного обеспечения;
- Ошибки аутентификации (Identification and Authentication Failures): защита процессов идентификации и аутентификации пользователей, предотвращение атак на учетные записи;
- Ошибки целостности ПО (Software and Data Integrity Failures): обеспечение целостности программного обеспечения и данных, защита от внедрения вредоносного кода и данных;
- Ошибки в мониторинге и логировании (Security Logging and Monitoring Failures): эффективное ведение журналов безопасности и мониторинг для своевременного обнаружения и реагирования на инциденты;
- Подделка запроса на сервере (Server-Side Request Forgery): защита от поддельных запросов на сервер, предотвращение несанкционированного доступа и выполнения команд на сервере.

Также WAF Lite способствует защите от:

- SQL Injection – тип атаки, в ходе которого злоумышленник отправляет вредоносные SQL-запросы на веб-сервер;
- Remote File Inclusion – уязвимость веб-приложений, которая позволяет злоумышленнику включать и выполнять файлы с удалённого сервера;
- Directory Traversal – уязвимость в системе безопасности, которая позволяет злоумышленнику получить доступ к файлам и каталогам за пределами разрешённого каталога веб-приложения;
- Cross-Site Scripting (XSS) – уязвимость веб-приложений, которая позволяет злоумышленнику внедрить вредоносный код прямо на страницу, где с сайтом взаимодействуют другие пользователи;
- Cross-Site Request Forgery (CSRF) – вид атак на веб-приложения, при котором злоумышленник обманом заставляет пользователя выполнить нежелательное действие на сайте, где тот уже авторизован;
- HTTP-атак (HTTP Request Splitting) – атака, которая использует уязвимость в обработке HTTP-запросов сервером. Злоумышленник отправляет специально сформированный запрос, ответ на который интерпретируется сервером как два разных ответа. Второй ответ полностью контролируется злоумышленником, что даёт ему возможность подделать ответ сервера;
- HTTP-атак (Protocol Violation) – атака, которая нарушает протокол HTTP, например, отправляет данные с пропущенными символами CRLF (возвратом каретки и подачей строки). Это приводит к ошибке «The server has committed a protocol violation»;
- Remote Code Execution – тип атаки, при котором злоумышленник использует уязвимости в приложении или системе для выполнения вредоносного кода на удаленном сервере.

Подсистема обеспечивает защиту в пределах того количества RPS, которое заказано и оплачено Лицензиатом, и только для тех доменов, которые включены Лицензиатом в Лицензию.

3.3. Личный кабинет

На весь срок действия Лицензии Лицензиар предоставляет Лицензиату доступ к Личному кабинету в течение 1 (одного) рабочего дня с даты начала срока действия Лицензии путем отправки на электронную почту, указанную в Иной договорной документации, информации для доступа (адрес Личного кабинета, логин и пароль).

В Личном кабинете Лицензиат получает круглосуточный доступ к веб-отчетам с аналитической информацией о трафике и работе ПО в графическом и табличном виде с возможностью выгрузки.

Функционал Личного кабинета:

- Панель мониторинга (Dashboard)
    - Обзор состояния системы: показ текущего состояния защиты, активных атак, производительности и состояния ресурсов.
    - Графики и статистика: визуальное отображение данных о трафике, атаках, успешных блокировках и других важных метрик.

- Управление защитой от DDoS-атак
    - Настройка уровней защиты: возможность настройки различных уровней защиты от DDoS-атак.
    - Реальные данные о трафике: отображение в реальном времени информации о трафике, включая легитимный и вредоносный трафик.
    - История атак: доступ к журналу атак с подробной информацией о времени, типах и интенсивности атак.
- Управление защитой от паразитных ботов
    - Обнаружение и блокировка ботов: настройки для автоматического обнаружения и блокировки вредоносных ботов.
    - Белые и черные списки: управление списками доверенных и заблокированных IP-адресов и доменов.
    - Отчеты о ботах: статистика и отчеты о выявленных ботах, их активности и принятых мерах.
- Управление WAF Lite
    - Настройка правил безопасности: создание и управление правилами для фильтрации трафика и защиты от атак. Система содержит преднастроенные режимы, которые выбираются Лицензиатом, а также Лицензиат может донастроить их с учетом своих потребностей.
    - Анализ запросов и ответов: возможность анализа HTTP/HTTPS-запросов и ответов на предмет угроз.
    - Автоматические обновления сигнатур: обновление правил и сигнатур атак для своевременной защиты от новых угроз. Периодичность и объем обновления определяются Лицензиаром в одностороннем порядке.
- Настройки и управление SSL/TLS
    - Управление сертификатами: выпуск, установка и продление SSL/TLS сертификатов, включая Let’s Encrypt и коммерческие сертификаты.
    - Настройка протоколов шифрования: выбор и настройка поддерживаемых протоколов шифрования (например, SSL/TLS 1.2 и 1.3).
- Управление пользовательскими сессиями и доступом
    - Отслеживание сессий: мониторинг активных сессий пользователей и их активности.
    - Настройка доступа: управление доступом к различным частям Личного кабинета и настройка прав пользователей.
- Уведомления и оповещения
    - Настройка уведомлений: настройка правил и каналов уведомлений (Email, мессенджеры) о начале и окончании атак, изменениях в состоянии системы и других событиях.
    - История уведомлений: просмотр истории отправленных уведомлений и оповещений.
- Отчеты и аналитика
    - Генерация отчетов: создание отчетов по защите, атакам и производительности за различные периоды времени.
    - Экспорт данных: возможность экспорта данных и отчетов в различные форматы (CSV, PDF).
- Помощь
    - Документация и FAQ: доступ к документации, часто задаваемым вопросам и руководствам по использованию Личного кабинета.

- Ответы на вопросы: возможность обращения к Лицензиару с вопросами о работе ПО через Личный кабинет, отслеживание статуса обращений и получение решений в рамках обеспечения работоспособности ПО.

3.4. Мероприятия в рамках предоставления Лицензии

(а) Предоставление доступа к ПО

До начала использования ПО Лицензиар выполняет подготовительные действия, необходимые для предоставления Лицензиату доступа к ПО.

Для предоставления доступа к ПО Лицензиат предоставляет Лицензиару следующие данные:

- перечень защищаемых доменных имен интернет-ресурсов Лицензиата;
- сведения о системе управления сайтом;
- информацию о количестве посетителей, пропускной способности (Мбит/с) и количестве запросов (RPS);
- дополнительные данные, запрашиваемые Лицензиаром и необходимые для настройки ПО с учетом состава и конфигурации защищаемых ресурсов Лицензиата.

Информация предоставляется путем заполнения Лицензиатом соответствующих опросных листов и направления указанных листов в адрес Лицензиара по контактным адресам, указанным в Личном кабинете.

Действия по подключению ПО к интернет-ресурсам Лицензиата включают:

- разработку и согласование плана подключения;
- подключение ПО посредством верификации TXT-записи домена и смены A-записи защищаемых ресурсов для постоянной фильтрации;
- настройку сетевого взаимодействия с интернет-ресурсами Лицензиата;
- создание и настройку политик обнаружения и блокирования атак на защищаемые интернет-ресурсы Лицензиата, а также минимизацию ложных срабатываний в течение срока действия Лицензии;
- конфигурацию WAF Lite для защиты от кибератак веб-приложений (при необходимости и при наличии указанной подсистемы в Лицензии);
- предоставление Лицензиату (его уполномоченным представителям) доступа в Личный кабинет для использования ПО, управления настройками и мониторинга;
- профилирование политик фильтрации трафика, поступающего на защищаемые интернет-ресурсы Лицензиата, с использованием анализа параметров поступающих запросов;
- предоставление документации по настройке и использованию ПО.

(б) Этапы заведения ресурса под защиту

- Регистрация в Личном кабинете
  - Создание учетной записи: ввод личной и контактной информации, создание логина и пароля.

- Подтверждение регистрации: получение и подтверждение кода активации, отправленного на указанный email.

- Добавление доменов под защиту
  - Ввод данных домена: указание доменов и поддоменов, которые необходимо защитить.
  - Проверка прав на домен: подтверждение владения доменом путем верификации через TXT-запись.
  - Подключение защиты: изменение A-записи в DNS для активации защиты.

- Настройка защиты от DDoS-атак
  - Выбор уровня защиты: настройка параметров защиты, включая уровень фильтрации.
  - Конфигурация правил: создание и настройка правил фильтрации трафика, включая черные и белые списки IP-адресов.
  - Настройка уведомлений: определение каналов и условий для получения уведомлений об атаках (email, мессенджеры).

- Установка и настройка SSL/TLS сертификатов
  - Автоматический выпуск SSL: настройка автоматического выпуска и установки бесплатных SSL-сертификатов (например, Let’s Encrypt).
  - Установка пользовательских SSL: ввод и настройка пользовательских SSL-сертификатов, если используется коммерческий сертификат.

- Запуск защиты
  - Изменение DNS-серверов для домена: обновление доменной зоны на DNS-серверах регистратора занимает от нескольких минут до 3 часов. Для других публичных DNS-серверов этот процесс может занять от 2 до 4 часов. В общей сложности рекомендуется учитывать срок от 6 до 12 часов для полного распространения изменений.
  - Активное наблюдение: мониторинг состояния системы и производительности в первые часы после запуска.

Об окончании подключения интернет-ресурсов к ПО и переходе к его использованию Лицензиар уведомляет Лицензиата по адресу электронной почты, указанному в Личном кабинете.

(в) Использование и обеспечение работоспособности ПО

В течение срока действия Лицензии Лицензиаром обеспечиваются:

- Круглосуточный мониторинг доступности и работоспособности платформы;
- Фильтрация трафика Лицензиата в соответствии с параметрами, указанными в опросном листе, в целях распознавания и блокировки Паразитного трафика, DDoS-атак, ботов и атак, направленных на эксплуатацию уязвимостей;
- Обновление ПО Лицензиаром для защиты от новых видов угроз (регулярность обновления – на усмотрение Лицензиара);

- Обновление правил и политик безопасности WAF Lite (при необходимости и при наличии указанной подсистемы в Лицензии, регулярность обновления – на усмотрение Лицензиара);
- Формирование средствами ПО отчетов о состоянии безопасности, обнаруженных угрозах и принятых мерах;
- Устранение Лицензиаром выявленных недостатков в работе ПО по результатам мониторинга и (или) обращений Лицензиата;
- Проведение профилактических регламентных работ на ПО с уведомлением Лицензиата не менее чем за 24 часа до их начала;
- Проведение аварийных работ на ПО. Лицензиат уведомляется об аварийных работах по электронной почте при первой возможности;
- Обработка обращений Лицензиата в рамках обеспечения работоспособности ПО;
- Проактивное совершенствование политик противодействия киберугрозам;
- Осуществление иного обеспечения работоспособности ПО.

3.5. Тестовый доступ к ПО

Лицензиар вправе, но не обязан предоставлять тестовый доступ к ПО для ознакомления с его функциональными возможностями на период не более 14 календарных дней.

Лицензиат вправе запросить у Лицензиара тестовый доступ к ПО, обосновав его необходимость и представив примерный план тестирования. Каждый запрос рассматривается Лицензиаром индивидуально, о принятом решении Лицензиат уведомляется отдельно.

Функциональность тестового доступа может быть ограничена; тестовый доступ предназначен только для ознакомления и тестирования и не допускает коммерческого или иного штатного использования, включая постоянную либо временную защиту интернет-ресурсов. По итогам тестирования Лицензиат уведомляет Лицензиара о наличии или отсутствии намерения приобрести право пользования ПО.

Обязательства Лицензиара по SLA не распространяются на тестовый доступ. Лицензиат несет ответственность за использование ПО в рамках тестового доступа.

3.6. Основные параметры

Предоставление Лицензии и обеспечение работоспособности ПО в рамках настоящего документа осуществляются в соответствии со следующими параметрами:

Таблица 1. Основные параметры (SLA)

Параметр	**Целевые значения**
Группа параметров «Период действия Лицензии»	
Срок действия Лицензии	Согласно оплаченному периоду
Начало срока действия Лицензии	• Автоматически через Личный кабинет; • Через менеджера/службу поддержки – не позднее, чем через 2 (два) рабочих дня с даты

	предоставления Лицензиатом опросного листа на подключение.	
Группа параметров «Период доступности»		
Тариф	**Стандарт**	**Эксперт**
Период доступности ПО	24x7x365 – 24 часа в сутки, 7 дней в неделю, 365 дней в году	
Время работы службы поддержки (обеспечение работоспособности ПО)	8x5 – 8 часов в сутки, с 10:00 до 18:00 (UTC+3), 5 дней в неделю (с понедельника по пятницу при пятидневной рабочей неделе за исключением праздников и выходных дней по законодательству РФ)	24x7x365 – 24 часа в сутки, 7 дней в неделю, 365 дней в году
% (процент) доступности ПО	не менее 98%	не менее 99,5%
Максимальная мощность атаки[1]	Не более 50 Гбит/с для для DDoS-атак, использующих протоколы транспортного уровня OSI Не более 500 000 RPS для атак уровня приложений L7 OSI	
Группа параметров «Обработка обращений»		
Приоритет	**Время реакции**	**Время решения**
Критический (П1) *ПО полностью неработоспособно либо возникла неотложная серьезная проблема, которая вызывает значительные ограничения в эксплуатации и обслуживании ПО*	до 15 минут	до 4 астроном. часа
Высокий (П2) *Неработоспособность одной или нескольких функций ПО, влияющая на бизнес-процессы Лицензиата, либо существенное снижение производительности ПО*	до 30 минут	до 8 астроном. часов
Средний (П3) *Неработоспособность одной или нескольких функций ПО, в целом не влияющая на бизнес-процессы Лицензиата*	до 4 рабочих часов	до 48 астроном. часов
Низкий (П4)	до 8 рабочих часов	до 240 астроном. часов

[1] При атаке на инфраструктуру Лицензиара, обеспечивающую предоставление доступа к ПО, выше указанной мощности Лицензиар не гарантирует работоспособность ПО в принципе и не несет ответственности за причиненный такой атакой ущерб Лицензиату. Под атакой понимается одна атака или серия связанных атак с таким промежутком между атаками, которые не позволяют инфраструктуре сопротивляться каждой из них отдельно.

Консультация по функциональности ПО, установка обновлений и иные мероприятия, требующие планирования и предварительного согласования сроков выполнения.		
Запрос на изменение *Действия, требующие согласования с Лицензиаром и связанные с изменением конфигурации, конфигурационных единиц или настроек технических средств, которые используются ПО.*	до 8 рабочих часов	до 240 астроном. часов
Количество обрабатываемых обращений в календарный месяц	не ограничено	

Обращения и запросы Лицензиата принимаются по следующим каналам связи:

- Электронная почта support@solarspace.pro
- Номер телефона +7 (499) 911-87-08
- Личный кабинет https://my.solarspace.pro/

Приоритет обращения определяется Лицензиатом при его направлении. Приоритет может быть изменен Лицензиаром после оценки специалистом службы поддержки и в процессе работы над обращением, в следующих случаях:

- В случае некорректного выбора приоритета Лицензиатом;
- После предоставления Лицензиаром обходного решения, существенно снижающего влияние на деятельность Лицензиата (устранены препятствия для выполнения бизнес-процессов, выполнение которых обеспечивается поддерживаемым ПО).

При изменении приоритета обращения SLA, установленные для вновь присвоенного приоритета, начинают исчисляться заново с момента фиксации такого изменения приоритета в соответствующей системе учета обращений Лицензиара. Время, затраченное на обработку обращения до момента изменения приоритета, в расчет новых SLA не засчитывается.

В случае отсутствия обратной связи от Лицензиара по предоставленному решению или запросу дополнительной информации в течение 40 календарных дней Лицензиат вправе закрыть обращение и прекратить работу по нему.

4. Заключительные положения

4.1. Ответственность и иные условия

Общие ограничения ответственности:

(а) Лицензиар соглашается с тем, что успешность выполнения мероприятий (включая обеспечение параметров SLA, предусмотренных настоящим документом, соблюдение сроков) зависит, в т.ч., от исполнения Лицензиаром обязанностей по содействию Лицензиату. В случае неисполнения или ненадлежащего исполнения таких обязанностей Лицензиатом Лицензиар не несет ответственности за неисполнение или ненадлежащее исполнение обязательств в рамках настоящего документа.

(б) Лицензиар не несет ответственности за нарушение параметров SLA в период подготовительных действий и до даты предоставления Лицензиатом в полном объеме данных, предусмотренных подразделом «Предоставление доступа к ПО».

(в) Лицензиар не несет ответственности за нарушение параметров SLA при невыполнении Лицензиатом обязанности по смене A-записи DNS доменного имени защищаемого интернет-ресурса. В указанных случаях лицензионное вознаграждение выплачивается Лицензиатом в полном объеме.

(г) Лицензиар несет ответственность исключительно за умышленные нарушения обязательств, а также нарушения, совершенные по грубой неосторожности.

(д) Лицензиар не несет ответственности за наступление и негативные последствия случайных обстоятельств (казуса), находящихся вне зоны ответственности и влияния Лицензиара.

(е) В случае нарушения обязательств Лицензиаром Лицензиат имеет право взыскать реальный ущерб. При этом размер реального ущерба, который может быть взыскан с Лицензиара по всем случаям нарушений в рамках договора, ограничен суммой лицензионного вознаграждения по договору за период, в который произошло нарушение. Любые суммы сверх указанной суммы не подлежат взысканию, за исключением случаев умышленных нарушений.

(ж) Лицензиар отвечает только за работоспособность собственной инфраструктуры, обеспечивающей функционирование ПО. Если иное не установлено в остальной договорной документации, Лицензиар не отвечает за соответствие технических (функциональность, совместимость и т.п.) и юридических характеристик (договорные условия использования результатов интеллектуальной деятельности и т.п.) инфраструктуры/оборудования Лицензиата требованиям настоящего документа.

(з) Лицензиар осуществляет обеспечение работоспособности только в отношении своего ПО. В обеспечение работоспособности ПО не входит обслуживание инфраструктуры Лицензиата и/или третьих лиц, а также добавление новых функций, изменение логики работы ПО.

(и) Лицензиар прилагает максимальные усилия для обеспечения бесперебойной, точной и безошибочной работы ПО в целом и его отдельных функциональных возможностей. Лицензиат соглашается с тем, что Лицензиар не может предоставить заверений или гарантий в отношении соответствия ПО (как в целом, так и отдельных составляющих, функций, функциональности и т.п.) конкретным целям и ожиданиям Лицензиата, а также не может предоставить в отношении ПО и иных обязательств никаких иных гарантий, прямо не указанных в настоящем документе и Иной договорной документации (например, работоспособность выпущенных SSL/TLS сертификатов).

(к) Лицензиар обеспечивает доступность ПО в соответствии с Таблицей 1, за исключением периодов аварийных и профилактических работ. Время профилактических работ не считается временем недоступности ПО и компенсации не подлежит.

(л) В рамках предоставления Лицензии Лицензиар не осуществляет деятельность по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет, и не выступает в качестве провайдера хостинга.

(м) Лицензиар выполняет те мероприятия, которые описаны в договорной документации. Иные мероприятия/работы/услуги, в том числе дополнение функционала, описанного в настоящем документе, являются правом, а не обязанностью Лицензиара, и могут быть выполнены по отдельному соглашению.

(н) Исключительные права на созданные Лицензиаром в процессе исполнения обязательств результаты интеллектуальной деятельности принадлежат Лицензиару и не отчуждаются в пользу Лицензиата. Порядок и условия передачи таких результатов интеллектуальной деятельности Лицензиату (включая необходимость заключения отдельного лицензионного договора) определяются единолично Лицензиаром.

4.2. Поручение на обработку персональных данных

В связи с предоставлением Лицензии и обеспечением функционирования ПО Лицензиат поручает Лицензиару обработку персональных данных:

(а) Работников и/или представителей Лицензиата:
- фамилия, имя, отчество (при наличии); должность и структурное подразделение работника; информация о полномочиях представителя; номер телефона; адрес электронной почты; логин, использующийся для доступа к корпоративной учетной записи в Личном кабинете; история действий в Личном кабинете.
- Способы обработки персональных данных: сбор, получение, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), блокирование, удаление, уничтожение.

(б) Пользователей интернет-ресурсов (включая, но не ограничиваясь, сайт(ы) в сети Интернет и мобильное(ые) приложение(я)) Лицензиата:
- фамилия, имя, отчество (при наличии); IP-адрес; номер телефона; адрес электронной почты; данные учетной записи пользователя (имя пользователя); сведения, которые пользователь указал о себе в формах обратной связи и формах регистрации на интернет-ресурсах Лицензиата; персональные данные, содержащиеся в документах, которые пользователь загрузил на интернет-ресурсах Лицензиата, включая цифровые образы таких документов; сетевой трафик пользователя на интернет-ресурсах Лицензиата; действия пользователя на интернет-ресурсах Лицензиата, включая историю таких действий (логи); информация об устройстве и браузере пользователя, посредством которых осуществляется доступ на интернет-ресурсы Лицензиата.
- Способы обработки персональных данных: (1) в части всех персональных данных: получение, передача (предоставление, доступ); (2) в части логов: запись, систематизация, накопление, хранение, извлечение, удаление, уничтожение.

Обработка персональных данных осуществляется автоматизировано.

Лицензиат соглашается с тем, что в рамках исполнения настоящего поручения для достижения цели их обработки персональные данные могут быть переданы Лицензиаром:

- Обществу с ограниченной ответственностью «РТК Информационная безопасность» (место нахождения 125009, г. Москва, пер. Никитский, д. 7, стр. 1, эт. 2, пом. I, ком. 58, ОГРН 1167746458065, ИНН 7704356648);
- лицам, оказывающим Лицензиару услуги по хранению и обработке данных.

Срок действия настоящего поручения: с момента передачи Лицензиатом персональных данных Лицензиару до полного исполнения Договора.

Обязанности Лицензиара:

(а) Соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных.

(б) Обеспечивать конфиденциальность персональных данных, в том числе не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом или настоящим поручением.

(в) Принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных, в том числе:

- При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.
- Обеспечивать безопасность персональных данных при их обработке и принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, а также принимать иные меры, предусмотренные статьями 18.1 и 19 Закона о персональных данных.
- По запросу Лицензиата в течение срока действия поручения, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Лицензиата требований, установленных в соответствии с частью 3 статьи 6 Закона о персональных данных.
- В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, уведомить Лицензиата в порядке и сроки, установленные частью 3.1 статьи 21 Закона о персональных данных.

(г) Уничтожить персональные данные на основании распоряжения Лицензиата в случае достижения цели их обработки.

Обязанности Лицензиата:

(а) Лицензиат заверяет и гарантирует, что он выполнил все требования законодательства о персональных данных в отношении субъектов, обработка персональных данных которых поручается Лицензиару, в том числе, но не ограничиваясь, получил согласия таких лиц на поручение обработки их персональных данных Лицензиару в предусмотренных законодательством случаях. По письменному запросу Лицензиара Лицензиат в течение 5 (пяти) рабочих дней обязуется предоставить достаточные и исчерпывающие доказательства правомерности обработки и передачи персональных данных Лицензиару.

(б) Своевременно, а именно с соблюдением сроков, установленных Законом о персональных данных, информировать Лицензиара о необходимости принятия мер по уточнению, блокированию, прекращению обработки, уничтожению или удалению персональных данных, обработка которых поручена Лицензиару.

(в) Любые сообщения Лицензиата, включая уведомления и запросы, в рамках настоящего поручения подлежат направлению (передаче) по адресу места нахождения Лицензиара с обязательным направлением копии такого сообщения в электронной форме по адресу: privacy@rt-solar.ru.