ДОКУМЕНТАЦИЯ SOLAR SPACE

SOLAR Space

Оглавление

Описание платформы Solar Space

Облачная платформа киберзащиты Solar Space — продукт компании "Солар", предназначенный для бизнеса любого масштаба. Сервисы платформы просты в установке и доступны по стоимости даже для небольших компаний.

Описание платформы

Solar Space — комплекс автоматизированных сервисов информационной безопасности. Только самый востребованный функционал "из коробки" без переплаты за ненужные опции.

Основные принципы платформы:

1. **Автоматизация** — сервисы сразу готовы к работе без долгой настройки.
2. **Быстрота** — подключение онлайн за 20 минут в личном кабинете даже во время атаки.
3. **Доступность**:
   - от **1200** рублей в месяц за защиту сайта от DDoS
   - от **1800** рублей в месяц за защиту сайта от DDoS и ботов
   - от **7800** рублей в месяц за защиту сайта от DDoS, ботов и веб-атак, направленных на взлом

Стоимость указана с учетом НДС.

Доступные сервисы

На платформе развернуты сервисы веб-защиты WEB AntiDDoS, WEB Antibot на базе ML-алгоритма и WAF Lite. Они предназначены для защиты сайтов и веб-приложений от DDoS-атак, ботов и веб-атак, направленных в том числе на взлом ресурсов и кражу чувствительных данных. Подробная информация о сервисах доступна по ссылкам:

- Общее описание веб-защиты
- AntiDDoS
- Antibot
- WAF Lite
- Тарифы на веб-защиту

Дополнительно для всех пользователей доступно сканирование веб-ресурса сервисом ScanGuard на предмет фишинговых сайтов и утечек электронной почты.

Сервисы в разработке

1. **Security Awarness** для обучения сотрудников навыкам кибербезопасности.
2. **Zero Day** для глубокого сканирования ИТ-инфраструктуры на уязвимости.
3. **SEG** для защиты электронной почты от фишинга и спама.
4. **Security DNS** для обеспечения безопасности DNS-запросов.
5. **StressTest** для тестирования устойчивости системы к экстремально высоким нагрузкам.

Если вы заинтересованы в том, чтобы протестировать новые сервисы в числе первых, напишите на почту solarspace@rt-solar.ru. С вами свяжется менеджер.

Варианты сотрудничества и предоставления платформы

Solar Space предполагает 3 варианта реализации: облачную SaaS-версию, PaaS с покупкой лицензий, on-prem для установки в периметре компании. Если вас интересует PaaS или on-prem, напишите на почту solarspace@rt-solar.ru. С вами свяжется менеджер для обсуждения условий сотрудничества.

Кроме того, любая компания может без вложений и первоначального взноса стать партнером Solar Space и расширить свой продуктовый портфель за счет востребованных услуг киберзащиты. Это позволит зарабатывать на продаже наших сервисов, созданных командой экспертов с профильным опытом в информационной безопасности. Если вы заинтересованы в партнерстве, также напишите на почту solarspace@rt-solar.ru. С вами свяжется менеджер.

Начало работы с платформой

Для защиты ваших ресурсов необходимо выполнить следующие действия:

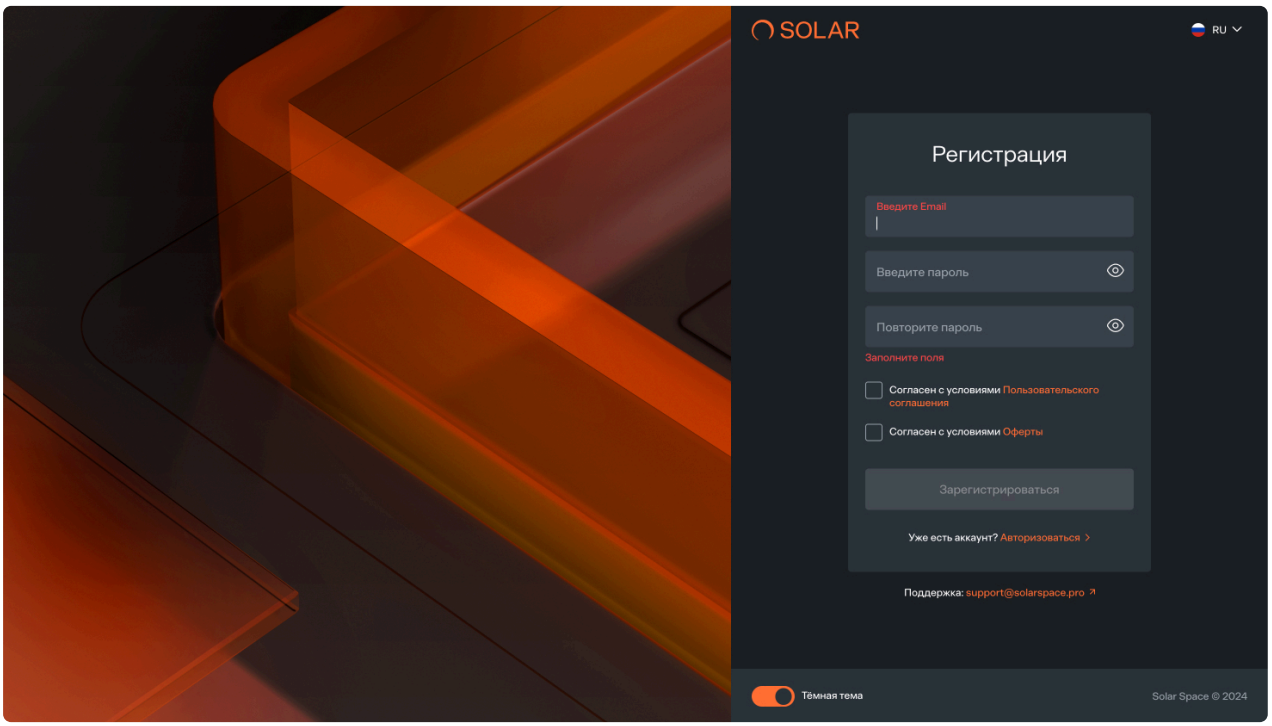
1. Перейдите по ссылке https://my.solarspace.pro/ и зарегистрируйтесь на платформе Solar Space
2. Подтвердите свой аккаунт
3. Выберите сервисы, которые вы хотите подключить
4. Оплатите сервисы
5. Создайте свой первый ресурс
6. Настройте верификацию и перенаправление трафика для защиты вашего ресурса
7. Добавьте SSL-сертификат для безопасного шифрования ваших данных

Регистрация

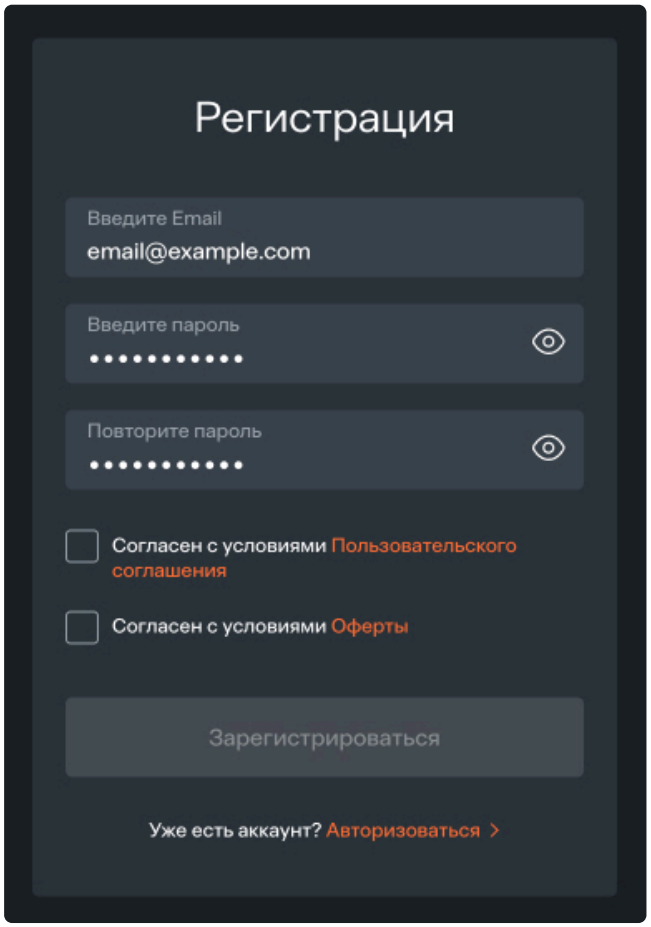
Если у вас уже есть аккаунт, вы можете авторизоваться.

Если вы новый пользователь, выполните следующие действия для регистрации на платформе:

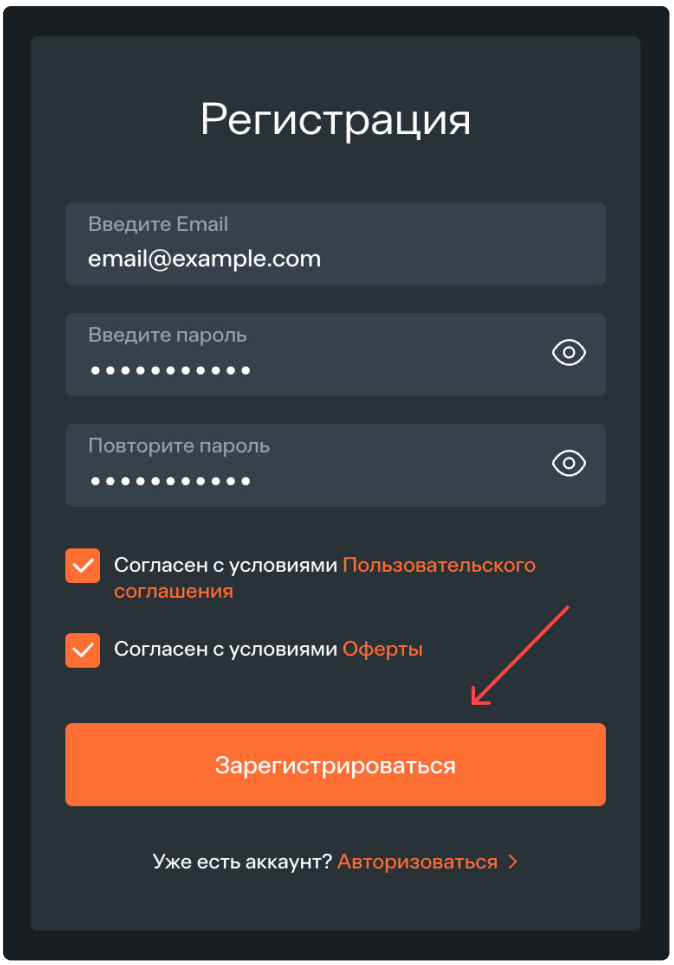
1. Перейдите на страницу регистрации – https://my.solarspace.pro/sign-up
   На форме размещаются обязательные поля для заполнения: "Введите Email", "Введите пароль", "Повторите пароль" и кнопка "Зарегистрироваться".



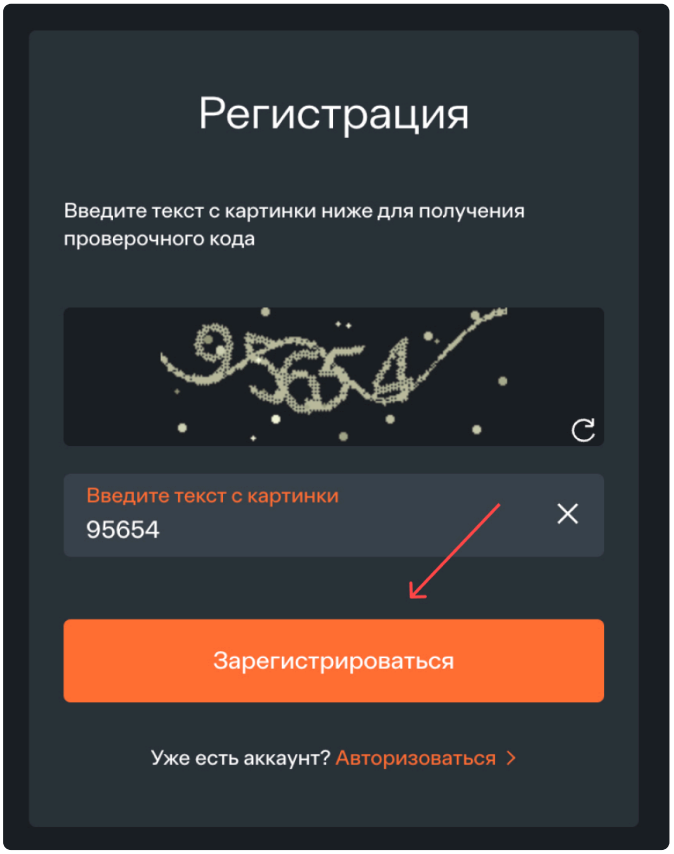
2. Заполните поля в соответствии с требованиями:
   - Email должен содержать символ @ и точку, разделяющую уровни домена (например, email@example.com)
   - Пароль должен содержать не менее 8 символов и включать как минимум одну цифру и буквы разных регистров



3. Подтвердите согласие на условия Пользовательского соглашения и Оферты. Нажмите на кнопку "Зарегистрироваться".



4. Далее вам необходимо пройти капчу. Так система убедится, что форму заполняет реальный пользователь. Для этого введите текст с картинки в соответствующее поле и нажмите кнопку "Зарегистрироваться".

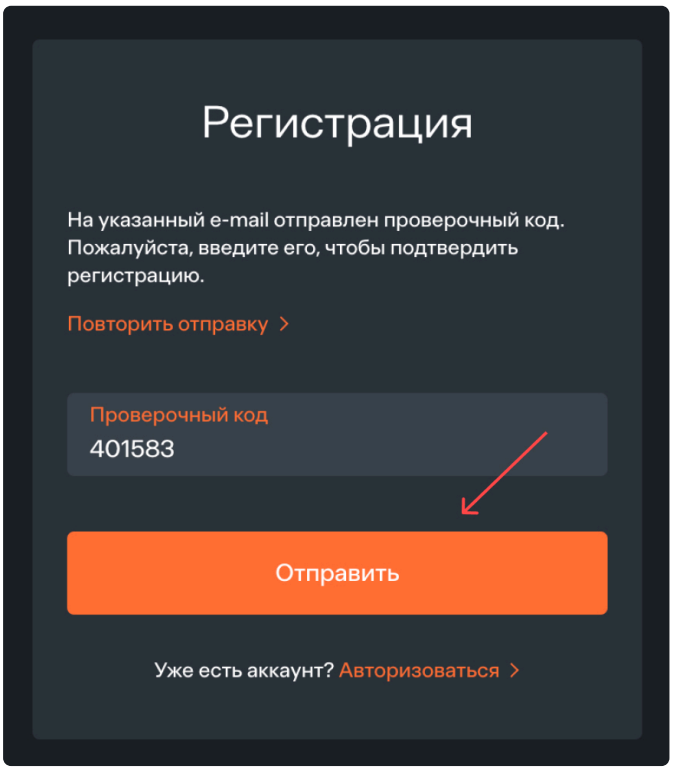


5. На ваш адрес электронной почты, указанный на шаге 3, придет письмо с кодом подтверждения регистрации. Откройте его и скопируйте 6-значный код из сообщения.

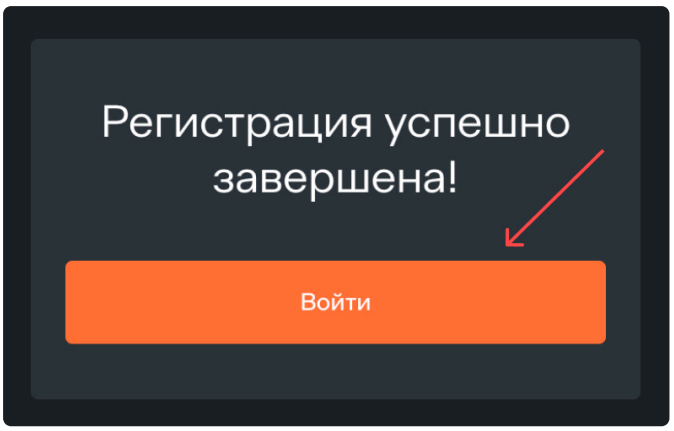
Если данного письма нет в папке "Входящие", проверьте папку "Спам". В случае, если письмо не пришло, перепроверьте введенную электронную почту и отправьте код повторно,

нажав на кнопку "Повторить отправку". Запросить повторный код можно 1 раз в 60 секунд. Код действителен в течение 10 минут.

6. Вставьте 6-значный проверочный код в соответствующее поле и нажмите на кнопку "Отправить".



7. После успешного подтверждения кода появится сообщение об успешной регистрации.



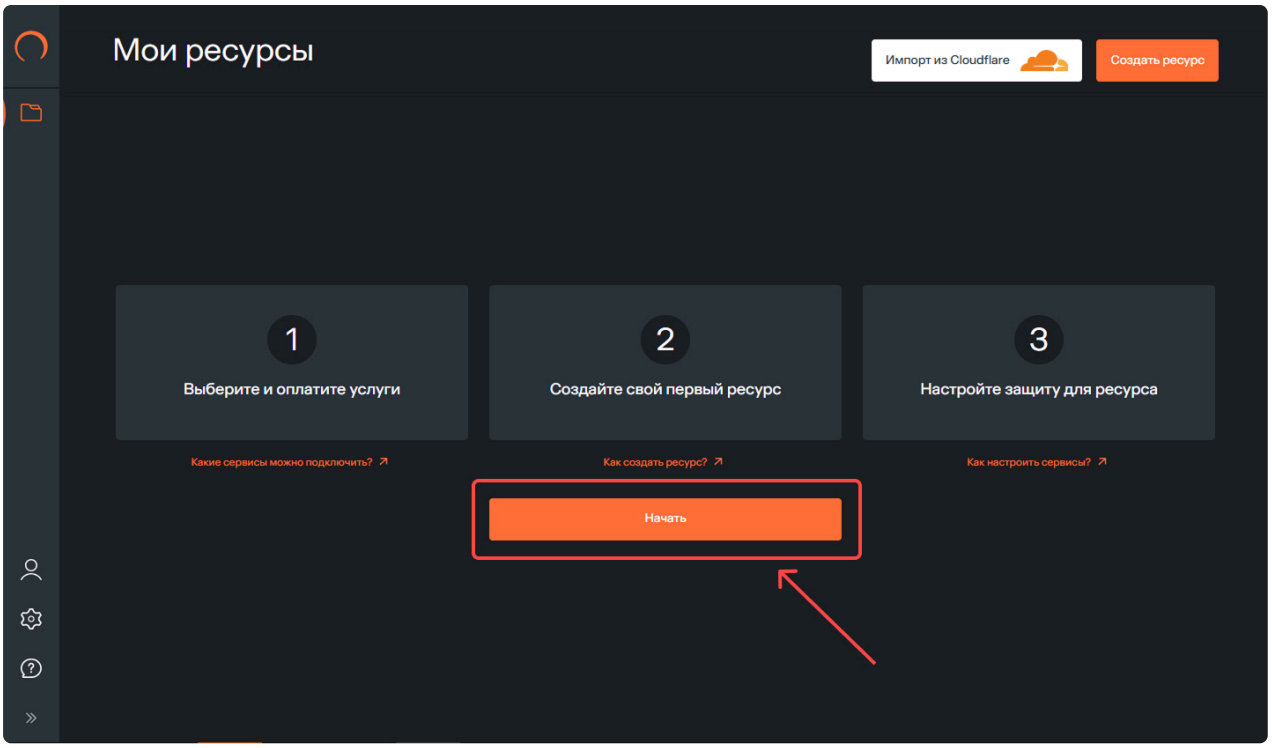
8. При нажатии на кнопку "Войти" откроется страница с авторизацией. Используйте свой email и пароль для входа в личный кабинет.

Подтверждение аккаунта

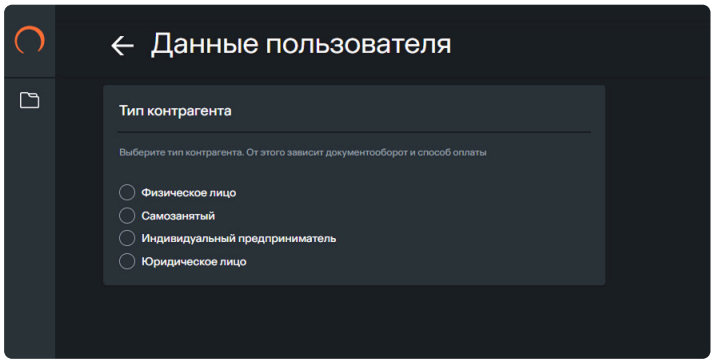
Подтверждение аккаунта — обязательный этап подключения Веб-защиты, без которого невозможна оплата и дальнейшая настройка защиты. Для подтверждения аккаунта необходимо заполнить данные пользователя. От этого зависит документооборот и способ оплаты.

> **Обратите внимание**
>
> Оплата по карте доступна для типов контрагента "Физическое лицо" и "Самозанятый". Пользователям с типом контрагента "Индивидуальный предприниматель" и "Юридическое лицо" доступна оплата по коду выбранных услуг через поддержку Solar Space support@solarspace.pro

1. На главной странице после регистрации нажмите на кнопку "Начать".



2. Выберите тип контрагента:
   - Физическое лицо
   - Самозанятый
   - Индивидуальный предприниматель
   - Юридическое лицо

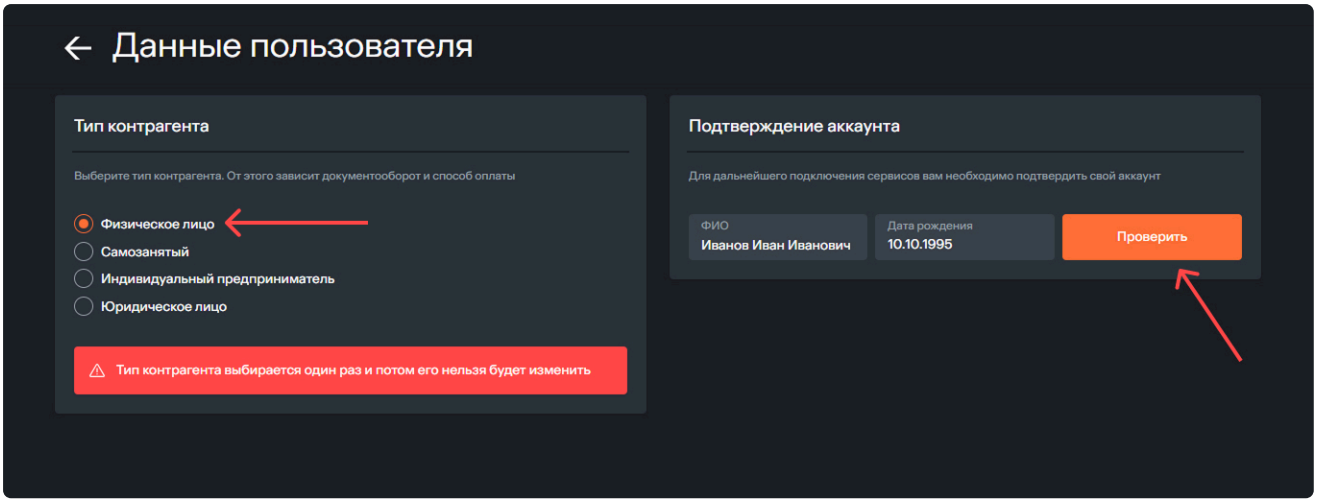


3. Заполните обязательные поля в зависимости от выбранного типа контрагента.
4. Проверьте данные и нажмите на кнопку "Подтвердить" для перехода к подключению сервисов Веб-защиты.

> ⚠ Важно
>
> Тип контрагента выбирается один раз и потом его нельзя будет изменить

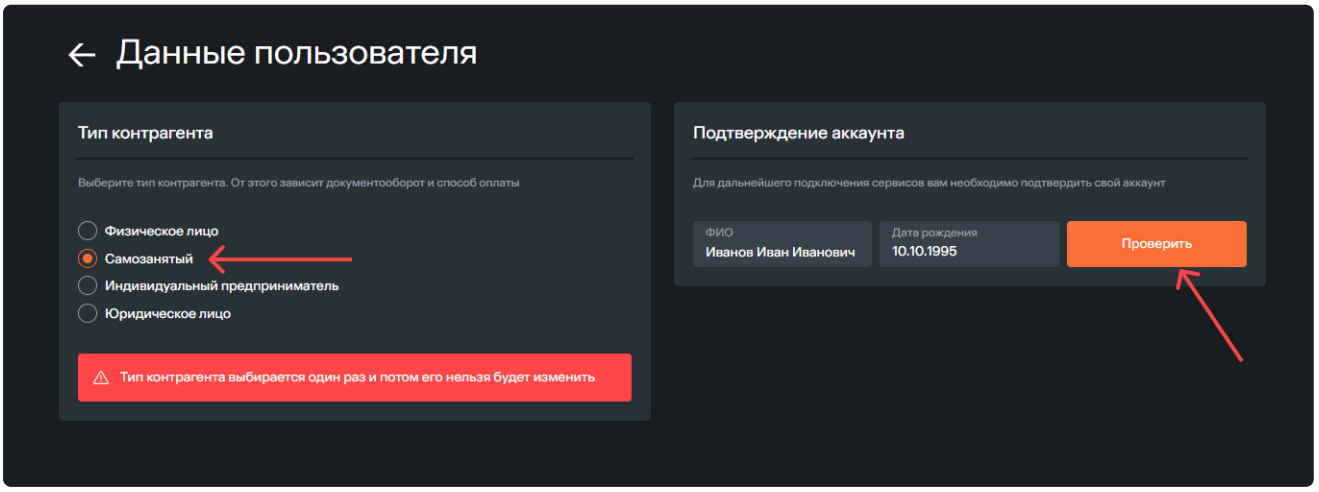
Физическое лицо

Для типа контрагента "Физическое лицо" заполните поля "ФИО" и "Дата рождения" и нажмите на кнопку "Проверить".



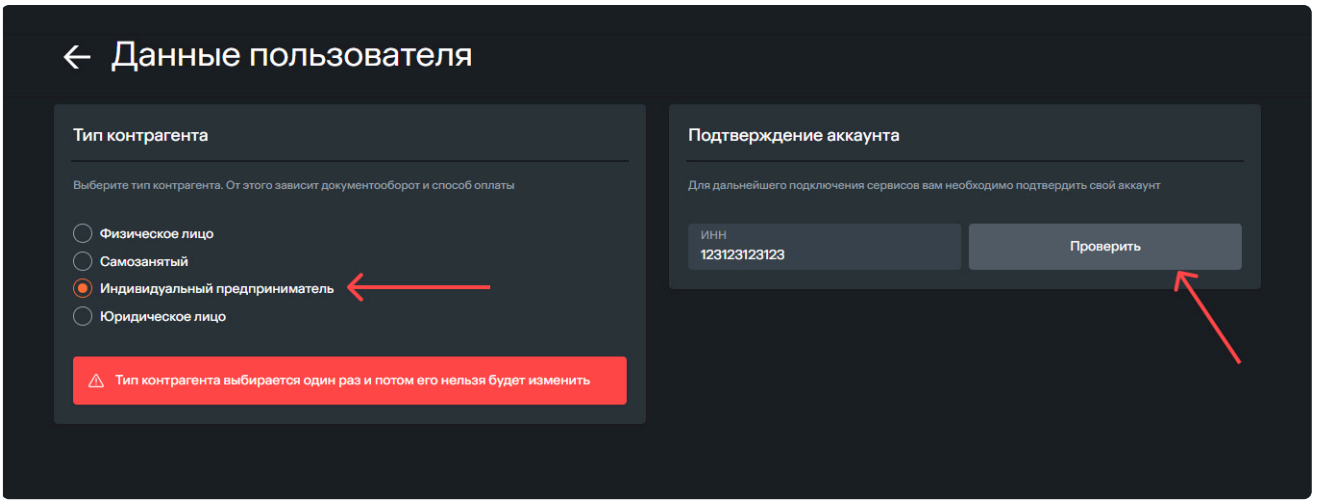
Самозанятый

Для типа контрагента "Самозанятый" заполните поля "ФИО" и "Дата рождения" и нажмите на кнопку "Проверить".



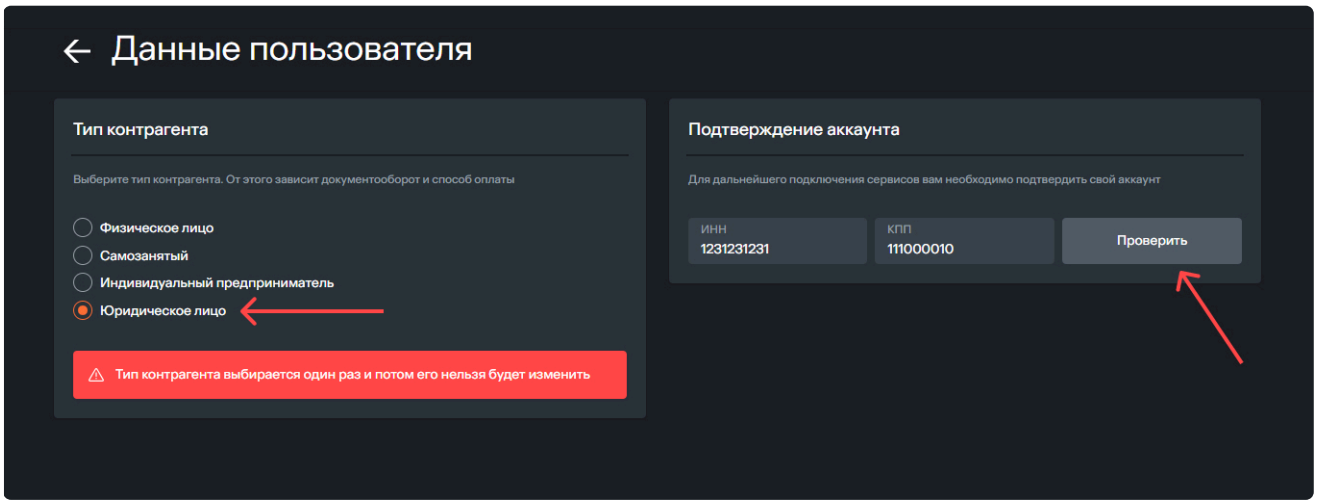
Индивидуальный предприниматель

Для типа контрагента "Индивидуальный предприниматель" введите ИНН, состоящий из 12 цифр, и нажмите на кнопку "Проверить". Система проверит информацию по вашему ИНН и если он зарегистрирован, то отобразятся данные вашей организации.



Юридическое лицо

Для типа контрагента "Юридическое лицо" введите ИНН, состоящий из 10 цифр, и КПП, состоящий из 9 цифр, и нажмите на кнопку "Проверить". Система проверит информацию по вашему ИНН и КПП, и если они зарегистрированы, то отобразятся данные вашей организации.


Данные пользователя
Тип контрагента
Выберите тип контрагента. От этого зависит документооборот и способ оплаты
Физическое лицо
Самозанятый
Индивидуальный предприниматель
Юридическое лицо
Тип контрагента выбирается один раз и потом его нельзя будет изменить
Подтверждение аккаунта
Для дальнейшего подключения сервисов вам необходимо подтвердить свой аккаунт
ИНН
1231231231
КПП
111000010
Проверить

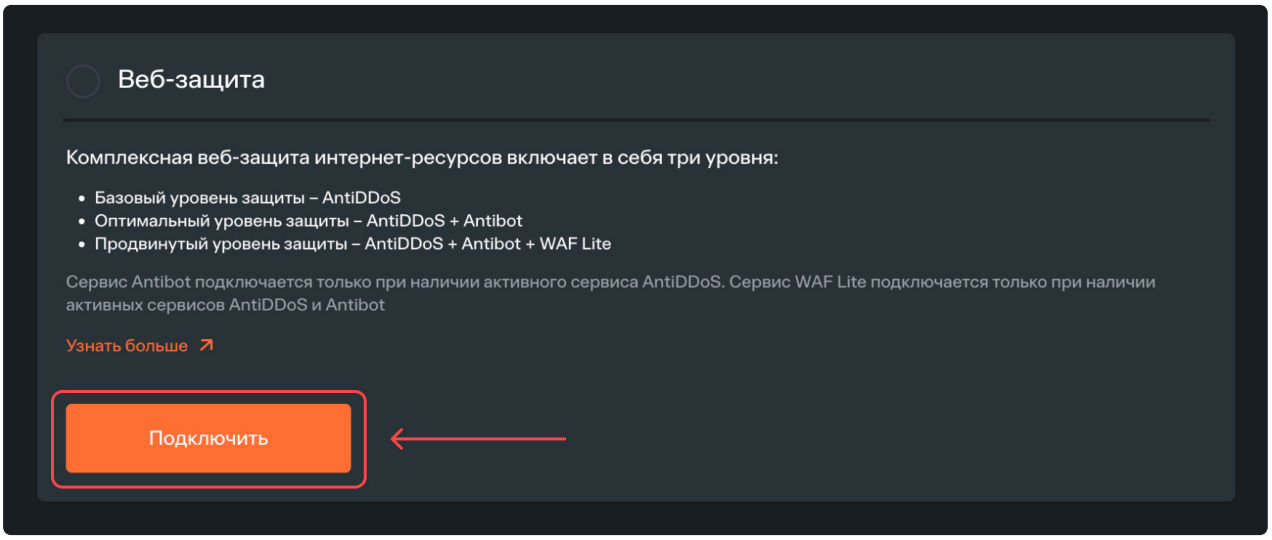
Подключение сервисов

На этой странице вы можете выбрать уровни защиты для подключения сервисов:

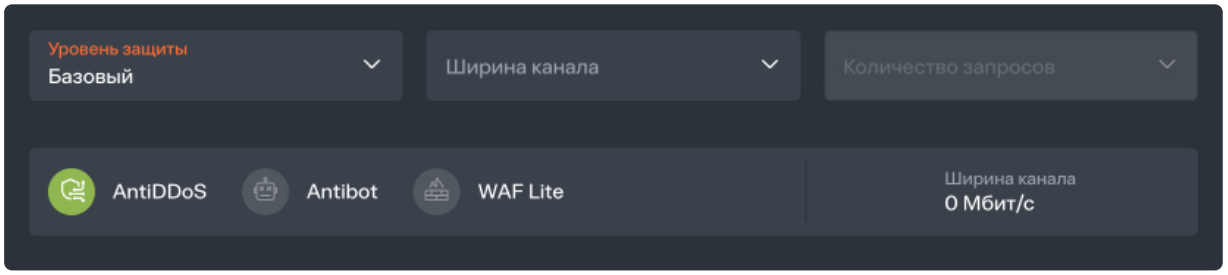
- Базовый уровень защиты – сервис AntiDDoS
- Оптимальный уровень защиты – сервисы AntiDDoS + Antibot
- Продвинутый уровень защиты – сервисы AntiDDoS + Antibot + WAF Lite

Для подключения сервисов выполните следующие действия:

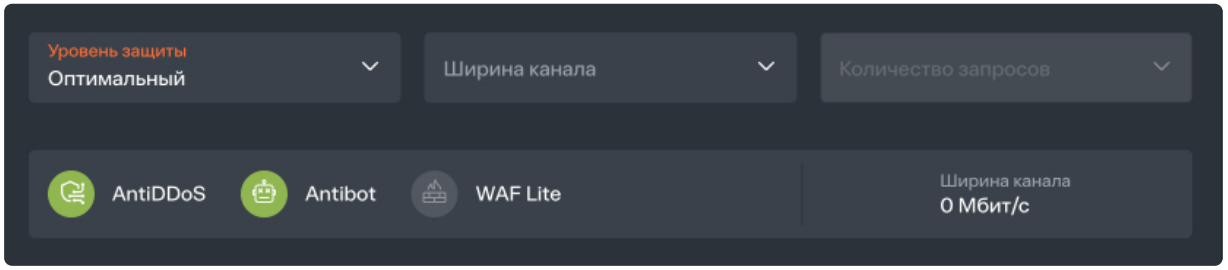
1. Нажмите на кнопку "Подключить" в тарифе "Веб-защита" после подтверждения аккаунта.



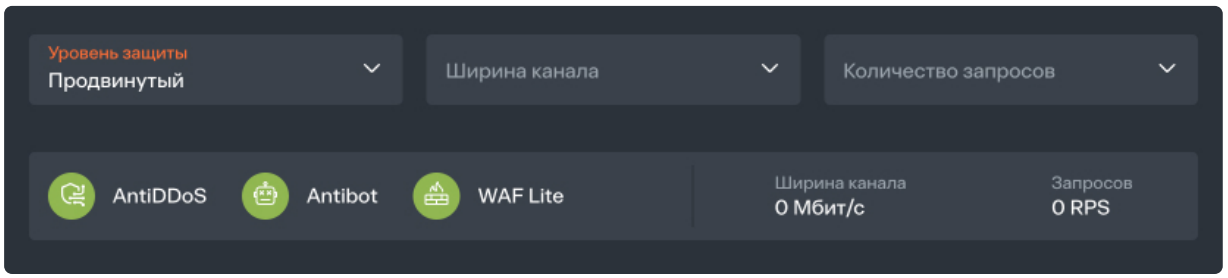
2. Укажите желаемый уровень защиты:
   - При выборе базового уровня защиты доступен только сервис AntiDDoS
   - При выборе оптимального уровня защиты доступны сервисы AntiDDoS + Antibot
   - При выборе продвинутого уровня защиты доступны сервисы AntiDDoS + Antibot + WAF Lite
3. После выбора уровня защиты поля "Ширина канала" и "Количество запросов" станут видимыми.
   - Для базового уровня защиты доступна возможность изменения параметра "Ширина канала"



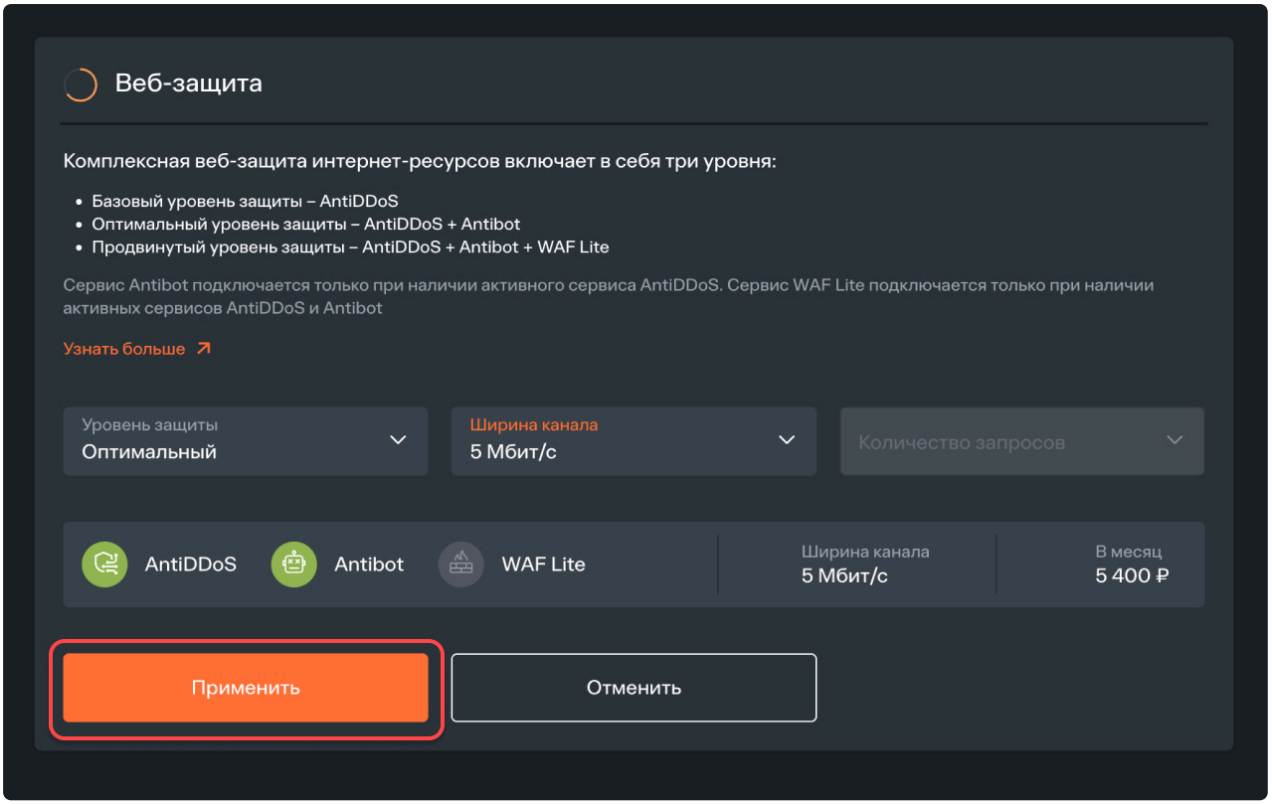
- Для оптимального уровня защиты доступна возможность изменения параметра "Ширина канала"



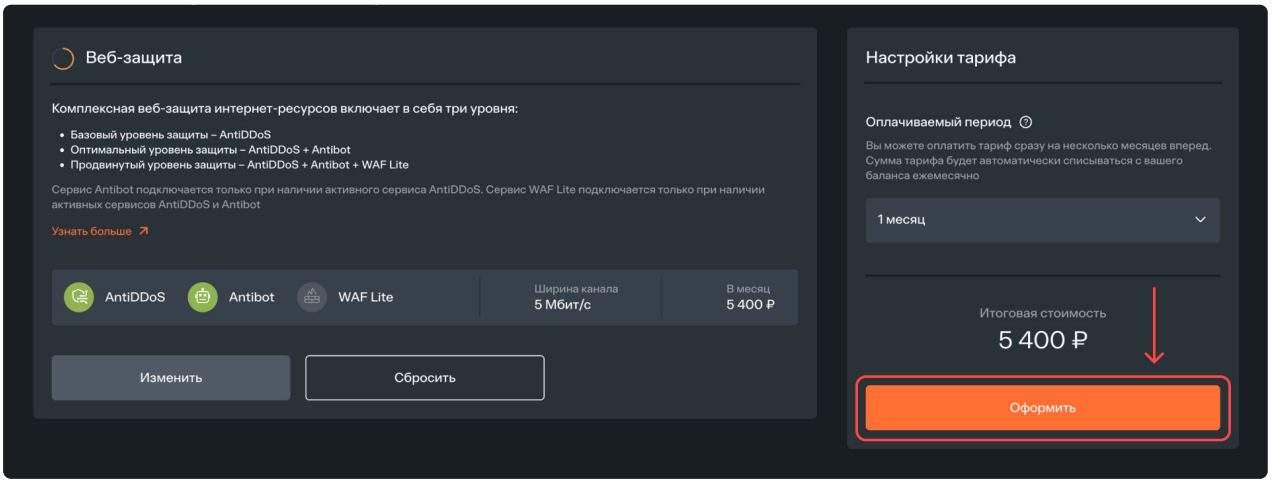
- Для продвинутого уровня защиты доступна возможность изменения параметров "Ширина канала" и "Количество запросов"



4. Убедитесь, что параметры тарифа настроены верно, и нажмите на кнопку "Применить".



5. На форме "Настройки тарифа" выберите оплачиваемый период – количество оплачиваемых месяцев по подключенному тарифу (от 1 до 12 месяцев) и нажмите на кнопку "Оформить".

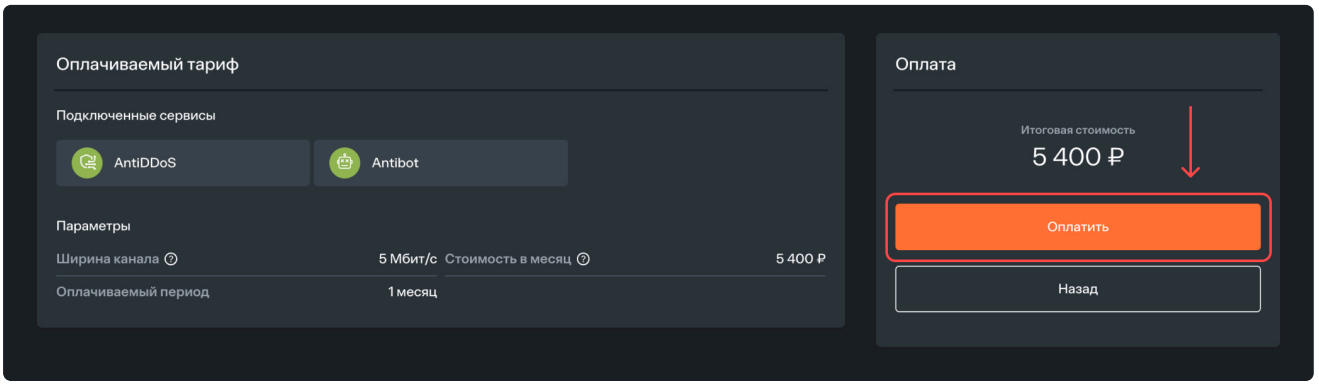


6. После выбора сервисов перейдите к шагу оплаты.

Оплата

Оплата — следующий шаг после подключения сервисов.

На странице оплаты вы сможете увидеть добавленные сервисы по тарифу Веб-защита, выбранные параметры тарифа и итоговую стоимость в разделе "Оплата". Проверьте информацию по выбранным ранее сервисам и нажмите на кнопку "Оплатить" для перехода к оплате.



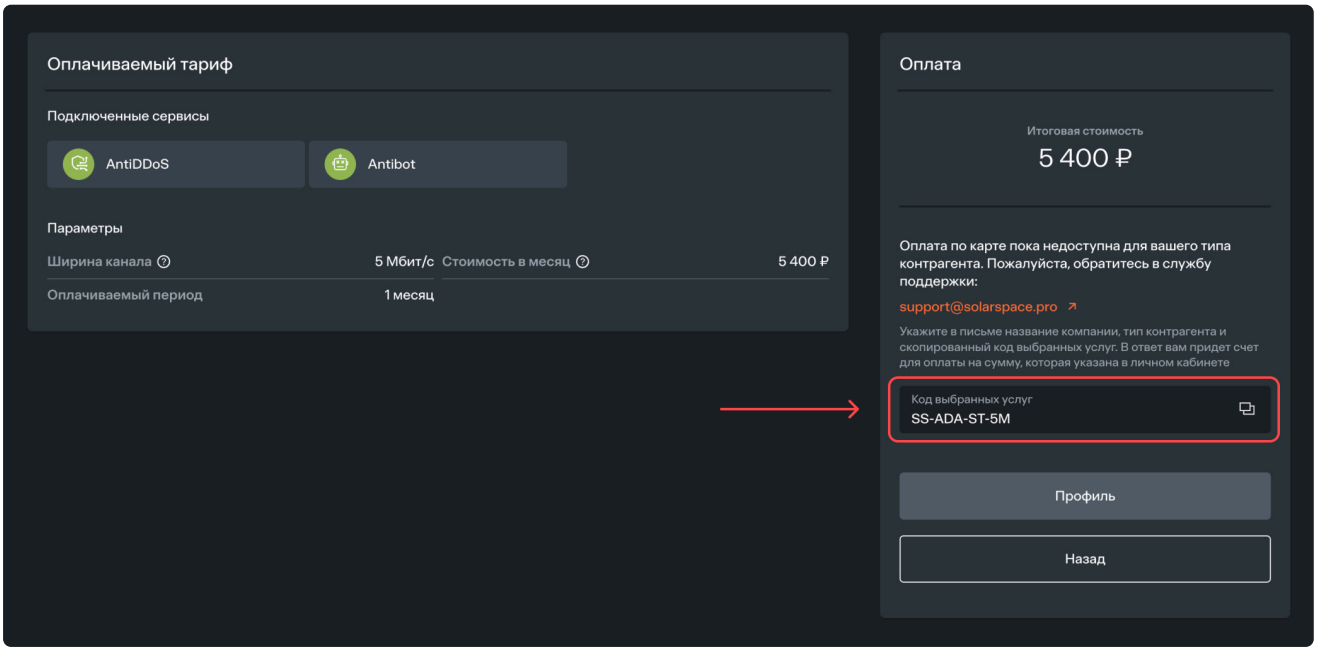
> Обратите внимание
>
> Способ оплаты зависит от выбранного типа контрагента

Оплата для юридических лиц и ИП

Пользователям с типом контрагента "Индивидуальный предприниматель" или "Юридическое лицо" доступна оплата по коду выбранных услуг. Для этого скопируйте его, напишите в поддержку Solar Space solar@rt-solar.ru и укажите в письме:

- Название вашей компании
- Тип контрагента
- Скопированный код выбранных услуг

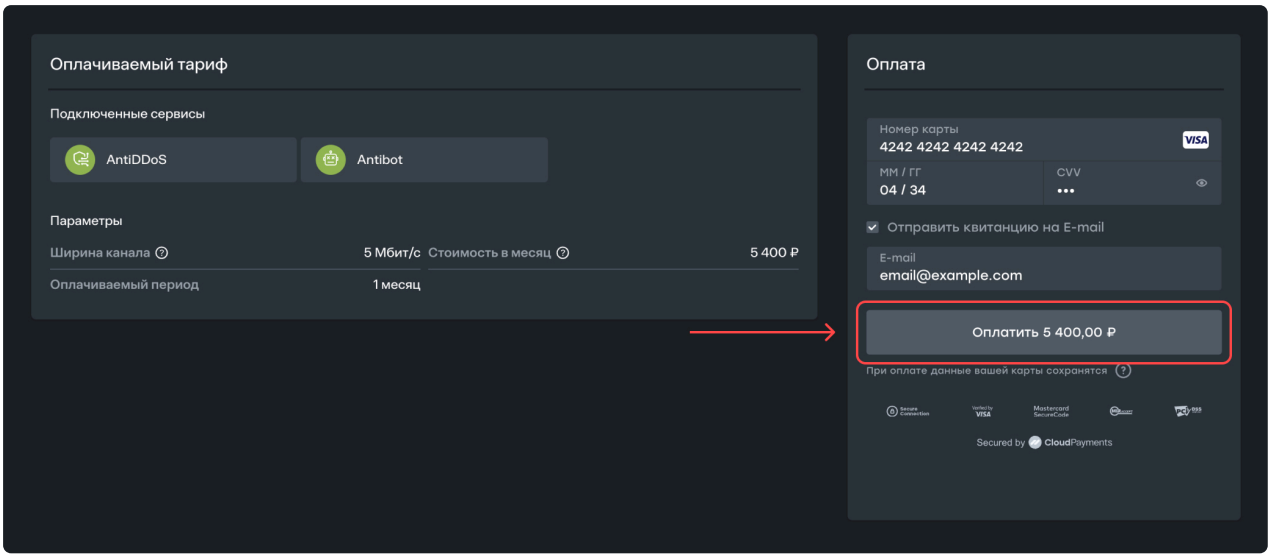
В ответ вам придет счет для оплаты на сумму, которая указана в личном кабинете при офомлении Веб-защиты.



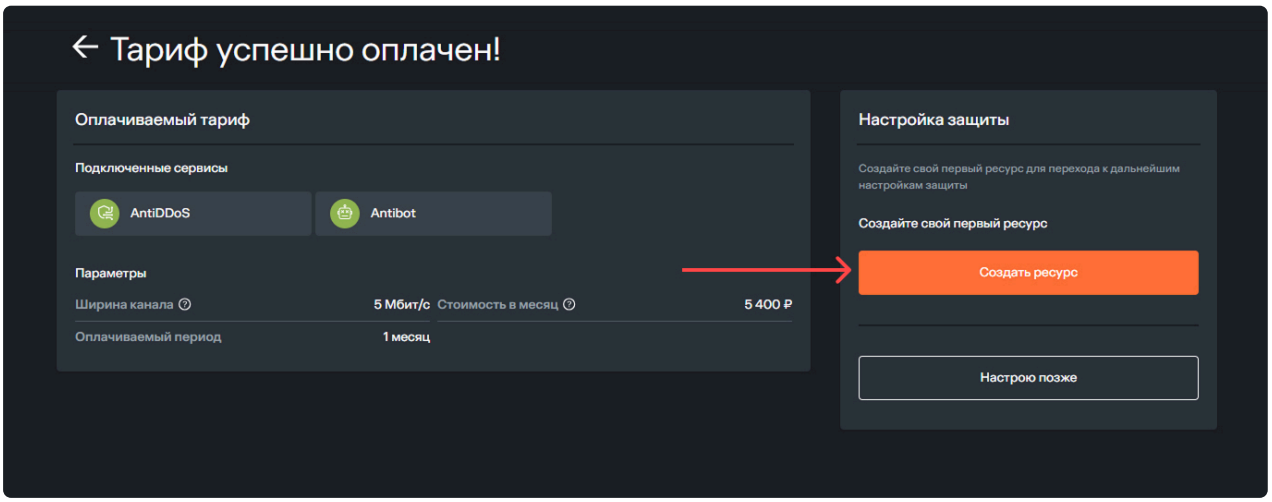
Оплата для физических лиц и самозанятых

Пользователям с типом контрагента "Физическое лицо" и "Самозанятый" доступна оплата по карте.

1. На форме оплаты введите данные своей банковской карты (поле email заполняется автоматически вашем адресом электронной почты, указанным при регистрации).
2. После ввода данных нажмите на кнопку "Оплатить".



3. На странице успешно оплаченного тарифа вы можете создать ресурс.

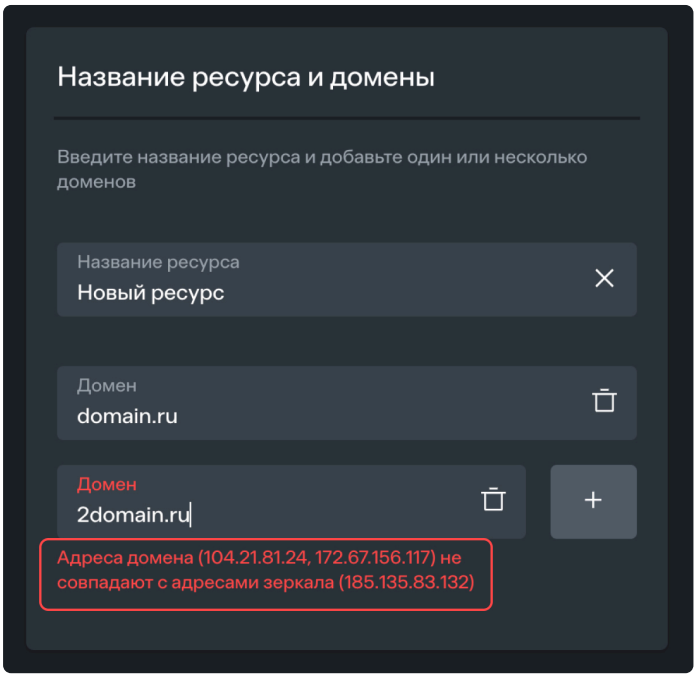

← Тариф успешно оплачен!
Оплачиваемый тариф
Подключенные сервисы
AntiDDoS
Antibot
Параметры
Ширина канала
5 Мбит/с
Стоимость в месяц
5 400 ₽
Оплачиваемый период
1 месяц
Настройка защиты
Создайте свой первый ресурс для перехода к дальнейшим настройкам защиты
Создайте свой первый ресурс
Создать ресурс
Настрою позже

Создание ресурса

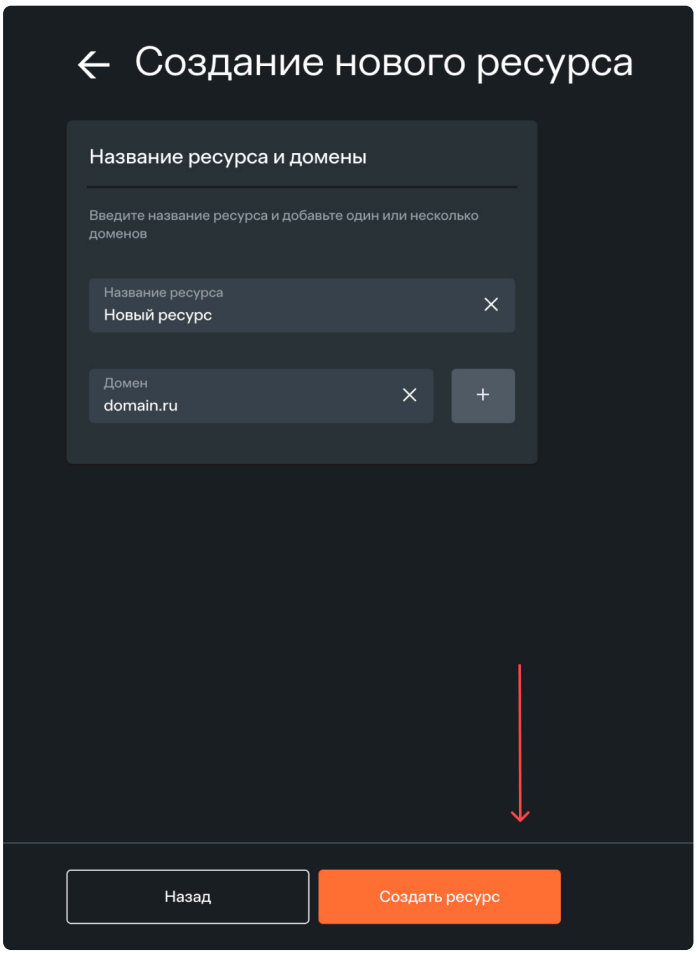
Для создания ресурса выполните следующие действия:

1. На странице создания ресурса заполните обязательные поля в соответствии с требованиями:
    - Домен должен быть зарегистрирован в системе доменных имен (DNS)
    - Домен должен быть уникальный
    - Домен должен иметь корректный формат (например example.com)
    - При добавлении второго домена их адреса должны совпадать

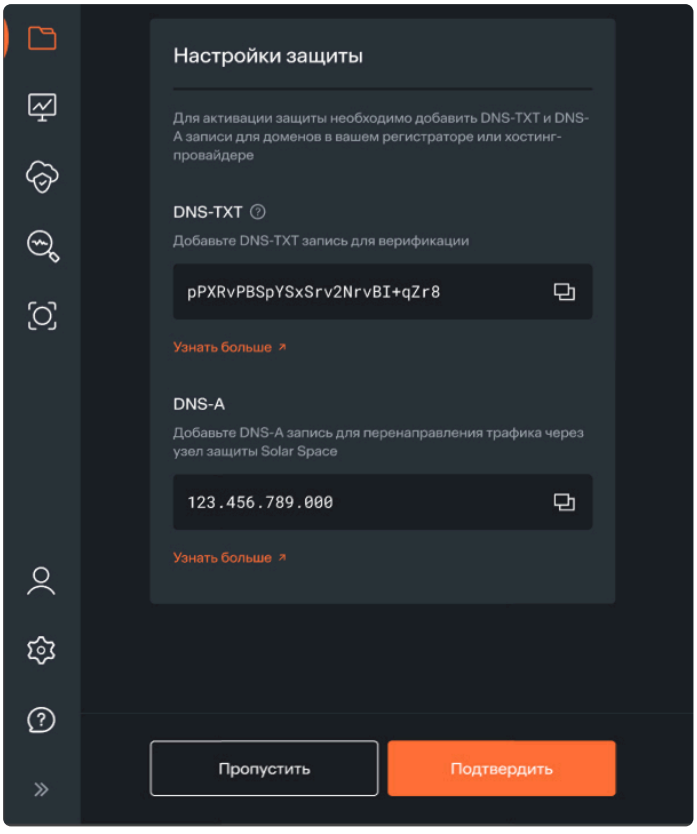
Если у вашего ресурса есть еще один домен, нажмите на кнопку "Добавить домен" (адреса доменов должны совпадать).



3. Нажмите на кнопку "Создать ресурс".



4. Далее вам необходимо его верифицировать и настроить перенаправление трафика, чтобы ваши домены были защищены и весь трафик проходил через безопасный узел защиты Solar Space.



5. После добавления DNS-TXT и DNS-A записей в ваш регистратор или хостинг-провайдер, нажмите на кнопку "Подтвердить" для отправки запроса на обновление DNS-записей.

Верификация

Верификация — обязательный этап в защите ресурса, она подтверждает право собственности на домен.

Как это работает?

Для верификации используется TXT-запись в системе DNS, которая содержит уникальную информацию, связанную с доменом. TXT-запись нужно скопировать из личного кабинета Solar Space и добавить в настройки вашего DNS регистратора или хостинг-провайдера. Это доказывает, что именно вы являетесь владельцем вашего доменного имени.

Добавление TXT-записи не нарушит и не затормозит работу вашего сайта.

> Обратите внимание
>
> Без верификации вы не сможете активировать защиту своих ресурсов, и ваш ресурс будет отображаться в статусе "Не подтвержден". DNS-TXT запись нужно добавлять для каждого домена. Если у вас несколько доменов, вы можете добавить TXT-запись через API вашего регистратора или хостинг-провайдера.

Верификацию можно пройти:

- Сразу после создания ресурса (при оплаченном тарифе "Веб-защита" для Физических лиц и Самозанятых)
- Со страницы настроек ресурса для пользователей с любым типом контрагента

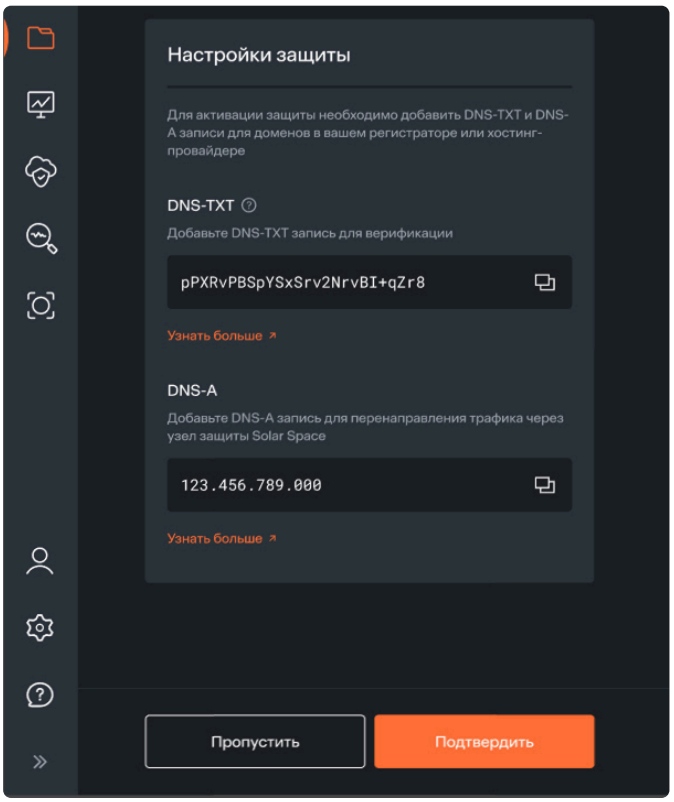
После создания ресурса

В блоке "Настройки защиты" есть два поля с DNS-записями:

- DNS-TXT запись необходима для верификации
- DNS-A запись необходима для настройки перенаправления трафика

Сначала нужно пройти шаг верификации. Для этого выполните следующие действия:

1. На странице "Настройки защиты" после создания ресурса скопируйте представленную DNS-TXT запись Solar Space.



2. Перейдите на сайт вашего регистратора или хостинг-провайдера и откройте раздел управления доменами.

> **Обратите внимание**
>
> Раздел управления доменами в интерфейсах различных регистраторов или хостинг-провайдеров может называться по-разному, например: "Домены", "Управление доменами" или "DNS-настройки"

3. Если у вас несколько доменов, выберите тот, для которого вы хотите добавить TXT-запись. Убедитесь, что вы открыли нужный домен.
4. Перейдите в редактирование DNS-записей и добавьте новую запись типа TXT, которая была скопирована в личном кабинете Solar Space.

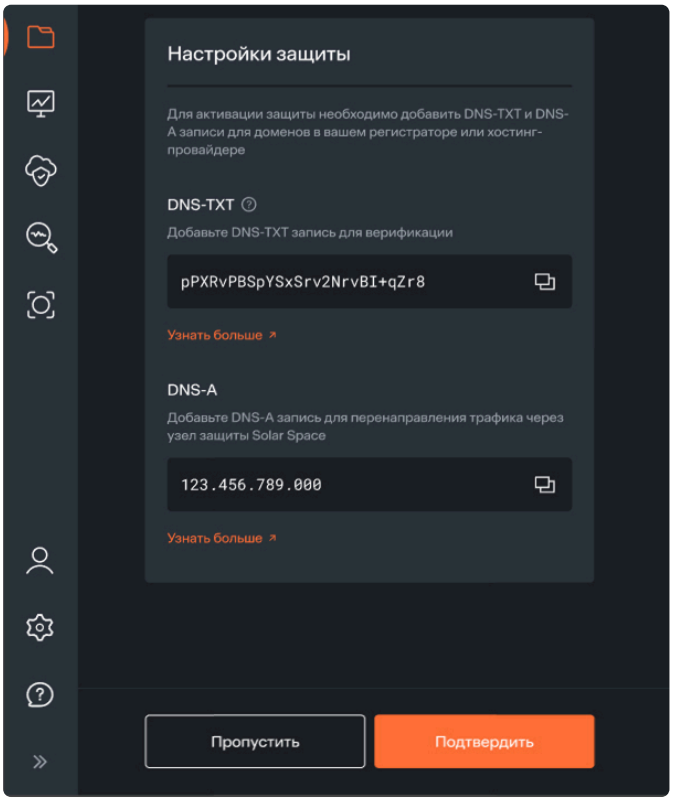
Type	Name	Content	Proxy status	TTL	Actions
TXT	domain.ru	"sc-domain-verificatio...	DNS only	Auto	Edit

Если у вас в личном кабинете Solar Space ресурс содержит несколько доменов, TXT-запись нужно добавить для каждого из них, как на примере ниже.

TXT	domain2.ru	"sc-domain-verificatio...	DNS only	Auto	Edit
TXT	domain3.ru	"sc-domain-verificatio...	DNS only	Auto	Edit
TXT	domain.ru	"sc-domain-verificatio...	DNS only	Auto	Edit

5. Сохраните изменения и вернитесь в личный кабинет Solar Space.

6. После этого настройте перенаправление трафика через смену DNS-A записи.



7. **Прежде чем нажать на кнопку "Подтвердить", нужно добавить в настройки своего регистратора или хостинг-провайдера обе записи: DNS-TXT и DNS-A.**

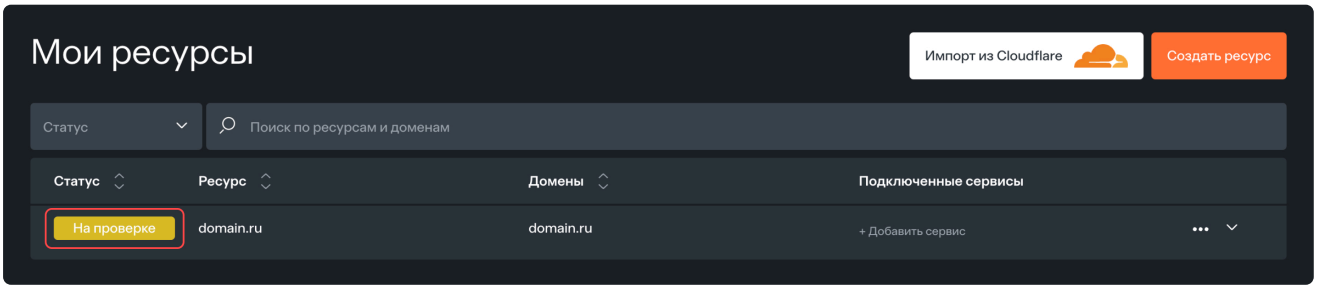
> Обратите внимание
>
> Если у вас появились вопросы, ознакомьтесь с подробной информацией о том, как добавить TXT-записи для регистратора: Инструкция для Timeweb

На странице ресурса

Верифицировать ресурс также можно со страницы настроек ресурса.

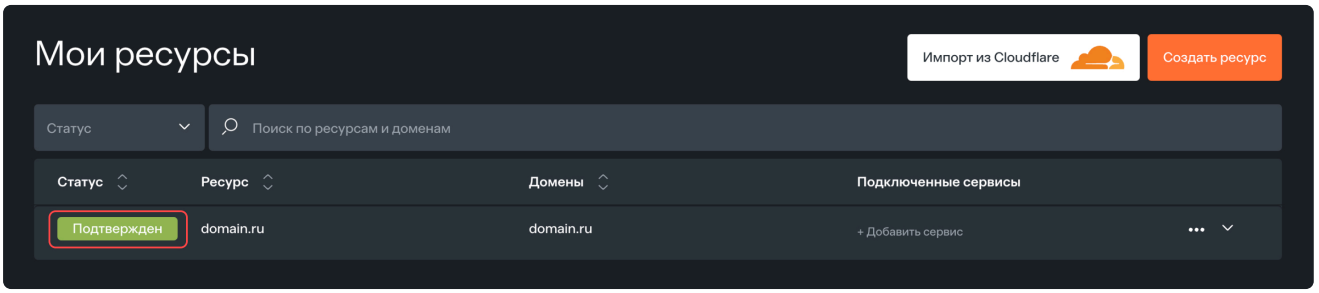
Статусы

Пока идет верификация, ресурс в личном кабинете будет отображаться со статусом "На проверке".

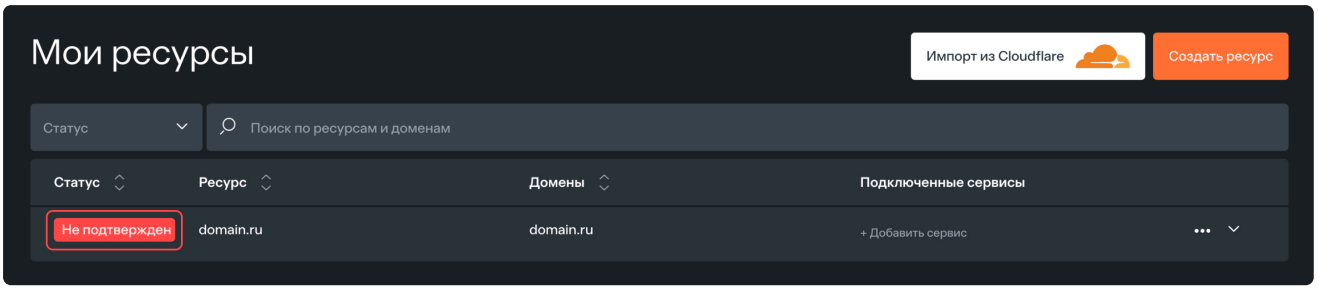


После успешного завершения процесса верификации статус ресурса изменится на "Подтвержден".

> **Обратите внимание**
>
> Активировать сервисы защиты можно только для ресурсов со статусом "Подтвержден"



Если верификация не пройдена, у ресурса будет статус "Не подтвержден". Для ресурсов с таким статусом защиту активировать нельзя. Подробнее о возможных ошибках при верификации читайте здесь.



Постановка домена под защиту

Для постановки домена под защиту по тарифам Веб-защиты, необходимо настроить перенаправление трафика.

Как это работает?

Перенаправление трафика означает изменение существующей DNS-A-записи у домена в вашем регистраторе или хостинг-провайдере на A-запись, которая содержит IP-адрес защищенного сервера Solar Space. Остальные A-записи и AAAA-записи необходимо удалить. Это нужно, чтобы весь трафик проходил через один IP-адрес, что является безопасным узлом фильтрации для всех входящих запросов к вашему домену.

Для перенаправления трафика через сервер защиты Solar Space ваш домен должен быть верифицирован**.**

> ⚠ Важно!
>
> Без смены DNS-TXT и DNS-A записей защита домена не активируется

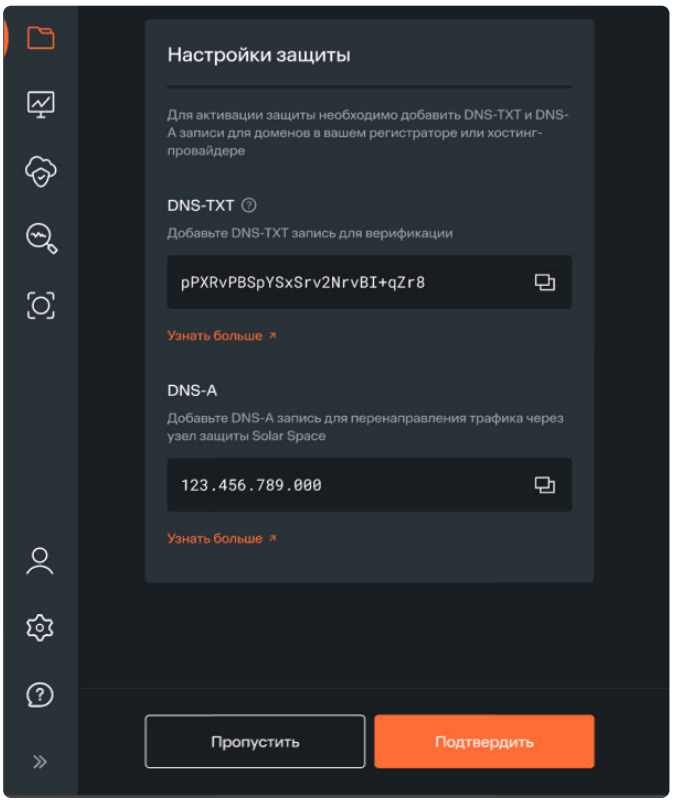
Перенаправление трафика можно настроить:

- Сразу после создания ресурса (при оплаченном тарифе "Веб-защита" для Физических лиц и Самозанятых)
- На вкладке "Домен и SSL" в разделе Веб-защиты для пользователей с любым типом контрагента

Настройка после создания ресурса

Добавьте DNS-A запись после добавления DNS-TXT записи, чтобы настроить перенаправление трафика. Для этого выполните следующие действия:

1. На странице "Настройки защиты" после создания ресурса скопируйте представленную DNS-A запись Solar Space.



2. Перейдите на сайт вашего DNS-регистратора или хостинг-провайдера и откройте раздел управления доменами.

> **Обратите внимание**
>
> Раздел управления доменами в интерфейсах различных регистраторов или хостинг-провайдеров может называться по-разному, например: "Домены", "Управление доменами" или "DNS-настройки"

3. Если у вас несколько доменов, выберите тот, для которого хотите добавить A-запись. Убедитесь, что вы открыли нужный домен.
4. Перейдите в редактирование DNS-записей и измените A-запись вашего домена на ту, которую скопировали в личном кабинете Solar Space.

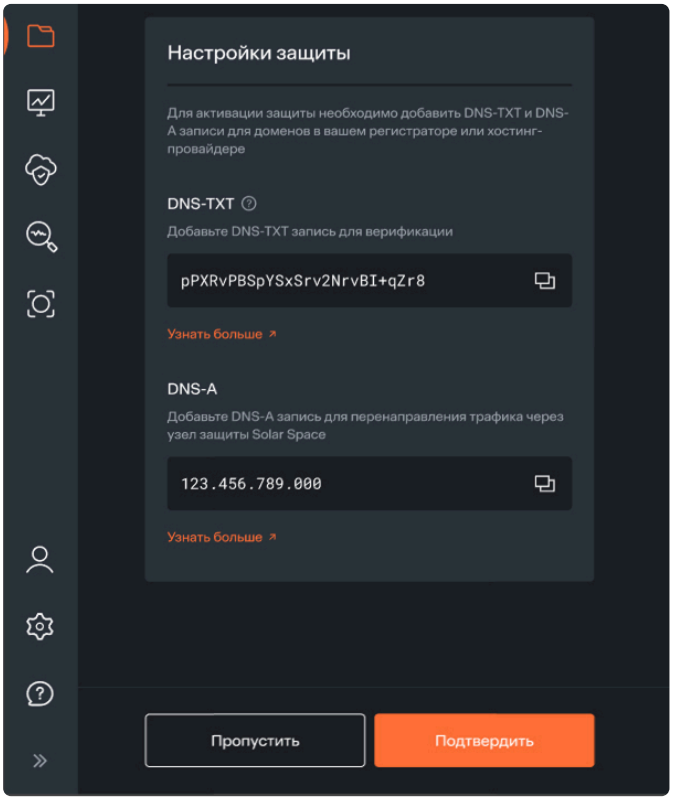
Хост	Тип	Значение	TTL	Дата	+ фильтр
api	A	195.18.27.150		2024-12-05 14:07:35	

5. Если у вас в личном кабинете Solar Space ресурс содержит несколько доменов, A-запись нужно добавить для каждого из них.

Хост	Тип	Значение	TTL	Дата	+ фильтр
@	A	195.18.27.150		2024-12-05 14:07:31	
api	A	195.18.27.150		2024-12-05 14:07:35	
mail	A	195.18.27.150		2024-12-05 14:07:38	

> ⚠ Важно!
>
> Убедитесь, что в настройках DNS у вас для каждого домена только одна A-запись, скопированная из личного кабинета Solar Space. Остальные A-записи и AAAA-записи необходимо удалить, чтобы трафик проходил через узел фильтрации Solar Space

6. Сохраните изменения и вернитесь в личный кабинет Solar Space.
7. **Прежде чем нажать на кнопку "Подтвердить", убедитесь, что добавили в настройки своего регистратора или хостинг-провайдера обе записи:** DNS-TXT **и DNS-A.**



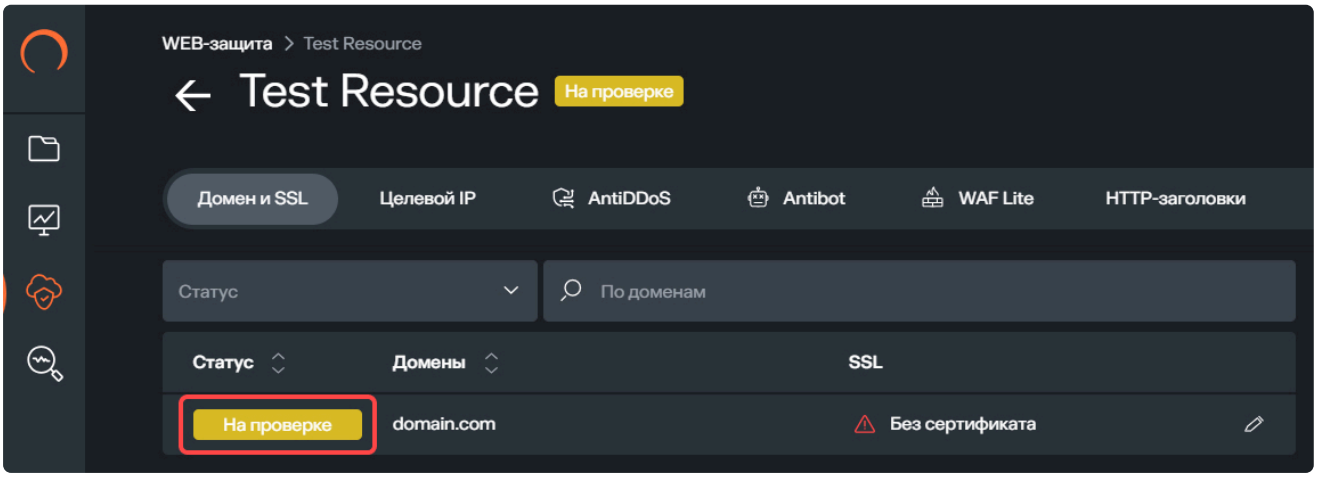
8. После нажатия на кнопку "Подтвердить" система запрашивает у вашего регистратора или хостинг-провайдера обновленные DNS-записи. Обычно обновление занимает не более 1 часа, но в некоторых случаях может произойти позже. Одной из причин может быть высокое значение для параметра TTL в настройках регистратора или хостинг-провайдера.

Настройка на странице ресурса

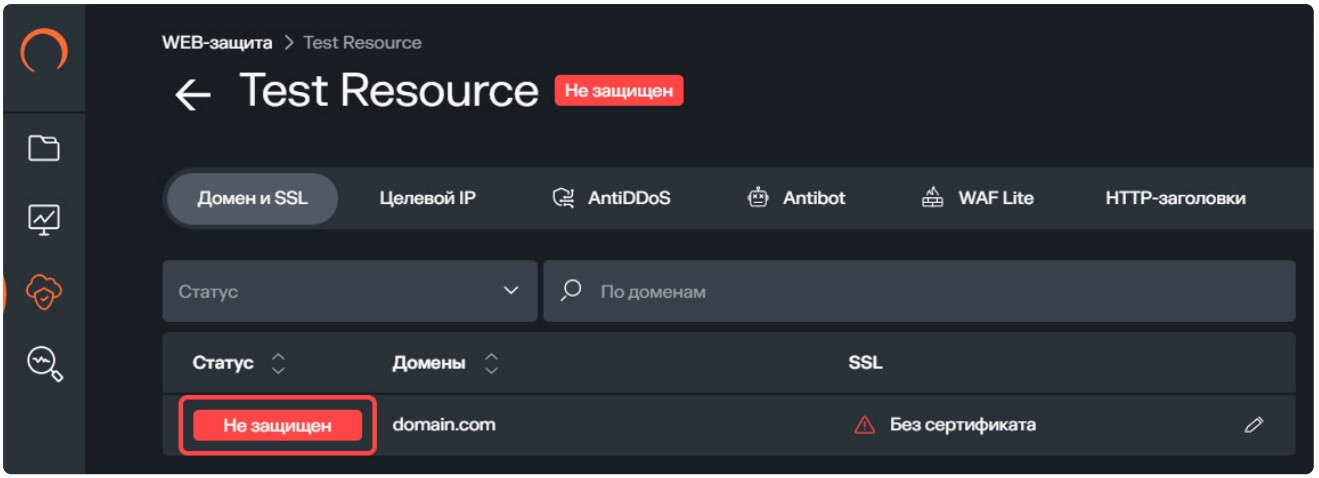
Перенаправление трафика также можно настроить на вкладке "Домен и SSL" в разделе Веб-защиты.

Статусы

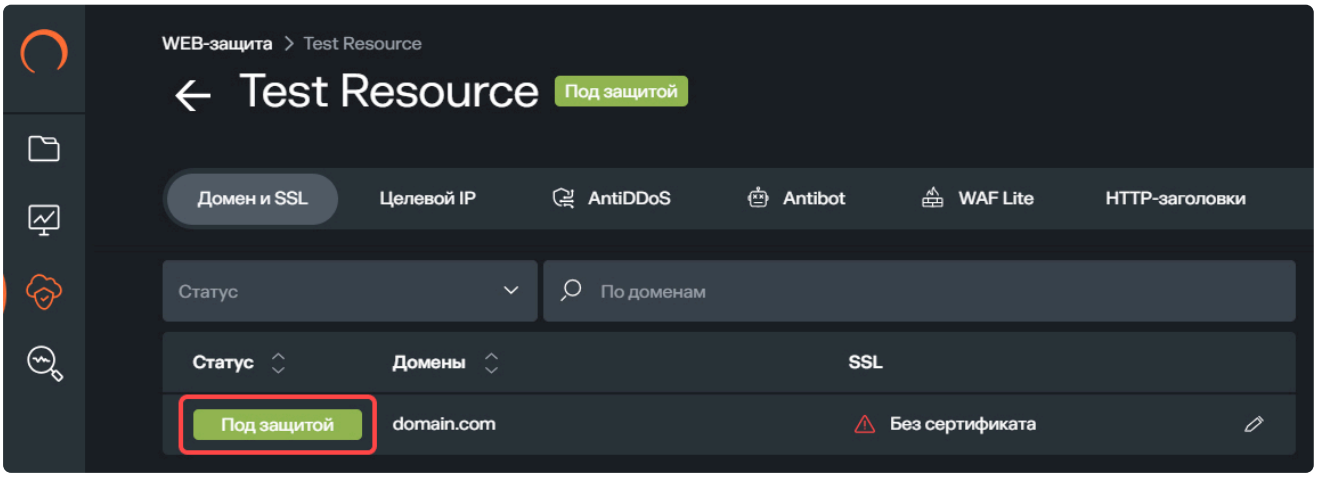
Пока идет процесс обновления DNS-записей, домен на странице "Веб-защита" будет отображаться со статусом "На проверке".



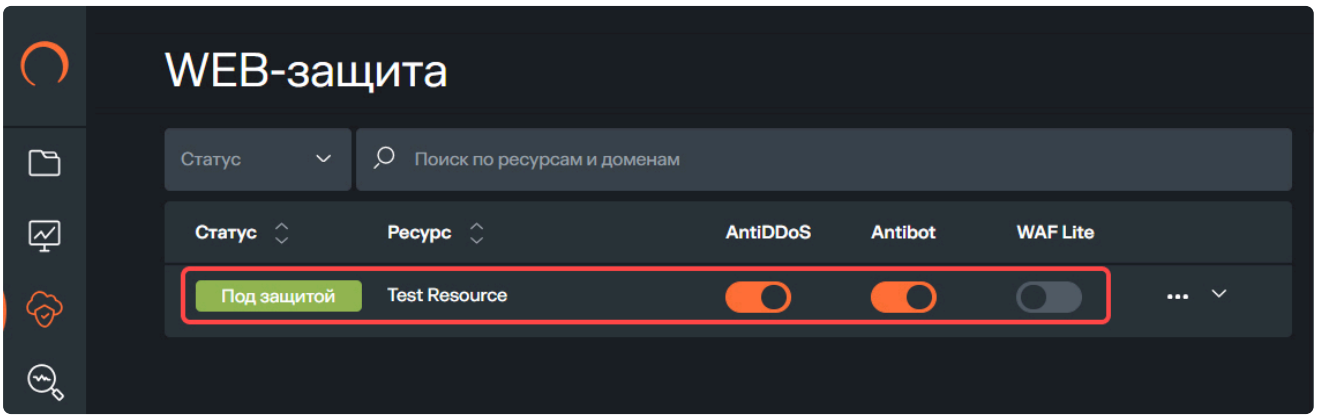
Если через какое-то время вы увидели, что статус домена "На проверке" изменился на статус "Не защищен", то перепроверьте DNS-A-запись в хостинг-провайдере. Убедитесь, что она соответствует DNS-A-записи Solar Space и повторите попытку подтверждения перенаправления трафика. Подробнее о возможных ошибках при перенаправлении трафика читайте здесь.

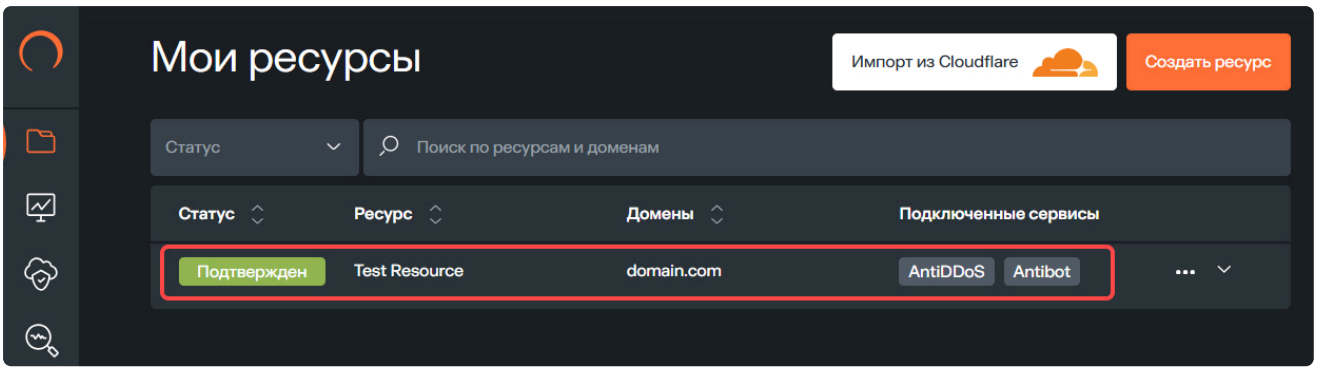


Если статус домена "Под защитой", значит, трафик успешно перенаправлен через узел фильтрации Solar Space, и подключенные вами услуги Веб-защиты активны.



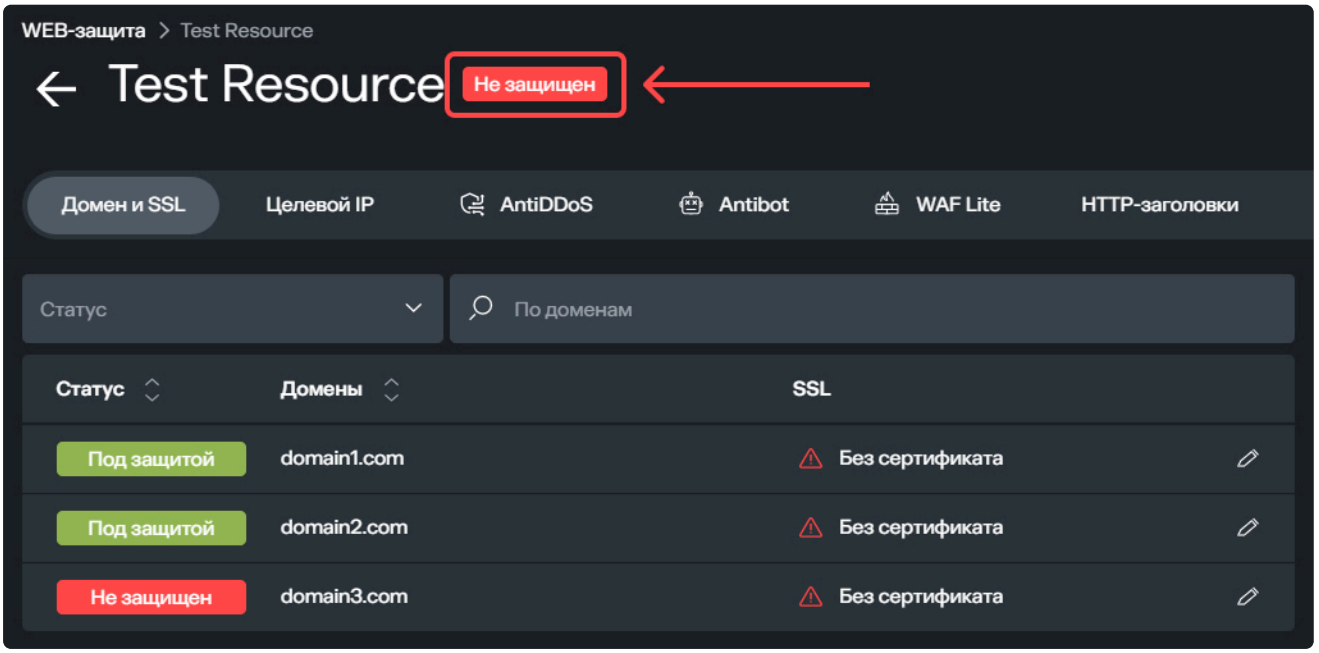
Ресурсы с актуальными сервисами и статусами отображаются на страницах "Веб-защита" и "Мои ресурсы".





Обратите внимание

Если у ресурса несколько доменов, и хотя бы один из них не защищен, то статус всего ресурса будет "Не защищен"

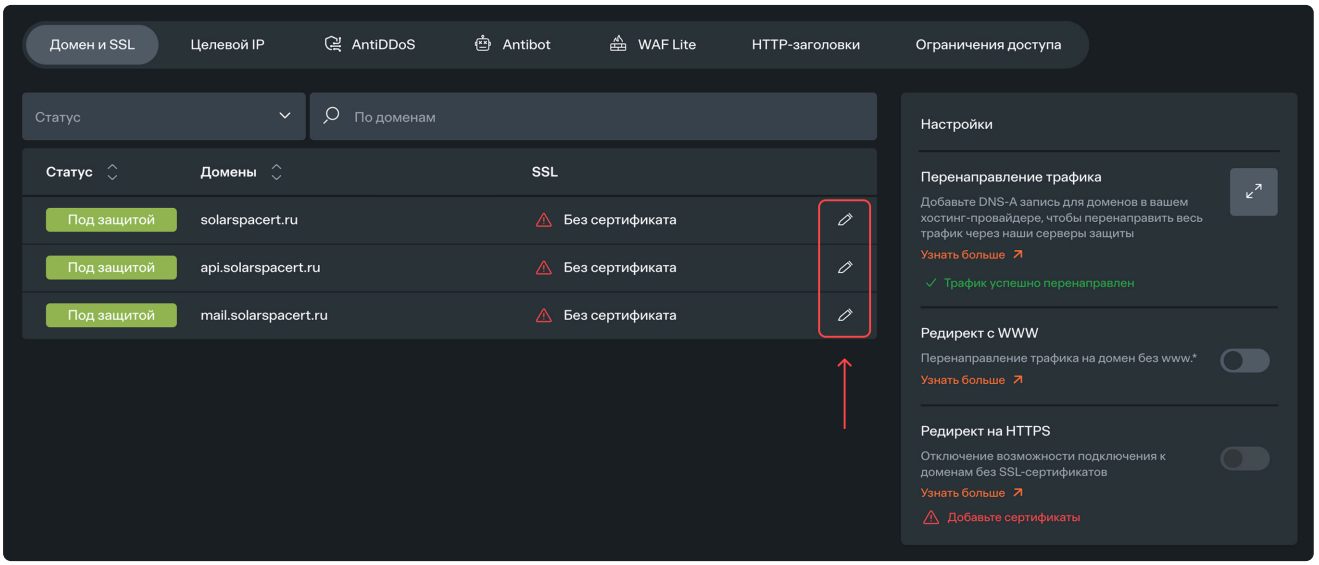

WEB-защита > Test Resource
Test Resource
Не защищен
Домен и SSL
Целевой IP
AntiDDoS
Antibot
WAF Lite
HTTP-заголовки
Статус
По доменам
Статус
Домены
SSL
Под защитой
domain1.com
Без сертификата
Под защитой
domain2.com
Без сертификата
Не защищен
domain3.com
Без сертификата

Добавление SSL-сертификата

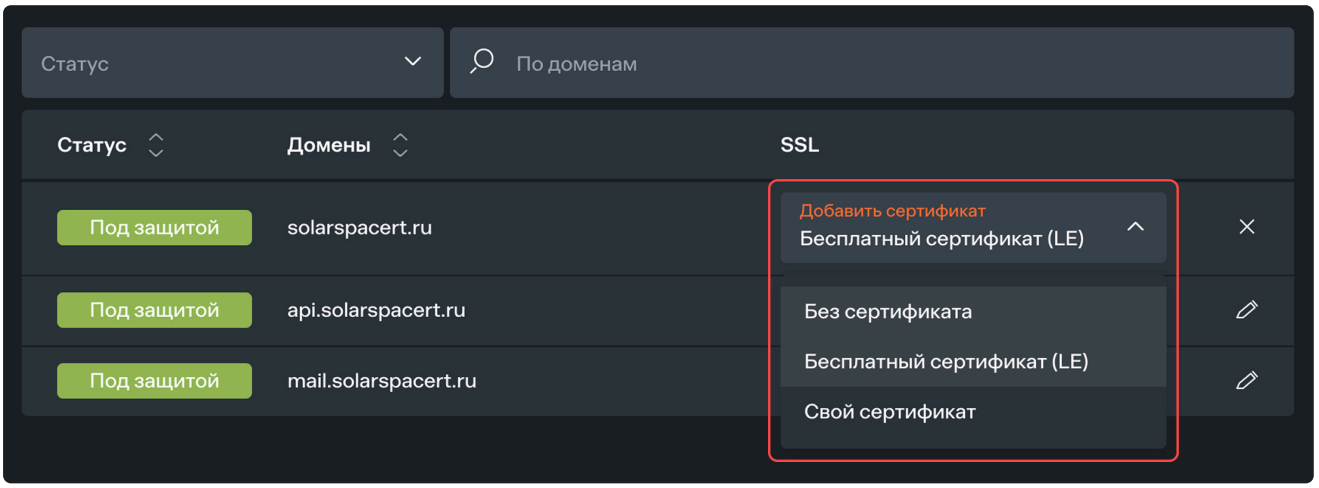
Для корректной работы ресурса необходимо добавить SSL-сертификат. Он шифрует всю информацию, которая передается между пользователем и сайтом, чтобы защитить конфиденциальные данные в случае перехвата их злоумышленниками.

SSL-сертификат можно добавить только для домена, который прошел проверку по DNS-A-записи и находится в статусе "Под защитой".

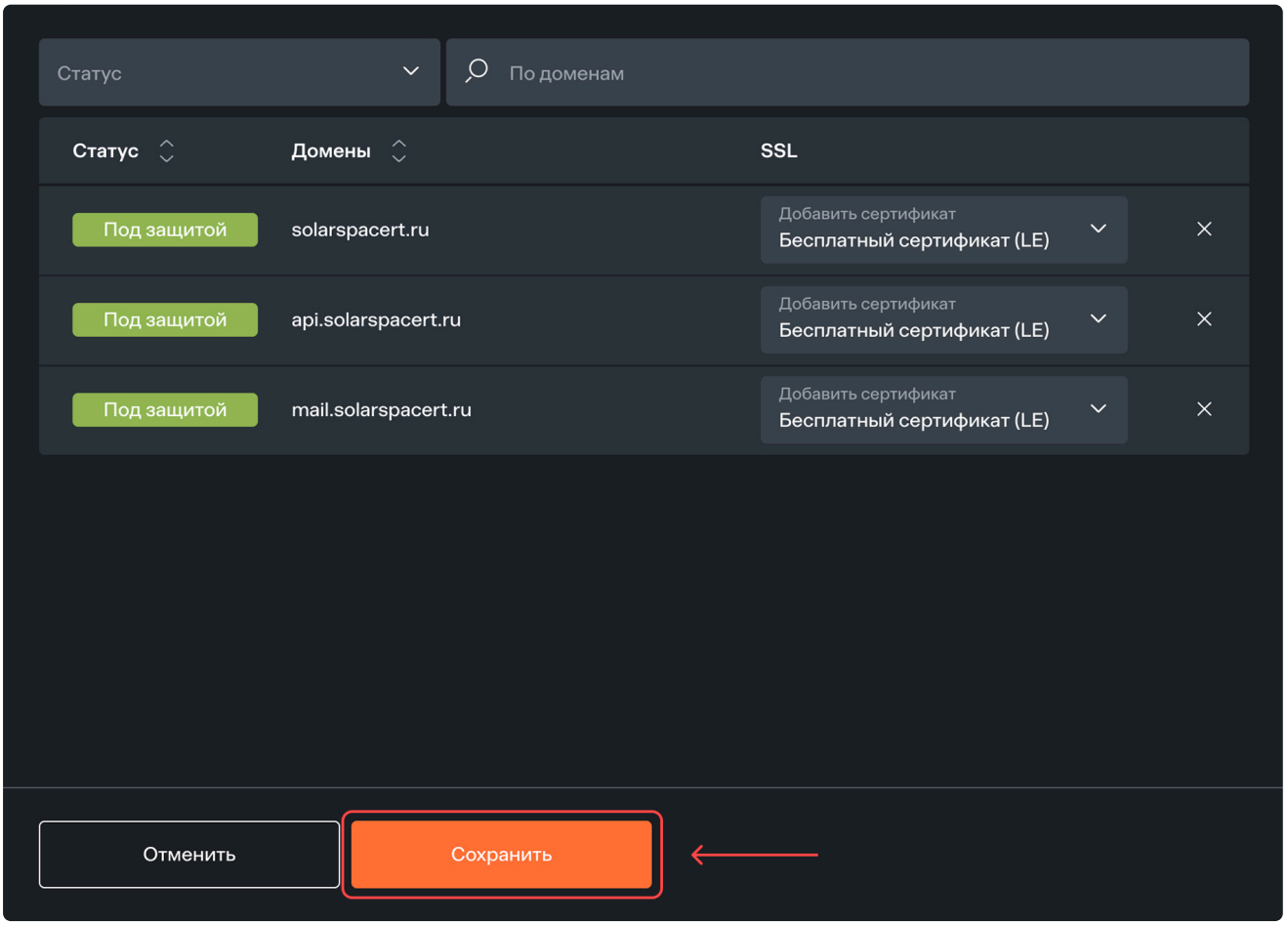
Перейдите в раздел Веб-защита и справа в строке ресурсов нажмите на иконку редактирования.



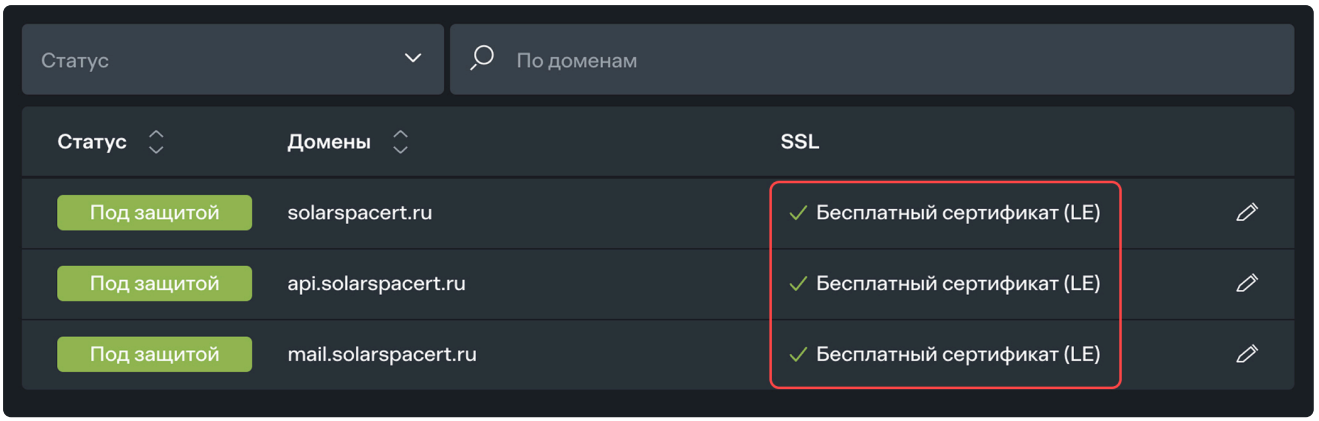
Вы можете загрузить свой сертификат или сгенерировать бесплатный сертификат LE (Let's Encrypt), который будет автоматически продлеваться на платформе Solar Space.



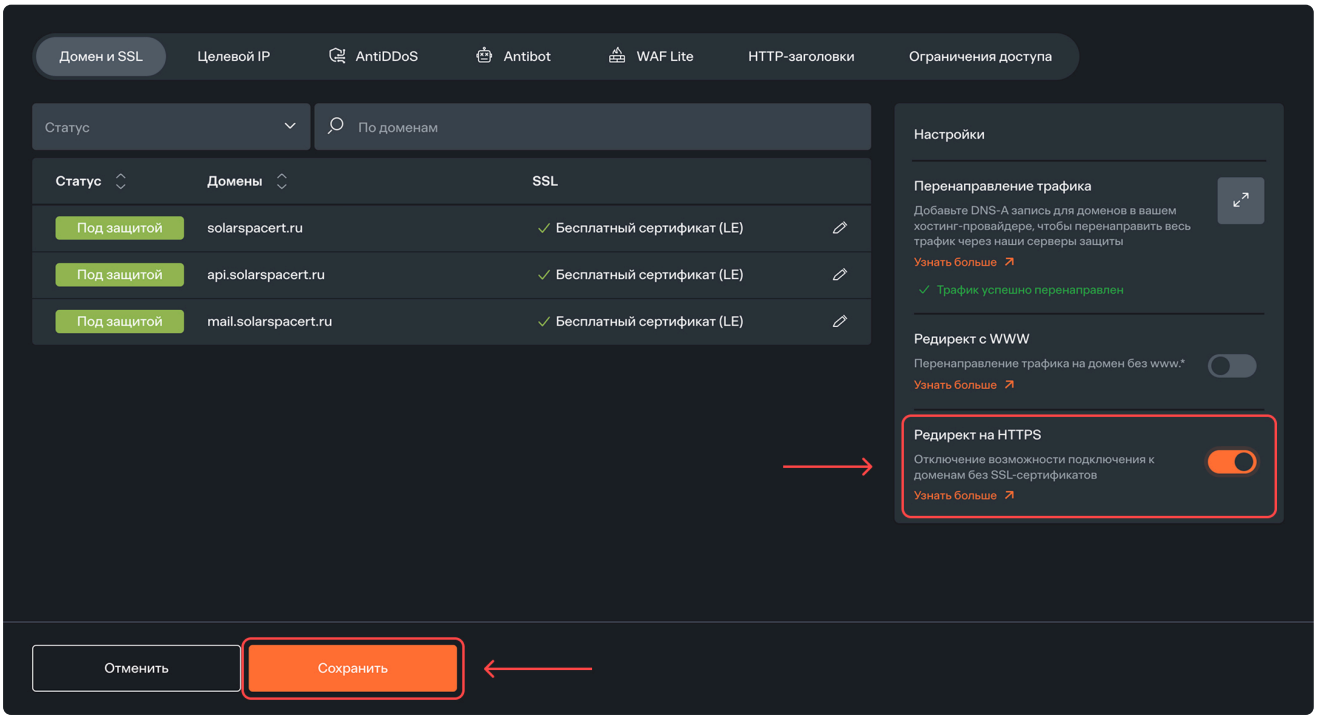
2. Выберите нужный вариант добавления сертификата и нажмите на кнопку "Сохранить".



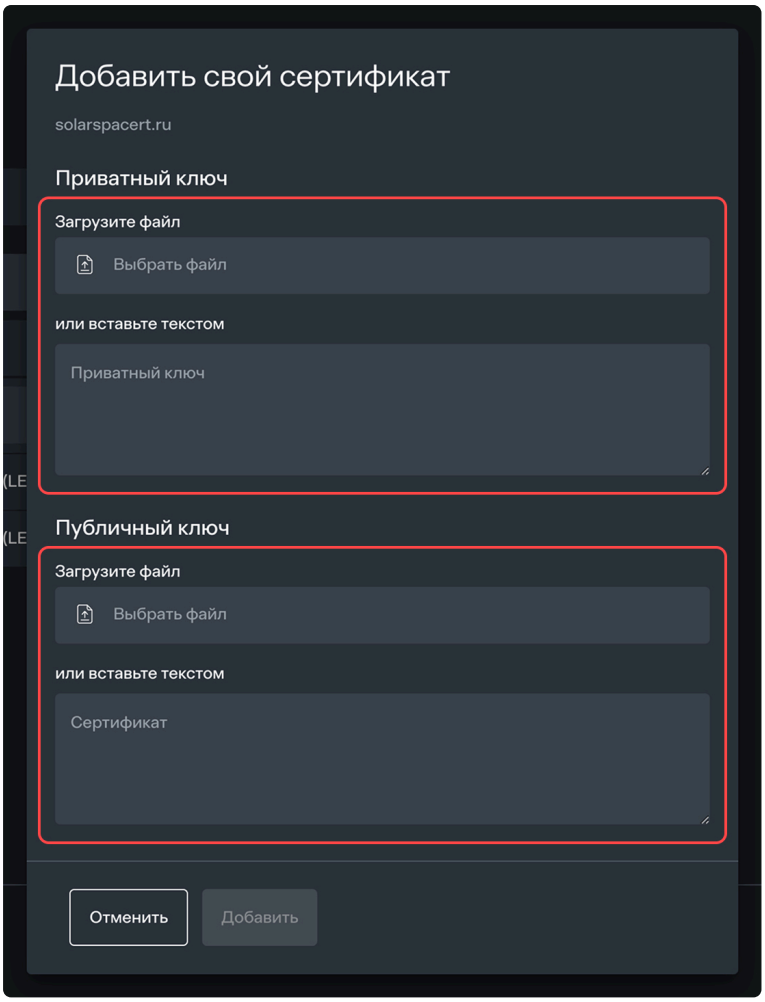
В течении нескольких секунд статус SSL-сертификата изменится.



3. Теперь вы можете переключить галочку в блоке "Редирект на HTTPS", чтобы обеспечить безопасное взаимодействие пользователей с вашим сайтом.



Для добавления собственного сертификата на платформу вы можете загрузить файл приватного и публичного ключа, либо вставить его текстом и нажать кнопку "Добавить".

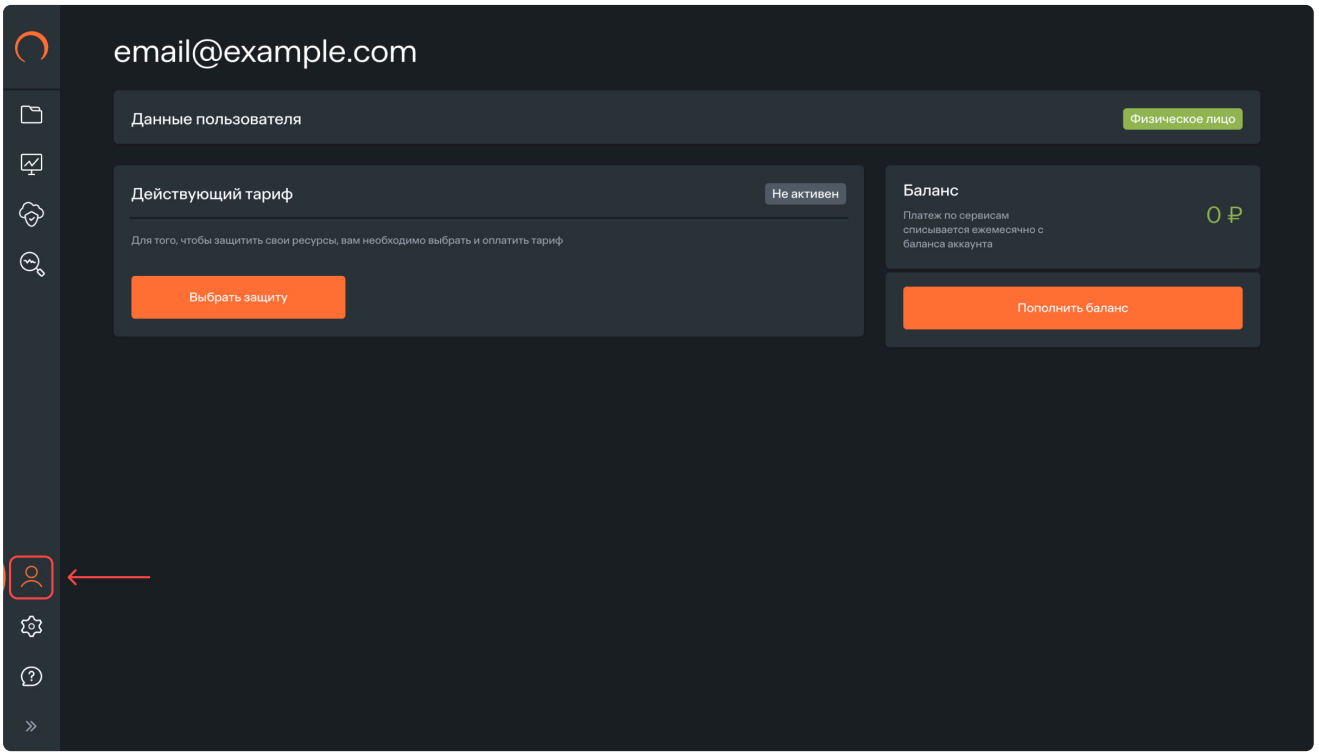


Профиль

На странице профиля вы можете:

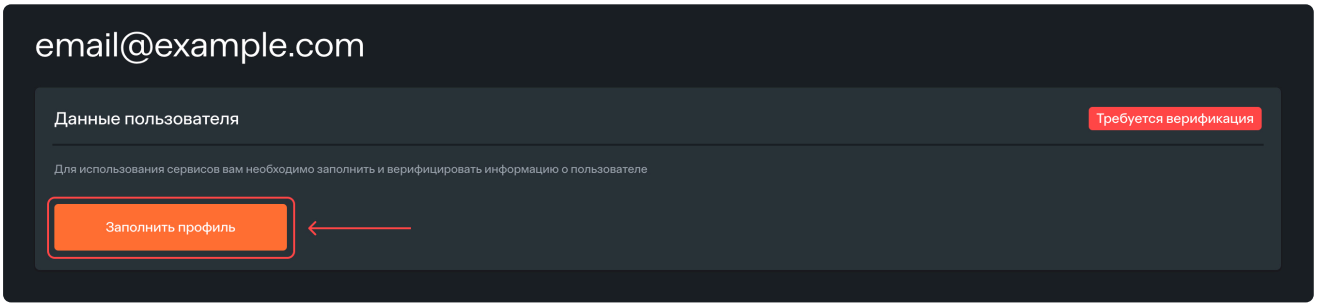
- Просмотреть информацию о своем аккаунте
- Подключить или изменить защиту
- Пополнить баланс

Для того, чтобы попасть на страницу профиля из любого раздела, нажмите на иконку в боковом меню.



Новый пользователь

Если вы новый пользователь, внесите данные в профиль. Без них не получится подключить и активировать защиту. Для заполнения профиля нажмите на кнопку "Заполнить профиль".



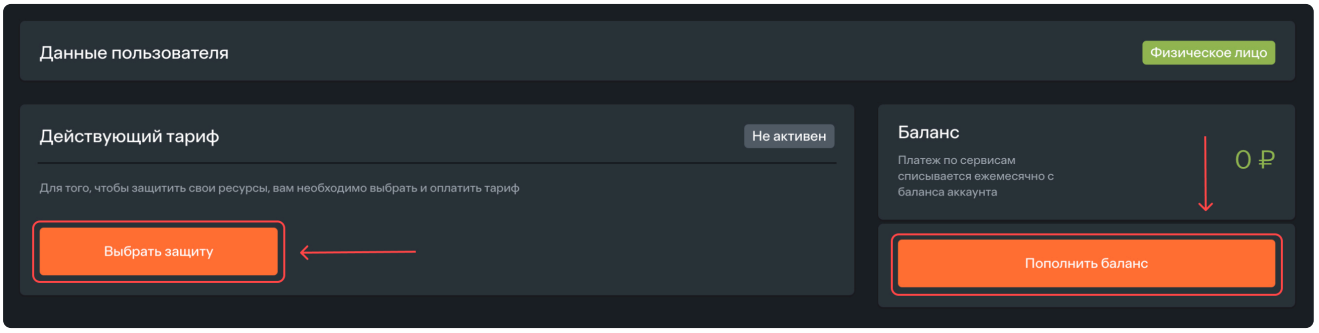
Откроется страница "Подтверждение аккаунта". Далее следуйте инструкциям.

Подтвержденный пользователь без активных услуг

После подтверждения своего аккаунта в разделе "Данные пользователя" появится индикатор зеленого цвета с типом контрагента, который был выбран при заполнении данных: "Физическое лицо", "Самозанятый", "Индивидуальный предприниматель" или "Юридическое лицо".

На странице профиля вы можете:

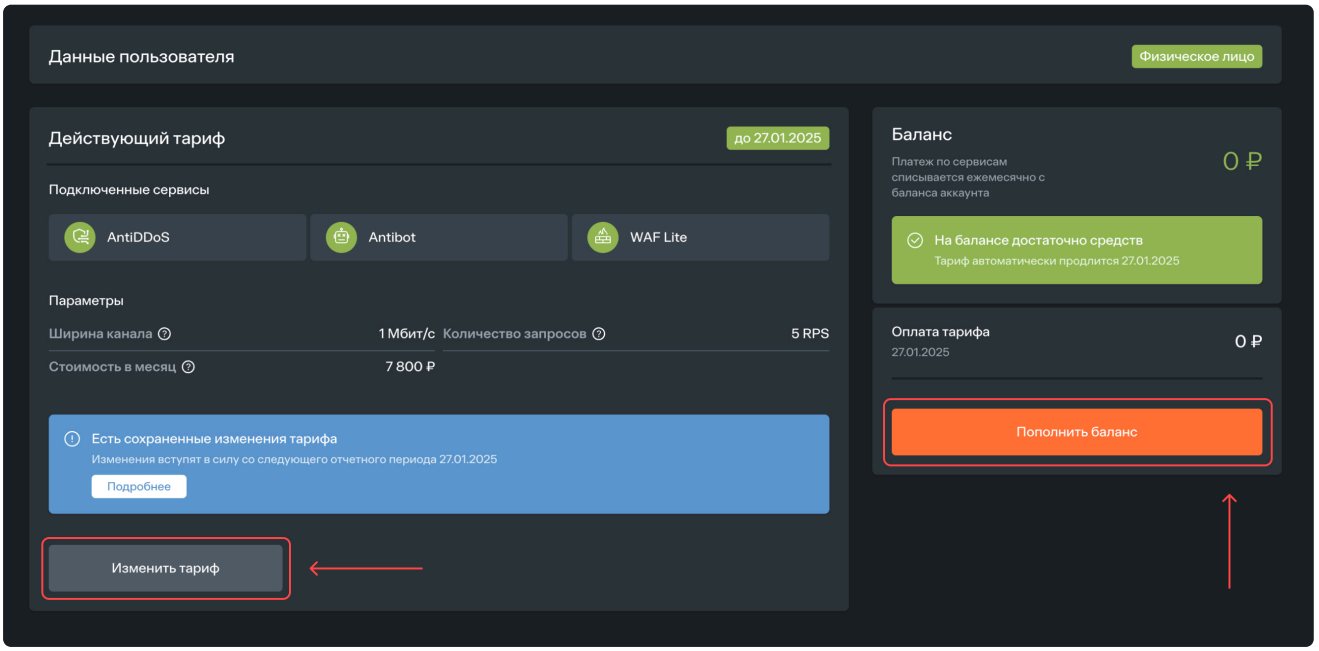
- Подключить сервисы, нажав на кнопку "Выбрать защиту". Далее следуйте инструкциям по подключению
- Пополнить баланс



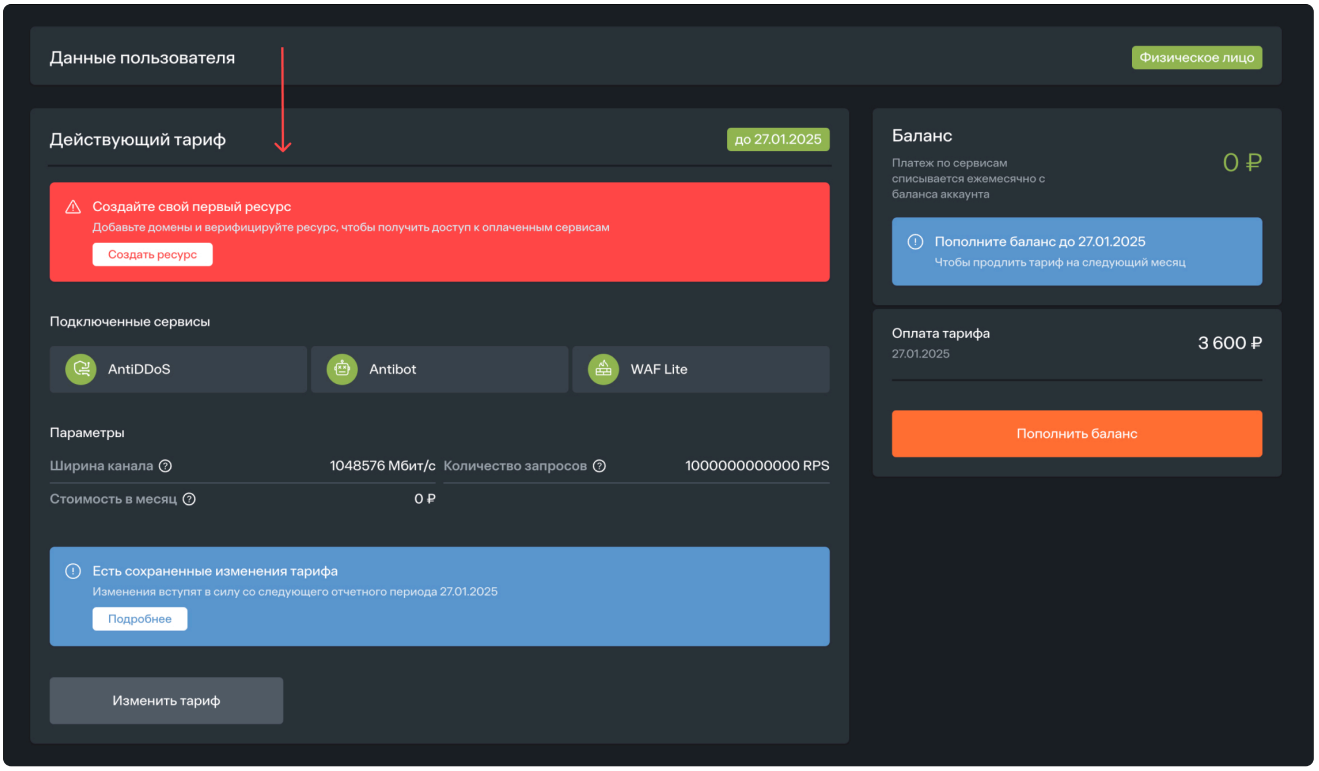
Подтвержденный пользователь с активными услугами

Пользователю с подтвержденным аккаунтом и активными услугами на странице профиля доступны следующие действия:

- Пополнение баланса
- Изменение тарифа



В случае, если у вас еще нет ресурса, то вы можете его создать, нажав на кнопку "Создать ресурс". Далее следуйте инструкциям.



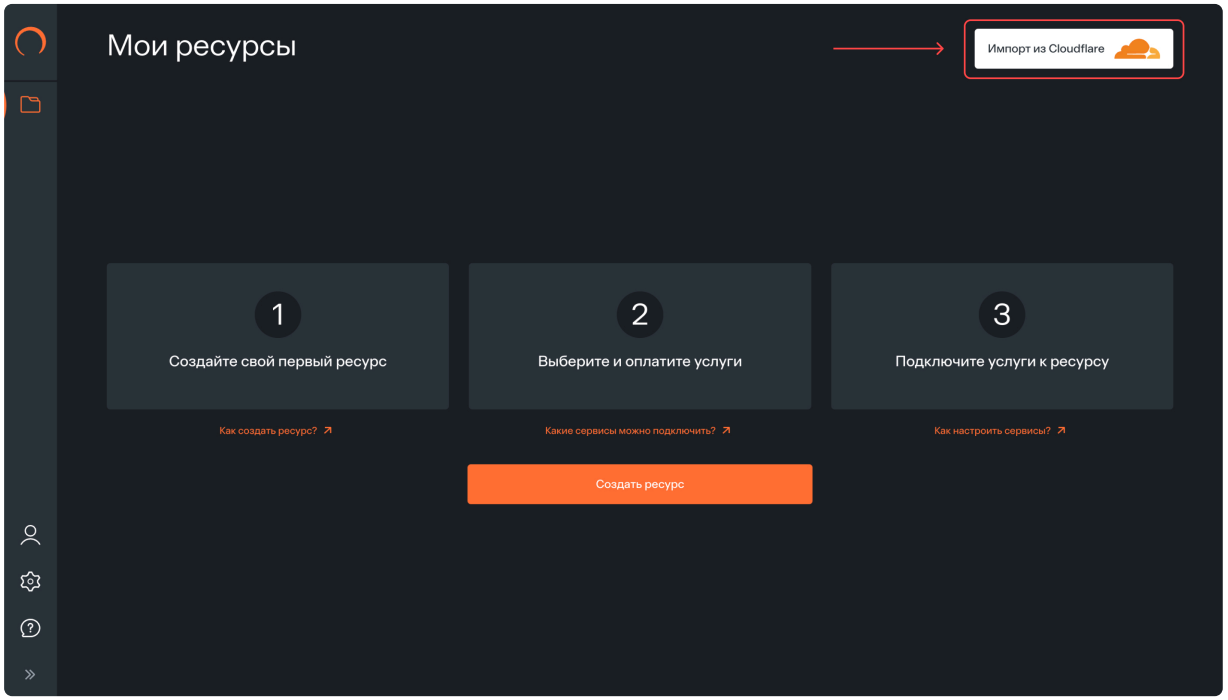
Импорт из CloudFlare

Функция импорта из CloudFlare предназначена для быстрого автоматического переноса ресурсов со всеми доменами в личный кабинет Solar Space.

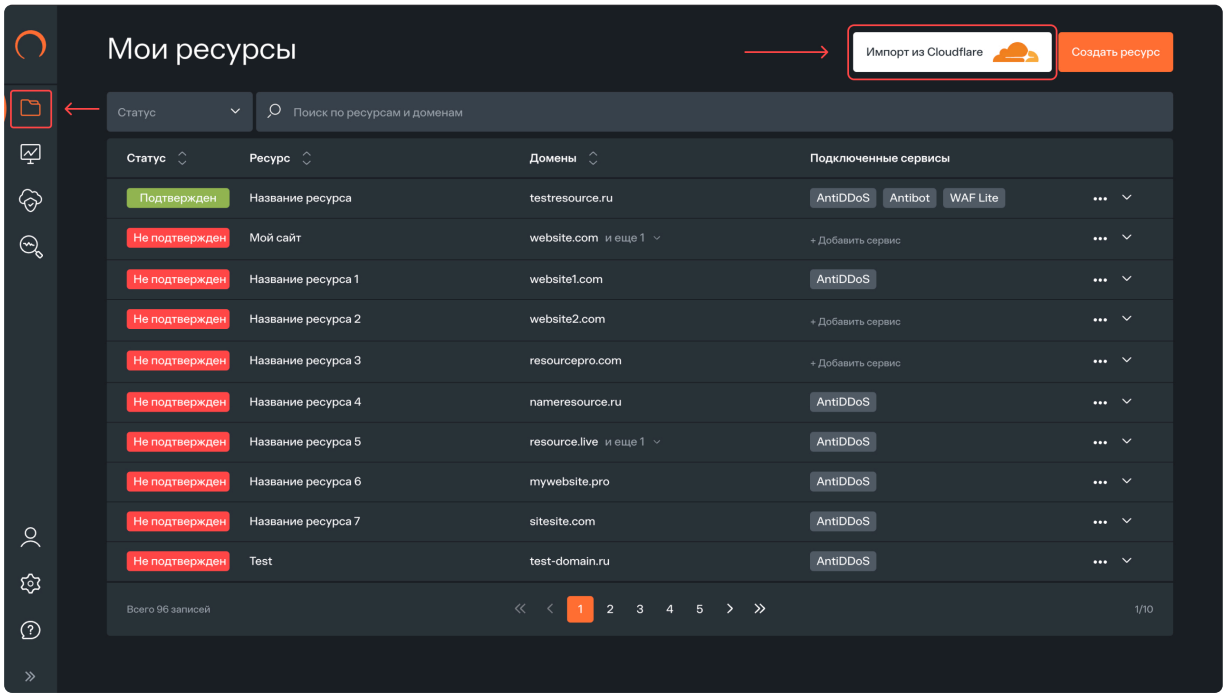
Это избавит от необходимости переносить ресурсы вручную, а значит, сэкономит время и снизит риск ошибок при миграции.

Для импорта ресурсов из CloudFlare выполните следующие действия:

1. Нажмите на кнопку "Импорт из CloudFlare" в правом верхнем углу экрана:
    - Если вы новый пользователь без ресурсов

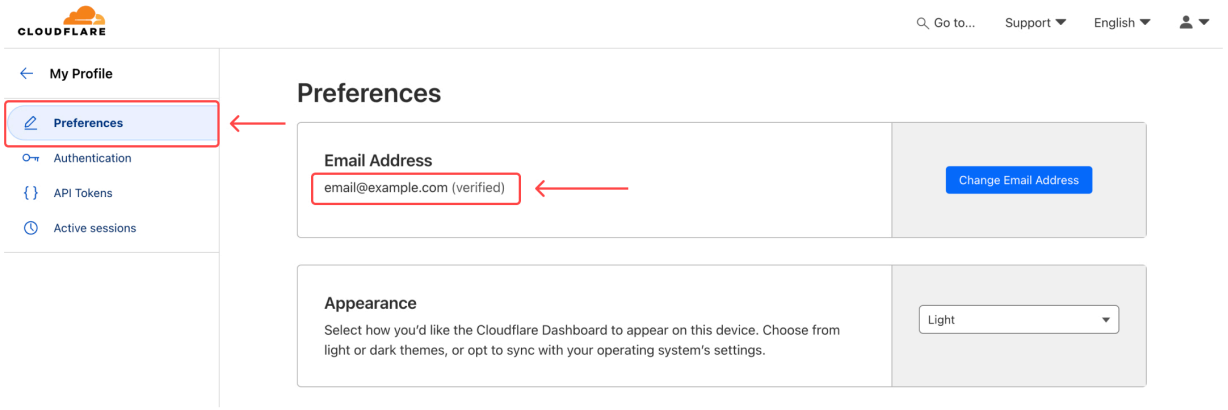


    - Если у вас уже есть аккаунт с созданными ресурсами на странице "Мои ресурсы"

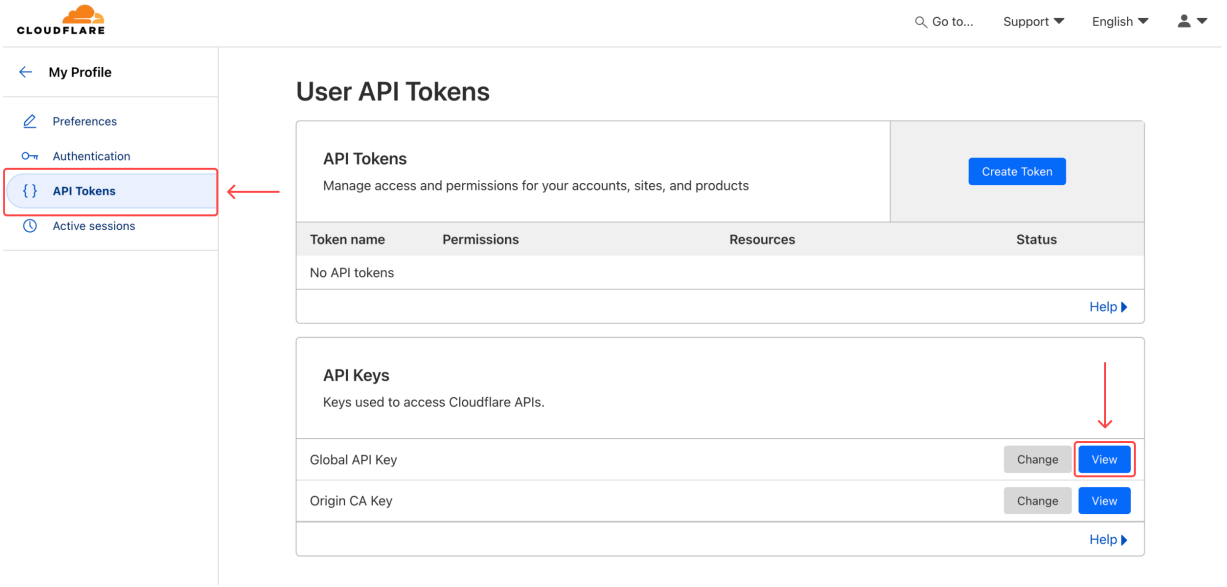


2. Перейдите в личный кабинет CloudFlare и скопируйте значения из полей:

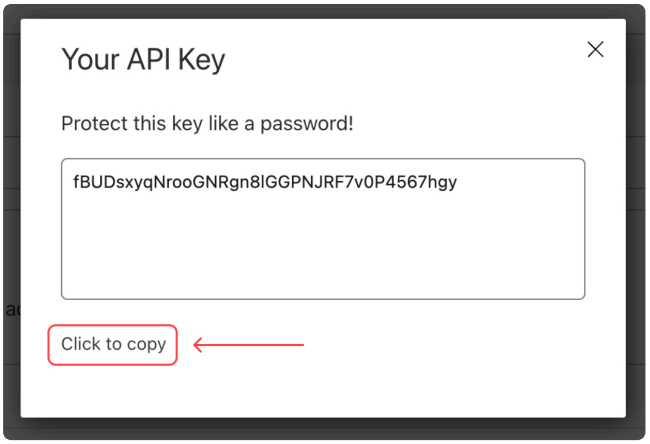
- **Email Address** — это поле находится на этой странице в разделе "Preferences" сервиса CloudFlare



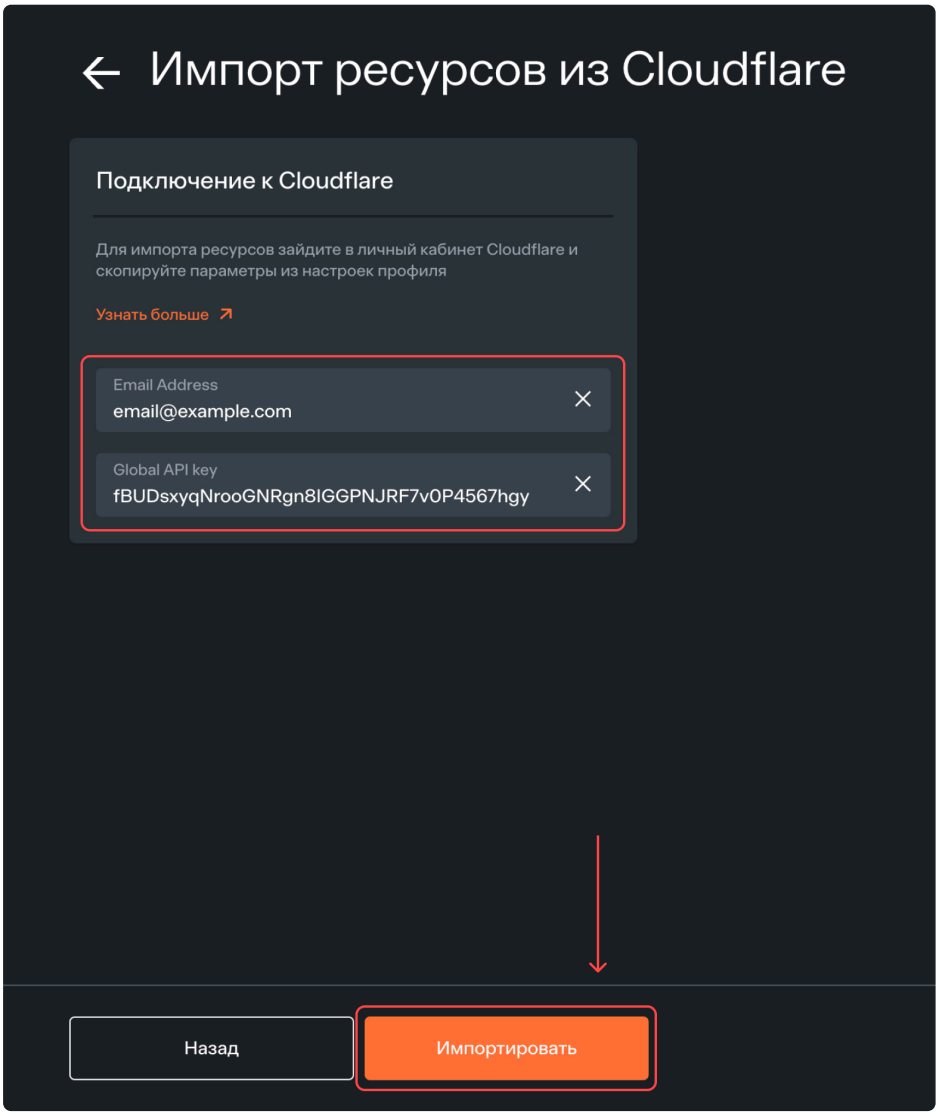
- **Global API Key** — это поле находится на этой странице в разделе "API Keys" сервиса CloudFlare. Нажмите на кнопку "View" для просмотра поля



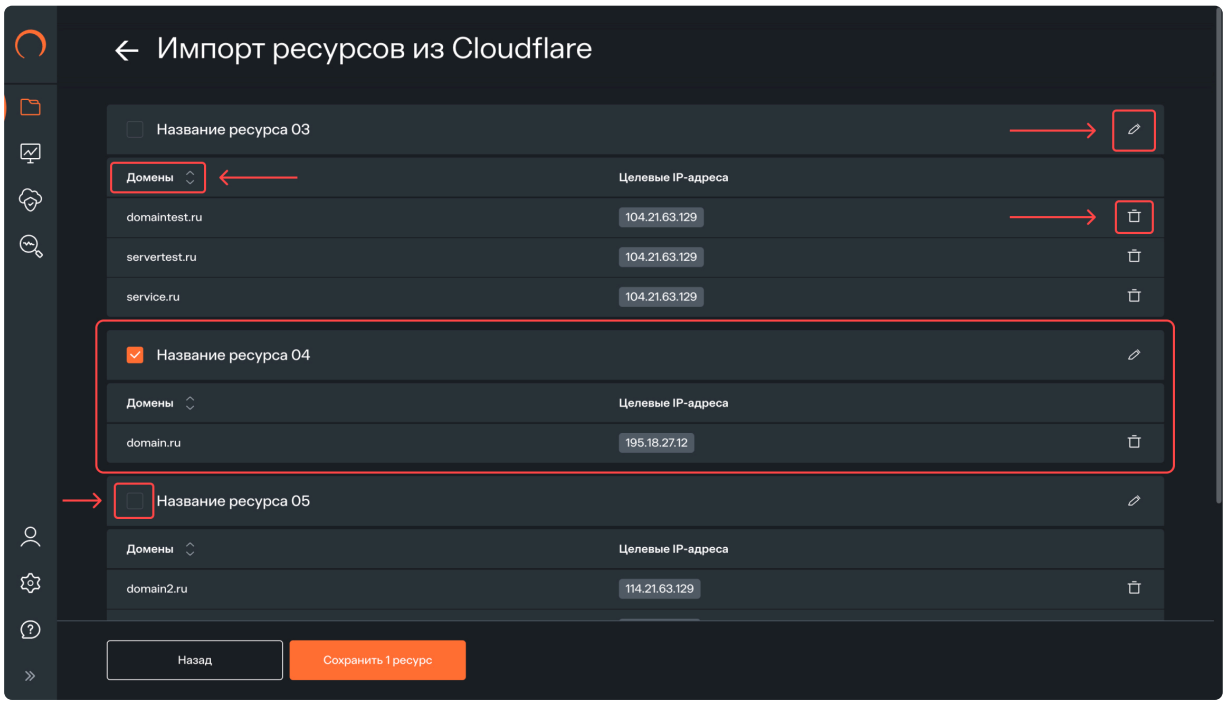
Введите пароль от CloudFlare для подтверждения действия и скопируйте ключ, указанный в поле



3. Вернитесь на платформу Solar Space и введите эти значения в соответствующие поля:
   - **Email Address** — адрес электронной почты, на который зарегистрирован аккаунт в CloudFlare. Он может отличаться от email, указанного при регистрации в Solar Space
   - **Global API key** — ключ, по которому осуществляется импорт
4. Нажмите на кнопку "Импортировать".

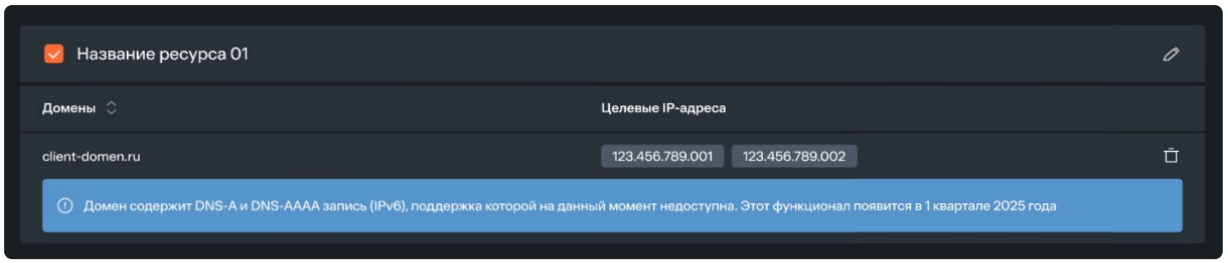


5. Импорт ресурсов займет не более 1 минуты. После этого появится список перенесенных ресурсов со всеми доменами. Успешно импортированные ресурсы отмечены по умолчанию "галочкой". Вы можете:
   - **Удалять** домены у ресурсов (для импорта ресурс должен содержать хотя бы один домен)
   - **Редактировать** названия ресурсов
   - **Снимать** "галочку" с тех ресурсов, которые вы не хотите добавлять в личный кабинет Solar Space
   - **Сортировать** домены в алфавитном порядке

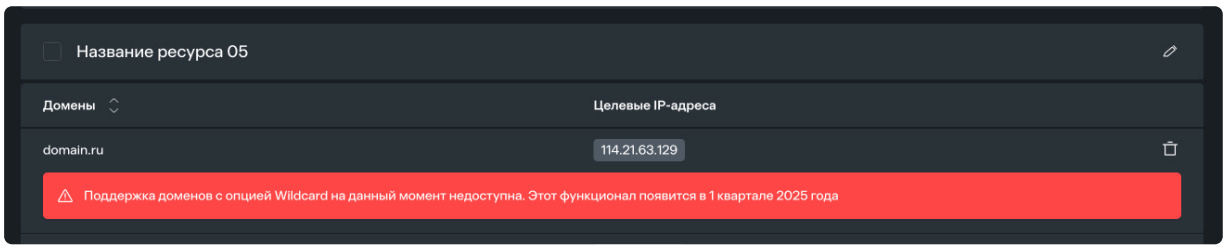


6. В 2025 году появится возможность поддержки ресурсов с IPv6 и SSL-сертификатами WildCard, которые обеспечивают защиту всех поддоменов. Пока при импорте таких ресурсов появляются предупреждающие сообщения:

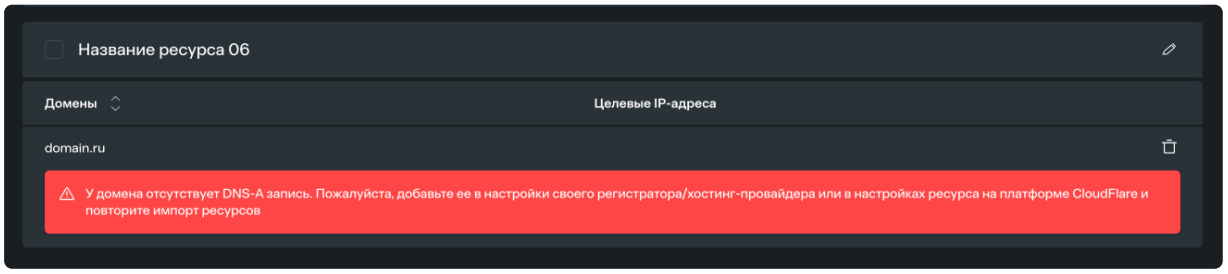
   - **Для доменов в формате IPv6**: "Домен содержит DNS-A и DNS-AAAA запись (IPv6), поддержка которой на данный момент недоступна. Этот функционал появится в 1 квартале 2025 года"



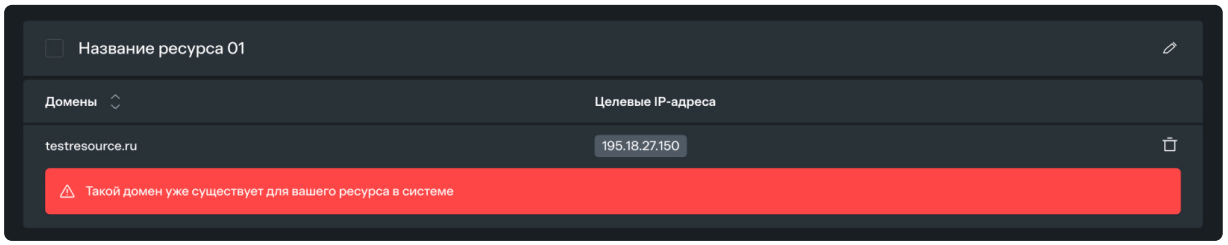
   - **Для доменов с WildCard-сертификатом**: "Поддержка доменов с опцией Wildcard на данный момент недоступна. Этот функционал появится в 1 квартале 2025 года"



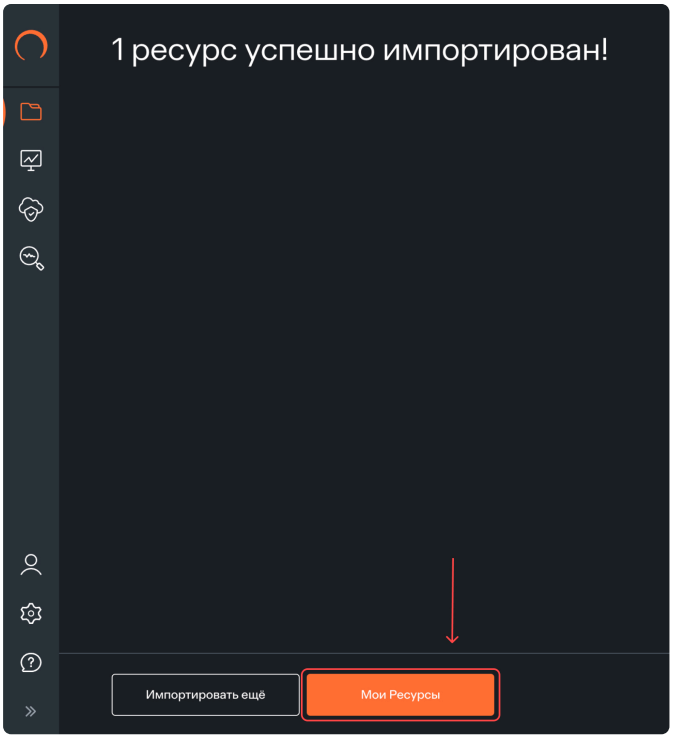
   - **Для доменов, у которых отсутствует A запись**: "У домена отсутствует DNS-A запись. Пожалуйста, добавьте ее в настройки своего регистратора/хостинг-провайдера или в настройках ресурса на платформе CloudFlare и повторите импорт ресурсов"



- Если **домен уже существует на платформе Solar Space**, появится соответствующее предупреждение



7. После выбора всех ресурсов и нажатия на кнопку "Сохранить" появится сообщение об успешном импорте ресурсов. Они будут отображаться на странице "Мои ресурсы". Для перехода на нее нажмите на кнопку "Мои ресурсы" в нижней части страницы.



Сервисы

Платформа Solar Space объединяет сервисы для комплексной кибергигиенты по нескольким направлениям:

- Веб-защита
- Сканирование уязвимостей
- Security Awareness
- Sec DNS
- StressTest
- SEG

Общее описание Веб-защиты

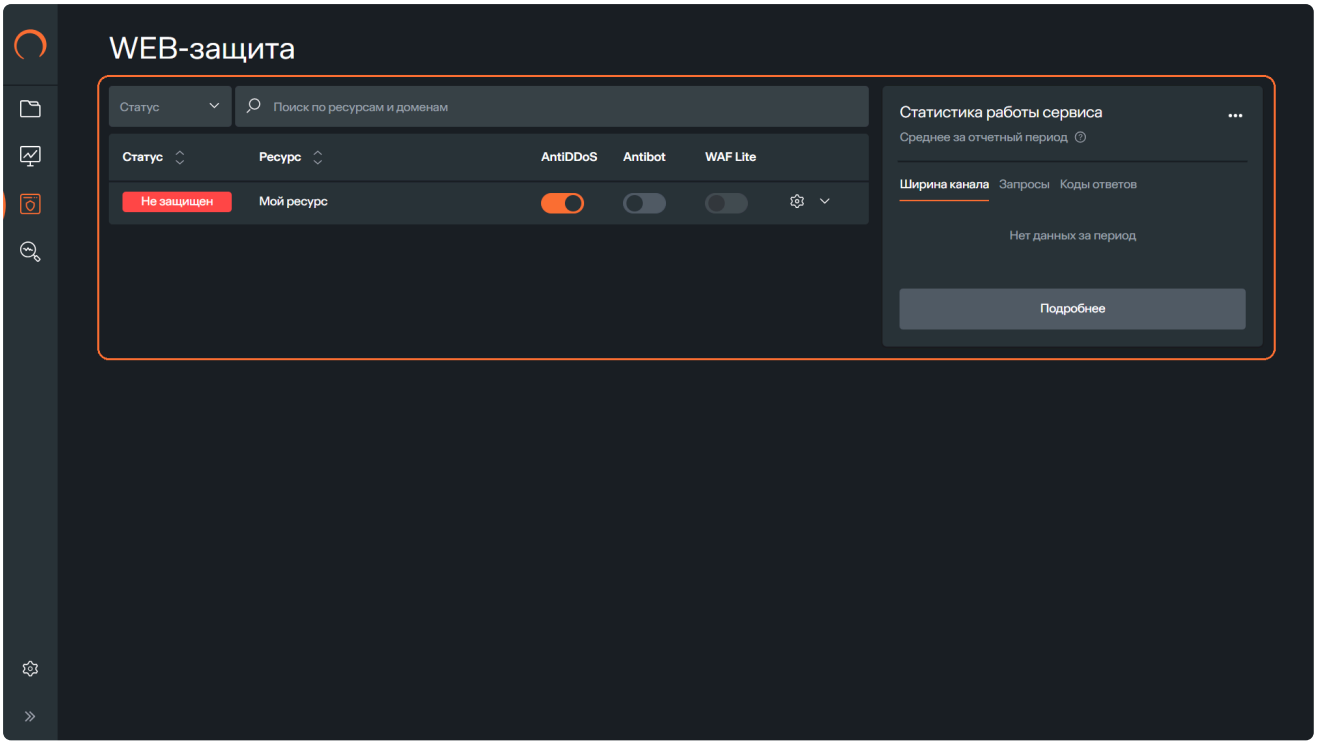
Веб-защита — это пакет услуг для защиты сайтов и веб-приложений. В него входят три сервиса:

- WEB AntiDDoS
- WEB Antibot
- WAF Lite

Вы можете выбрать один из 3 уровней защиты:

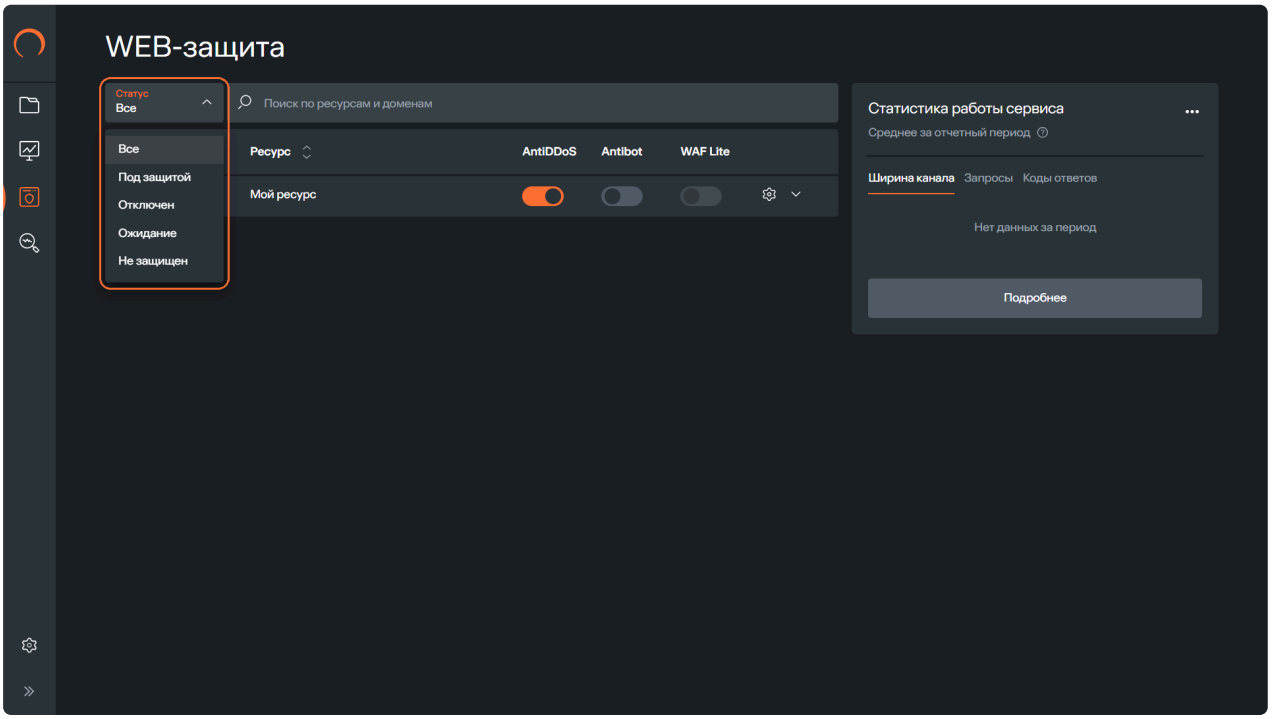
1. **Базовый** — сервис WEB AntiDDoS, который включает в себя только защиту от DDoS-атак. Без WEB AntiDDoS невозможна работа других сервисов веб-защиты.
2. **Оптимальный** — сервисы WEB AntiDDoS + WEB Antibot. Защита от DDoS-атак + защита от ботов и спама.
3. **Продвинутый** — сервисы WEB AntiDDoS + WEB Antibot + WAF Lite. Защита от DDoS-атак + защита от ботов + защита от веб-атак, направленных на взлом сайта и утечку данных.

На главной странице раздела вы увидите список всех ресурсов. Напротив каждого из них отображается статус в зависимости от того, подключена ли для него защита:



- **Не защищен** — для ресурса не подключен ни один из сервисов веб-защиты
- **Ожидание** — идет верификация ресурса по DNS-A записи для постановки под защиту
- **Под защитой** — для ресурса подключен хотя бы один из сервисов веб-защиты

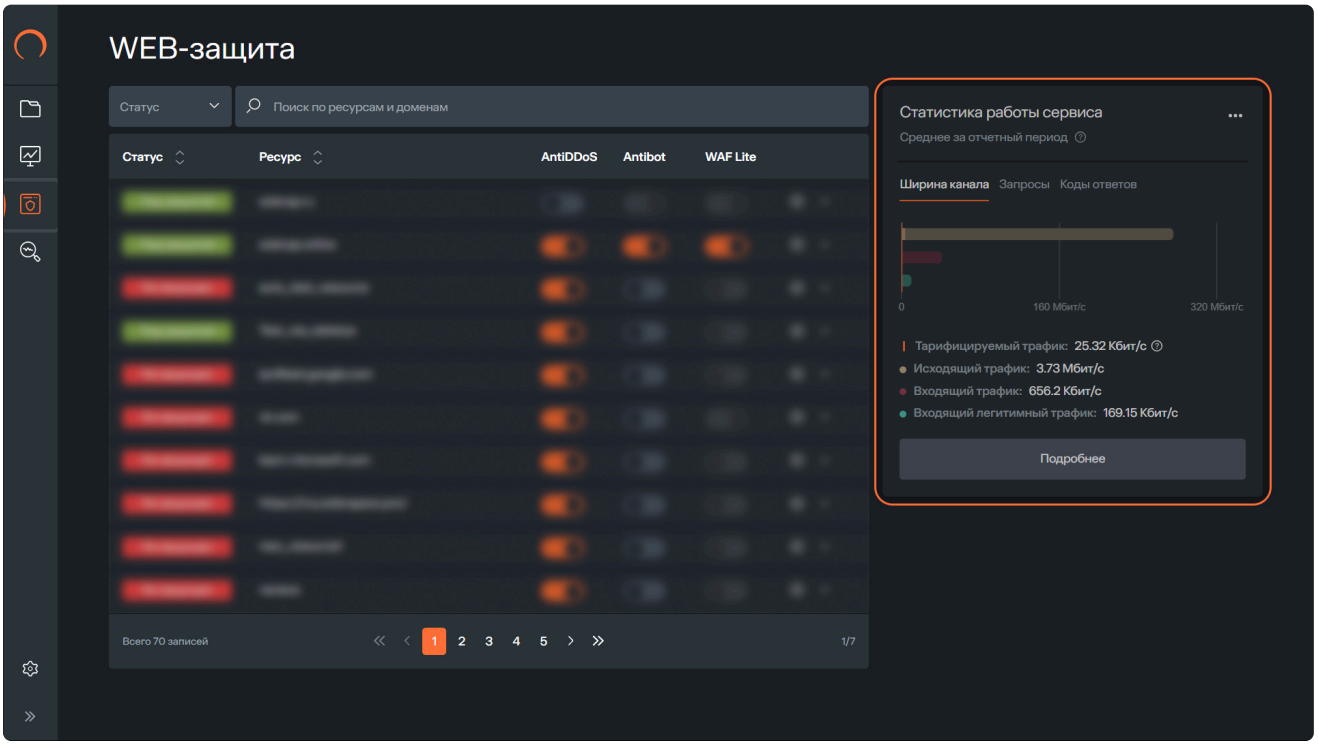
- **Отключен** — ресурс отключен



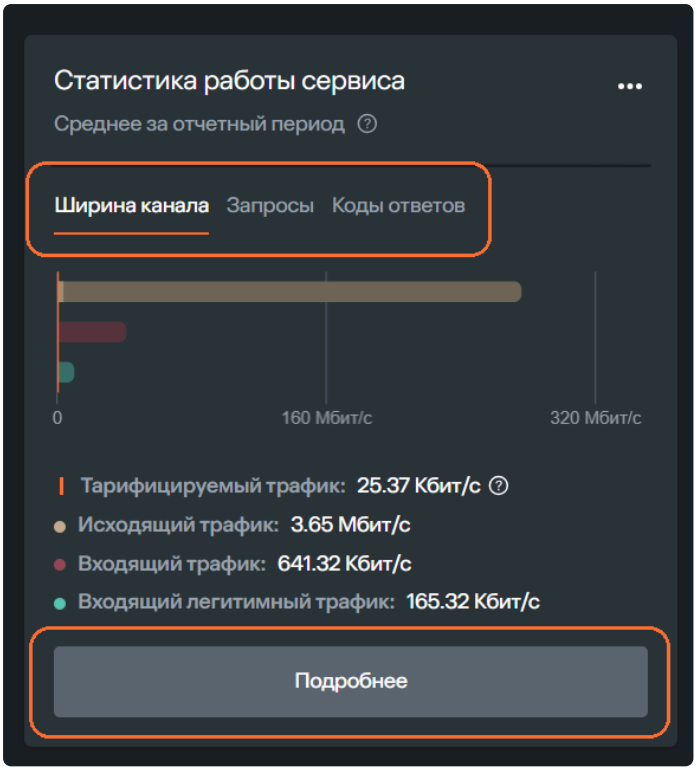
> Обратите внимание
>
> Для наиболее эффективной защиты веб-ресурсов рекомендуется подключать все три сервиса. Они отражают разные виды атак и в комплексе обеспечивают эшелонированную (многоуровневую) защиту

Статистика

На главной странице раздела "WEB-защита" в блоке "Статистика работы сервиса" отображается информация с графиком средних значений по всем ресурсам за отчетный период.

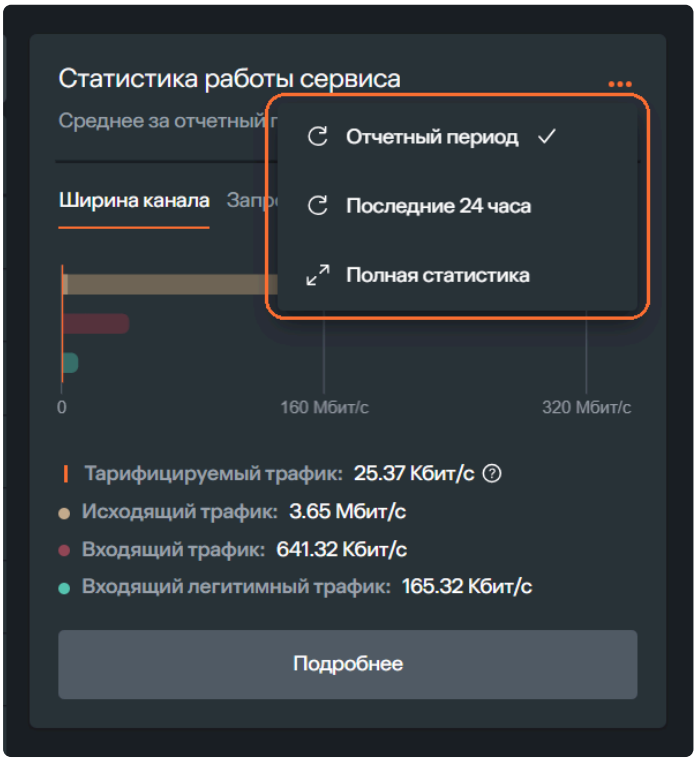


В блоке отображается три вкладки: "Ширина канала", "Запросы" и "Коды ответов". На каждой из них есть кнопка "Подробнее".

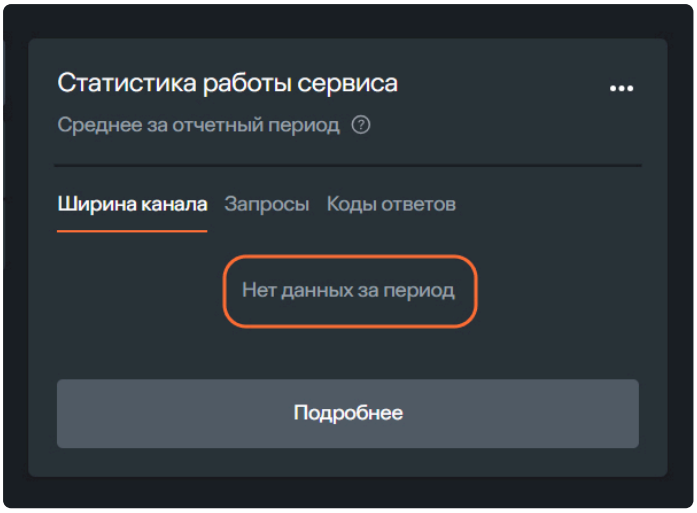


При нажатии на кнопку "Подробнее" вы перейдете на аналогичную вкладку страницы Статистика с подробным отчетом по этому параметру – ширине канала, запросам или кодам ответов.

В правом верхнем углу блока "Статистика работы сервиса" есть иконка в виде трех точек, при нажатии на которую раскрывается меню из трех пунктов.



Отчетный период (установлен по умолчанию) — средняя статистика за последние 30 дней Если данные за это время отсутствуют, вы увидите сообщение "Нет данных за период".



Последние 24 часа — статистика за последние сутки.

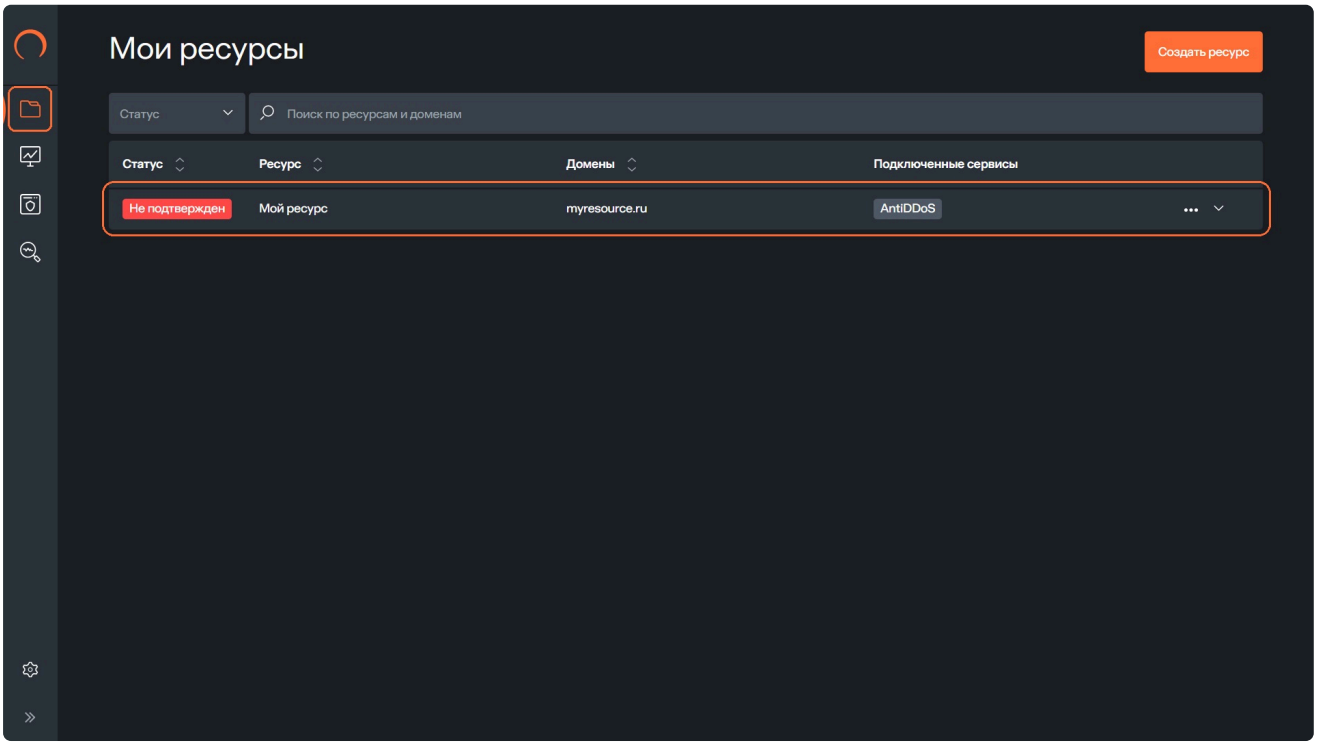
Полная статистика — переход на страницу "Статистика" с подробными отчетами.

Настройки сервисов

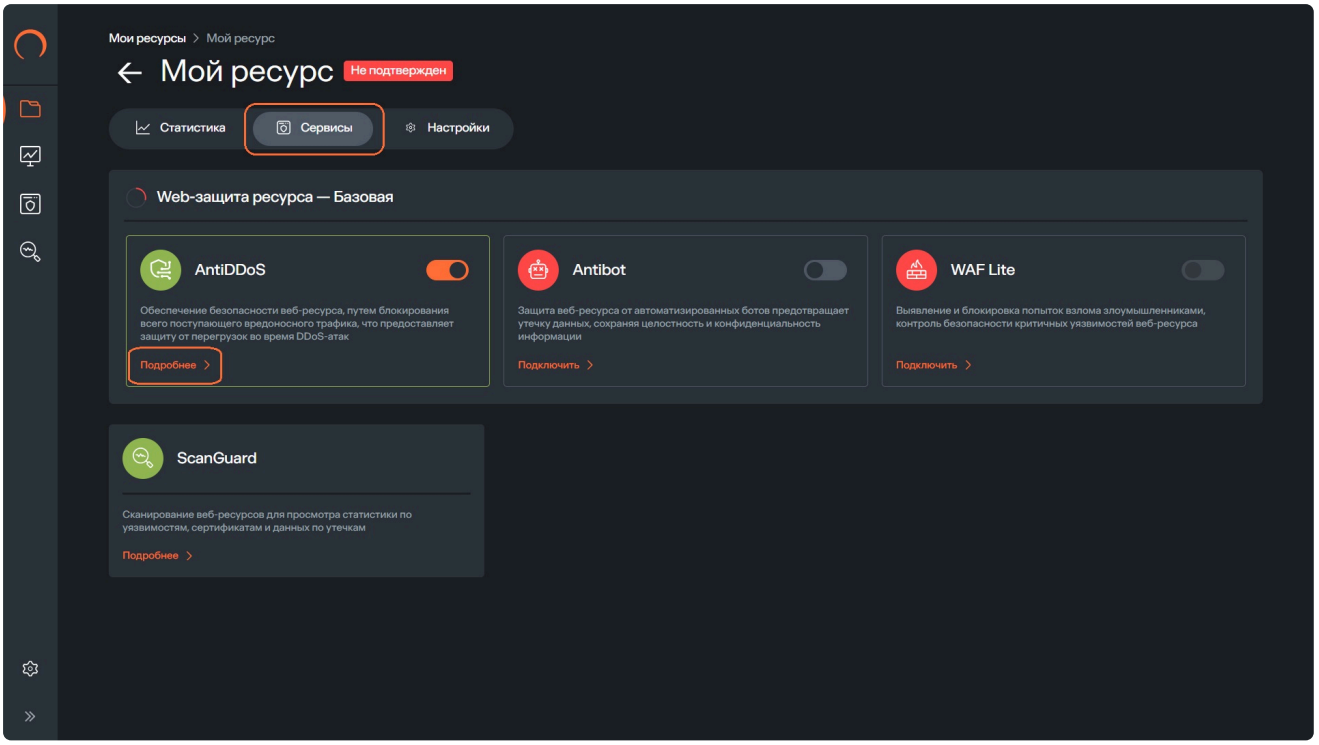
Для перехода на страницу настроек веб-защиты есть 4 способа:

1 способ

На странице "Мои ресурсы" кликните по строке нужного ресурса.

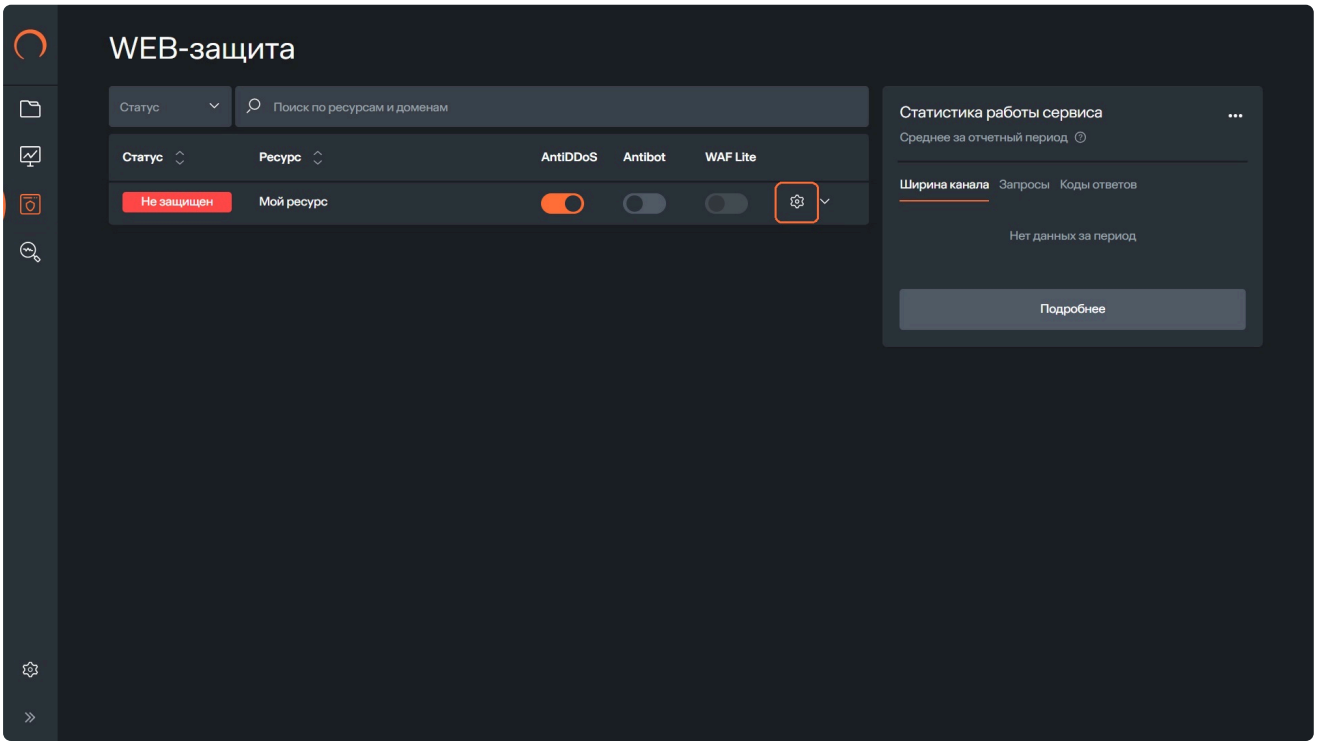


Вы перейдете на страницу ресурса, где вам нужно открыть вкладку "Сервисы". На вкладке "Сервисы" нажмите на кнопку "Подробнее" в блоке активного сервиса, чтобы перейти на страницу настроек защиты.



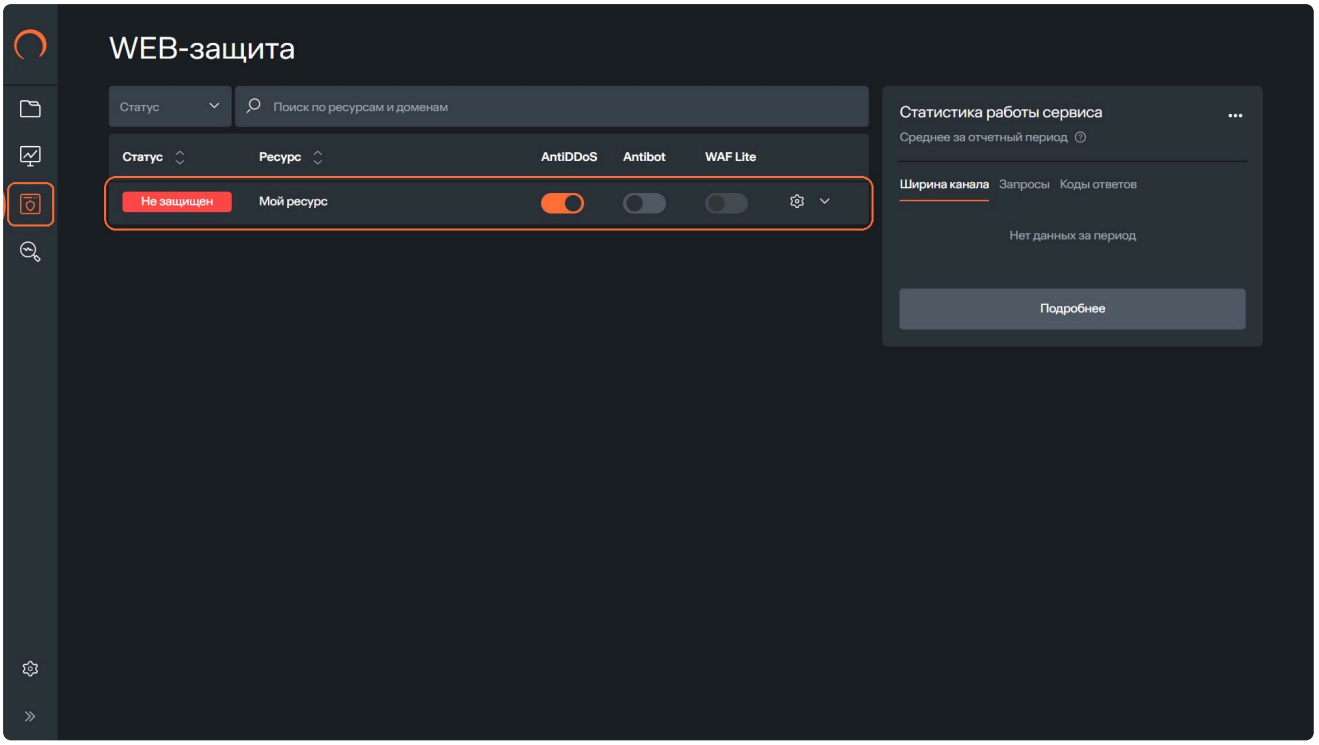
2 способ

На странице "WEB-защита" кликните по иконке шестеренки справа в строке нужного ресурса.



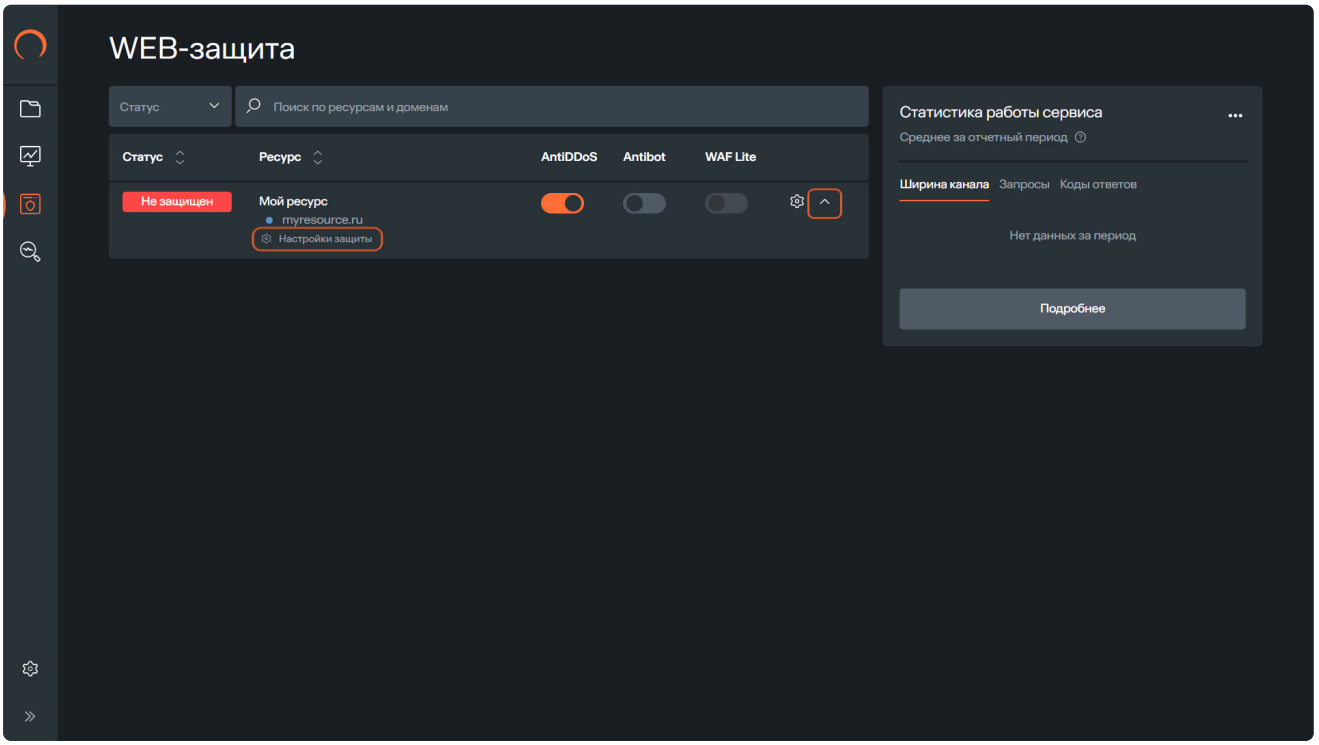
3 спооcб

На странице "WEB-защита" кликните по строке нужного ресурса.

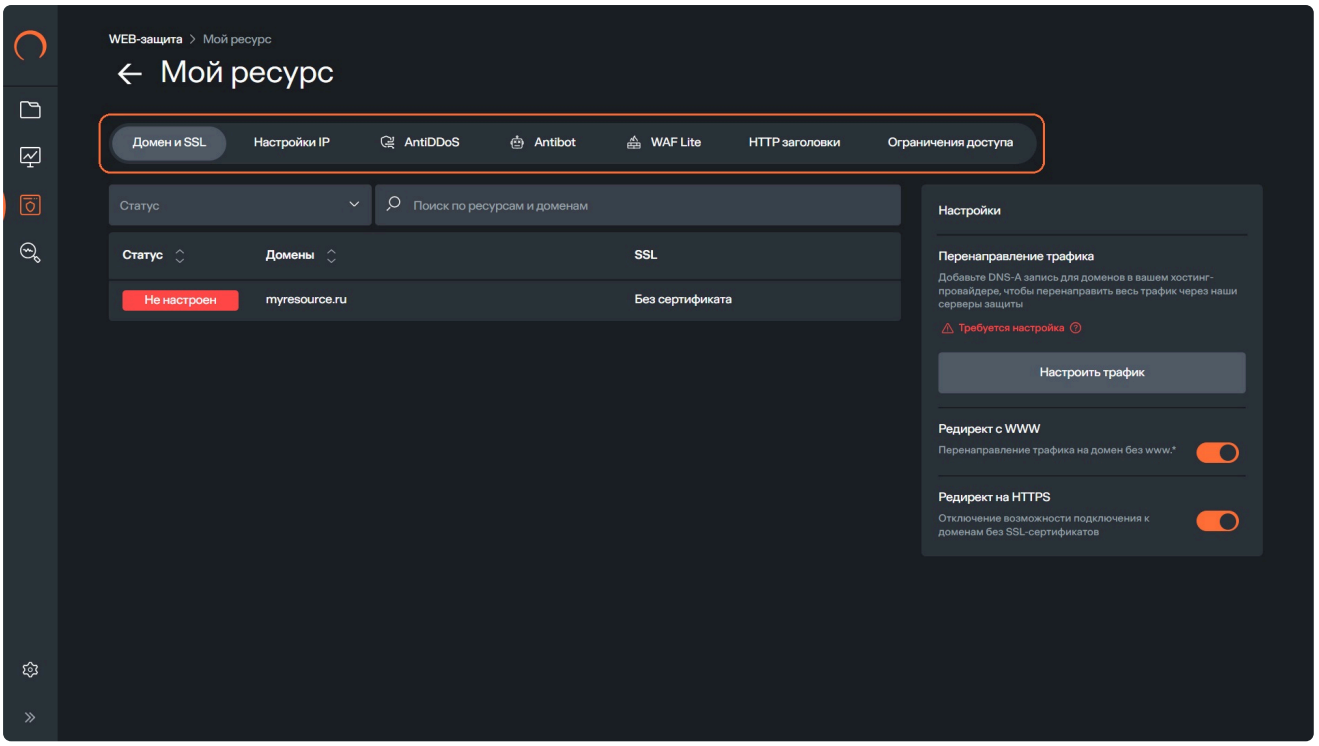


4 способ

На странице "WEB-защита" найдите в списке нужный ресурс. Справа в строке ресурса нажмите на иконку в виде галочки и в появившемся меню выберите пункт "Настройки защиты".



На странице настроек защиты есть несколько вкладок.



AntiDDoS

WEB AntiDDoS обеспечивает базовый уровень веб-защиты в рамках комплексного решения Solar Space.

Сервис защищает сайты и веб-приложения от DDoS-атак.

DDoS-атака *(от англ. Distributed Denial of Service — распределенный отказ в обслуживании)* состоит в отправке множества запросов к веб-ресурсу. Этот "паразитный" трафик перегружает ресурсы сервера, и сайт начинает работать медленно или совсем перестает загружаться.

В основе **WEB AntiDDoS** от Solar Space лежит механизм reverse proxy — обратного прокси-сервера. Это означает, что для защиты веб-ресурса нужно заменить его IP-адрес на IP-адрес нашего сервера. Таким образом весь входящий трафик перенаправится сначала на сервер Solar Space. Там система проводит технический и статистический анализ трафика:

- Технический анализ предполагает анализ сетевых данных, данных протоколов и SSL-сертификатов (цифровых сертификатов подлинности сайта)
- Статистический анализ отслеживает всплески трафика или признаки аномального пользовательского поведения Анализ занимает доли секунды, поэтому WEB AntiDDoS не влияет на скорость работы самого сайта

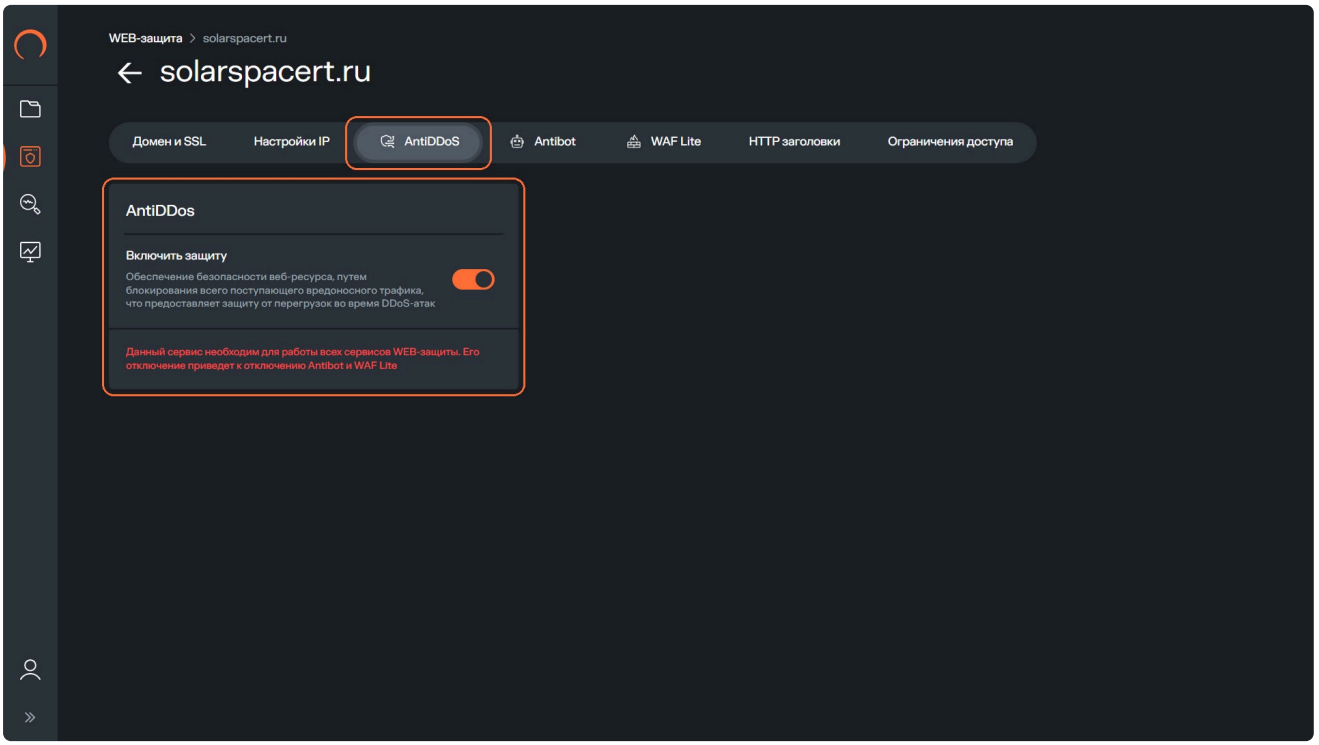
На основе анализа **WEB AntiDDoS** отсеивает часть трафика, которая не соответствует заданным параметрам, а остальную переадресовывает на защищаемый сайт. Именно поэтому настройка перенаправления трафика с помощью смены DNS-A записи – обязательный пункт при подключении защиты в личном кабинете Solar Space. Пока трафик не перенаправлен, защита не работает.

WEB AntiDDoS обезопасит веб-ресурс от атаки массовыми запросами **на уровне L3-L4 модели OSI**. При этом ботов сервис отсеять не сможет, поскольку настроен на анализ других параметров. Для комплексной защиты ресурса рекомендуем подключать WEB AntiDDoS в комплексе с сервисами:

- WEB Antibot — для фильтрации ботов, которые ищут уязвимости веб-ресурса, замедляют скорость работы сайта, спамят в комментариях и формах обратной связи, негативно влияют на поведенческие факторы, которые оценивают поисковые системы
- WAF Lite — для защиты от вредоносных запросов, которые «маскируются» под обращения реальных пользователей и приводят к взлому пользовательских аккаунтов и утечке данных

> ⚠ Важно
>
> WEB AntiDDoS — это обязательный уровень защиты, без которого не могут быть подключены WEB Antibot и WAF Lite

На странице сервиса AntiDDoS доступно его краткое описание и переключатель для активации услуги. AntiDDoS – базовый уровень защиты ресурса, без него невозможна работа Antibot и WAF Lite. Поэтому активация других сервисов возможна только при условии активного AntiDDoS.



Antibot

WEB Antibot в комплексе с WEB AntiDDoS обеспечивает оптимальный уровень веб-защиты в рамках комплексного решения Solar Space.

Сервис защищает веб-ресурсы от ботов на уровне L7, которые ищут уязвимости веб-ресурса, сканируют страницы, замедляют скорость работы сайта, спамят в комментариях и формах обратной связи, негативно влияют на поведенческие факторы, которые оценивают поисковые системы.

WEB Antibot анализирует трафик, который уже прошел через фильтрующий сервер **WEB AntiDDoS**, и определяет, кто отправил запрос — робот или человек. При каждом обращении к сайту пользователь отправляет нам определенный набор параметров. WEB Antibot анализирует этот набор с помощью алгоритмов машинного обучения и вычисляет процент вероятности того, что запрос отправлен роботом.

Если этот процент ниже порогового значения, система определяет его как человека и пропускает запрос к сайту.

Если процент выше порогового значения, WEB Antibot предполагает, что запрос отправил робот, но не блокирует его сразу, а показывает капчу. Это дополнительный тест на "человечность". Если капча пройдена, сервис пропускает запрос к сайту. Если нет – блокирует.

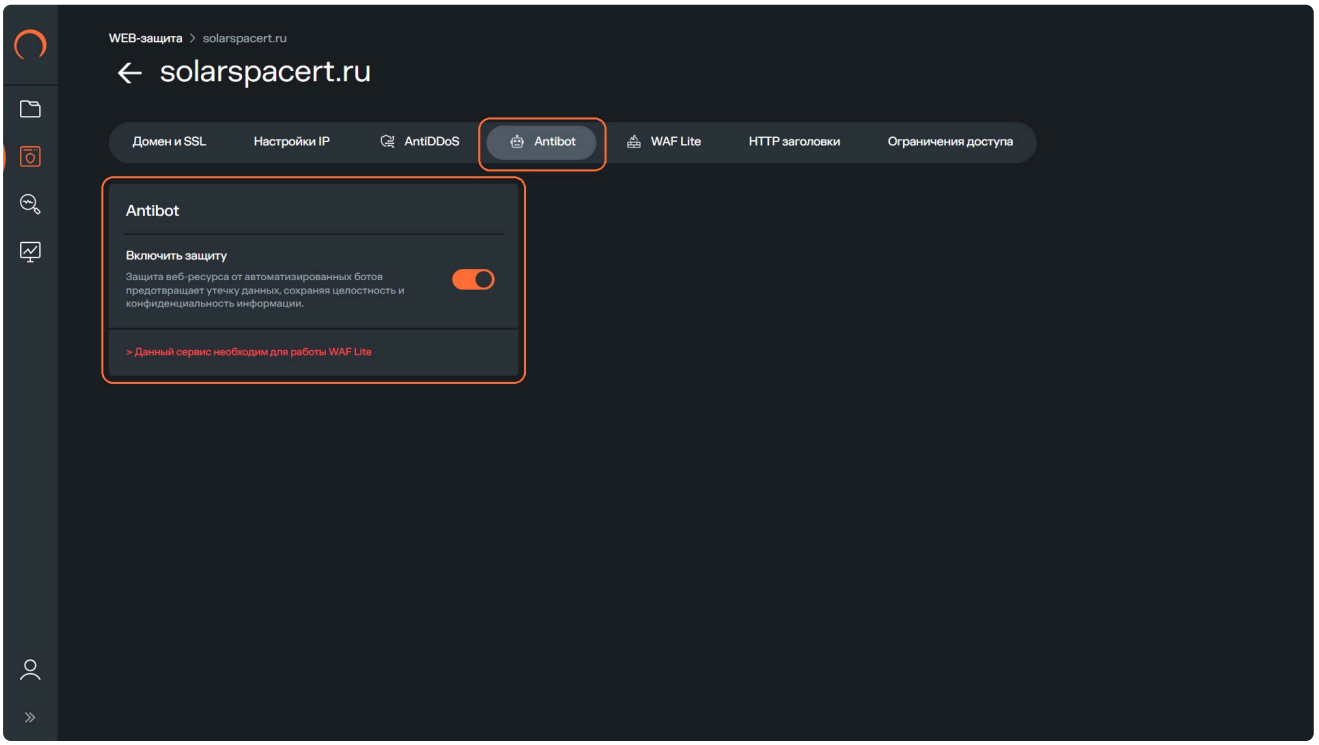
Таким образом WEB AntiDDoS на первом уровне отражает атаки массовыми запросами, а WEB Antibot работает как фильтр для ботов, еще больше "очищая" трафик.

При этом они не смогут обезопасить сайт от таких типов атак, как SQL-инъекции, цель которых состоит в похищении конфиденциальных данных или межсайтового скриптинга. Он заключается во внедрении вредоносных скриптов, которые начинают выполняться, когда обычный пользователь открывает страницу. Цель таких атак – использование уязвимостей веб-ресурса, например, для подмены контента на сайте или взлома пользовательских аккаунтов. Для защиты от этих типов атак необходим WAF Lite.

> ⚠ Важно
>
> WEB AntiDDoS и WEB Antibot — это обязательные уровни защиты, без которых не может быть подключен WAF Lite

На странице сервиса Antibot вы можете прочитать краткое описание и подключить его.

Если вы выбрали Оптимальную версию защиты, в состав которой входит WEB Antibot, то ползунок на этой странице уже находится в состоянии "Подключено".



Если вы только планируете подключить сервис, передвиньте переключатель вправо. Обратите внимание, что подключение возможно при соблюдении следующих условий:

- Ваши домены имеют статус "Под защитой" (это означает, что ваши домены верифицированы, и у вас активирован сервис AntiDDoS)
- Для доменов добавлен SSL-сертификат (добавляется на вкладке "Домен и SSL")
- У вашего ресурса включен расширенный функционал "Редирект на HTTPS" (на вкладке "Домен и SSL")

WAF Lite

WAF Lite в комплексе с WEB Antibot и WEB AntiDDoS обеспечивает продвинутый уровень веб-защиты в рамках комплексного решения Solar Space.

WAF Lite — это «облегченная» версия стандартного WAF (Web Application Firewall). Защищает интернет-ресурсы от веб-атак на уровне L7, направленных на эксплуатацию уязвимостей, например, для подмены контента на сайте, похищения чувствительных данных или взлома пользовательских аккаунтов. Оптимален для защиты небольших веб-ресурсов или в случаях, когда нужна базовая защита без сложных настроек.

Сервис проверяет все входящие запросы к сайту на наличие вредоносных сигнатур – параметров, соответствующих конкретному типу атак. Если запрос содержит такие параметры, WAF Lite блокирует его. Он защищает от атак из списка OWASP Top 10 — это регулярно обновляемый рейтинг основных угроз безопасности веб-приложений, который составляют международные эксперты по информационной безопасности.

Типы атак, от которых защищает WAF Lite

- **RCE (Remote Code Execution)** — тип атаки, при котором злоумышленник использует уязвимости в приложении или системе для выполнения вредоносного кода на удаленном сервере. В случае успешной атаки это может привести к полному захвату системы, утечке или потере конфиденциальных данных. Защита от атак типа RCE включает контроль входящего трафика, блокировку вредоносных команд и сетевых запросов.
- **LFI (Local File Inclusion)** — тип атаки, позволяющий получить доступ к чтению и изменению конфиденциальных файлов на сервере, что может нарушить работу системы и привести к утечке данных. Это происходит, когда приложение неправильно обрабатывает путь к файлу в запросе. Для защиты от таких угроз применяется ограничение доступа к критическим файлам и проверка путей при обработке запросов, что препятствует загрузке или внедрению нежелательных файлов.
- **XSS (Cross-Site Scripting)** — при этом типе атаки злоумышленник внедряет в веб-страницу вредоносные скрипты, которые выполняются в браузере легитимного пользователя. Это позволяет злоумышленнику украсть сессионные данные, подменить содержимое страниц сайта и получить доступ к личной информации пользователя. Фильтрация данных и блокировка непроверенных скриптов помогают предотвратить выполнение вредоносных команд в браузере.
- **SESSION** — тип атаки, при котором злоумышленник перехватывает данные сессии (куки или токены) для получения контроля над учетной записью. После чего он может выполнить действия от имени пользователя, чьи сессионные данные были украдены, включая

получение доступа к конфиденциальной информации. Для защиты от перехвата сессий используется шифрование сессионных данных и безопасное управление сроком их действия. Это исключает возможность их кражи и повторного использования.

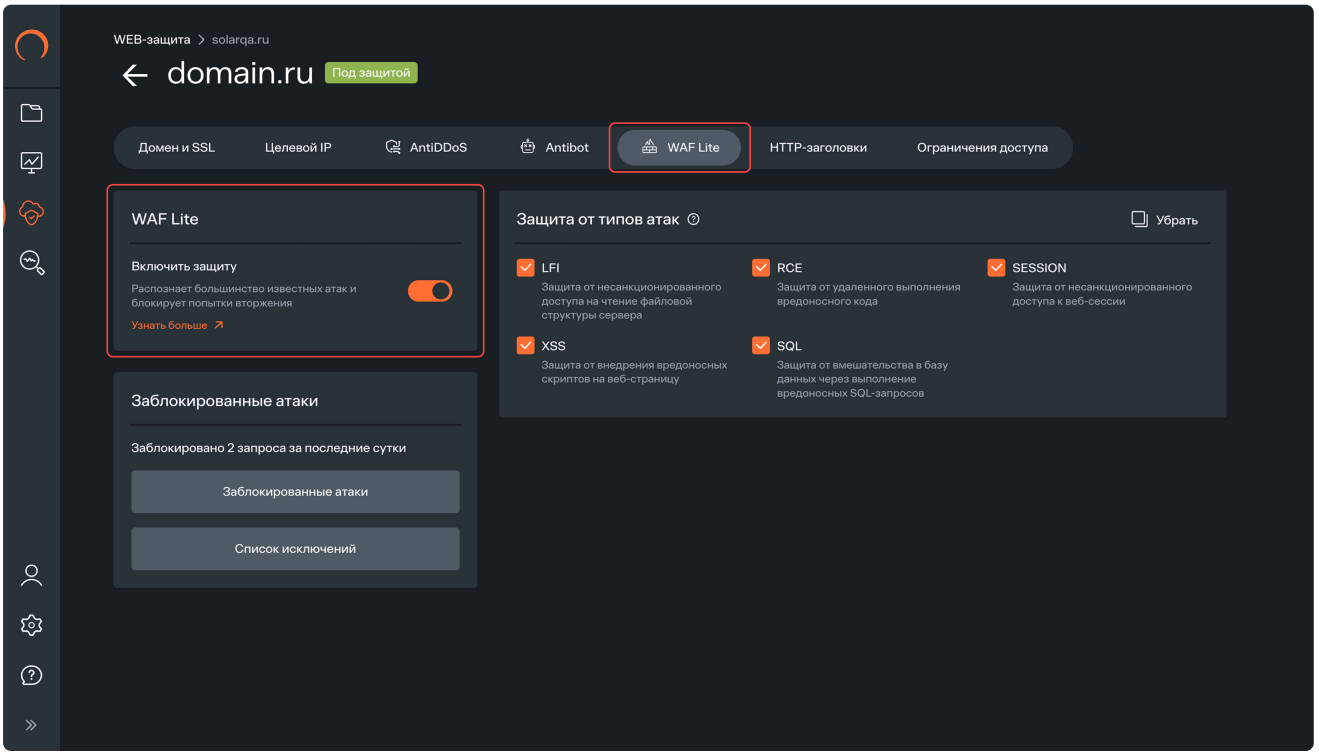
- **SQL** — тип атаки, в ходе которого злоумышленник отправляет вредоносные SQL-запросы на веб-сервер. В случае успешной эксплуатации уязвимости атакующий может изменять, удалять или извлекать данные. Это может привести к утечке конфиденциальной информации, повреждению базы данных или получению прав администратора на веб-ресурсе. Для защиты от типов атак SQL используются параметризированные запросы и фильтрация данных, что предотвращает внедрение вредоносных команд в запросы к базе данных.

> ⚠ Важно
>
> Подключение WAF Lite доступно только при условии активных сервисов WEB AntiDDoS и WEB Antibot. Все три подсистемы обеспечивает максимальную эффективность комплексной защиты веб-ресурсов

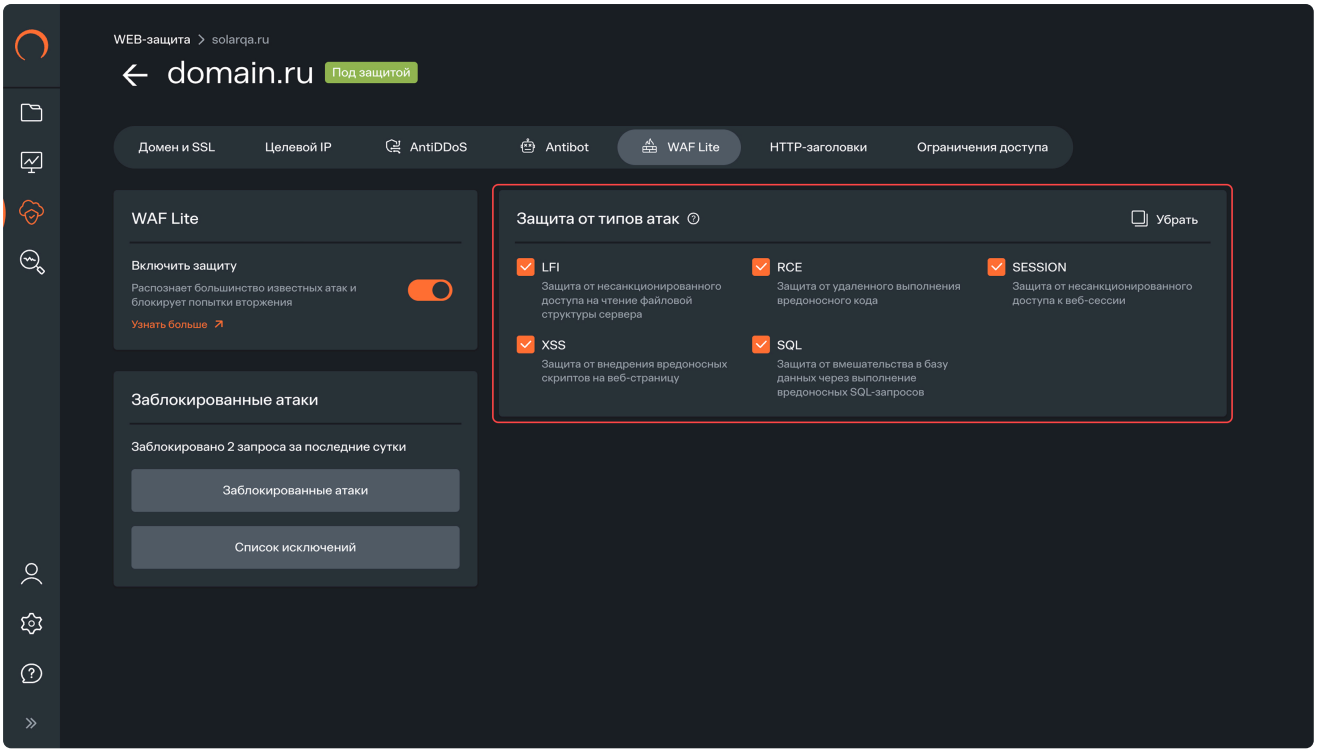
На странице сервиса WAF Lite вы можете прочитать краткое описание и подключить его.

Если вы выбрали версию защиты, в состав которой входит WAF Lite, то ползунок на этой странице уже находится в состоянии "Подключено".
Вы можете активировать WAF Lite при условии, что у вас уже активированы сервисы AntiDDoS и Antibot.

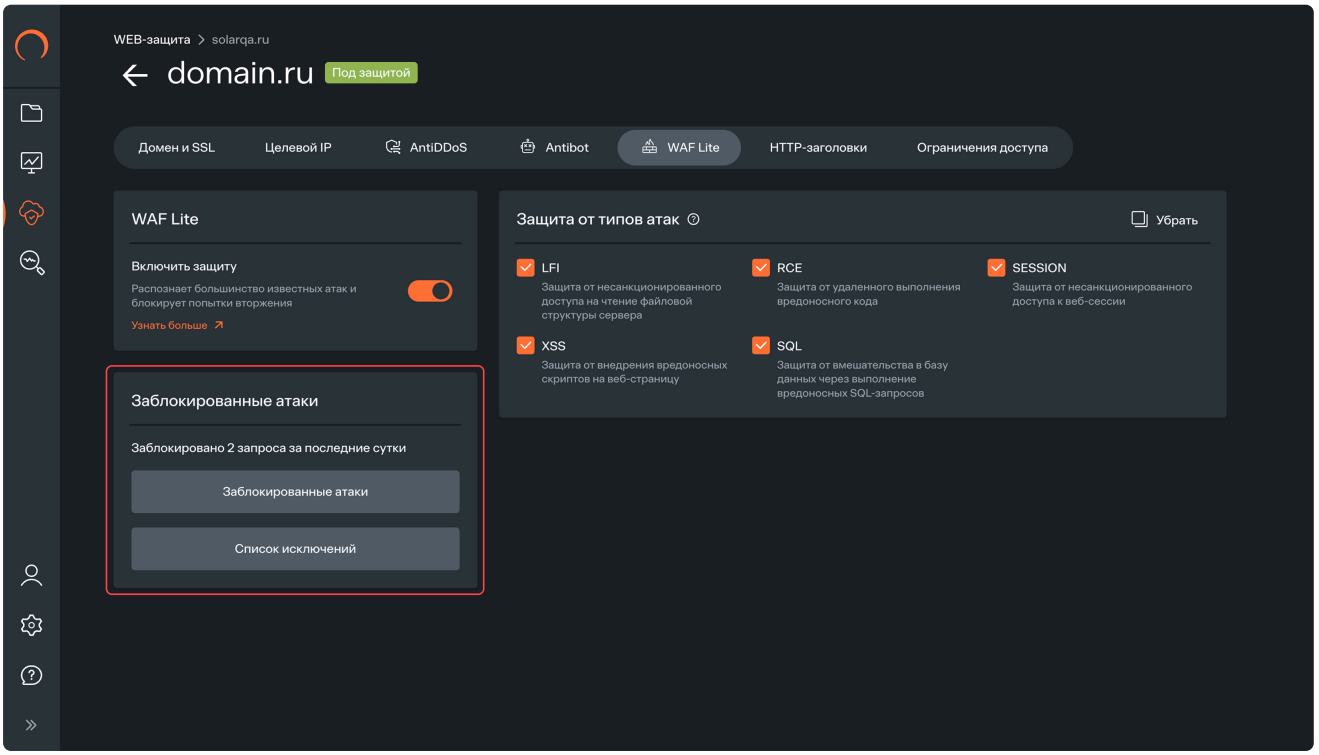
Если сервис отключен, вы увидите текст: "WAF Lite подключен, но не работает, потому что вы выключили Antibot".



На странице сервиса есть список типов атак, защиту от которых обеспечивает WAF Lite.

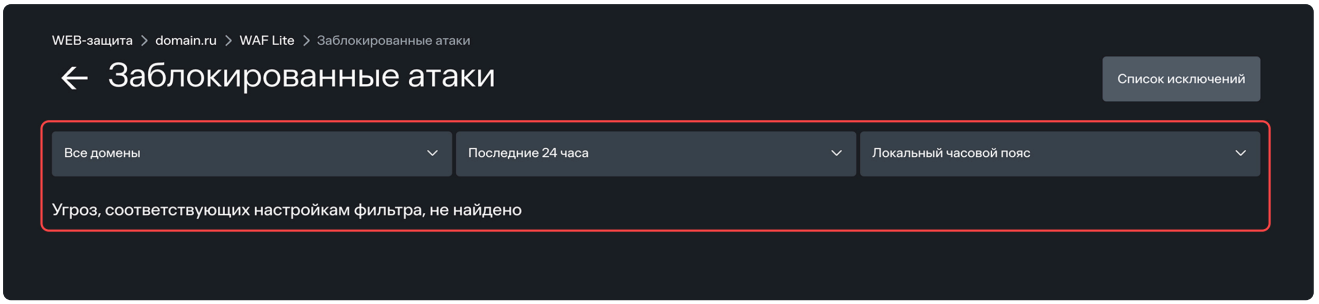


В блоке "Заблокированные атаки" расположены кнопки "Заблокированные атаки" и "Список исключений". При нажатии на них можно просмотреть подробную информацию.

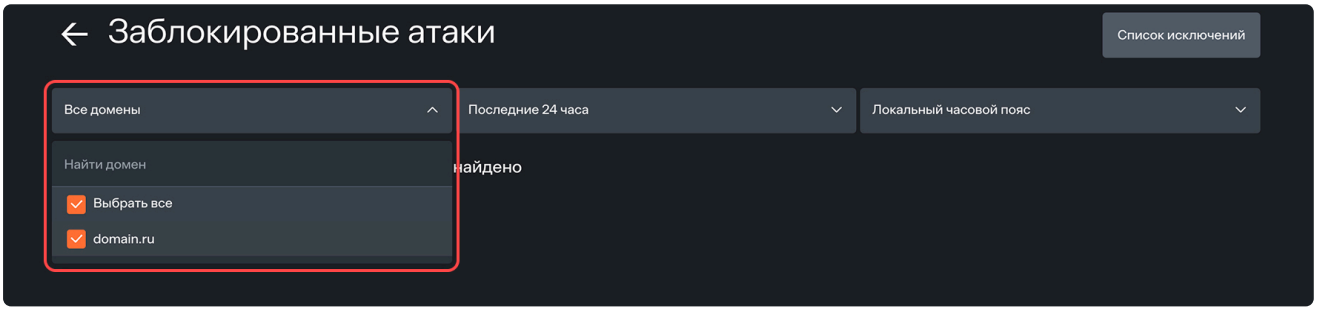


Заблокированные атаки

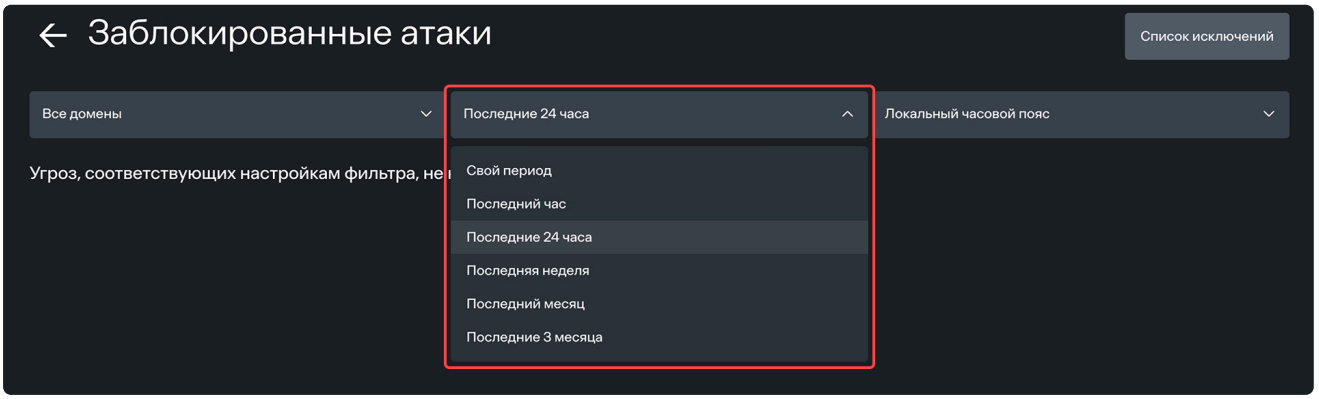
При нажатии на кнопку "Заблокированные атаки" вы перейдете на страницу заблокированных сервисом атак. По умолчанию откроется список за последние сутки, но период можно изменить. Если система не зафиксировала атак за этот период, вы увидите сообщение "Угроз, соответствующих настройкам фильтра, не найдено".



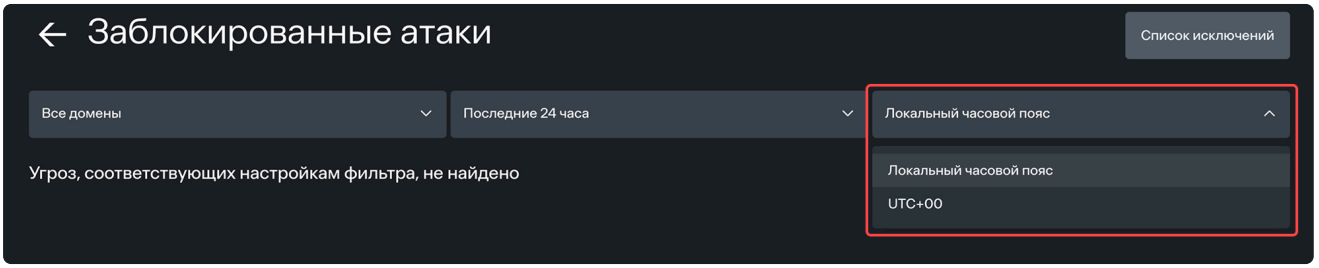
В первом поле можно выбрать ресурсы, для которых будет отображаться отчет.



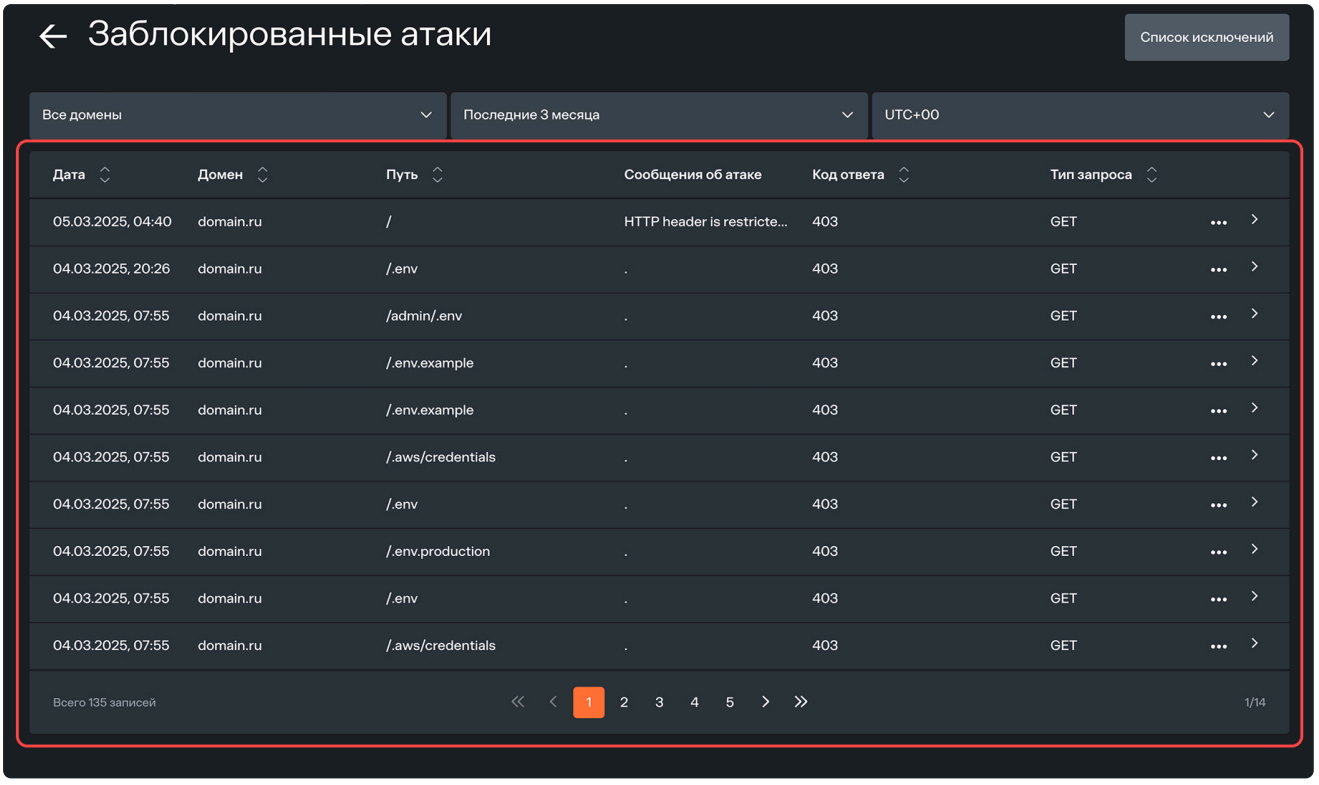
Во втором поле можно изменить период отображения отчета. После выбора вы увидите список атак за нужные даты.



В третьем поле можно изменить часовой пояс. Выберите "Локальный часовой пояс" или "UTC + 00".



Список заблокированных атак:

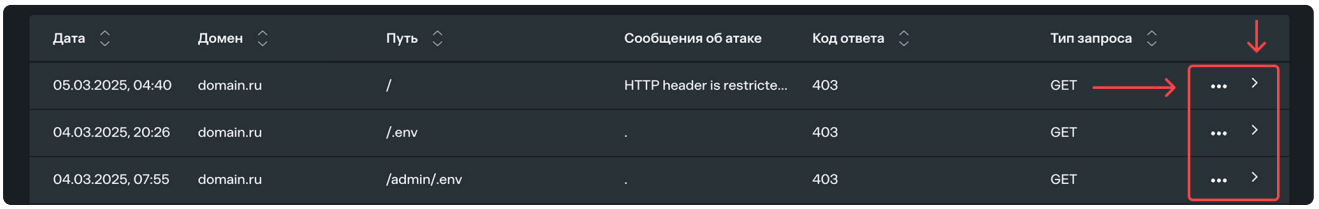


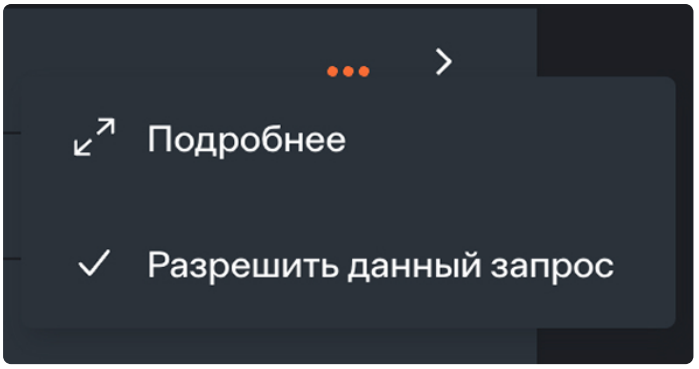
Краткая информация об атаке отражается в следующих полях:

- **Дата** — дата совершения атаки на ресурс
- **Домен** — домен, подвергшийся атаке
- **Путь** — по какому пути была совершена атака
- **Сообщение об атаке** — название типа атаки
- **Код ответа** — код ответа WAF Lite на совершенную атаку
- **Тип запроса** — метод совершения атаки

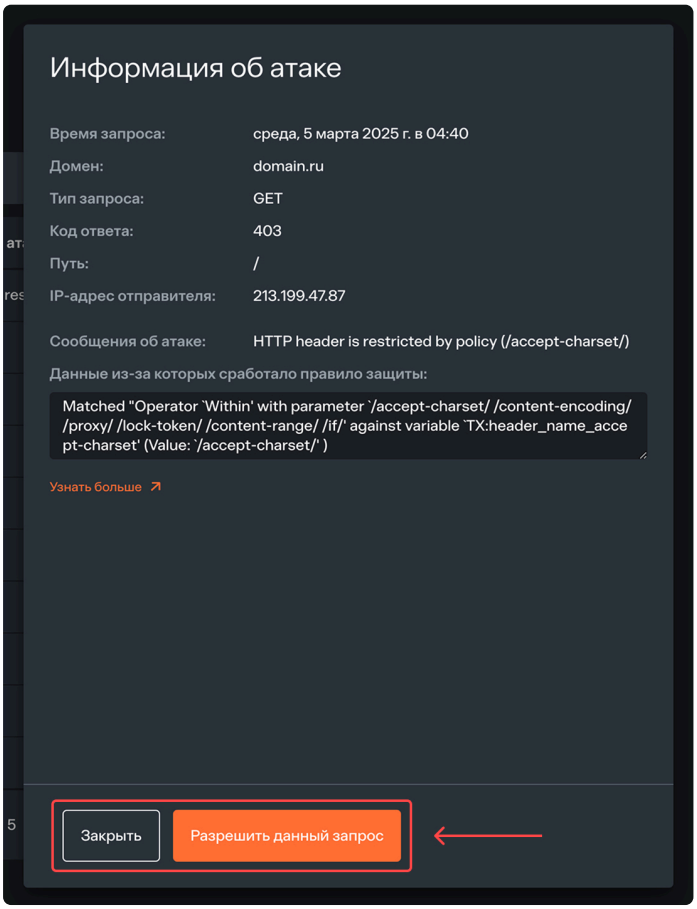
Для всех полей кроме "Сообщения об атаке" доступна сортировка по возрастанию/убыванию.

Для просмотра подробной информации об атаке нажмите на стрелочку в правой части строки или на иконку троеточия для вызова меню.





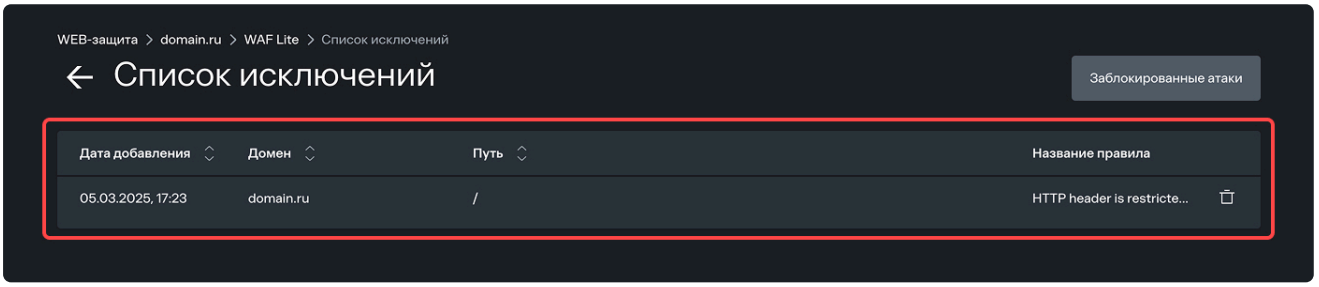
При нажатии на стрелочку или на пункт меню "Подробнее" в правой части экрана откроется окно с информацией об атаке.



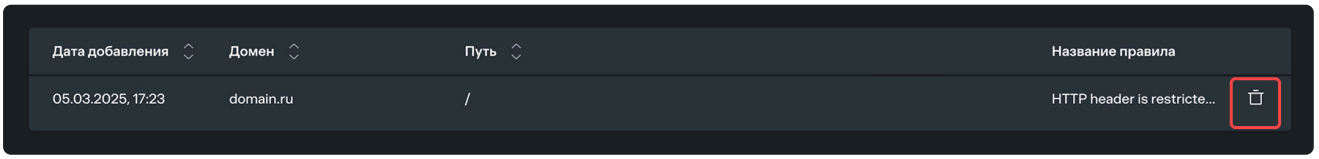
Если нажмете "Закрыть", окно закроется. Если нажмете "Разрешить данный запрос", он пропадет из списка заблокированных атак и в дальнейшем не будет блокироваться при условии, что придет по тому же пути. Также вы можете выбрать вариант "Разрешить данный запрос", не открывая это окно. Достаточно нажать на три точки в строке атаки и кликнуть по второму пункту в появившемся меню.

Список исключений

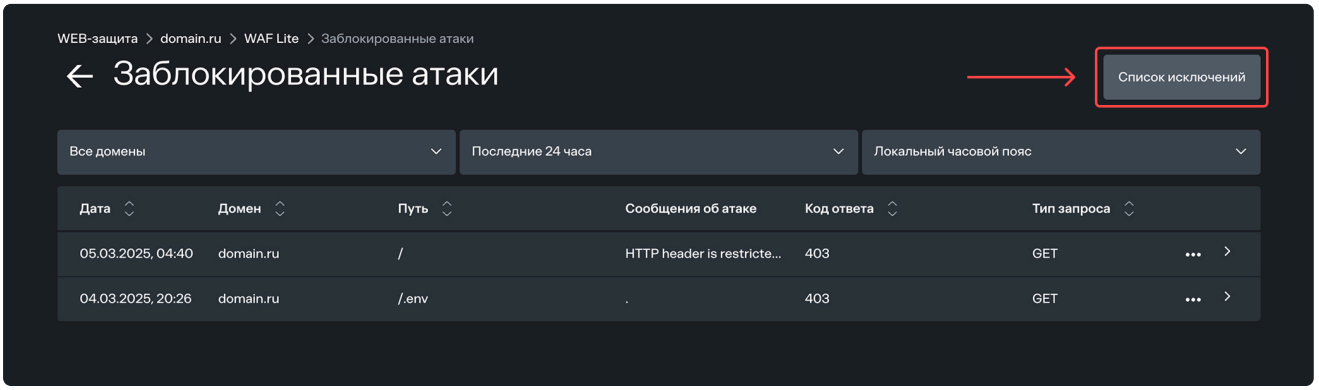
Список разрешенных запросов вы найдете в разделе "Список исключений" на вкладке WAF Lite.

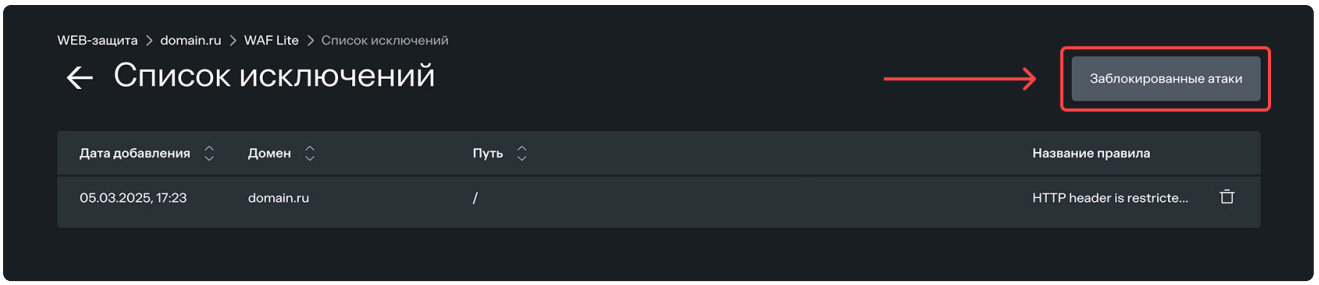


Запрос можно удалить из списка разрешенных. Для этого нажмите на иконку корзины справа в строке.



Для быстрого перемещения между страницами нажмите на кнопку "Список исключений" или "Заблокированные атаки" в правой верхней части страницы.
Название кнопки будет отличаться в зависимости от того, на какой странице вы сейчас находитесь.





Если вы не добавили ни одно исключение, при переходе в "Список исключений" вы увидите надпись "Исключений не найдено".

Настройки

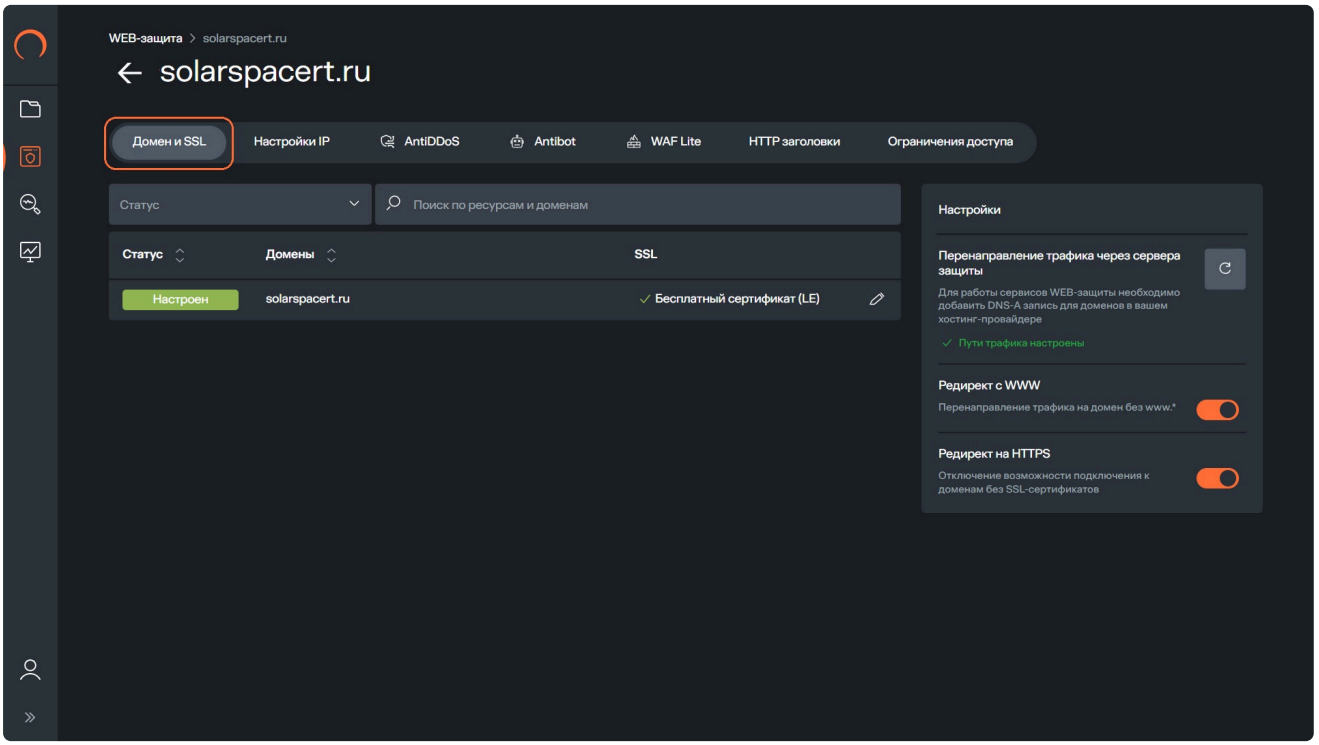
На странице ресурса в рамках Веб-защиты вам доступен функционал на следующих вкладках:

- Домен и SSL
- Целевой IP
- AntiDDoS
- Antibot
- WAF Lite
- HTTP-заголовки
- Ограничения доступа

Домен и SSL

На этой вкладке вы можете:

- Добавить SSL-сертификат
- Настроить перенаправление трафика
- Включить дополнительные настройки



Добавление SSL-сертификата

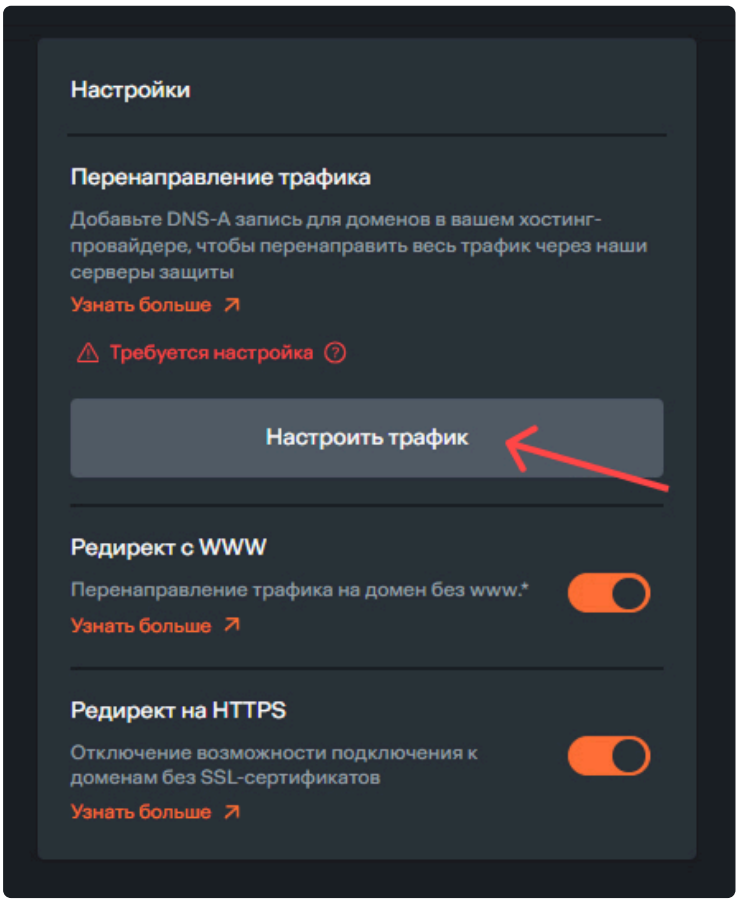
SSL-сертификат можно добавить только для домена, который прошел проверку по DNS-A записи и находится в статусе "Под защитой". Подробную инструкцию по добавлению SSL-сертификата читайте здесь.

> **Обратите внимание**
>
> Если вы используете SSL-сертификат Let's Encrypt (LE), вам не нужно его обновлять. Он будет продлеваться автоматически. Если вы используете свой сертификат, не забывайте загружать в личный кабинет актуальную версию после его обновления.

Перенаправление трафика

Для перенаправления трафика выполните следующие действия:

1. В блоке "Перенаправление трафика" нажмите на кнопку "Настроить трафик".

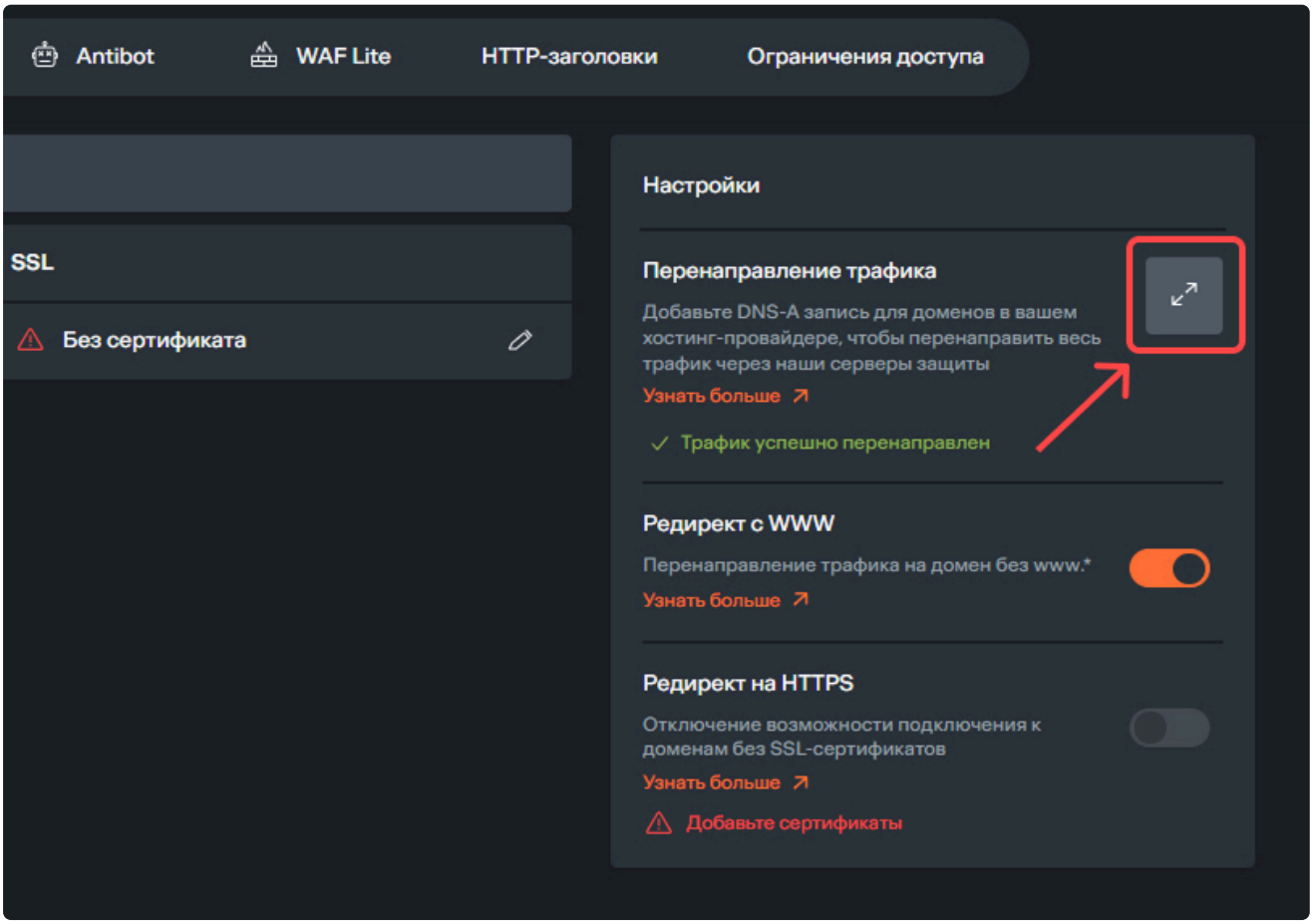


2. В появившемся окне скопируйте представленную DNS-A запись Solar Space.
3. Дальнейшие действия аналогичны настройке перенаправления трафика после создания ресурса, начиная с пункта 2.

> Обратите внимание
>
> Если после повторной настройки перенаправления трафика ваш ресурс находится в статусе "Не защищен", читайте статью о возможных ошибках при верификации и перенаправлении трафика

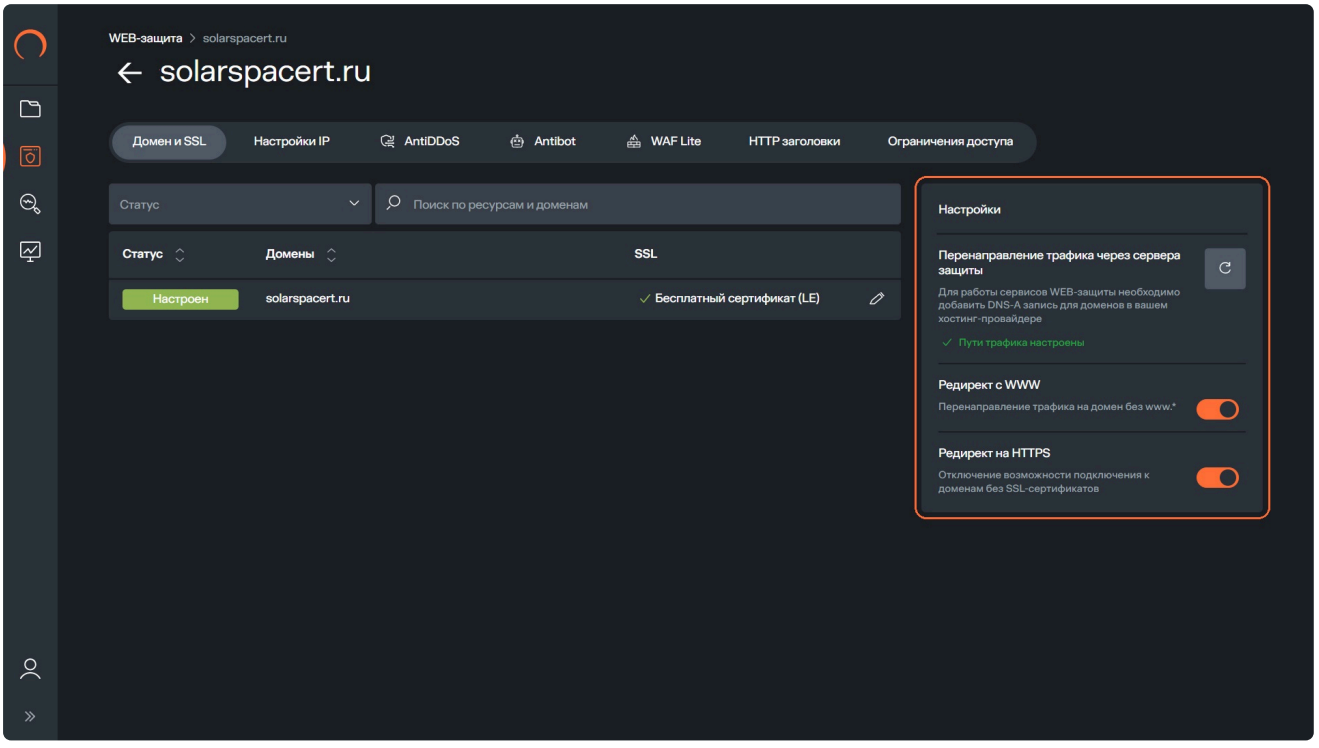
После успешного обновления DNS-записей в блоке "Настройки" вы увидите уведомление "Трафик успешно перенаправлен".

Для просмотра A-записи — IP-адреса сервера защиты Solar Space — нажмите на иконку с двумя стрелочками.



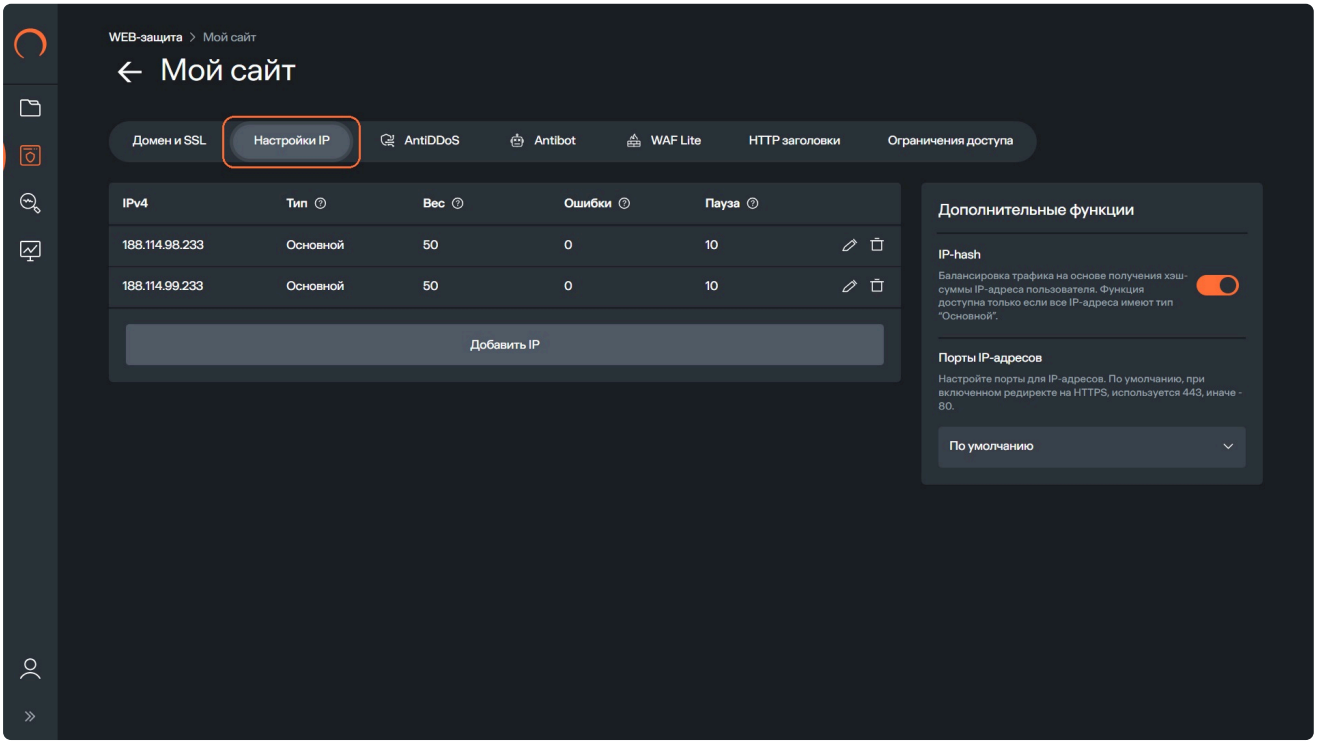
Дополнительные настройки

На вкладке "Домен и SSL" можно включить расширенный функционал: "Редирект с WWW" и "Редирект на HTTPS".



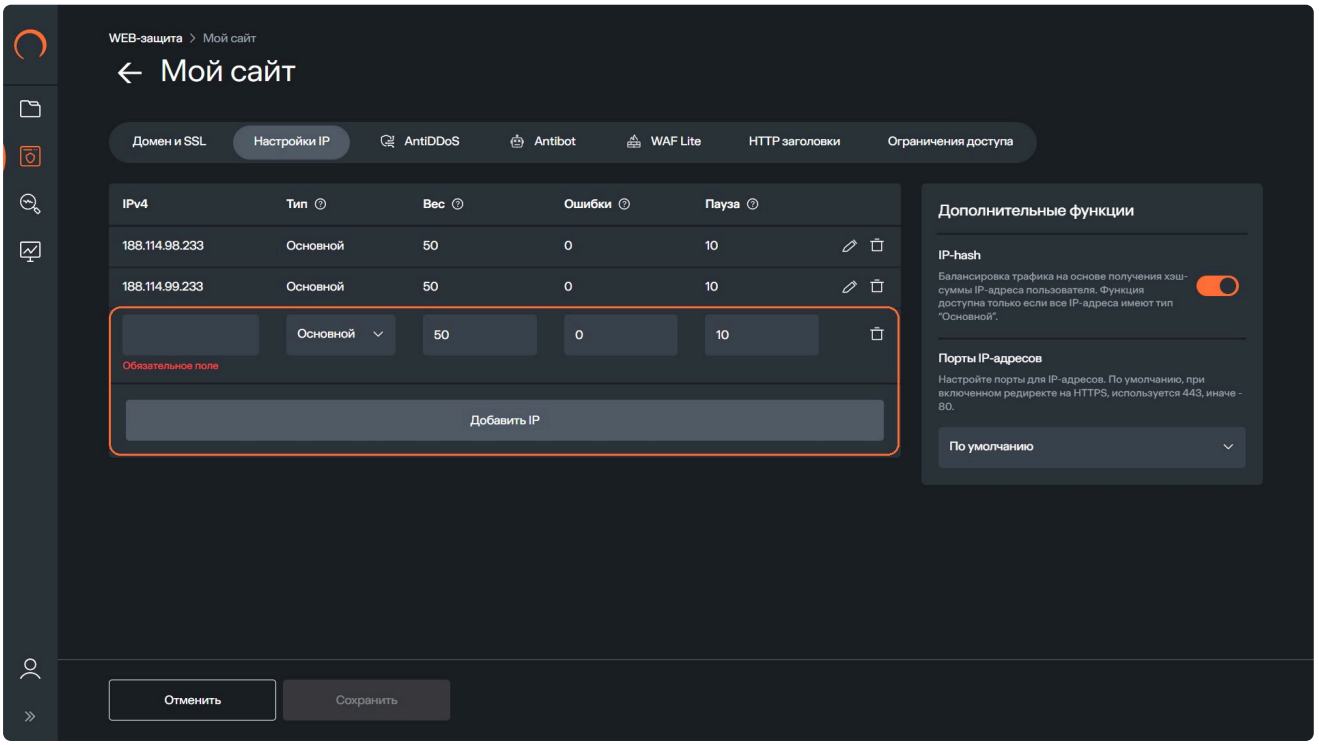
- **Редирект с WWW** — перенаправление трафика на домен с WWW. Поисковые системы рассматривают URL-адреса с "WWW" и без "WWW" как разные страницы, а для пользователей эта разница неочевидна. Если в адресе вашего сайта используется "WWW", а пользователи для экономии времени вводят адрес без "WWW", то включенный редирект перенаправит их на ваш сайт. При отключенном редиректе сервер не найдет нужную страницу
- **Редирект на HTTPS** — если подключить эту функцию, все запросы к серверу, отправленные по небезопасному протоколу HTTP, будут автоматически переходить на безопасный протокол HTTPS, что сделает взаимодействие пользователя с сайтом защищенным

Целевой IP



Нажмите "Добавить IP" для добавления IP-адреса вашего ресурса. Если у вас несколько IP-адресов, вы увидите форму расширенных настроек с возможностью добавить новый IP и подключить расширенный функционал.

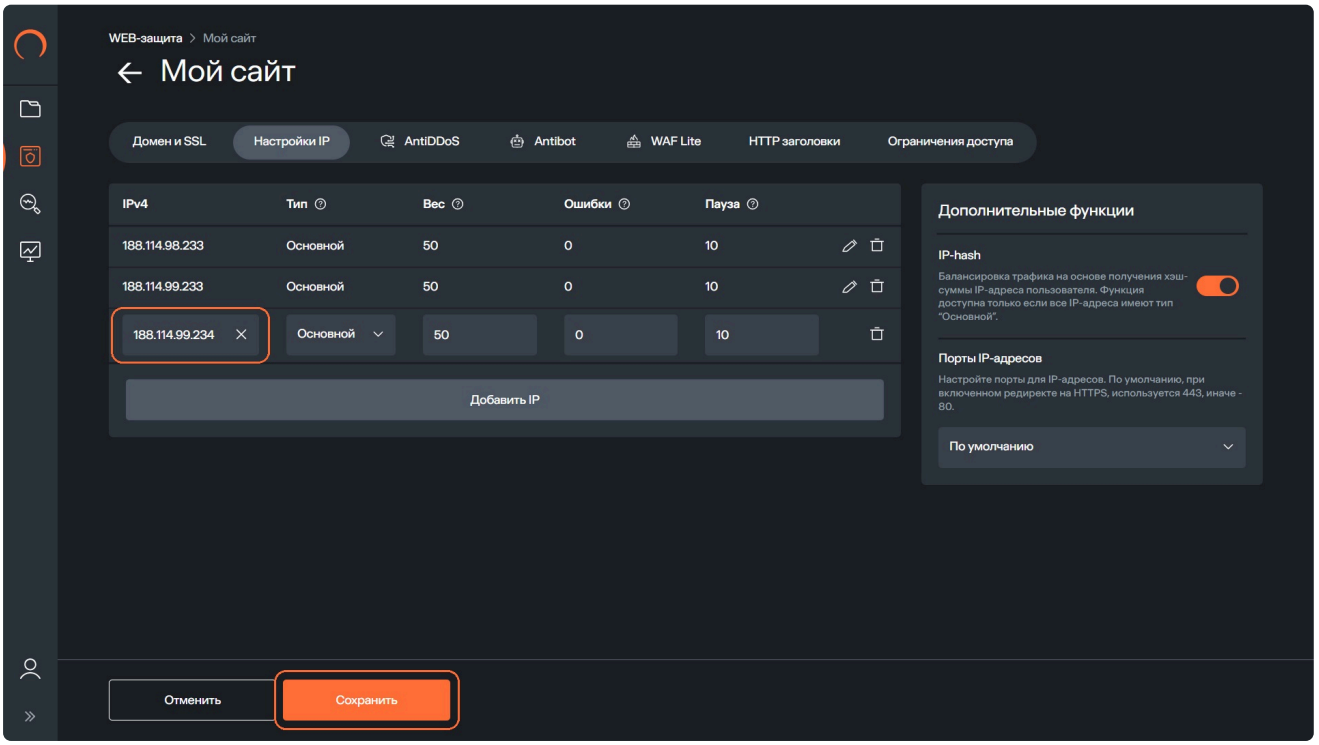
Откроется страница настроек IP, где все поля предзаполнены по умолчанию, кроме поля "IPv4". Если у вас есть дополнительный IP-адрес, его нужно ввести в это поле. Появится строка с полями для вашего IP-адреса.



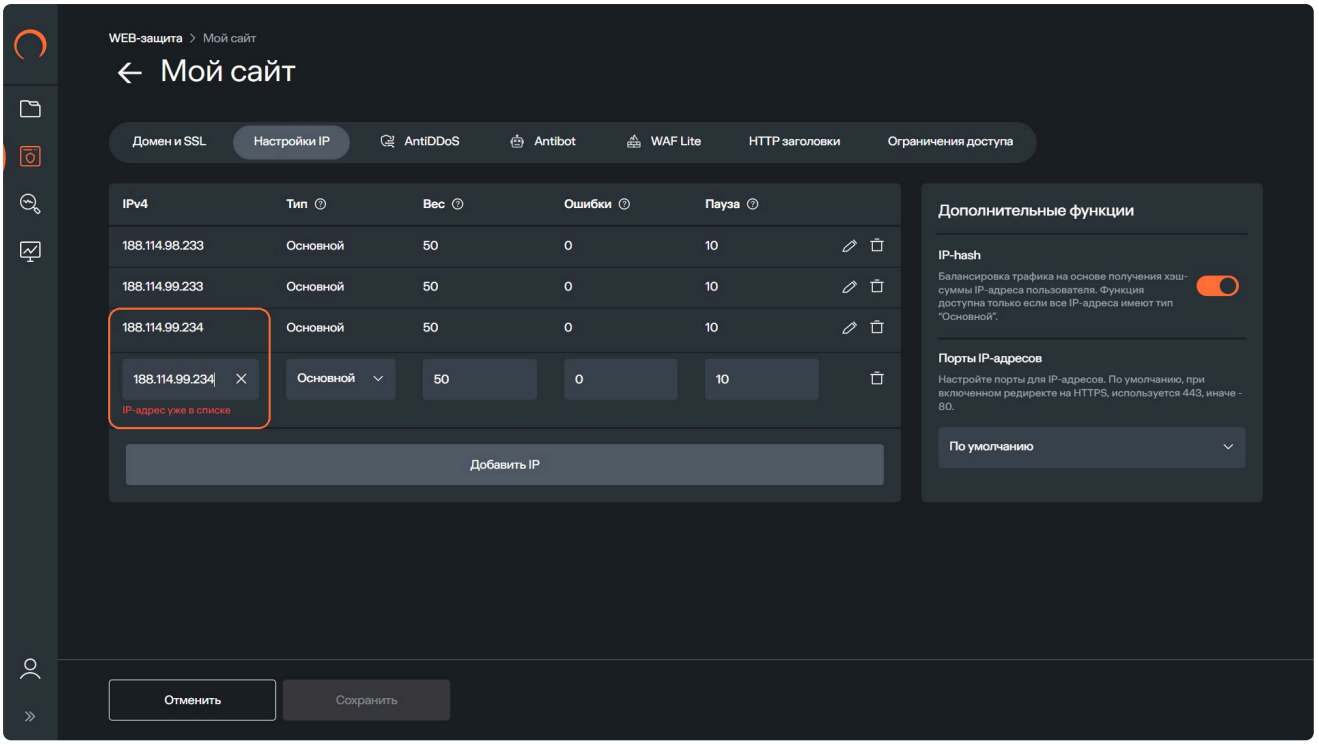
Все предзаполненные поля можно редактировать:

- **Тип** — выберите из выпадающего списка "Основной или "Запасной". По умолчанию установлен "Основной". Если вы установите "Запасной" (резервный), он подключится только при недоступности основного IP-адреса
- **Вес** — значение от 1 до 100, которое отражает приоритет IP-адреса в рамках защиты от атак. Чем важнее и критичнее для вашего бизнеса доступность конкретного IP-адреса, тем выше должен быть его вес. Например, если у вас два IP-адреса, доступность которых одинаково важна, то в поле "Вес" для каждого должно быть значение "50". Если для одного поставить значение "70", а для другого "30", то система защиты будет направлять больше трафика на IP-адрес с бОльшим весом
- **Ошибки** — значение от 1 до 10 000, которое отражает количество допустимых ошибок при соединении с сервером. При превышении количества ошибок система пометит сервер недоступным и не будет переводить на него трафик. По умолчанию установлено "0", то есть при первой же ошибке соединения система присвоит серверу статус "Недоступен"
- **Пауза** — значение от 1 до 1800, обозначает время в секундах, через которое система попытается повторно восстановить соединение с сервером, помеченным статусом "Недоступен"

После этого нажмите кнопку "Сохранить" в нижней части страницы.



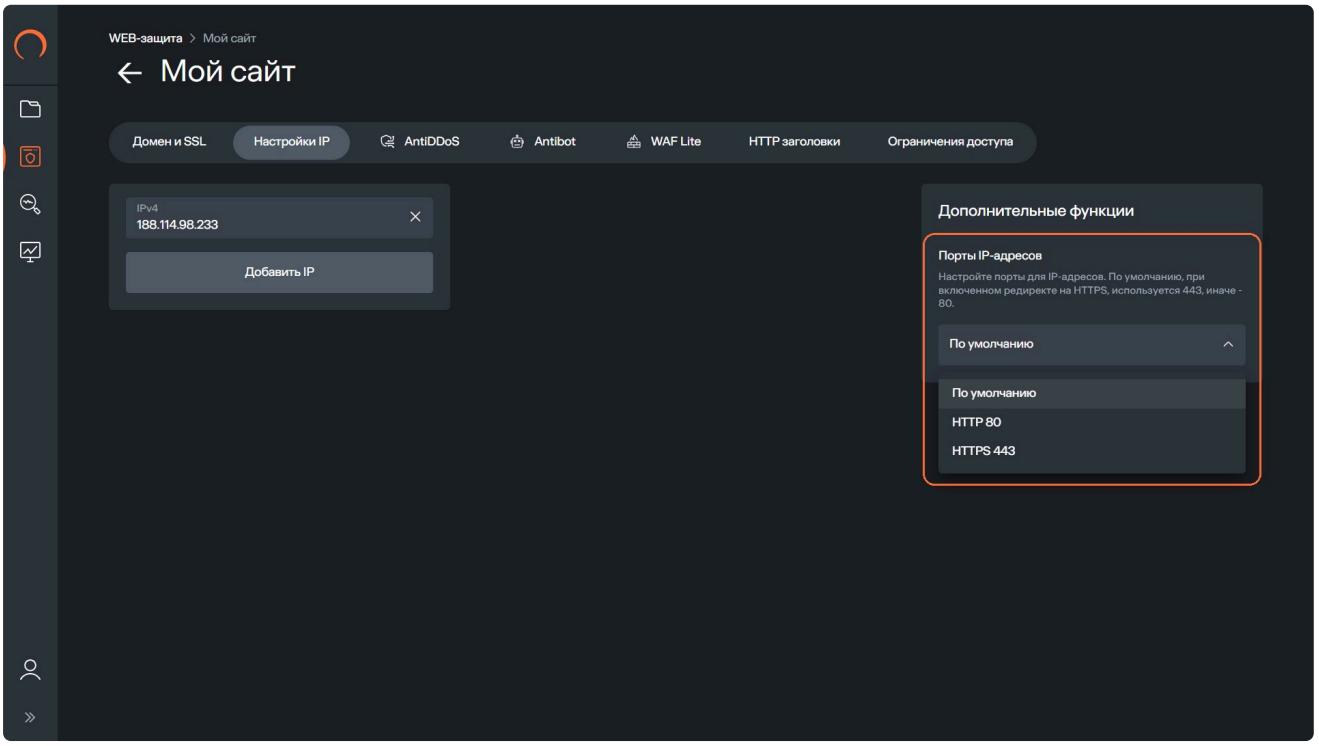
Если в поле ввода IP-адреса ввести уже существующий IP-адрес, отобразится соответствующая надпись о том, что такой IP-адрес уже есть.



Дополнительные функции

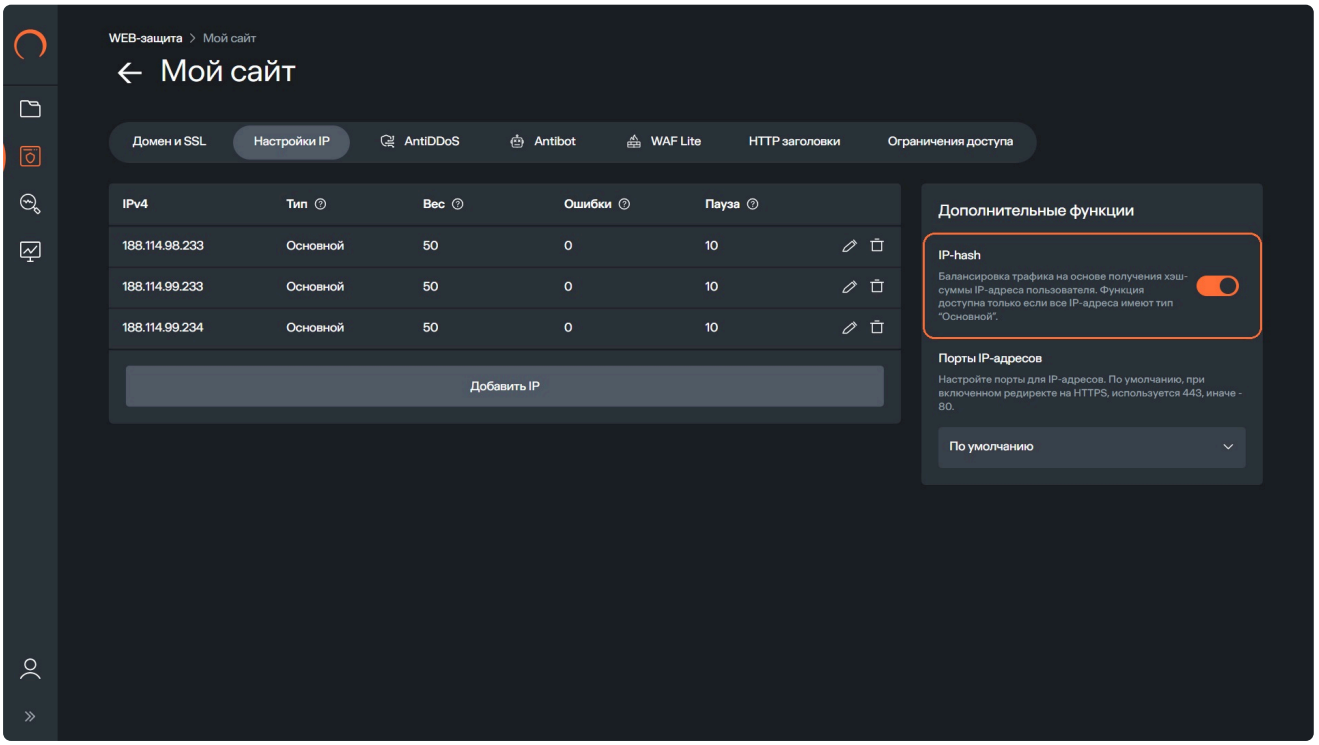
Если у вас один IP-адрес, то в правой части страницы будет раздел "Дополнительные функции", с возможностью настроить блок "Порты IP-адресов".

Порты установлены "По умолчанию", если вам нужно, вы можете изменить этот параметр на HTTP или HTTPS. Порты IP-адресов определяют, через какой порт будет устанавливаться соединение с сервером-источником. Доступны три варианта: "По умолчанию", "HTTP 80", "HTTPS 443".



- **Порт 80** поддерживает протокол HTTP — информация передается между браузером и сервером в виде обычного текста, что небезопасно
- **Порт 443** поддерживает протокол HTTPS — информация, передаваемая между сервером и браузером, зашифровывается, что повышает безопасность обмена данными
- **По умолчанию** — означает, что если на вкладке "Домен и SSL" у вас включен расширенный функционал "Редирект на HTTPS", то трафик проходит через безопасный порт 443. Если настройка "Редирект на HTTPS" на вкладке "Домен и SSL" у вас отключена, то трафик проходит через незащищенный порт 80

Если у вас несколько IP-адресов, то в правой части экрана отображается окно с еще одной дополнительной функцией: IP-hash. При введении нескольких IP-адресов с типом "Основной", она сразу будет активной.



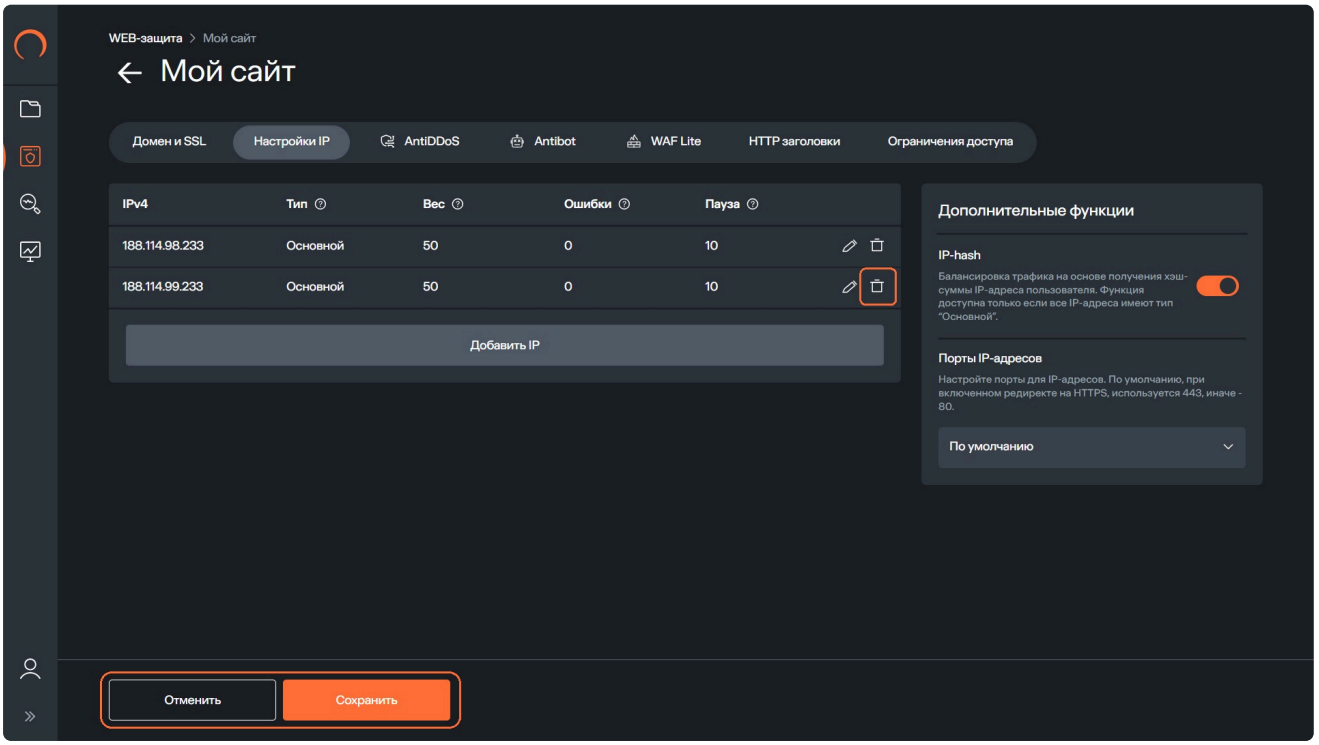
IP-hash — это метод распределения нагрузки между серверами. Он гарантирует, что пользователь с конкретным IP подключится к тому же серверу, с которым работал ранее. Этот алгоритм часто используют для веб-приложений, поскольку в них пользователь взаимодействует с интерфейсом, – например, заходит в личный кабинет, добавляет товары в корзину. При использовании IP-hash балансировки пользователь подключится к тому же сеансу: ему не понадобится снова заходить в личный кабинет.

> Обратите внимание
>
> Функция IP-hash доступна, если все введенные IP-адреса имеют тип "Основной"

Удаление IP-адреса

Для удаления IP нажмите на иконку корзины в строке с нужным адресом, в обновленной странице нажмите кнопку "Сохранить".

Если необходимо вернуть удаленный ресурс, нажмите кнопку "Отменить".


WEB-защита > Мой сайт
Мой сайт
Домен и SSL
Настройки IP
AntiDDoS
Antibot
WAF Lite
HTTP заголовки
Ограничения доступа
IPv4
Тип
Вес
Ошибки
Пауза
188.114.98.233
Основной
50
0
10
188.114.99.233
Основной
50
0
10
Добавить IP
Дополнительные функции
IP-hash
Балансировка трафика на основе получения хэш-суммы IP-адреса пользователя. Функция доступна только если все IP-адреса имеют тип "Основной".
Порты IP-адресов
Настройте порты для IP-адресов. По умолчанию, при включенном редиректе на HTTPS, используется 443, иначе - 80.
По умолчанию
Отменить
Сохранить

HTTP-заголовки

> **Обратите внимание**
> Эта вкладка необязательна для заполнения. Если вы не используете HTTP-заголовки для своего сайта, их не нужно добавлять. Наличие или отсутствие HTTP-заголовков не влияет на эффективность работы наших сервисов защиты.

HTTP-заголовки — это простой способ улучшить производительность сайта и повысить безопасность. Правильные заголовки снижают риск распространенных веб-атак, таких как межсайтовый скриптинг или кликджекинг. В этой статье рассмотрим, что такое HTTP-заголовки, как они работают, и какие заголовки нужно добавить в ответы сервера, чтобы оптимизировать работу сайта и сделать взаимодействие пользователей с ним более безопасным.

Что такое HTTP-заголовки

Когда пользователь хочет открыть какой-то сайт, его браузер отправляет запрос к серверу этого сайта. Сервер принимает запрос, отправляет в ответ нужный сайт, и он открывается в браузере. Для пользователя это взаимодействие выглядит, как пара кликов. Для того, чтобы это стало возможным, браузер и сервер обмениваются служебной информацией с помощью HTTP-сообщений: запросов и ответов.

В каждом HTTP-сообщении содержится HTTP-заголовок, благодаря которому браузер пользователя и сервер сайта понимают, как им взаимодействовать друг с другом.

Как работают HTTP-заголовки

HTTP-заголовки запроса передают серверу информацию о том, какой именно ресурс хочет открыть пользователь, как он намерен с ним взаимодействовать: к примеру, посмотреть видео или скачать документ.

HTTP-заголовки ответов, которые отправляет сервер, тоже содержат информацию: название открываемого сайта, в каком формате пользователь получит данные и так далее. Если мы пытаемся открыть сайт и видим ошибку 404, это тоже ответ сервера. Таким образом он сообщает браузеру, что нужная нам страница не найдена. Это происходит, если владелец сайта ее удалил.

Каждый HTTP-заголовок состоит из двух частей: ключа (key) и значения (value).

Ключ представляет собой название заголовка, которое описывает передаваемую информацию (например, Content-Type). Значение уточняет параметры или инструкции для обработки запроса или ответа (например, text/html; charset=UTF-8).

Key	Value	Что означает
Connection	keep-alive	Заголовок указывает серверу, что соединение нужно оставить открытым: сервер не закроет соединение сразу после отправки ответа, и следующий запрос от этого же клиента к серверу будет выполнен быстрее.
Cache-control	no-cache, no-store, must-revalidate сервер	Сообщает клиенту, что кэширование контента веб-ресурса запрещено, и каждая его копия должна быть получена непосредственно с сервера.

В личном кабинете Solar Space вы можете добавить HTTP-заголовки ответов, которые ваш сервер будет отправлять в ответ на запросы к нему. Далее приведем конкретные примеры заголовков, которые будут полезны для веб-ресурсов.

Зачем вашему сайту HTTP-заголовки

HTTP-заголовки, добавленные в ответ сервера, положительно влияют:

1. На уровень безопасности. Они снижают риск атак, цель которых – завладеть данными пользователей и перехватить конфиденциальную информацию.
2. На управление сайтом. Существуют атаки, позволяющие полностью или частично перехватить управление веб-ресурсом и использовать его в своих целях. С помощью определенных HTTP-заголовков можно минимизировать риски таких атак.
3. На производительность веб-ресурса. Некоторые HTTP-заголовки помогают сайту работать быстрее, а серверу — эффективнее использовать мощности.

Разберем подробнее примеры заголовков для каждого из этих пунктов.

Безопасность

Key	Value	Что означает
Strict-Transport-Security	max-age=31536000; includeSubDomains	Этот заголовок указывает браузеру использовать только защищенный протокол HTTPS для соединений с этим доменом и всеми его поддоменами в течение одного года (31536000 секунд). max-age=31536000 – задаёт срок действия политики (в данном случае 1 год). includeSubDomains – применяет политику ко всем поддоменам текущего домена. Это защищает взаимодействие сайта и пользователя от атак типа «человек посередине», которые возможны при незащищенной передаче данных с помощью протокола HTTP. Во время таких атак злоумышленник перехватывает данные, которыми обмениваются сервер и клиент.
Content-Security-Policy	default-src 'self'; script-src 'self	default-src 'self' – указывает, что все ресурсы (скрипты, стили, изображения и т.д.) могут загружаться только с собственного сервера. script-src 'self' – уточняет, что загружать и выполнять скрипты разрешено исключительно с того же домена. Это

Key	Value	Что означает
		помогает предотвратить атаки типа XSS (межсайтовый скриптинг). Во время такой атаки в веб-страницу внедряется вредоносный скрипт, который начинает выполняться, как только пользователь открывает эту страницу. Целью таких атак обычно становятся личные данные пользователей.

> Обратите внимание
>
> Заголовок Content-Security-Policy нуждается в постоянном обновлении. Используйте его, если готовы поддерживать актуальность данных.

Управление сайом и политикой доступов

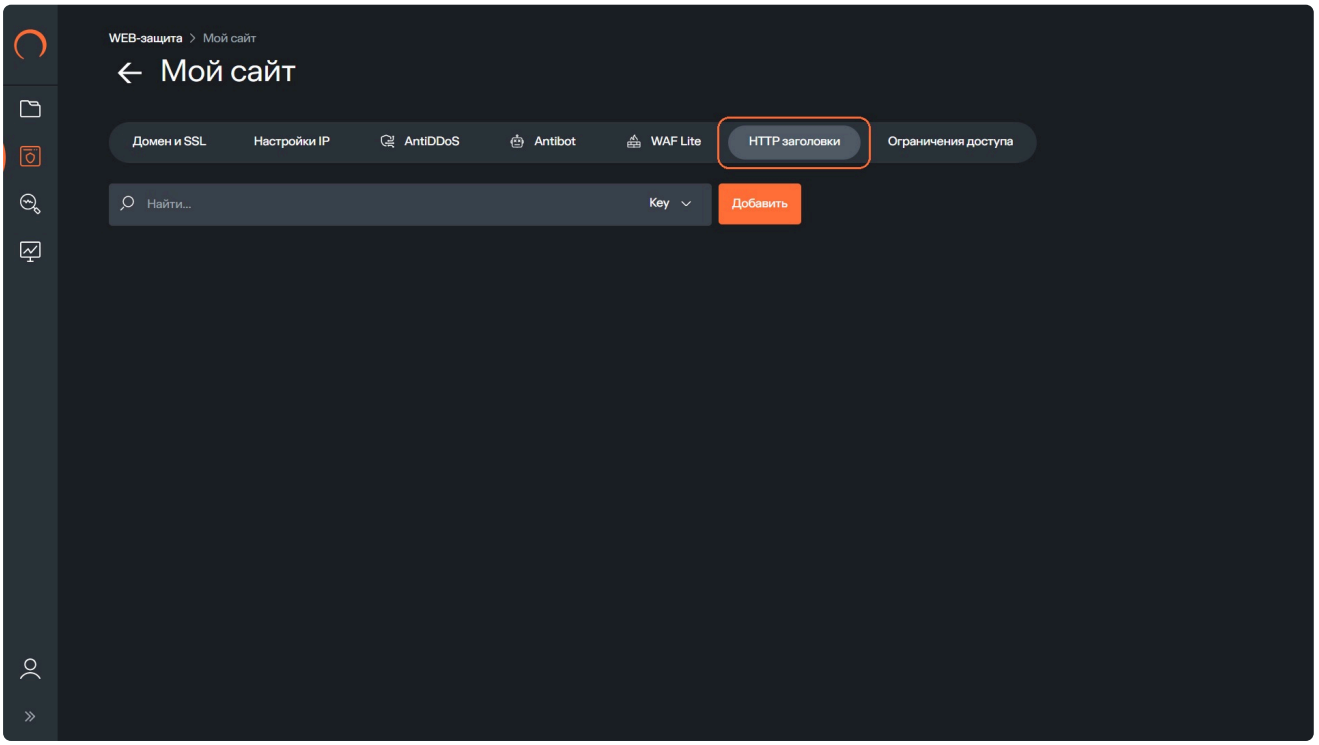
Key	Value	Что означает
X-Frame-Options	SAMEORIGIN	Указывает, что встроить вашу веб-страницу или ее фрагмент можно только на вашем же домене. Если вместо SAMEORIGIN в поле значения указать DENY, то встраивание веб-страницы будет запрещено на любых ресурсах. Обезопасит от атак вида clickjacking (кликджекинг): когда часть веб-страницы интегрируется на посторонний ресурс, настоящее содержимое которого будет невидимым для пользователя. Так вполне законопослушные сайты становятся орудием в руках мошенников.
X-XSS-Protection	1; mode=block	Указывает браузеру, что нужно включить встроенную защиту от атак вида XSS (межсайтовый скриптинг). При обнаружении подозрительных скриптов браузер не будет пытаться их очистить, а сразу заблокирует. Защищает пользователей от кражи данных или других последствий XSS-атак.

Повышение производительности

Key	Value	Что означает
Cache-Control	public, max-age=3600	Заголовок для управления кэшированием. Параметр public указывает, что сохранять ответ сервера можно в любом кэше – в браузере пользователя, на прокси-серверах или в сети доставки контента, если сайт использует ее. Параметр max-age=3600 сообщает, что ответ может быть сохранен на 3600 секунд (1 час). Это уменьшит количество запросов к серверу, так как браузер в течение часа будет использовать сохраненную копию веб-страницы, не обращаясь к серверу и не расходуя его ресурсы.
Content-Encoding	gzip	Этот заголовок указывает, что содержимое ответа сервера сжато с использованием алгоритма gzip. Браузер автоматически "разжимает" данные при получении, так что пользователь не заметит разницы, но страница загрузится быстрее.

Добавьте эти заголовки в личном кабинете Solar Space, чтобы повысить эффективность и безопасность вашего сайта.

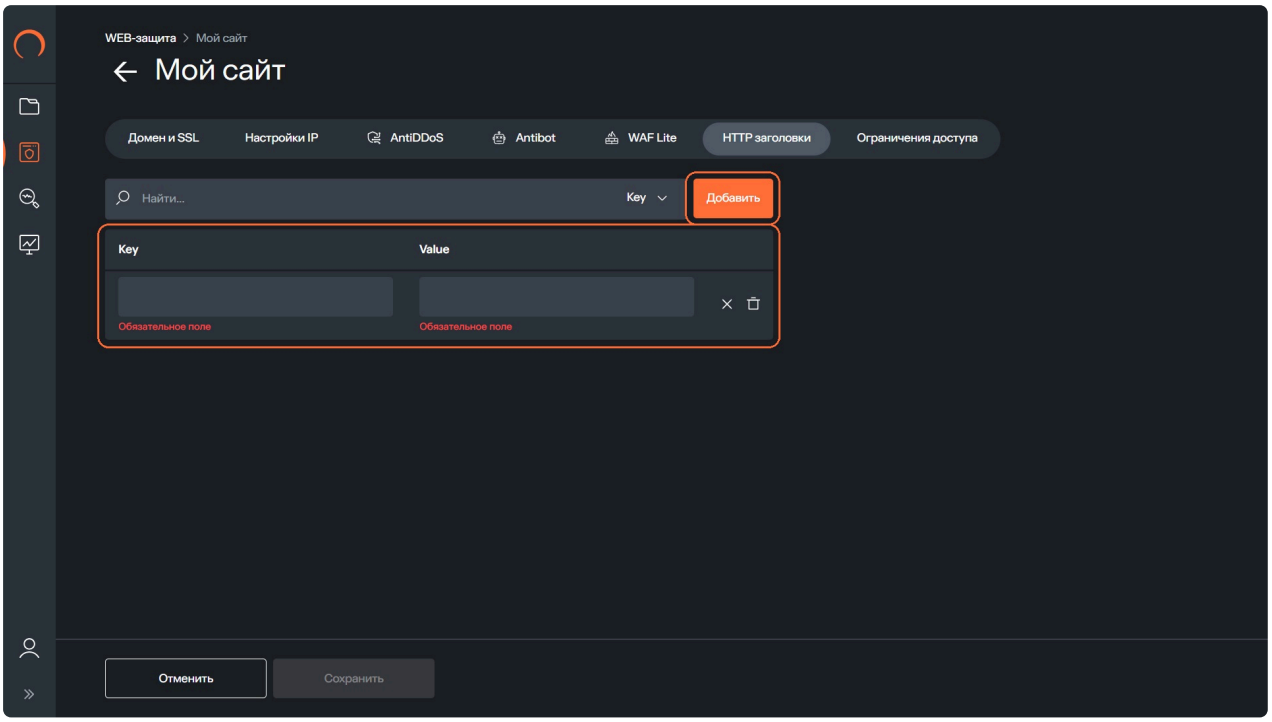
Как работать с HTTP-заголовками в личном кабинете



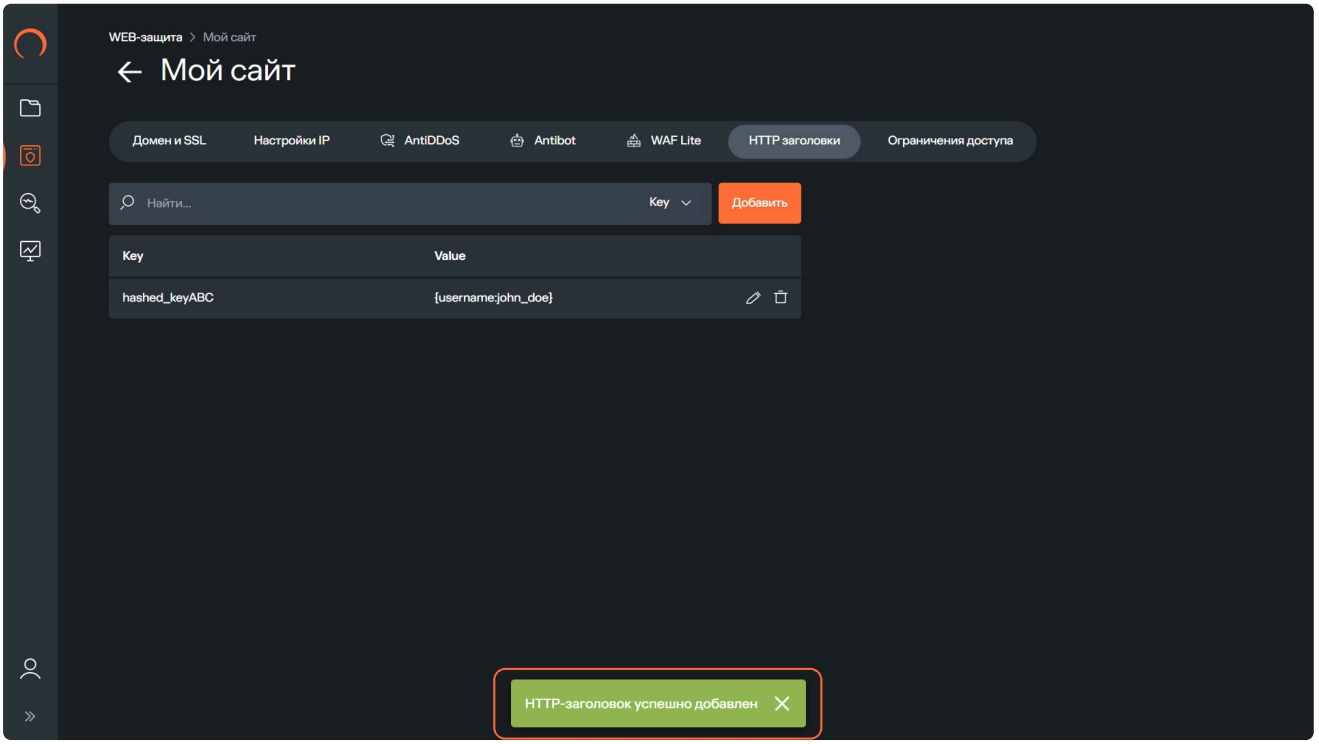
На этой вкладке вы можете управлять HTTP-заголовками. Они сообщают серверу, какое желаемое действие нужно выполнить для конкретного ресурса. Если у вас еще нет ни одного заголовка, отображается кнопка "Добавить".

При нажатии на эту кнопку открывается форма с двумя обязательными полями для заполнения "Key" и "Value".

- **Key** — ключ заголовка
- **Value** — значение заголовка

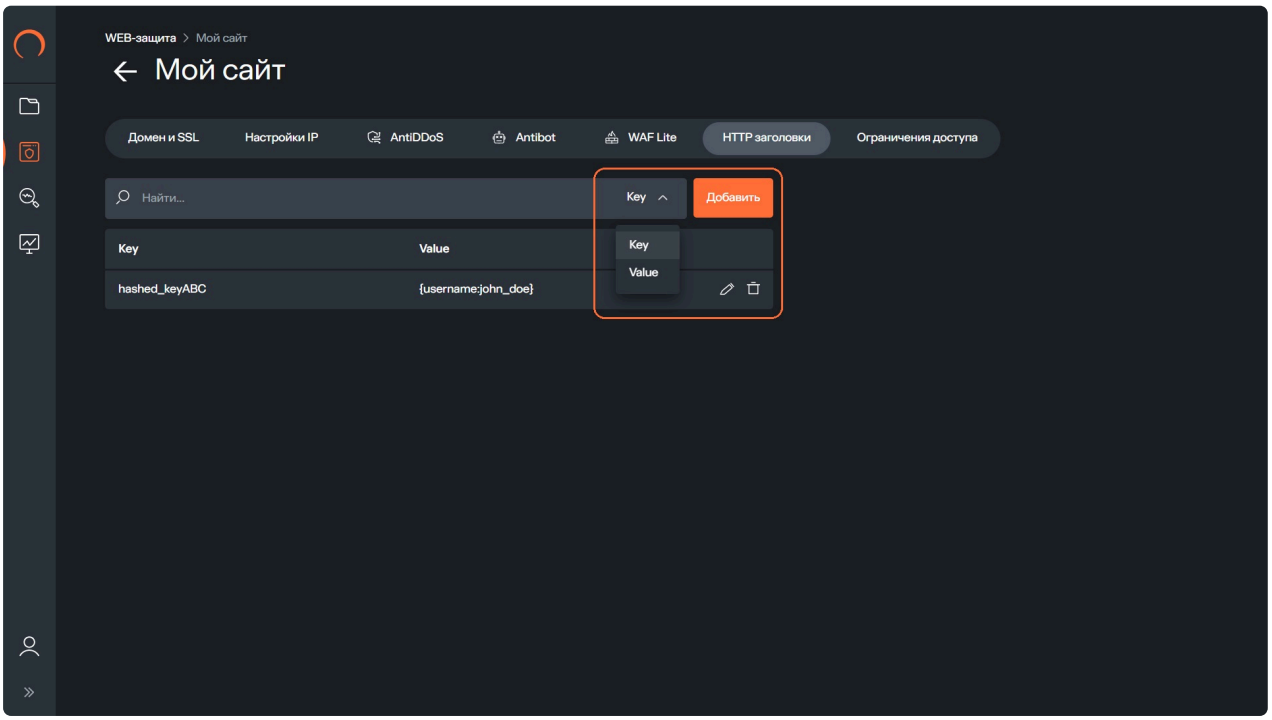


После заполнения полей "Key" и "Value" кнопка "Сохранить" станет активной. Нажмите на нее, чтобы сохранить HTTP-заголовок. Вы увидите сообщение "HTTP-заголовок успешно добавлен".

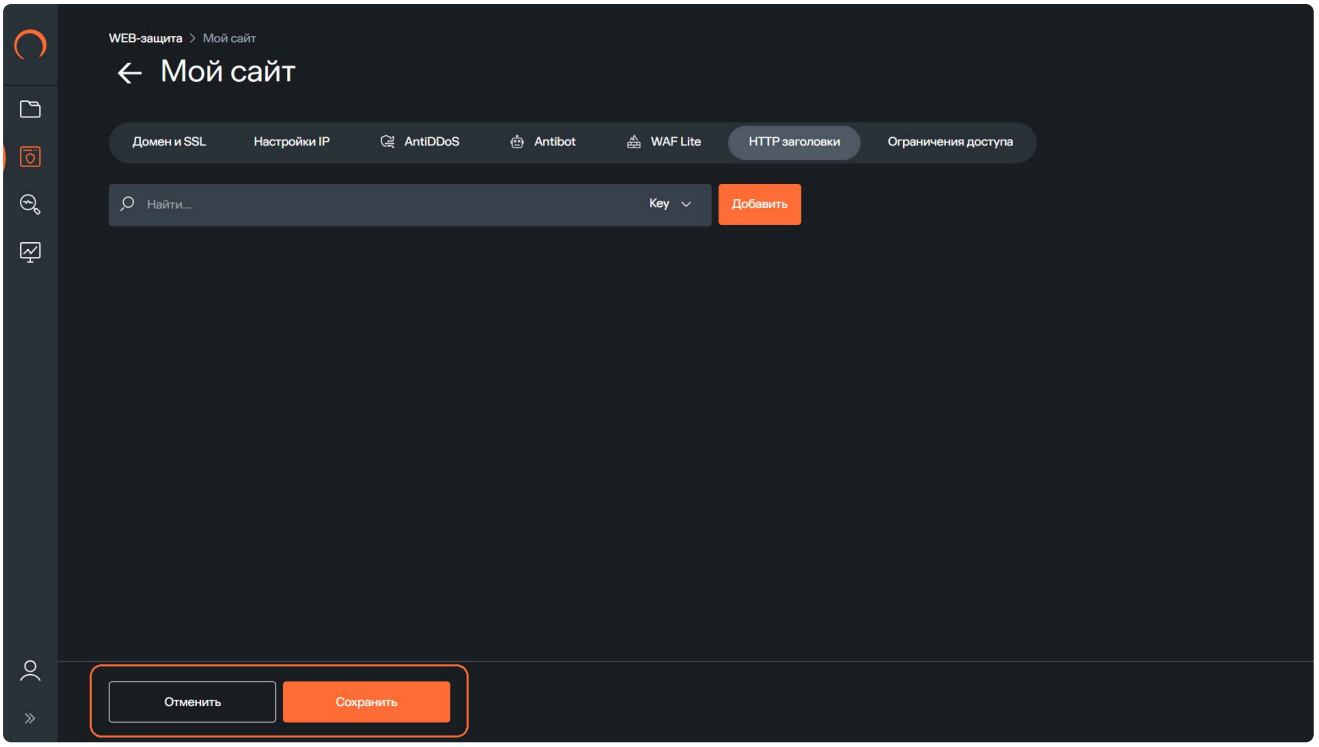


На этой вкладке вы можете:

- **Добавлять новые HTTP-заголовки**, нажав на кнопку "Добавить"
- **Редактировать существующие HTTP-заголовки**, нажав на иконку карандаша
- **Удалять существующие HTTP-заголовки**, нажав на иконку корзины
- **Выполнять поиск по полям "Key" или "Value"**. Нужное поле выберите в выпадающем списке



При удалении заголовка нажмите "Сохранить" для подтверждения действия. Вы увидите сообщение "HTTP-заголовок успешно удален".



Общее описание ограничений доступа

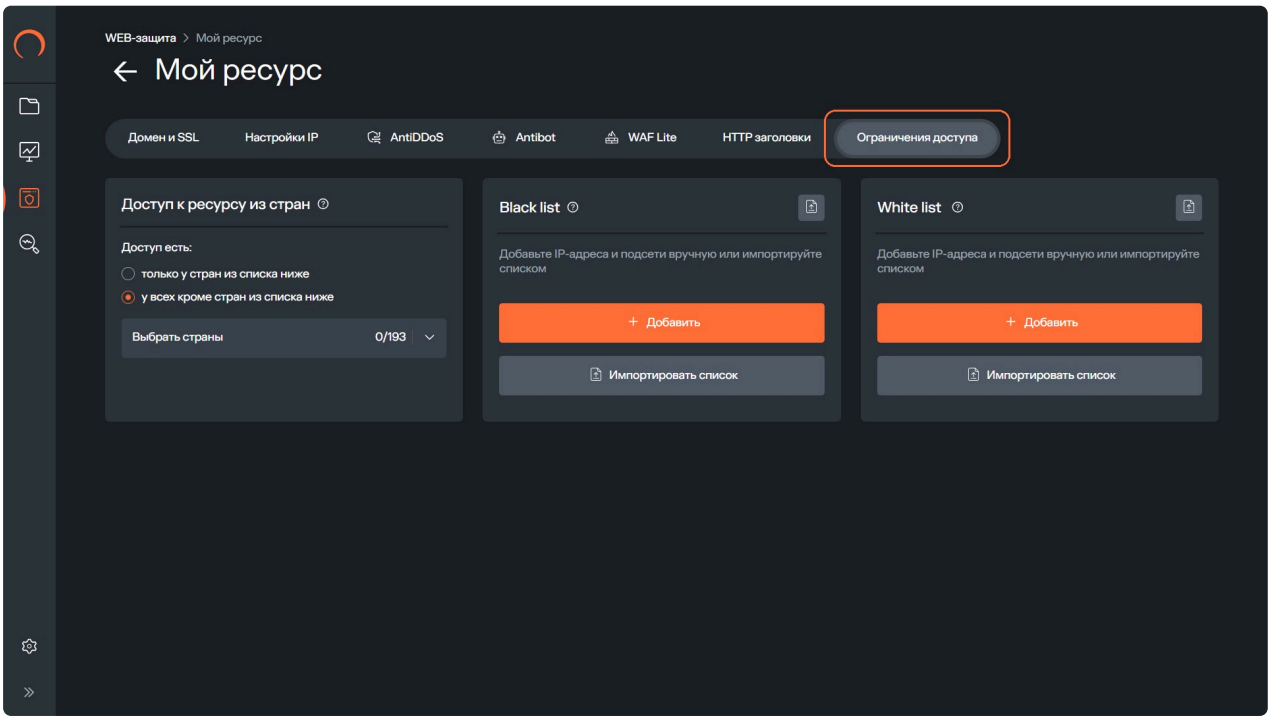
Ограничения доступа — это перечень настроек, которые позволяют управлять входящими запросами к вашему сайту.

На этой вкладке вы можете задать параметры ограничения доступа к вашему ресурсу. Доступны 3 типа ограничений:

- Доступ к ресурсу из стран – запрет доступа в зависимости от государства, из которого приходит запрос
- Black list — запрет доступа для конкретных IP-адресов или подсетей
- White list — разрешение доступа для конкретных IP-адресов или подсетей

Каждое входящее обращение к сайту система обрабатывает в следующей последовательности:

1. **Black list** — проверяет есть ли в Black list IP-адрес, с которого пришел запрос. Если есть, блокирует запрос. Если нет, переводит его на следующий этап проверки ограничений по геолокации.
2. **Доступ к ресурсу из стран** — сопоставляет страну, из которой пришел запрос, со списком стран, из которых запросы разрешены/запрещены. Если обращение пришло из "разрешенного" государства, система пропускает пользователя сразу на ресурс. Запросы из "запрещенной" страны перенаправляются на третий этап проверки — White list.
3. **White list** — если запрос пришел из "запрещенной" страны, но IP-адрес внесен в White list с разрешением доступа, то система пропускает пользователя на ресурс. Если IP-адрес не внесен в White list, то система перенаправляет его на проверку сервисами защиты — AntiDDoS, Antibot, WAF Lite — в зависимости от того, какие из них у вас подключены.

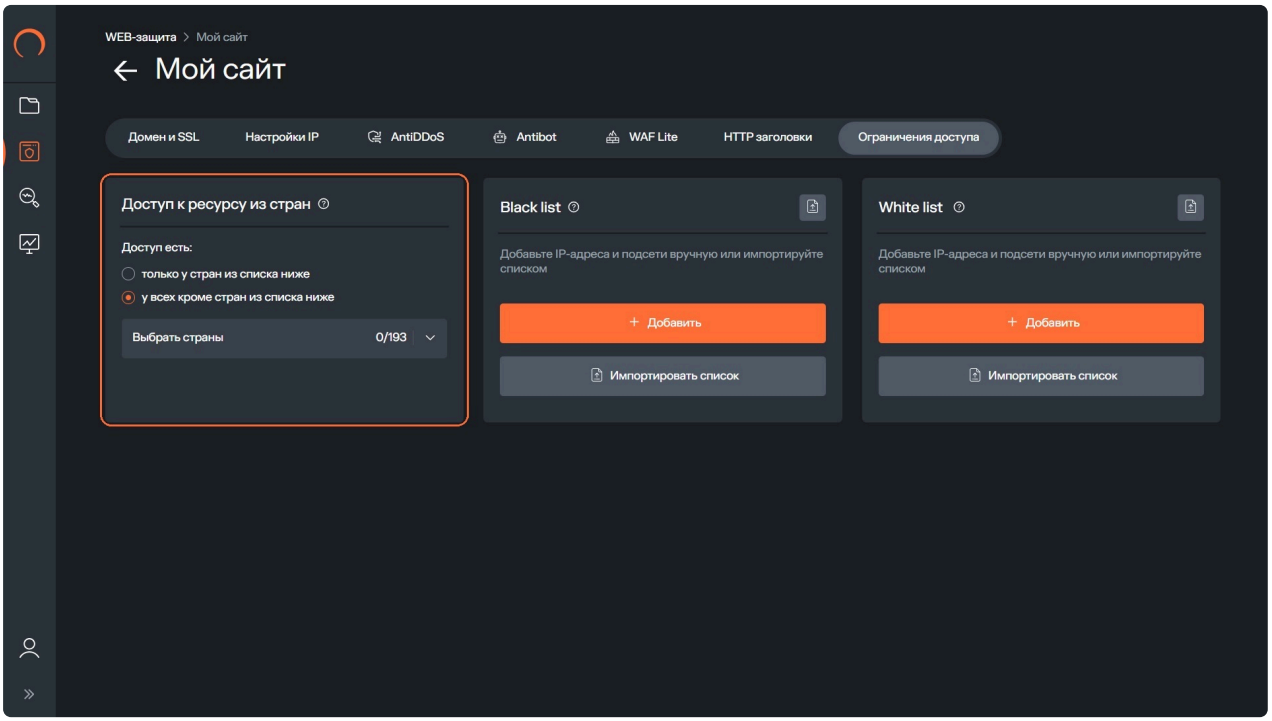

WEB-защита > Мой ресурс
Мой ресурс
Домен и SSL
Настройки IP
AntiDDoS
Antibot
WAF Lite
HTTP заголовки
Ограничения доступа
Доступ к ресурсу из стран
Доступ есть:
только у стран из списка ниже
у всех кроме стран из списка ниже
Выбрать страны
0/193
Black list
Добавьте IP-адреса и подсети вручную или импортируйте списком
Добавить
Импортировать список
White list
Добавьте IP-адреса и подсети вручную или импортируйте списком
Добавить
Импортировать список

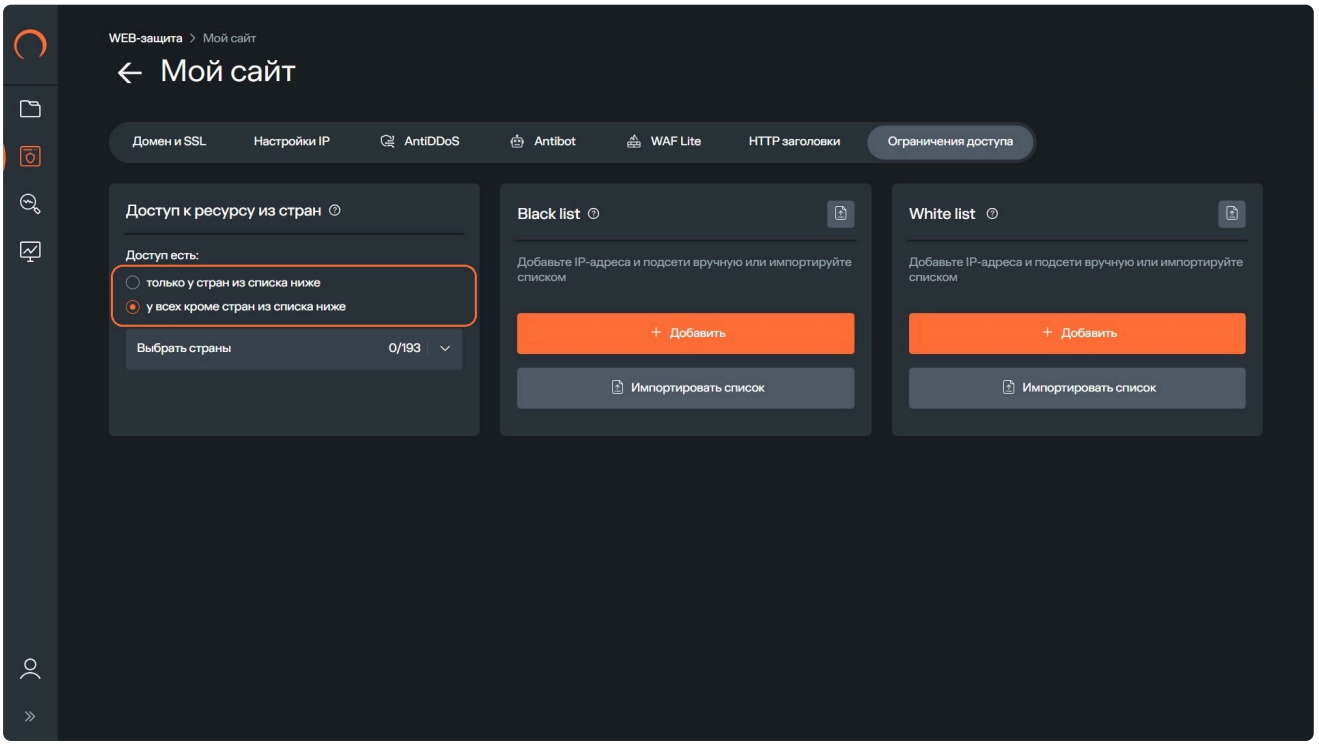
Доступ к ресурсу из стран

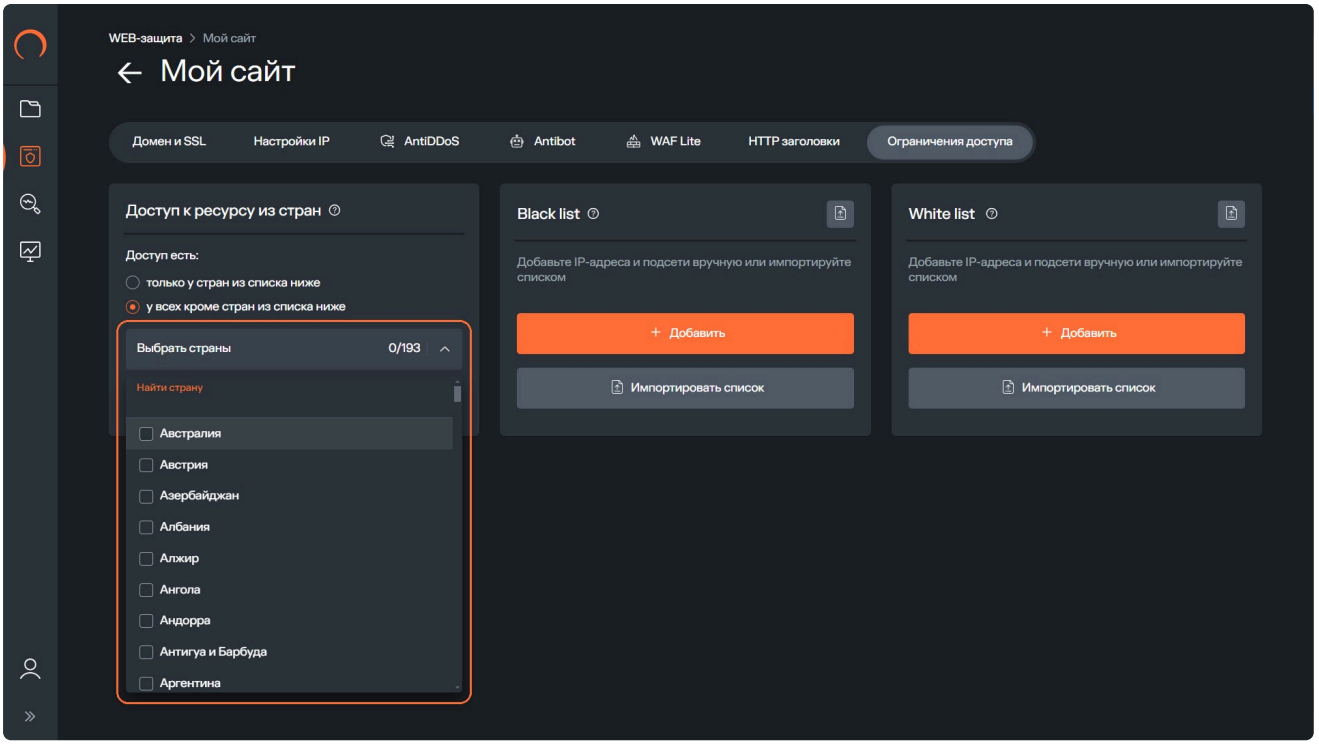
Доступ к ресурсу из стран определяет, из каких стран входящие запросы будут разрешены или запрещены.

Вы можете настроить 2 варианта ограничения доступа в зависимости от геолокации:

- Только у стран из списка ниже — выберите конкретные страны, доступ из которых будет разрешен
- У всех кроме стран из списка ниже (этот пункт выбран по умолчанию) — выберите конкретные страны, доступ из которых будет запрещен




WEB-защита > Мой сайт
Мой сайт
Домен и SSL
Настройки IP
AntiDDoS
Antibot
WAF Lite
HTTP заголовки
Ограничения доступа
Доступ к ресурсу из стран
Доступ есть:
только у стран из списка ниже
у всех кроме стран из списка ниже
Выбрать страны
0/193
Black list
Добавьте IP-адреса и подсети вручную или импортируйте списком
Добавить
Импортировать список
White list
Добавьте IP-адреса и подсети вручную или импортируйте списком
Добавить
Импортировать список

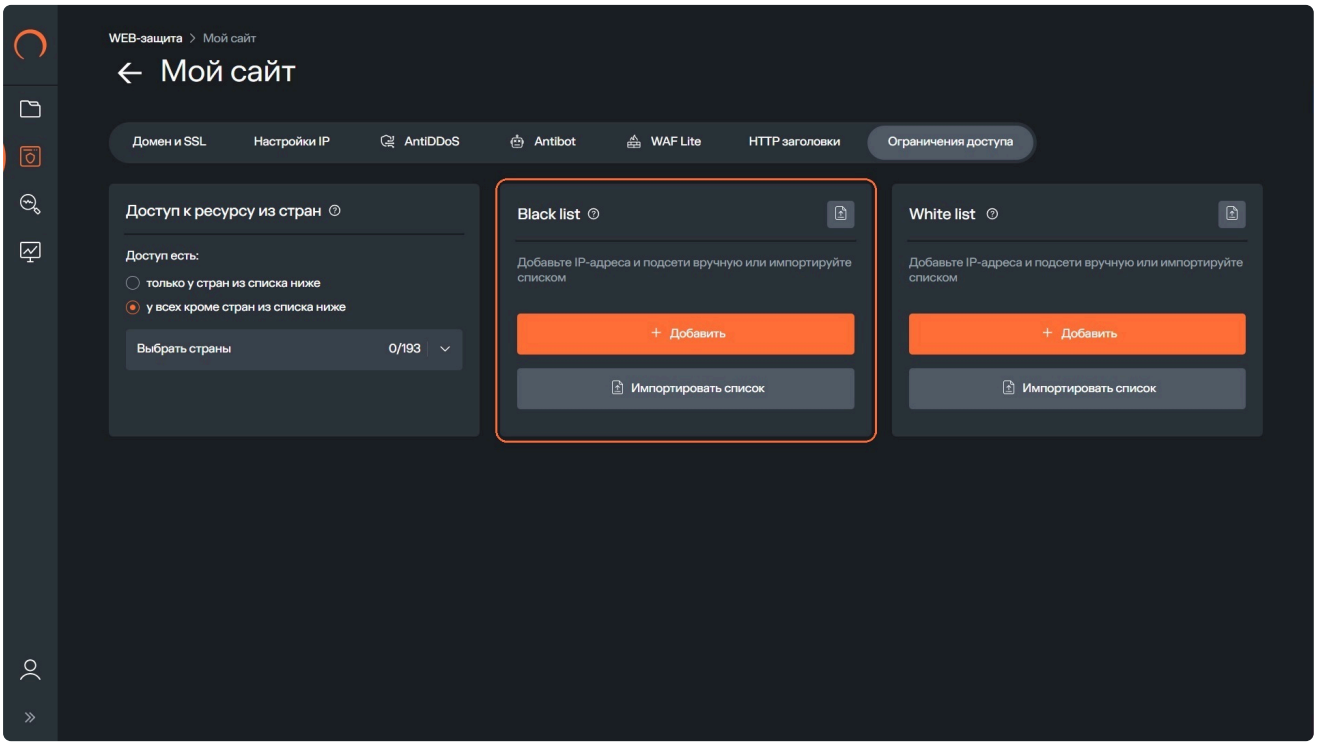

WEB-защита > Мой сайт
Мой сайт
Домен и SSL
Настройки IP
AntiDDoS
Antibot
WAF Lite
HTTP заголовки
Ограничения доступа
Доступ к ресурсу из стран
Доступ есть:
только у стран из списка ниже
у всех кроме стран из списка ниже
Выбрать страны
0/193
Найти страну
Австралия
Австрия
Азербайджан
Албания
Алжир
Ангола
Андорра
Антигуа и Барбуда
Аргентина
Black list
Добавьте IP-адреса и подсети вручную или импортируйте списком
Добавить
Импортировать список
White list
Добавьте IP-адреса и подсети вручную или импортируйте списком
Добавить
Импортировать список

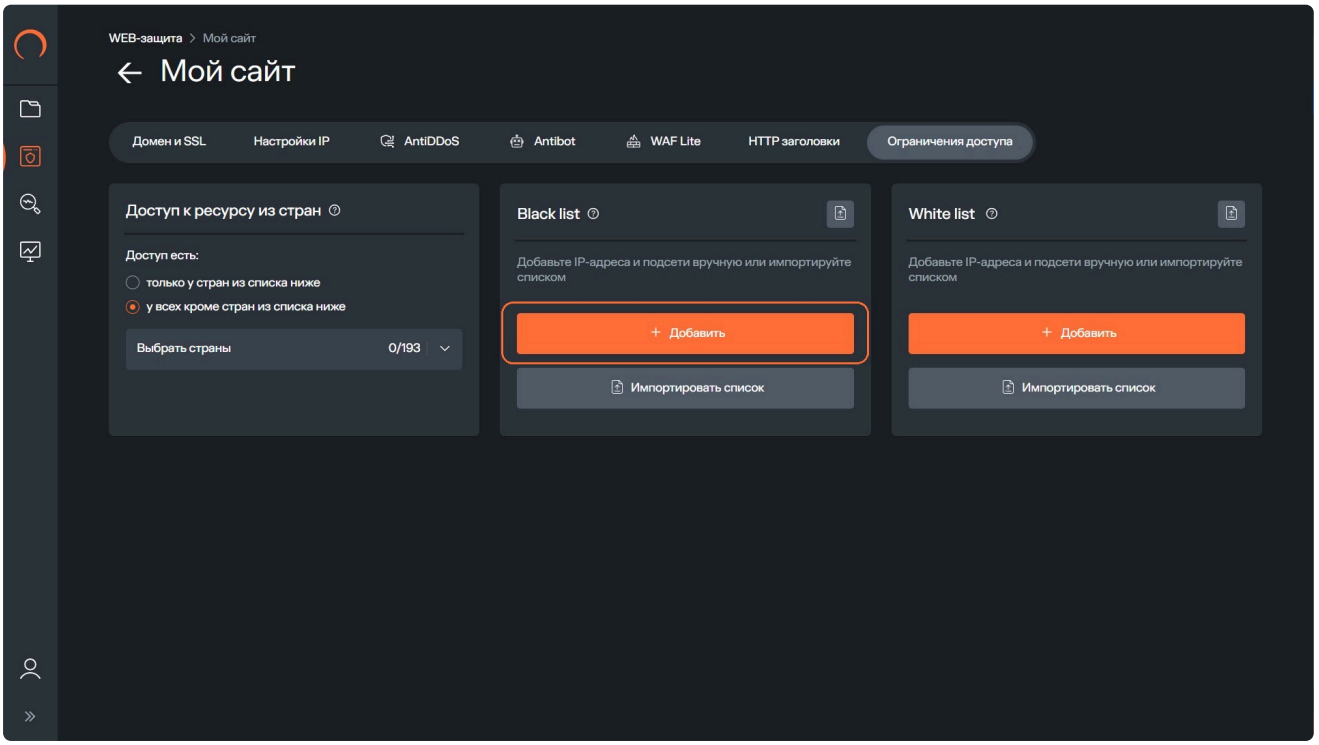
Black list

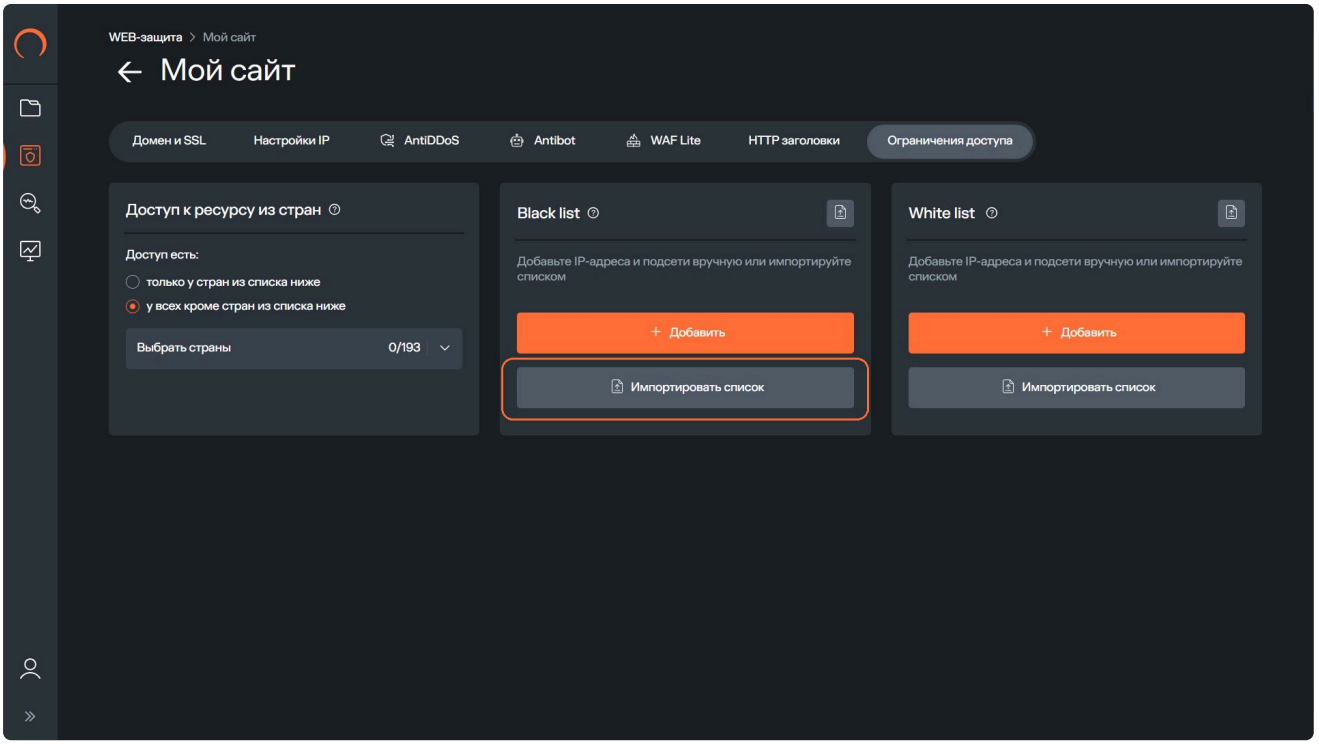
Black list — функция добавления IP-адресов в черный список. Если адрес был добавлен в Black list, он будет заблокирован.

Добавьте IP-адреса (IPv4) и подсети (группы IP-адресов), запрос от которых система будет сразу блокировать без дополнительных проверок. Их можно прописать вручную или загрузить списком в формате .csv.

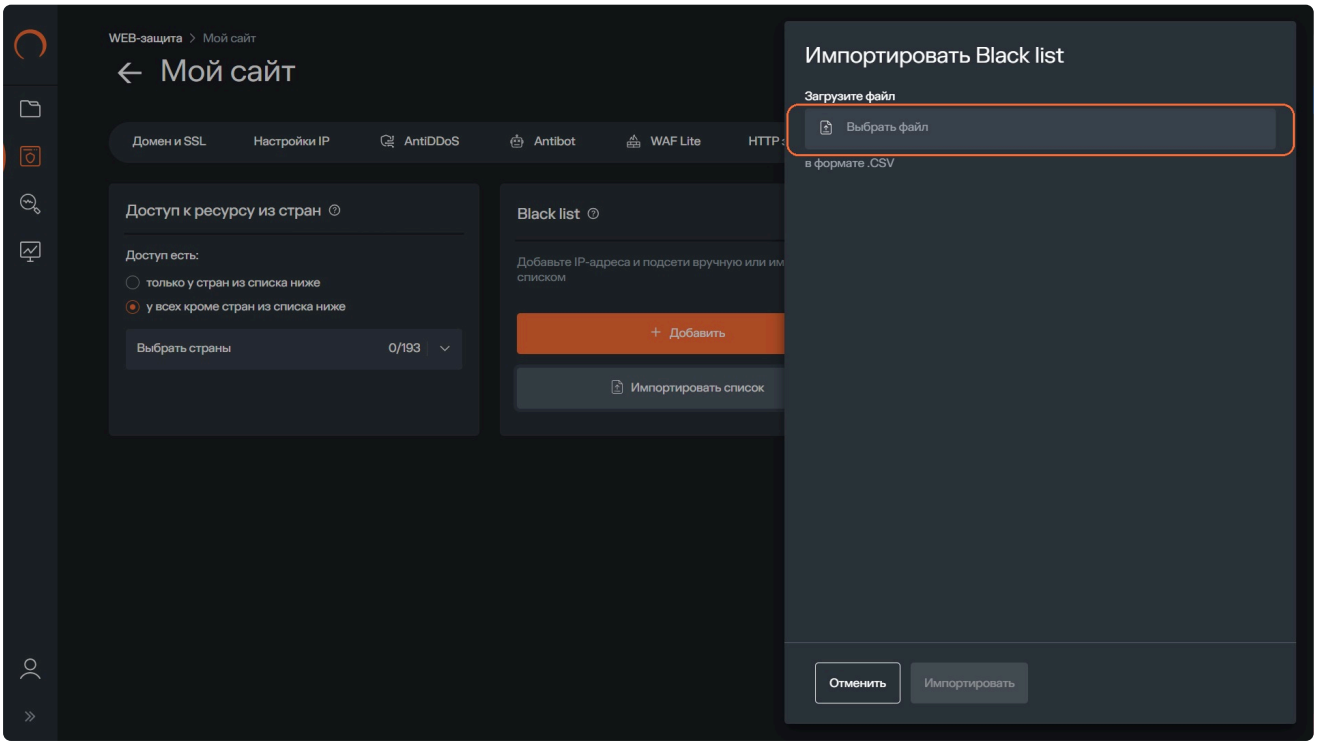
Если вы еще не добавили ни одного IP-адреса в Black list, то увидите кнопки "Добавить" (для добавления IP-адресов вручную) и "Импортировать список" (для загрузки файла со списком).



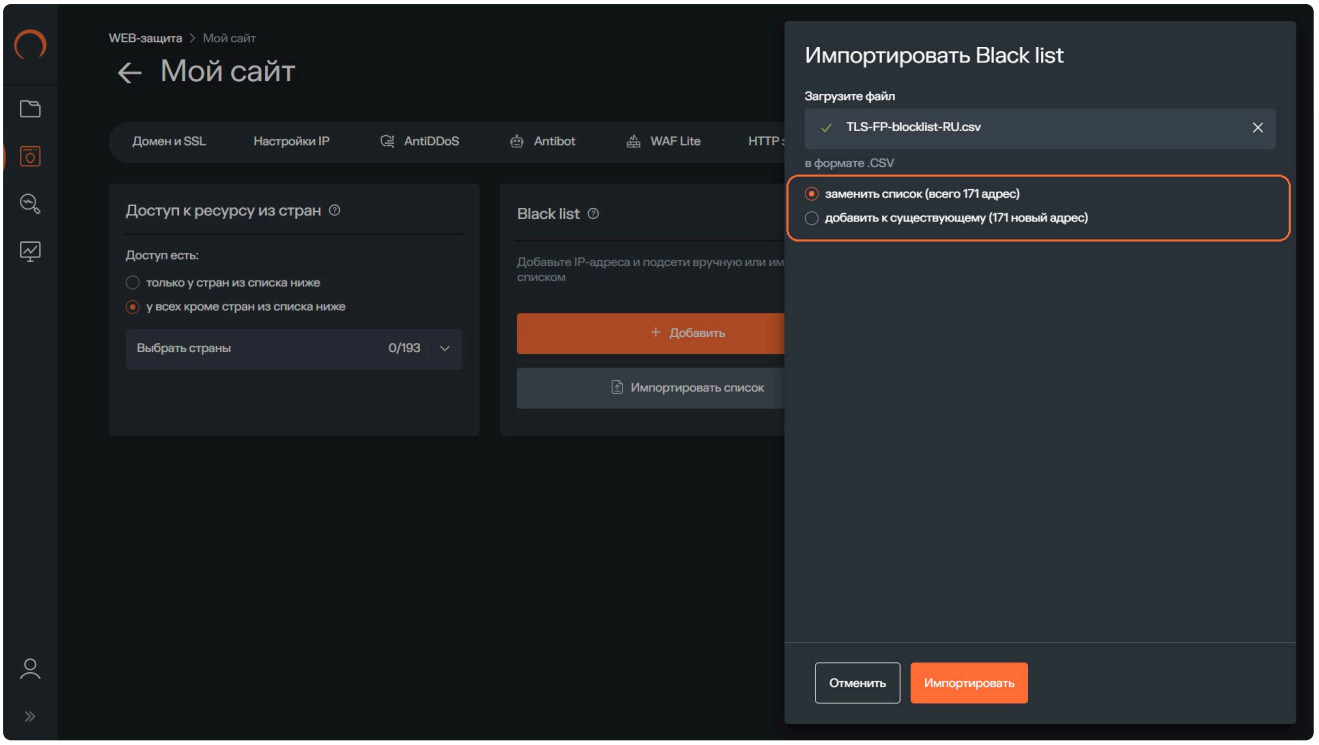


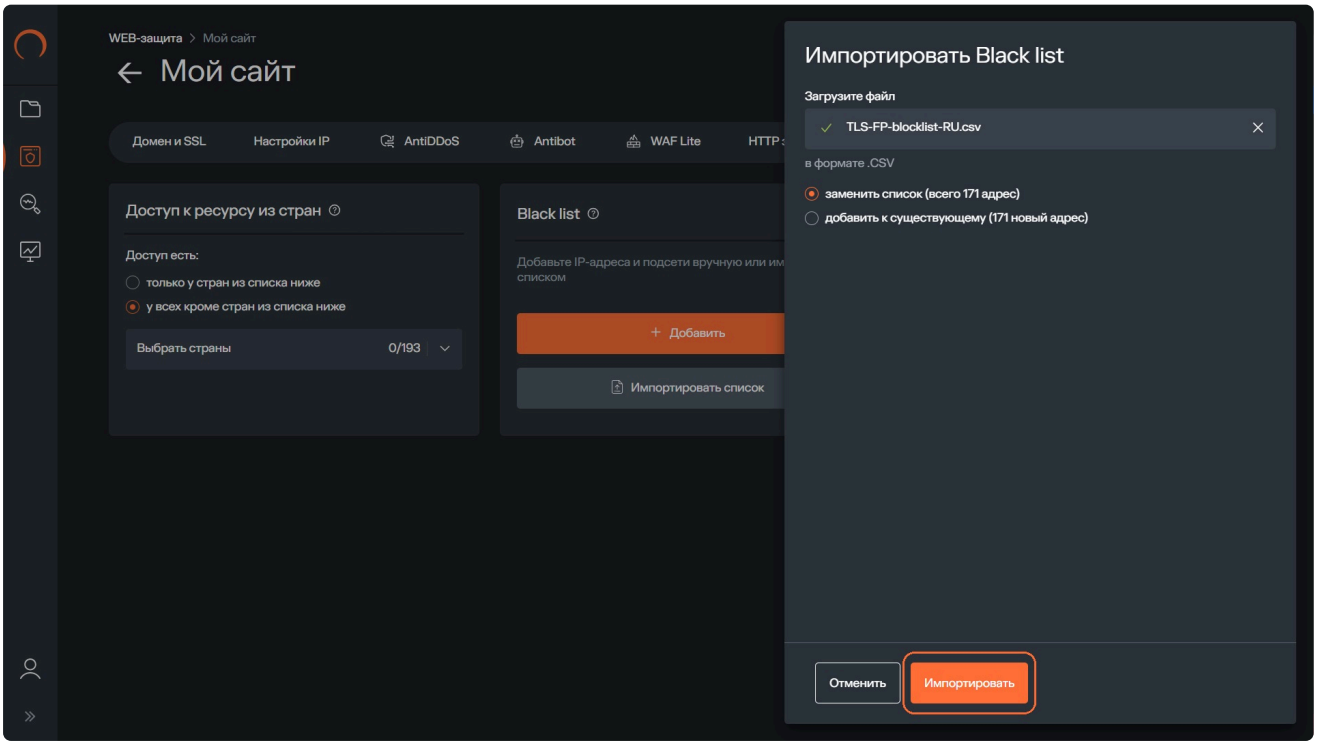


При нажатии на кнопку "Импортировать список" справа откроется окно для загрузки файла в формате .csv. Когда вы добавите файл, кнопка "Импортировать" в нижней части экрана станет активной.

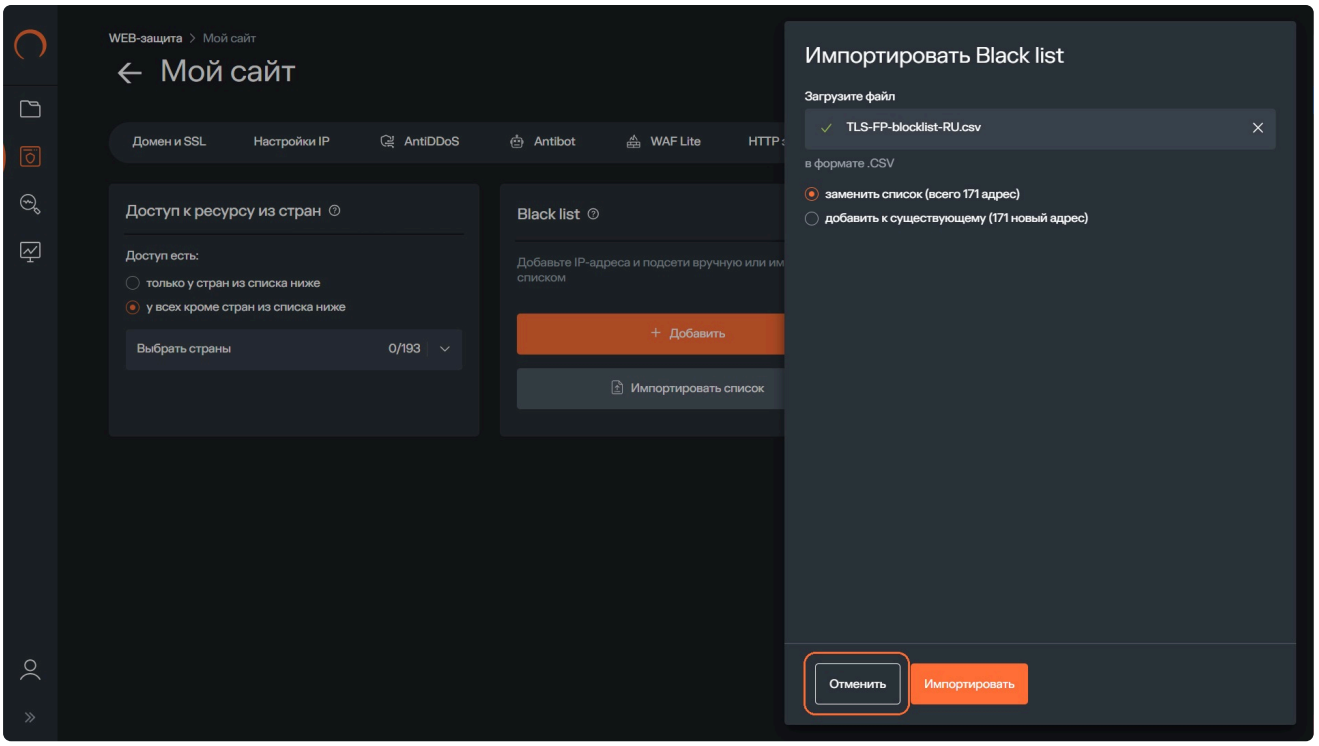


После загрузки файла, выберите один из способов его добавления в Black list и нажмите "Импортировать".





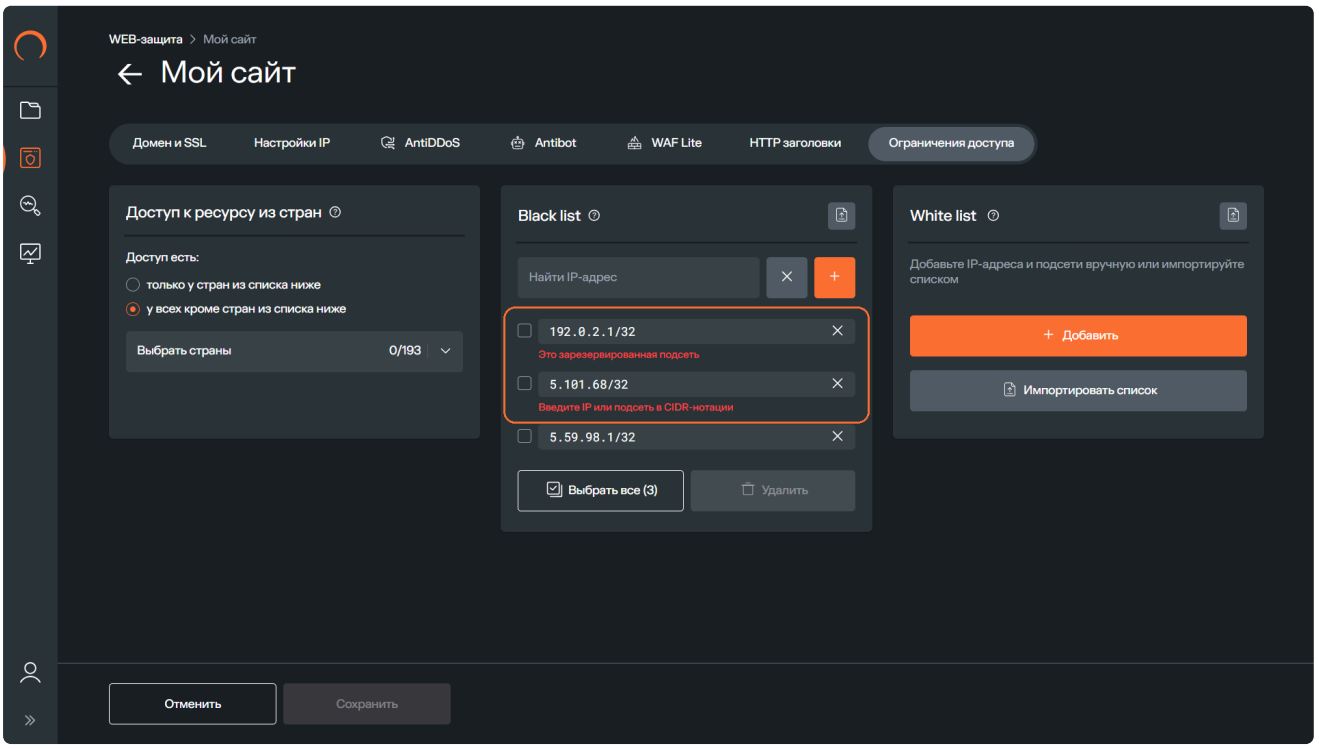
Если хотите отменить внесенные изменения, нажмите "Отменить", окно закроется.



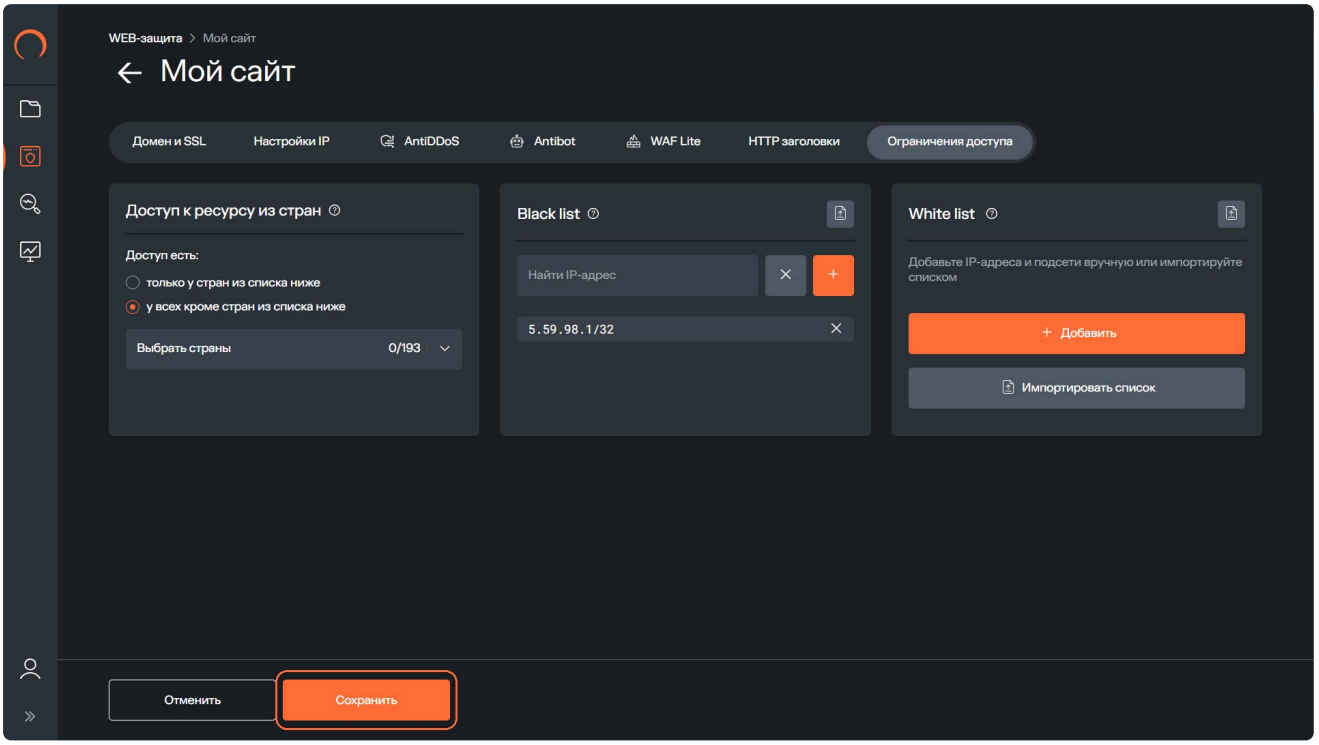
Если вы будете добавлять IP-адреса в Black list вручную, обратите внимание: IP-адрес должен состоять из уровней, разделенных точкой. Если ввести его в некорректном формате, система покажет сообщение "Введите IP или подсеть в CIDR-нотации".

Если ввести IP-адрес сети которая не используется в сети Интернет и предназначена только для частного пользования, под этим полем появится текст "Это зарезервированная подсеть".

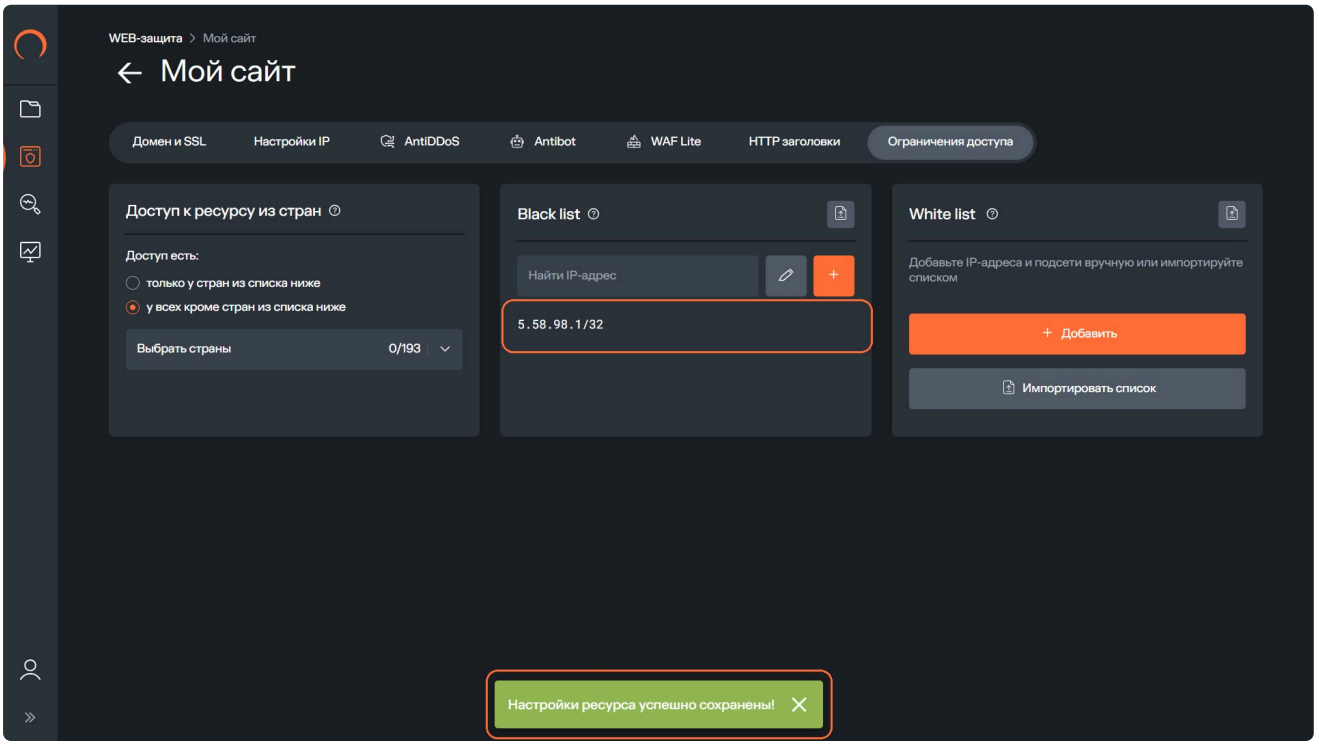
> **Обратите внимание**
>
> Слеш "/" и число "32" вводить не нужно. Система проставит их сама исходя из введенного вами IP-адреса.



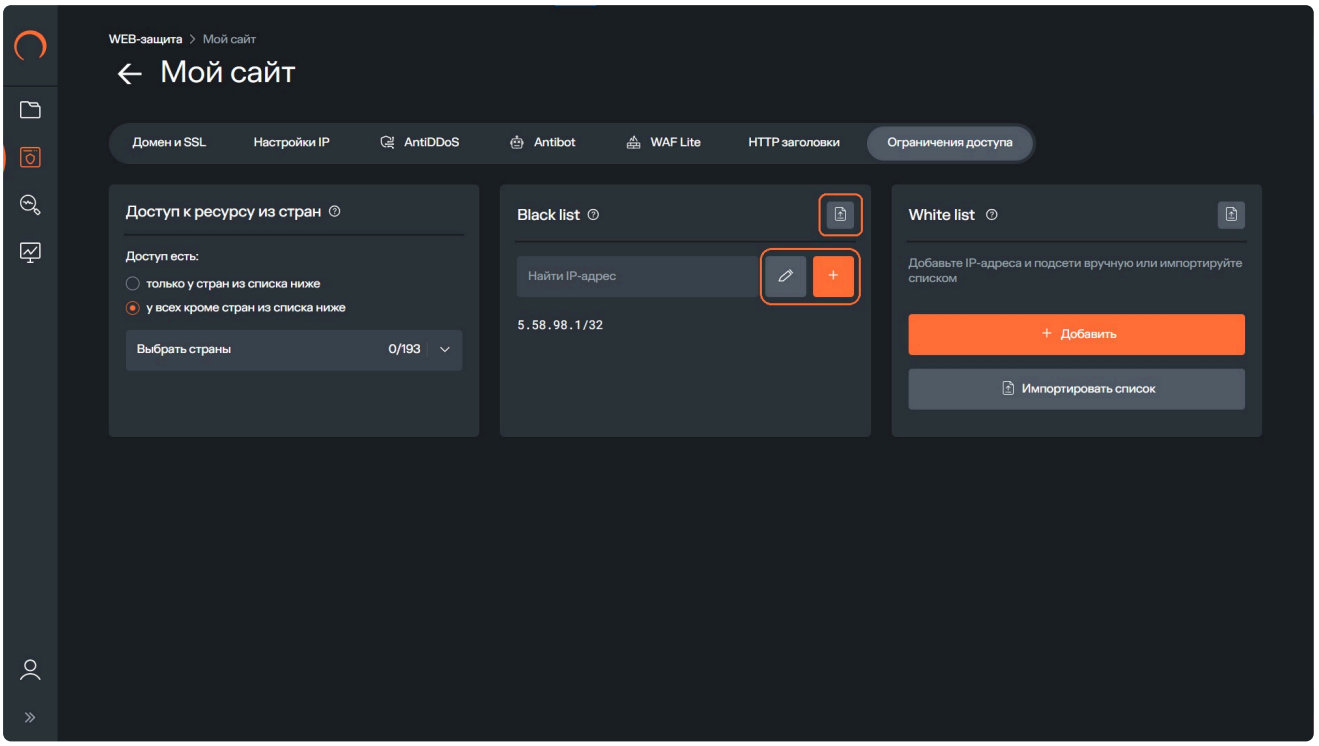
После введения IP-адреса/подсети или загрузки файла со списком нажмите кнопку "Сохранить" в нижней части экрана.



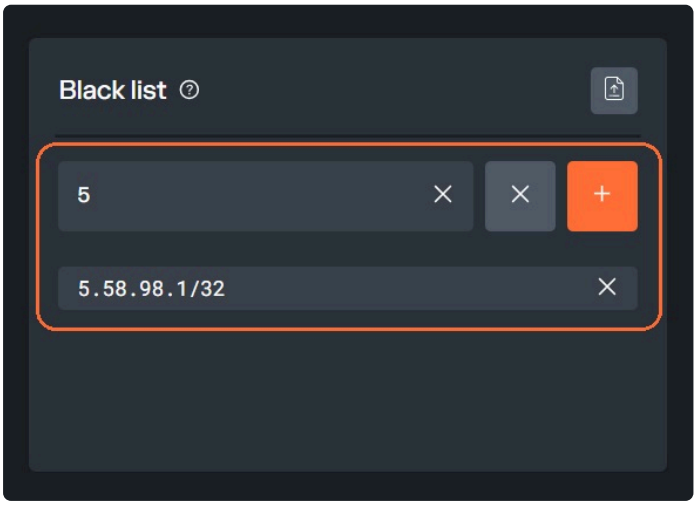
В нижней части экрана вы увидите сообщение "Настройки ресурса успешно сохранены". Добавленный IP-адрес отражается в списке подлежащих блокировке.



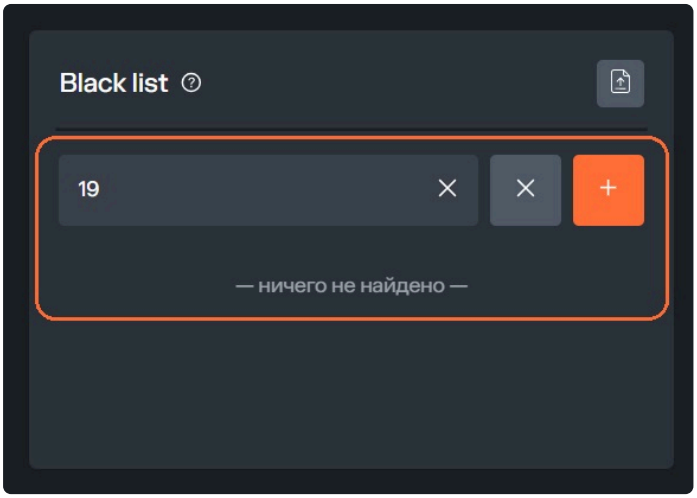
- Если хотите отредактировать введенные данные, нажмите на иконку редактирования рядом с полем поиска
- Если хотите добавить новые IP-адреса/подсети, нажмите на кнопку "+" рядом с полем поиска
- Для загрузки списка нажмите иконку загрузки файла в верхнем правом углу формы



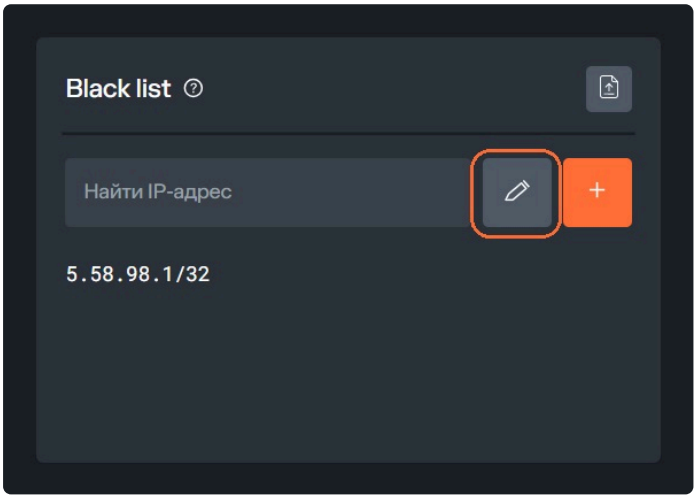
Нужный IP-адрес можно найти через поле поиска. Вы можете задать в нем любой уровень. Если IP-адрес есть в списке, система его найдет.

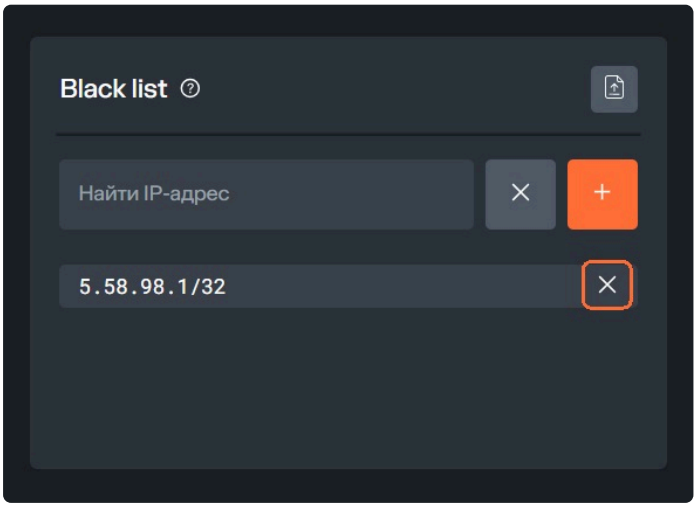


Если IP-адреса нет в списке, вы увидите сообщение "ничего не найдено".

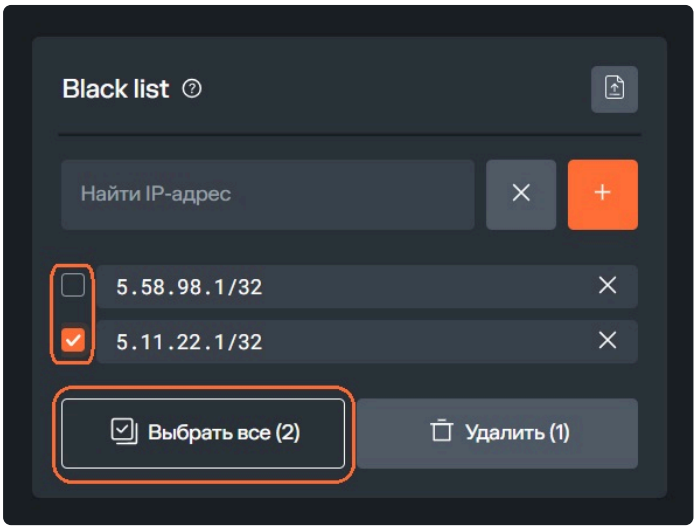


Для удаления IP-адреса из Black list нажмите на иконку редактирования в виде карандаша рядом с полем поиска. После этого найдите нужный IP-адрес в списке и нажмите на крестик справа от него.





Если нужно удалить несколько IP-адресов, отметьте их галочками слева от поля и нажмите на кнопку "Удалить" в нижней части формы. Также вы можете удалить все адреса из списка: нажмите на кнопку "Выбрать все" в нижней части формы и затем на кнопку "Удалить".



Обратите внимание

После внесения любых изменений в Black list нажимайте кнопку "Сохранить" в нижней части экрана. После этого ваши корректировки отразятся в интерфейсе.

White list

White list — функция добавления IP-адресов в белый список. Если адрес был добавлен в White list, он будет пропущен без дальнейших проверок сервисами защиты.

Это список IP-адресов и подсетей в формате **IPv4**, которым нужен гарантированный доступ к ресурсу. White list — финальный этап проверки запросов к сайту перед фильтрацией сервисами Solar Space.

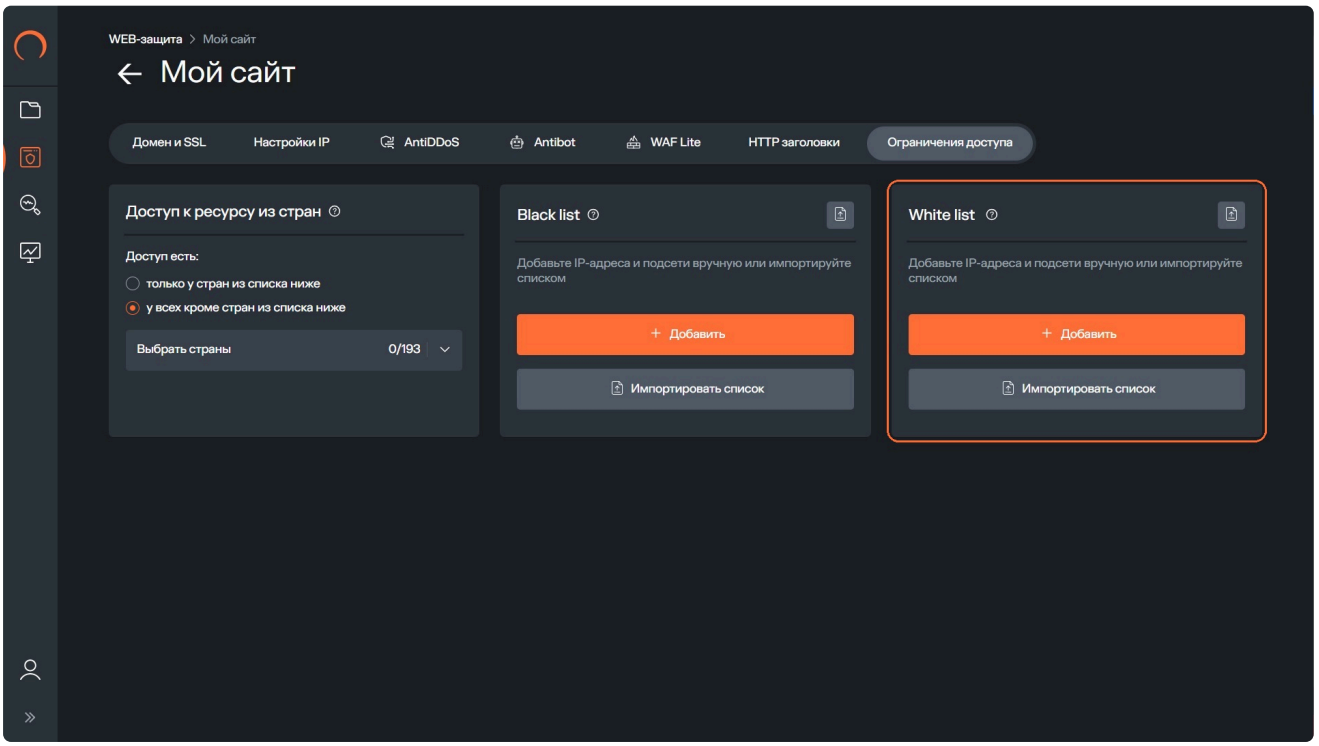
Когда трафик прошел проверку через Black list и по геолокации, система анализирует, внесен ли в White list IP-адрес, с которого идет запрос:

- **Если внесен**, пользователь сразу получает доступ к ресурсу
- **Если не внесен**, то запрос направляется на сервисы защиты Solar Space — AntiDDoS, Antibot, WAF Lite — в зависимости от того, какие из них у вас подключены. После анализа запроса этими сервисами система принимает решение: допустить пользователя на сайт или заблокировать запрос.

Алгоритм добавления IP-адресов/подсетей или файла со списком в White list аналогичен тому, что описан для Black list. Вам доступны те же действия с IP-адресами, что и в Black list: добавление, редактирование, удаление (выборочное или всех сразу).

Добавьте IP-адреса (IPv4) и подсети (группы IP-адресов), запрос от которых система будет пропускать без дополнительных проверок, за исключением проверок Black list и Доступа к ресурсу из стран. Их можно прописать вручную или загрузить списком в формате csv.

> Обратите внимание
>
> Настройки добавления и импортирования IP-адресов в White list идентичны настройкам Black list


WEB-защита > Мой сайт
Мой сайт
Домен и SSL
Настройки IP
AntiDDoS
Antibot
WAF Lite
HTTP заголовки
Ограничения доступа
Доступ к ресурсу из стран
Доступ есть:
только у стран из списка ниже
у всех кроме стран из списка ниже
Выбрать страны
0/193
Black list
Добавьте IP-адреса и подсети вручную или импортируйте списком
Добавить
Импортировать список
White list
Добавьте IP-адреса и подсети вручную или импортируйте списком
Добавить
Импортировать список

Дополнительные настройки безопасности

Настройка фаервола

Мы рекомендуем запретить подключения к целевому серверу с любых адресов, кроме адресов Solar Space, с которых осуществляется проксирование запросов. Для этого в фаерволе создайте правила на блокировку любых запросов, кроме запросов из доверенных сетей Solar Space.

Список сетей, которые необходимо добавить в белый список фаервола:

- **195.18.27.0/24**
- **93.185.164.0/24**

Примеры настроек для популярных фаерволов

> Обратите внимание
>
> Данные настройки приведены исключительно в качестве примеров. Перед их применением убедитесь, что они соответствуют требованиям вашего проекта и не приведут к сбоям в его работе

Пример настроек iptables

```
sudo iptables -A INPUT -s 195.18.27.0/24 -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -s 195.18.27.0/24 -p tcp --dport 443 -j ACCEPT
sudo iptables -A INPUT -s 93.185.164.0/24 -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -s 93.185.164.0/24 -p tcp --dport 443 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 80 -j DROP
sudo iptables -A INPUT -p tcp --dport 443 -j DROP
```

Пример настроек UFW

```
sudo ufw allow from 195.18.27.0/24 to any port 80 proto tcp comment "Allow HTTP
sudo ufw allow from 195.18.27.0/24 to any port 443 proto tcp comment "Allow HTTP
```

```
sudo ufw allow from 93.185.164.0/24 to any port 80 proto tcp comment "Allow HTTP
sudo ufw allow from 93.185.164.0/24 to any port 443 proto tcp comment "Allow HTT
sudo ufw deny to any port 80 proto tcp comment "Deny all other HTTP traffic"
sudo ufw deny to any port 443 proto tcp comment "Deny all other HTTPS traffic"
```

Пример настроек nftables

Пример настроек для командной строки (действуют до перезагрузки операционной системы):

```
sudo nft add table ip web_filter
sudo nft add chain ip web_filter input '{ type filter hook input priority 0; pol
sudo nft add rule ip web_filter input ip saddr 195.18.27.0/24 tcp dport {80, 443
sudo nft add rule ip web_filter input ip saddr 93.185.164.0/24 tcp dport {80, 44
sudo nft add rule ip web_filter input tcp dport {80, 443} drop
```

Для постоянного применения нужно добавить следующие строки в файл `/etc/nftables.conf`:

```
table ip web_filter {
    chain input {
        type filter hook input priority 0; policy drop;
        ip saddr 195.18.27.0/24 tcp dport { 80, 443 } accept
        ip saddr 93.185.164.0/24 tcp dport { 80, 443 } accept
    }
}
```

Пример настроек firewalld

```
firewall-cmd --permanent --new-zone=ss
firewall-cmd --permanent --zone=ss --add-port=80/tcp
firewall-cmd --permanent --zone=ss --add-port=443/tcp
firewall-cmd --permanent --zone=ss --add-source=195.18.27.0/24
firewall-cmd --permanent --zone=ss --add-source=93.185.164.0/24
firewall-cmd --reload
```

Дополнительные настройки сервера

Настройка расшифровки реальных IP

При проксировании трафика все запросы на ваш сервер поступают с IP-адресов сети Solar Space, а не с адресов реальных пользователей. Поэтому вы можете увидеть в логах IP-адрес 127.0.0.1. Чтобы сервер отображал реальные IP-адреса посетителей, необходимо настроить обработку заголовка X-Forwarded-For для сетей Solar Space:

- **195.18.27.0/24**
- **93.185.164.0/24**

Веб-сервер Nginx

Добавьте следующую строку в `/etc/nginx/nginx.conf` в секцию `http`:

```
http {
    ...
    set_real_ip_from 195.18.27.0/24;
    set_real_ip_from 93.185.164.0/24;
    real_ip_header X-Forwarded-For;
    ...
}
```

Проверьте конфигурацию Nginx перед перезагрузкой:

```
sudo nginx -t
```

Перезагрузите Nginx:

```
sudo systemctl reload nginx
```

Веб-сервер Apache

Модуль `mod_rpaf` (устаревший вариант), лучше использовать `mod_remoteip`.

Создайте или измените файл `/etc/apache2/mods-enabled/rpaf.conf`, добавив следующие строки:

```
<IfModule mod_rpaf.c>
    RPAF_Enable On
```

```
    RPAF_SetHostName On
    RPAF_ProxyIPs 127.0.0.1 195.18.27.0 93.185.164.0
</IfModule>
```

Активируйте модуль `mod_rpaf` и конфигурацию:

```
sudo a2enmod rpaf
sudo a2enconf rpaf
```

Проверьте конфигурацию Apache перед перезагрузкой:

```
sudo apache2ctl -t
```

Перезагрузите Apache:

```
sudo systemctl reload apache2
```

Модуль mod_remoteip

Если у вас ранее был установлен модуль `mod_rpaf`, деактивируйте его командой:

```
sudo a2dismod rpaf
```

Создайте или измените файл `/etc/apache2/conf-available/remoteip.conf`, добавив следующие строки:

```
<IfModule remoteip_module>
RemoteIPHeader X-Forwarded-For
RemoteIPTrustedProxy 127.0.0.1 195.18.27.0/24 93.185.164.0/24
</IfModule>
```

Активируйте модуль `mod_remoteip` и конфигурацию:

```
sudo a2enmod remoteip
sudo a2enconf remoteip
```

Проверьте конфигурацию Apache перед перезагрузкой:

```
sudo apache2ctl -t
```

Перезагрузите Apache:

```
sudo systemctl reload apache2
```

Настройка отображения реального IP-адреса в логах Apache

Инструкция для Ubuntu/Debian

Откройте файл `/etc/apache2/apache2.conf` и замените следующие строки:

```
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" v
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combine
LogFormat "%h %l %u %t \"%r\" %>s %O" common
```

на:

```
LogFormat "%a:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" v
LogFormat "%a %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combine
LogFormat "%a %l %u %t \"%r\" %>s %O" common
```

Проверьте конфигурацию Apache перед перезагрузкой:

```
sudo apache2 -t
```

Перезагрузите Apache:

```
sudo systemctl reload apache2
```

Инструкция для BitrixVM 7 на CentOS

В BitrixVM 9 отображение реальных IP-адресов в логах Apache работает корректно по умолчанию, и дополнительных изменений не требуется.

Откройте файл `/etc/httpd/conf/httpd.conf` и найдите следующие строки:

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combine
LogFormat "%h %l %u %t \"%r\" %>s %b" common
```

Замените символ `%h` на `%{X-Forwarded-For}i`, чтобы строки выглядели так:

```
LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-A
LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b" common
```

Сохраните изменения и закройте файл.

Проверьте конфигурацию Apache перед перезагрузкой:

```
sudo httpd -t
```

Перезагрузите Apache:

```
sudo systemctl reload httpd
```

Инструкция для IIS

Подробную инструкцию по настройке IIS вы можете прочитать здесь.

Сканирование уязвимостей

Сканирование уязвимостей — комплекс решений по мониторингу внешних цифровых угроз и сканированию ресурсов на уязвимости. Включает в себя сервисы:

- Сканер веб-сервера
- ScanGuard
- Zero Day

Сканер веб-сервера

Сервис для непрерывного поиска уязвимостей на внешних границах компании.

Сервис в разработке. Если хотите протестировать его одним из первых, сообщите об этом письмом на почту solarspace@rt-solar.ru. Мы свяжемся с вами, когда он будет готов к релизу.

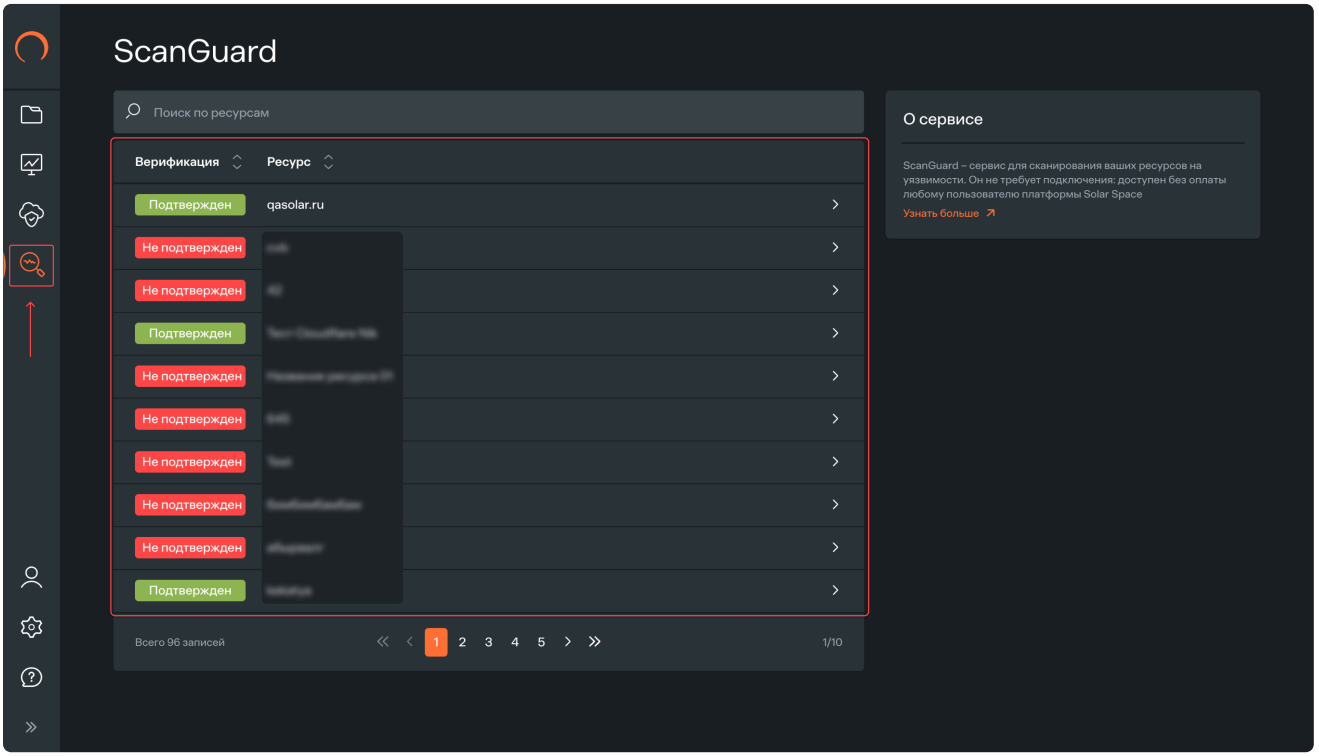
Сейчас вы можете подключить сервисы из WEB-защиты: AntiDDoS, Antibot и WAF Lite.

ScanGuard

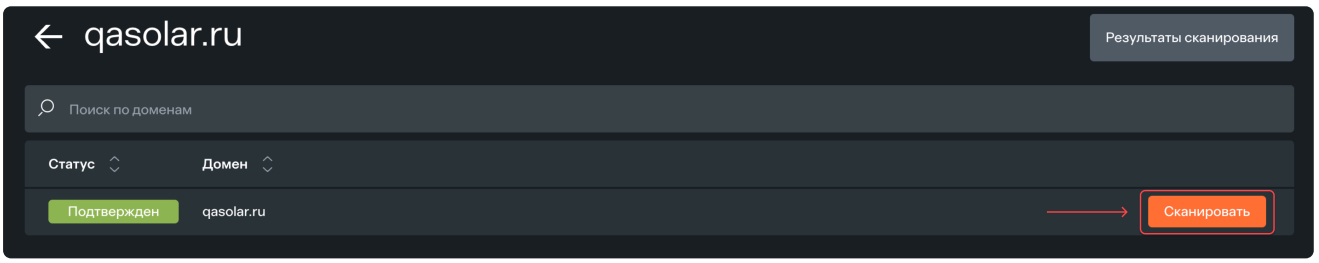
ScanGuard – сервис для сканирования ваших ресурсов на уязвимости. Он не требует подключения: доступен без оплаты любому пользователю платформы Solar Space сразу после регистрации. Сервис выявляет фишинговые домены, похожие на ваши, обнаруживает утечки логинов сотрудников, анализирует открытые порты.

Перейти на страницу "ScanGuard" вы можете из вкладки "Сервисы" на странице ресурса или из бокового меню, нажав на иконку "ScanGuard".

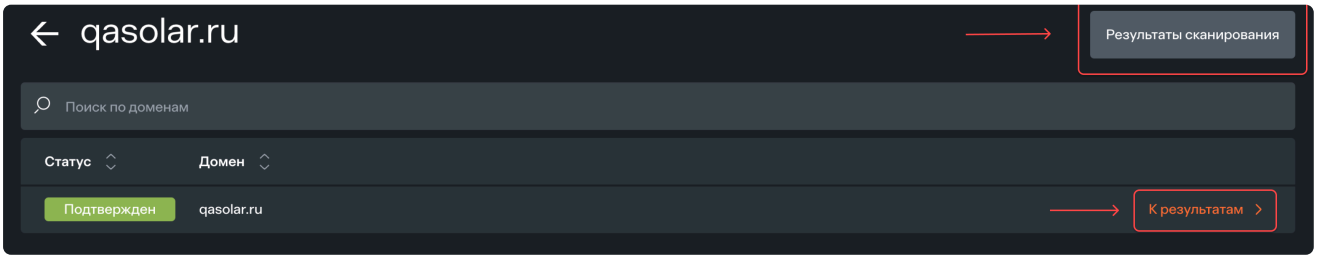
На странице сервиса вы увидите список всех ваших ресурсов. Выберите тот, который хотите просканировать, нажав на название ресурса.



Вы перейдете на страницу сканирования ресурса. Нажмите кнопку "Сканировать" справа от доменного имени, текст кнопки изменится на значок загрузки на несколько секунд и вернется в прежнее состояние.



Затем нажмите кнопку "Результаты сканирования".



Если у ресурса несколько доменов, они будут отображены в виде списка с соответствующей кнопкой "Сканировать" справа от их доменного имени.

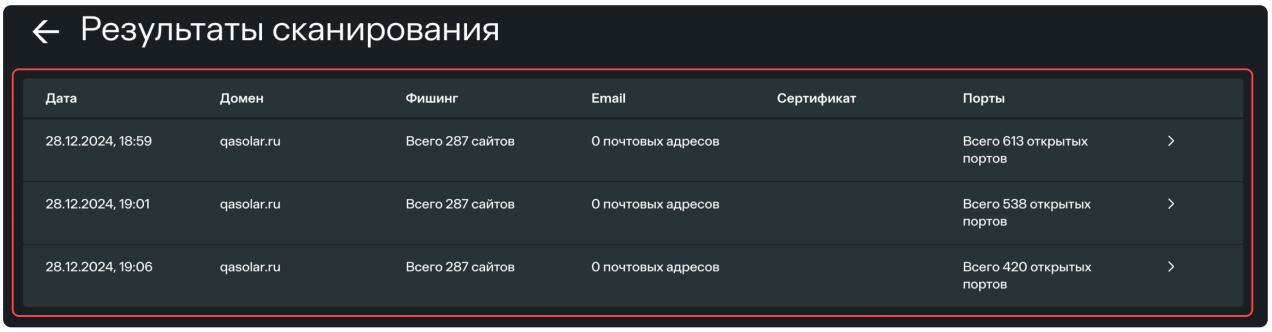
Сканирование доступно только **для ресурсов со статусом "Подтвержден"**, то есть для прошедших верификацию. Для них кнопка "Сканировать" будет активна, оранжевого цвета.

Если домен не прошел верификацию и имеет статус "Не подтвержден", кнопка "Сканировать" будет неактивна.

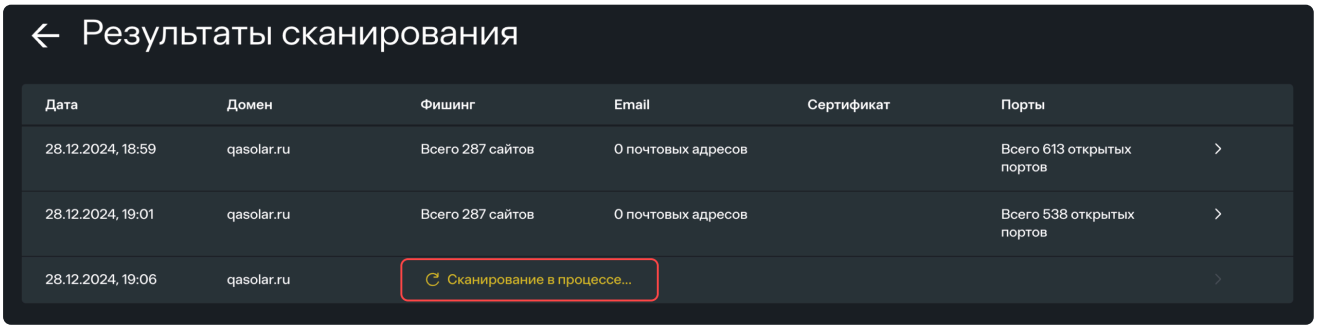
Результаты сканирования

При нажатии на кнопку "Результаты сканирования" вы перейдете на страницу с параметрами отчета:

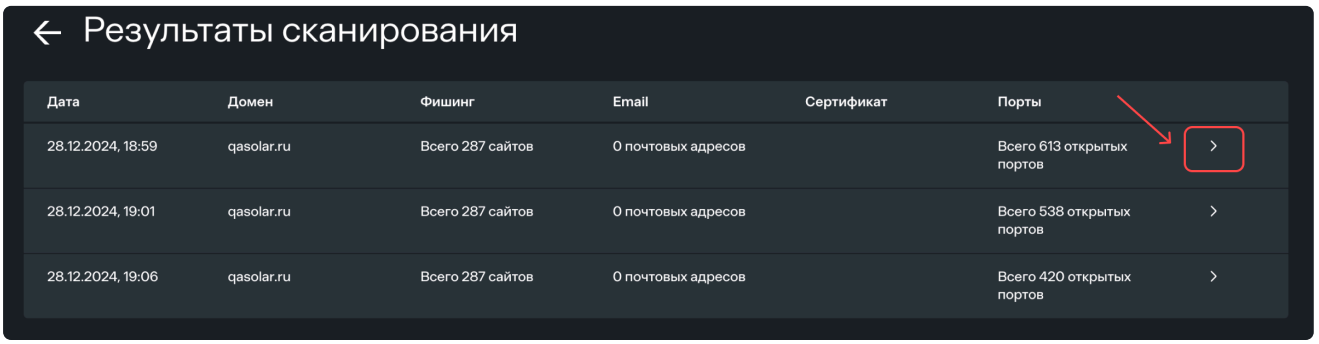
- **Дата** – даты сканирований
- **Домен** – доменное имя вашего ресурса
- **Фишинг** – копии ваших сайтов, которые могут использоваться для мошенничества и кражи личных данных пользователей
- **Email** – адреса электронной почты ваших сотрудников, оказавшиеся в свободном доступе из-за утечки данных
- **Сертификат** – действующий SSL-сертификат веб-ресурса
- **Порты** – открытые порты, доступные для внешних соединений



Если при переходе на страницу "Результаты сканирования", какое-то сканирование еще не было завершено, вы увидите соответствующий текст "Сканирование в процессе". Дождитесь, когда оно завершится. Обычно это занимает не более 3-5 минут в зависимости от количества ресурсов.

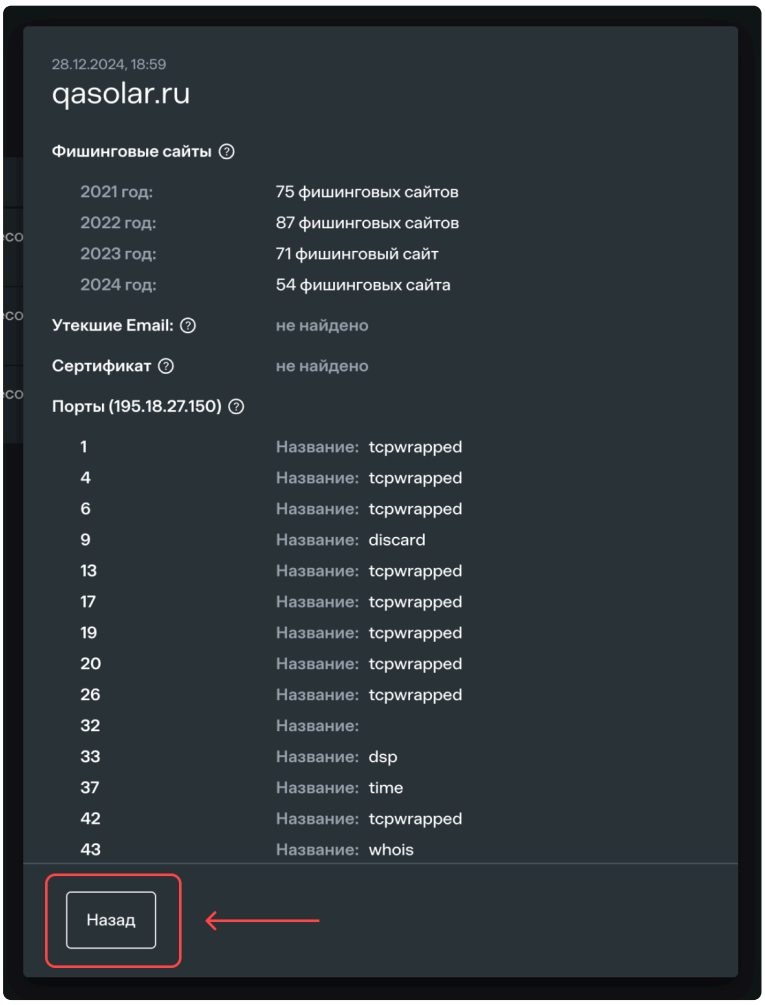


Для подробной информации о каждом сканировании нажмите на галочку справа в строке результатов.



Справа появится окно с более подробной информацией о результатах сканирования.

Чтобы закрыть его, нажмите кнопку "Назад". Далее, если хотите вернуться к списку ваших ресурсов для сканирования, нажмите стрелочку в левом верхнем углу рядом с названием страницы "Результаты сканирования".


28.12.2024, 18:59
qasolar.ru
Фишинговые сайты
2021 год: 75 фишинговых сайтов
2022 год: 87 фишинговых сайтов
2023 год: 71 фишинговый сайт
2024 год: 54 фишинговых сайта
Утекшие Email: не найдено
Сертификат не найдено
Порты (195.18.27.150)
1 Название: tcpwrapped
4 Название: tcpwrapped
6 Название: tcpwrapped
9 Название: discard
13 Название: tcpwrapped
17 Название: tcpwrapped
19 Название: tcpwrapped
20 Название: tcpwrapped
26 Название: tcpwrapped
32 Название:
33 Название: dsp
37 Название: time
42 Название: tcpwrapped
43 Название: whois
Назад

Zero Day

Сервис для углубленного сканирования сетевого периметра, выявления уязвимостей и предоставления четких инструкций по их устранению и защите.

Сервис в разработке. Если хотите протестировать его одним из первых, сообщите об этом письмом на почту solarspace@rt-solar.ru. Мы свяжемся с вами, когда он будет готов к релизу.

Сейчас вы можете подключить сервисы из WEB-защиты: AntiDDoS, Antibot и WAF Lite.

Security Awarness

Обучение персонала навыкам реагирования на фишинговые атаки для снижения риска утечек конфиденциальной информации.

Сервис в разработке. Если хотите протестировать его одним из первых, сообщите об этом письмом на почту solarspace@rt-solar.ru. Мы свяжемся с вами, когда он будет готов к релизу.

Сейчас вы можете подключить сервисы из WEB-защиты: AntiDDoS, Antibot и WAF Lite.

Security DNS

Защита внутренней границы компании. Сервис защищает ваши DNS-запросы, используя машинное обучение для категоризации веб-сайтов и ограничения доступа к нежелательному контенту.

Сервис в разработке. Если хотите протестировать его одним из первых, сообщите об этом письмом на почту solarspace@rt-solar.ru. Мы свяжемся с вами, когда он будет готов к релизу.

Сейчас вы можете подключить сервисы из WEB-защиты: AntiDDoS, Antibot и WAF Lite.

StressTest

Инструмент для тестирования устойчивости системы к экстремальным нагрузкам.

Сервис в разработке. Если хотите протестировать его одним из первых, сообщите об этом письмом на почту solarspace@rt-solar.ru. Мы свяжемся с вами, когда он будет готов к релизу.

Сейчас вы можете подключить сервисы из WEB-защиты: AntiDDoS, Antibot и WAF Lite.

Security Email Gateway

Защита электронной почты от вирусных вложений, фишинговых и спам-писем.

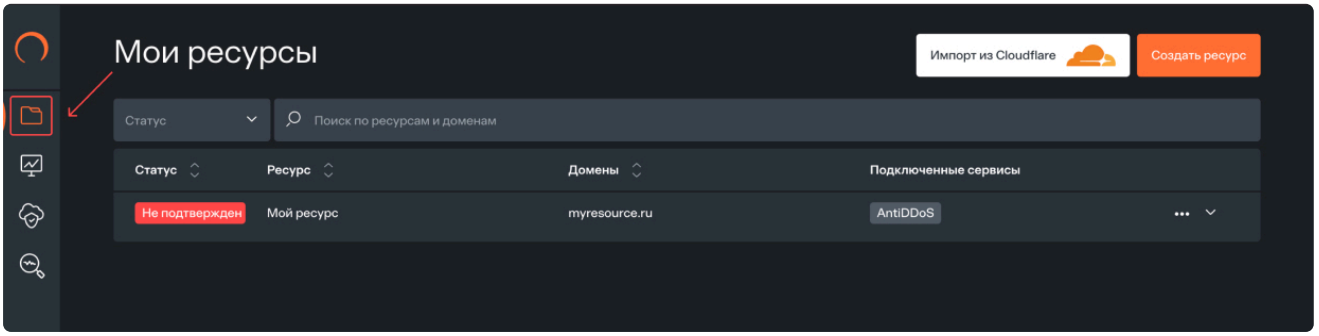
Сервис в разработке. Если хотите протестировать его одним из первых, сообщите об этом письмом на почту solarspace@rt-solar.ru. Мы свяжемся с вами, когда он будет готов к релизу.

Сейчас вы можете подключить сервисы из WEB-защиты: AntiDDoS, Antibot и WAF Lite.

Ресурсы

На странице "Мои ресурсы" отображается список всех созданных вами ресурсов.

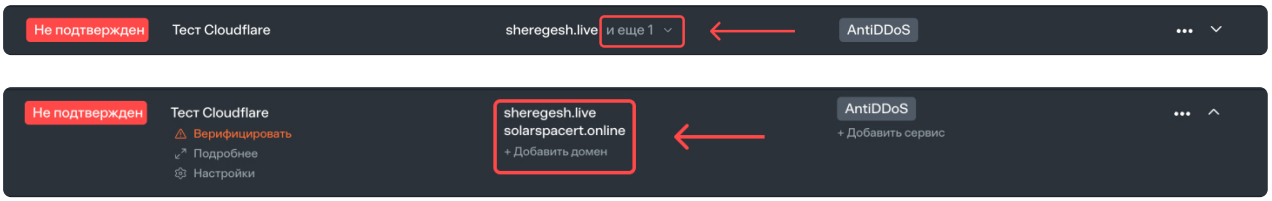
Для быстрого доступа к странице "Мои ресурсы" из любого раздела кликните на иконку в виде папки в боковом меню.



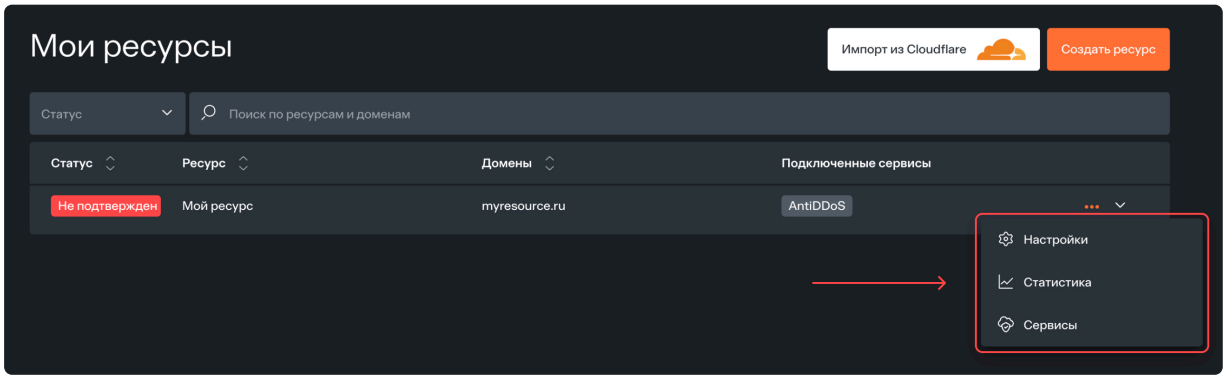
Если у вас еще нет ресурса, вы можете его создать.

В списке ресурсов можно:

- Применить сортировку по статусу и названию домена — результат отобразится в алфавитном порядке (по возрастанию или убыванию)
- Найти нужный домен через поле "Поиск по ресурсам и доменам"
- Если у ресурса несколько доменов, то их можно раскрыть, нажав на "и еще 1" рядом с именем домена

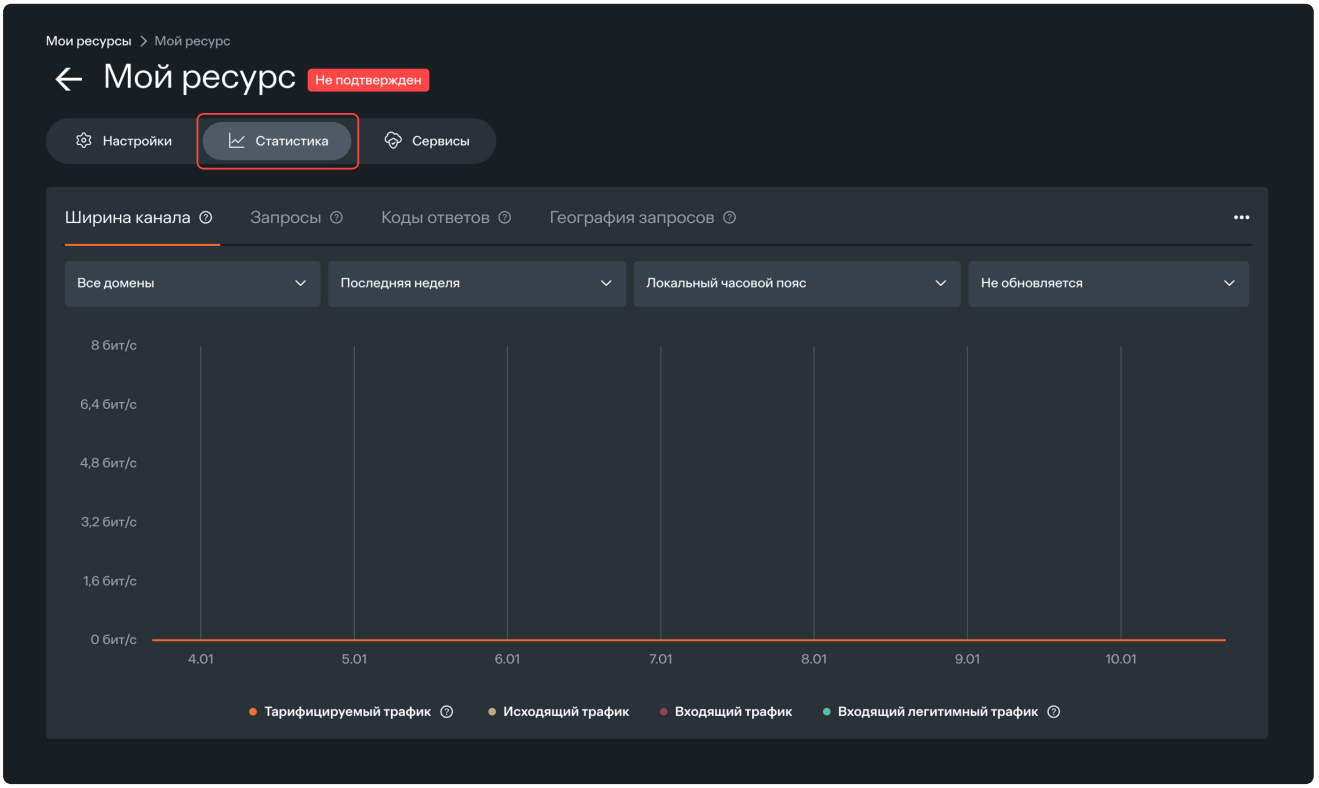


- Открыть вкладки ресурса:
  - Настройки
  - Статистика
  - Сервисы


Мои ресурсы
Импорт из Cloudflare
Создать ресурс
Статус
Поиск по ресурсам и доменам
Статус
Ресурс
Домены
Подключенные сервисы
Не подтвержден
Мой ресурс
myresource.ru
AntiDDoS
Настройки
Статистика
Сервисы

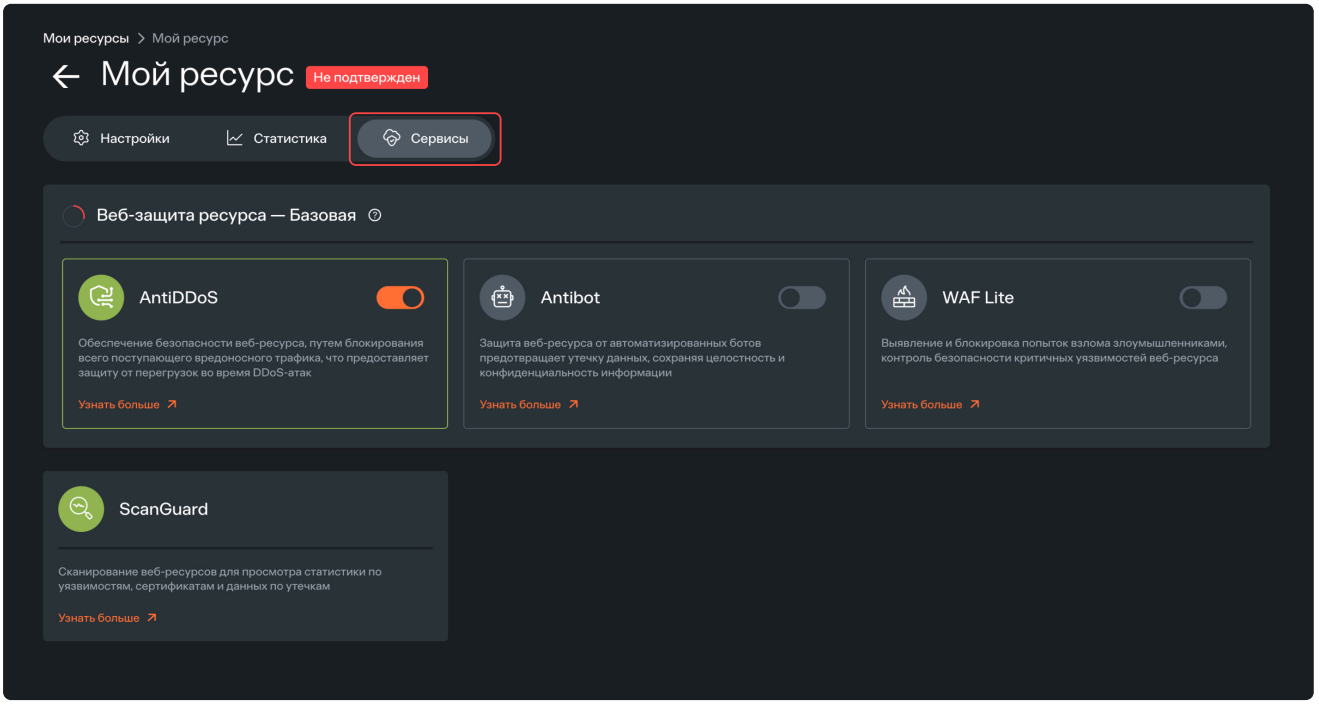
Статистика ресурса

На этой странице отображается статистика для конкретного ресурса по запросам к сайту, движению и источникам трафика. Она аналогична странице "Статистика".



Сервисы ресурса

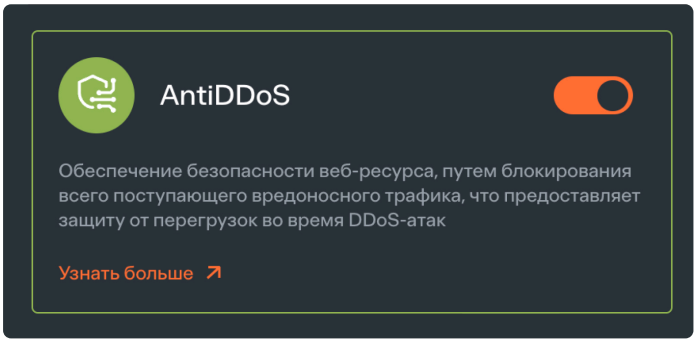
На странице указан полный перечень сервисов уже подключенных и доступных для подключения. Это сервисы веб-защиты: AntiDDoS, Antibot и WAF Lite, а также бесплатный сервис ScanGuard для сканирования ресурса на предмет утечек учетных записей и наличия фишинговых сайтов.



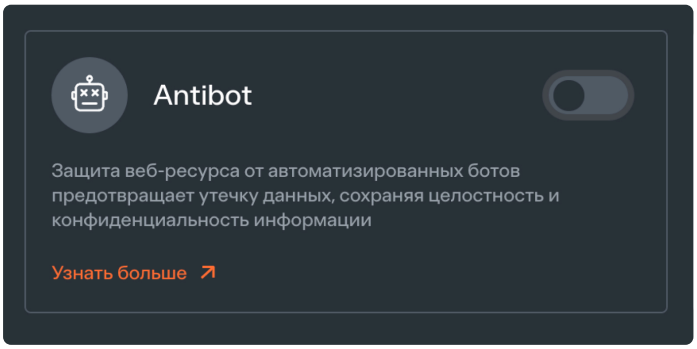
Если сервис активирован, иконка около его названия зеленого цвета, а переключатель справа активный. Если сервис не подключен, то иконка красная, а переключатель справа неактивный.

> **Обратите внимание**
>
> Иконка около сервиса ScanGuard всегда зеленого цвета, поскольку сервис для сканирования доступен бесплатно всем пользователям Solar Space

Если сервис активирован, в нижней части его блока будет кнопка "Подробнее".



При нажатии на нее вы перейдете на страницу настроек ресурса в раздел выбранного сервиса. Если сервис выключен, в нижней части его блока будет кнопка "Подключить".



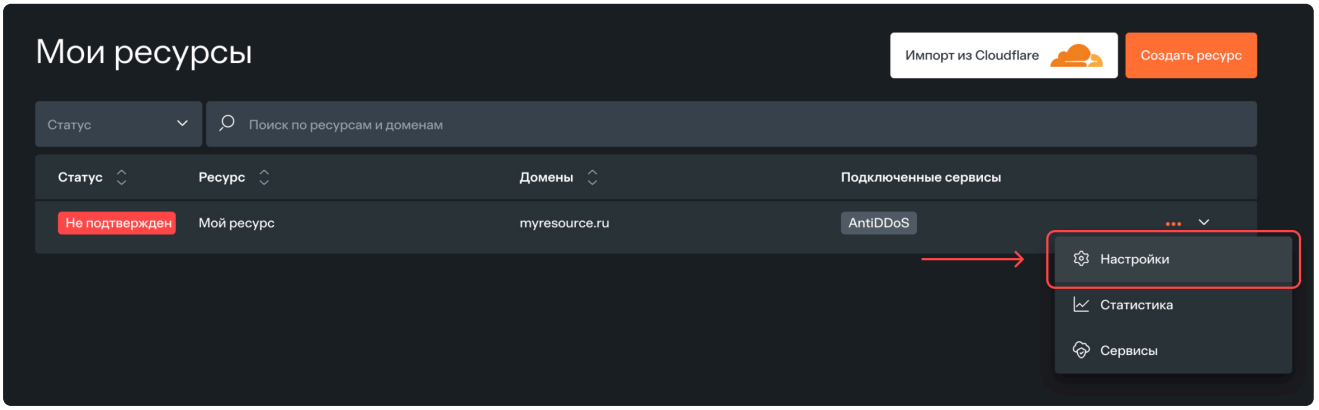
При клике на кнопку "Подключить" вы попадете на страницу с кратким описанием услуги и возможностью активации сервиса.

> **Обратите внимание**
>
> Подключение услуги Antibot доступно только при активной услуге AntiDDoS. Подключение услуги WAF Lite доступно только при активных услугах AntiDDoS и Antibot. Если вы хотите пользоваться WAF Lite, отключить Antibot нельзя: WAF Lite тоже перестанет работать

На странице доступных сервисов вы можете выбрать ScanGuard и проверить свой ресурс на уязвимость. Сервис сканирует выбранный ресурс и предоставляет статистику по нескольким параметрам. Чтобы перейти на страницу ScanGuard, нажмите кнопку "Подробнее" в разделе сервиса ScanGuard.

Настройки ресурса

Чтобы открыть настройки ресурса, перейдите на страницу "Мои ресурсы" и выберите пункт "Настройки", либо просто нажмите на нужный ресурс.



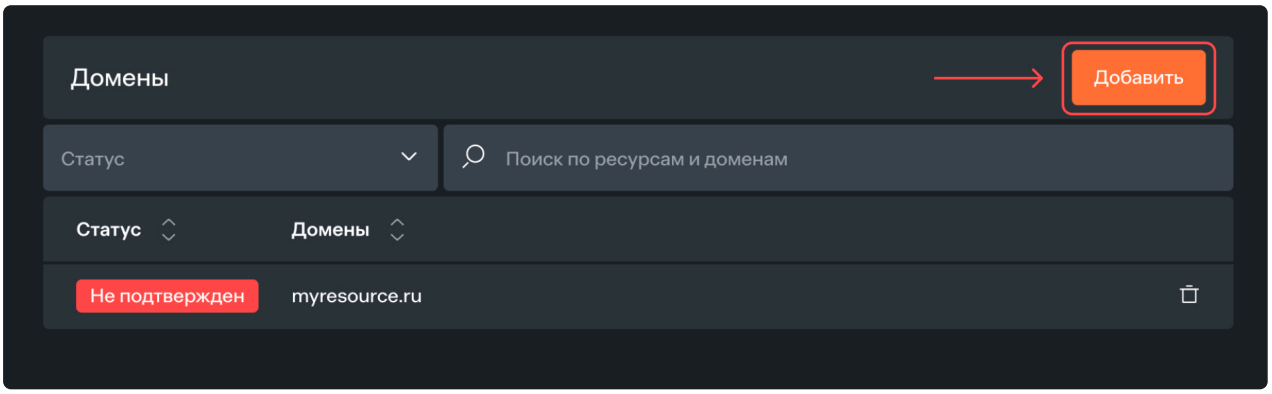
На странице настроек ресурса вы можете:

- Добавить домен
- Верифицировать ресурс
- Удалить ресурс

Добавление доменов

Если у вашего ресурса есть еще домены, которые вы хотите добавить для ресурса, выполните следующие действия:

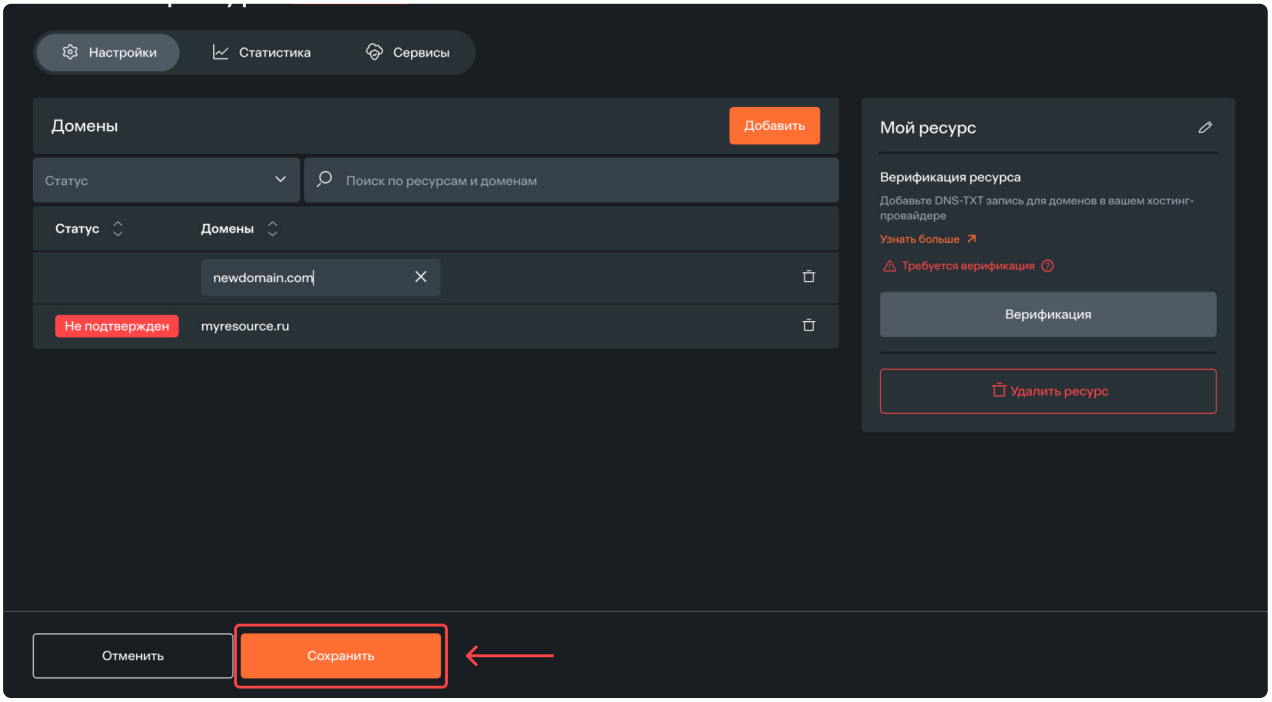
1. Нажмите на кнопку "Добавить"



2. В появившейся строке введите имя домена, соответствующее требованиям:
    - Поле домена не должно быть пустым
    - Домен зарегистрирован в системе доменных имен (DNS)
    - Домен уникальный

- Домен имеет корректный формат (например example.com)
- Адреса доменов должны совпадать

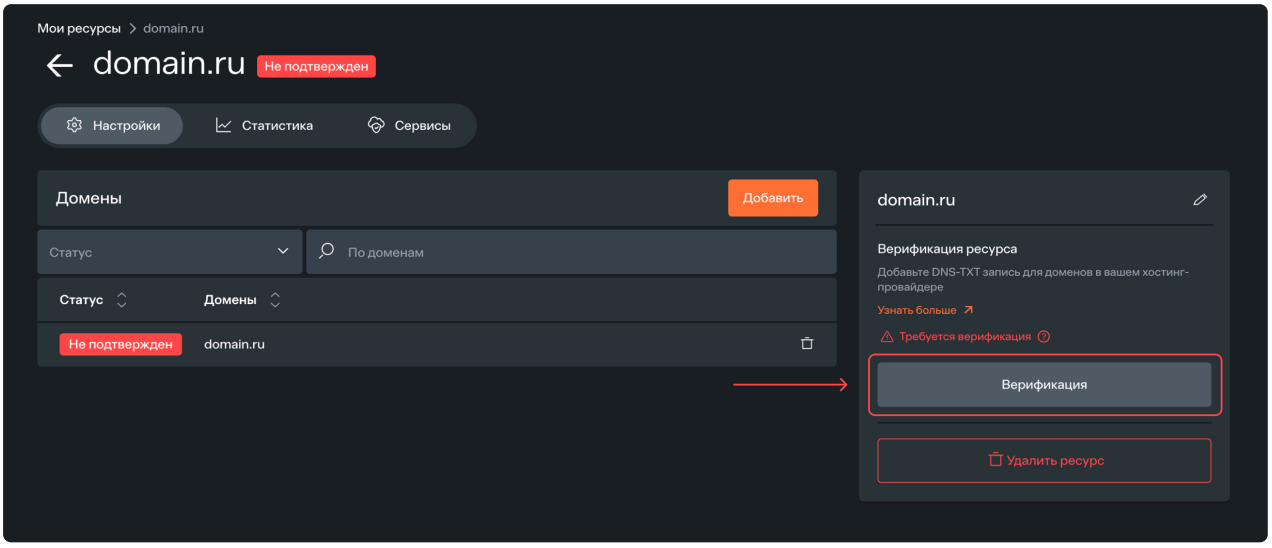
3. При корректном вводе доменного имени кнопка "Сохранить" станет активной. Нажмите на нее для добавления нового домена.



Верификация

Для верификации ресурса выполните следующие действия:

1. В разделе настроек ресурса нажмите на кнопку "Верификация".



2. В появившемся окне скопируйте представленную DNS-TXT запись Solar Space.
3. Далее следуйте инструкциям, аналогичным процессу верификации после создания ресурса начиная с пункта 2.

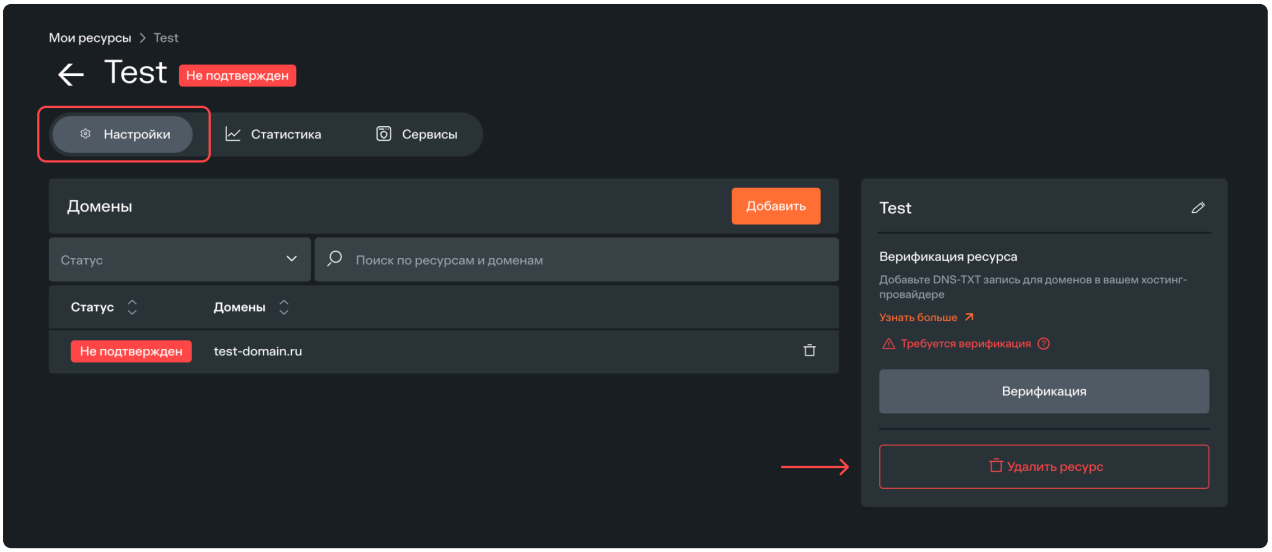
> Обратите внимание
>
> Если после повторной верификации ваш ресурс находится в статусе "Не подтвержден", читайте статью о возможных ошибках при верификации и перенаправлении трафика

Удаление ресурса

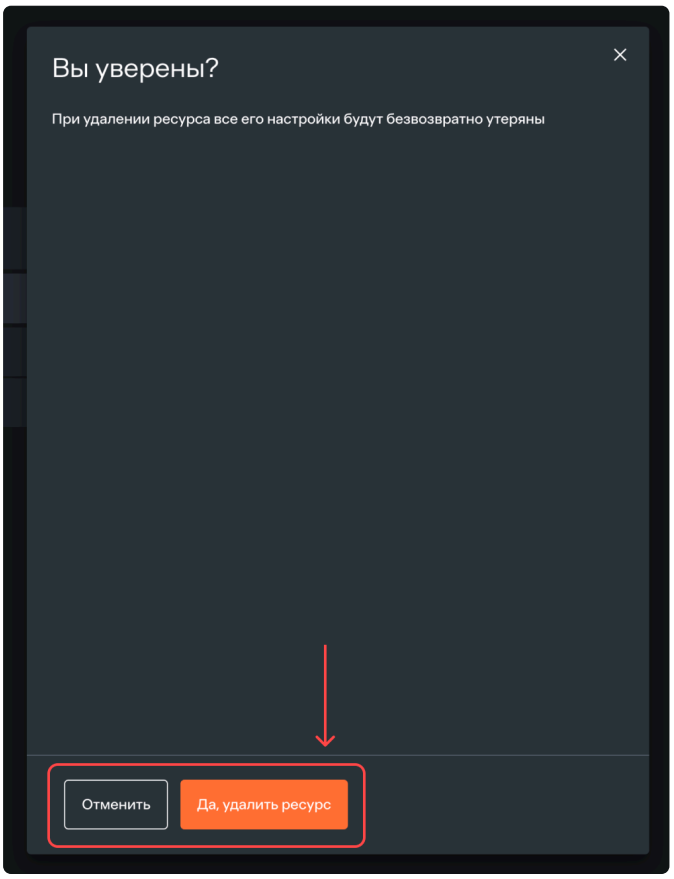
> Важно
>
> Удаление ресурса приведет к отключению всех его сервисов

Для удаления ресурса выполните следующие действия:

1. Нажмите кнопку "Удалить ресурс".



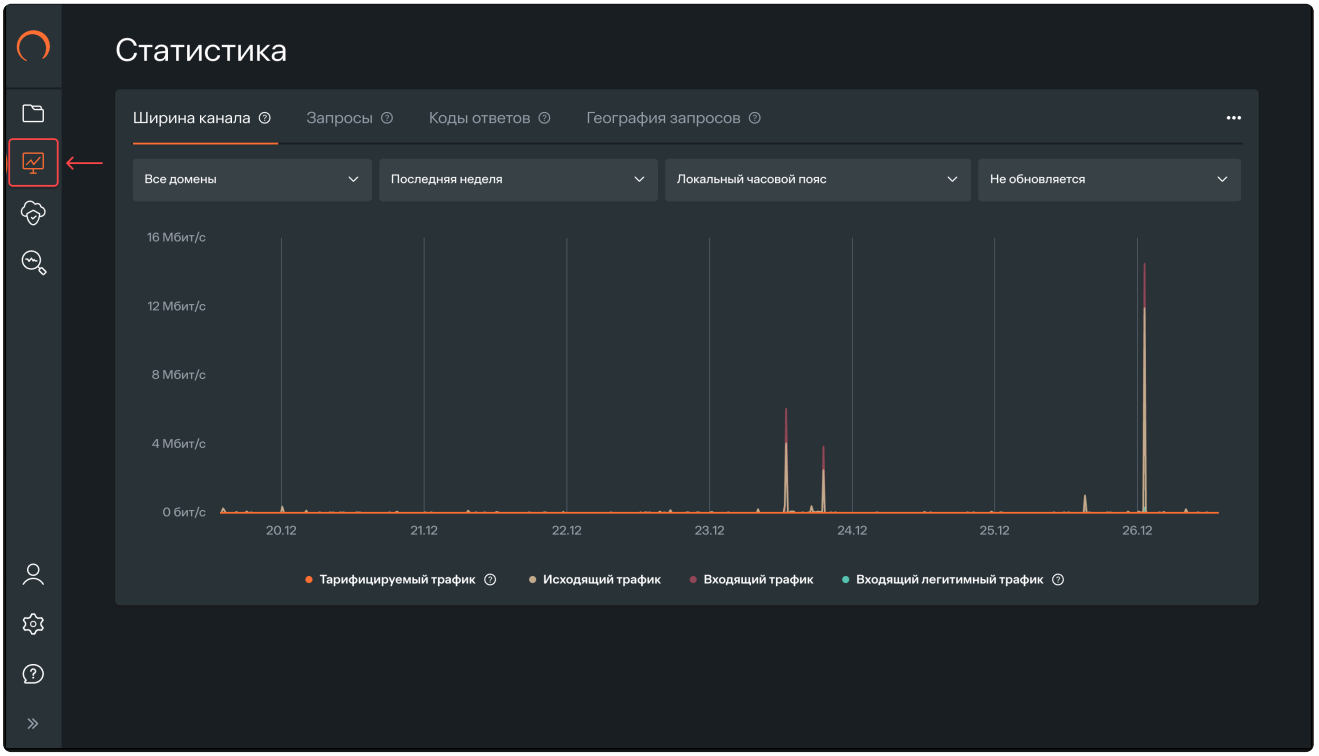
2. В появившемся окне нажмите на кнопку "Удалить" для удаления ресурса.



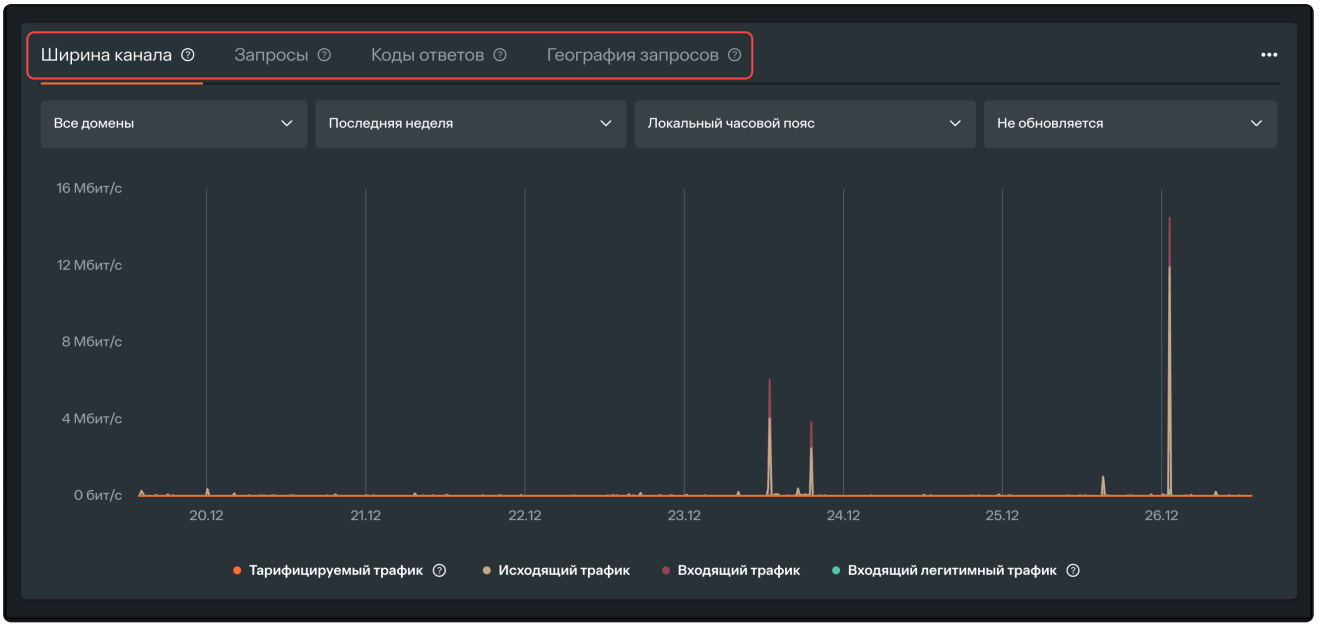
3. После подтверждения действия появится сообщение об успешном удалении. Ресурс будет исключен из списка всех ресурсов на странице "Мои ресурсы" и все его сервисы будут отключены.

Статистика

Для быстрого доступа к странице "Статистика" из любого раздела нажмите на иконку в боковом меню слева.



На странице отображаются отчеты по всем вашим ресурсам. Доступны 4 вкладки:

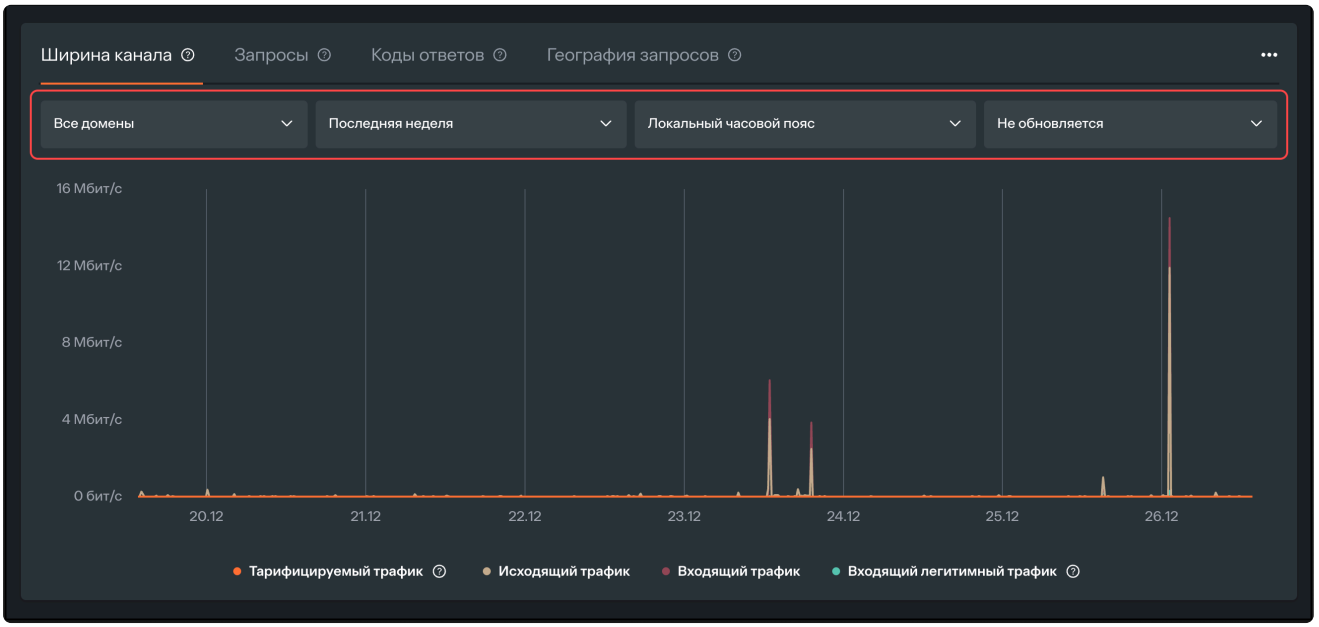


- **Ширина канала**
- **Запросы**
- **Коды ответов**

- **География запросов**

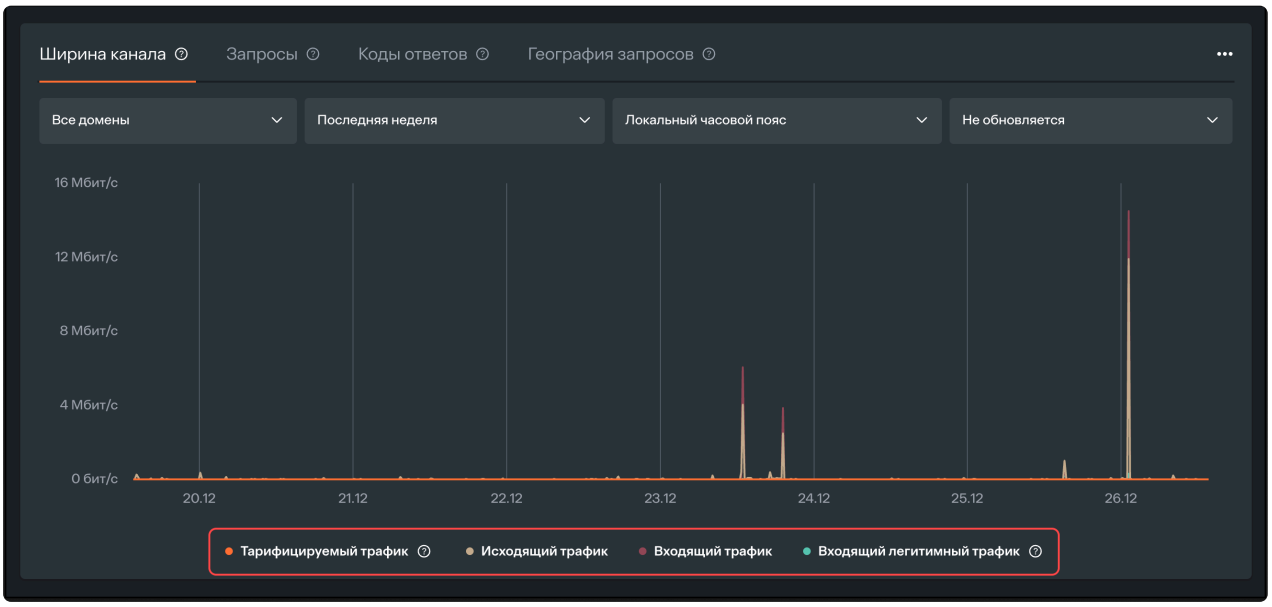
Ширина канала

Здесь вы можете посмотреть подробную информацию о трафике. В верхней части над графиком можно выбрать домены, установить период отображения отчета, часовой пояс и частоту обновления.



Под графиком обозначены 4 типа трафика:

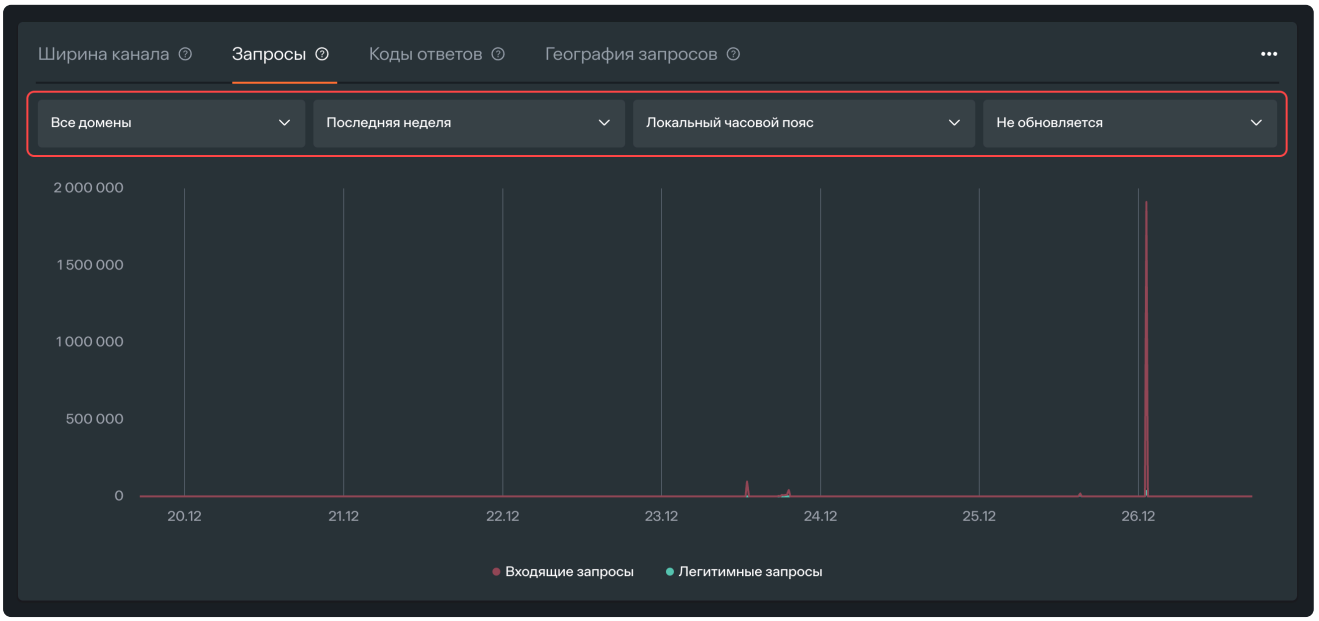
- **Тарифицируемый** — определяется объемом полосы трафика, зафиксированной в вашем тарифе. Для расчета используется алгоритм 95-го перцентиля по исходящему и входящему легитимному (очищенному) трафику. Это означает, что в течение месяца исходящий и входящий легитимный (очищенный) трафик измеряются и фиксируются каждые 5 минут. Для каждого из видов трафика в конце месяца исключаются 5% пиковых значений, и из оставшихся 95% выбирается максимальный показатель. Это и есть 95-й перцентиль. Система сравнивает 95-й перцентиль исходящего трафика и 95-й перцентиль входящего легитимного трафика. Из этих двух значений выбирается наибольшее, которое используется для расчета оплаты.
- **Исходящий** — трафик, который ваш сервер отправил посетителям вашего сайта.
- **Входящий** — общий трафик, который платформа фильтрации принимает и проверяет на предмет подозрительной активности. Включает в себя и реальных пользователей и паразитный трафик: DDoS-атаки, фишинг и спам, вредоносные файлы и коды, автоматические программы для сканирования на уязвимости.
- **Входящий легитимный** — трафик после очистки системой защиты и фильтрации вредоносных запросов, то есть только реальные пользователи и полезные роботы поисковых систем.



Нажимая на название типа трафика, вы можете исключить его из графика. В этом случае его название станет серым. Чтобы этот тип трафика снова отображался в отчете, повторно нажмите на его название.

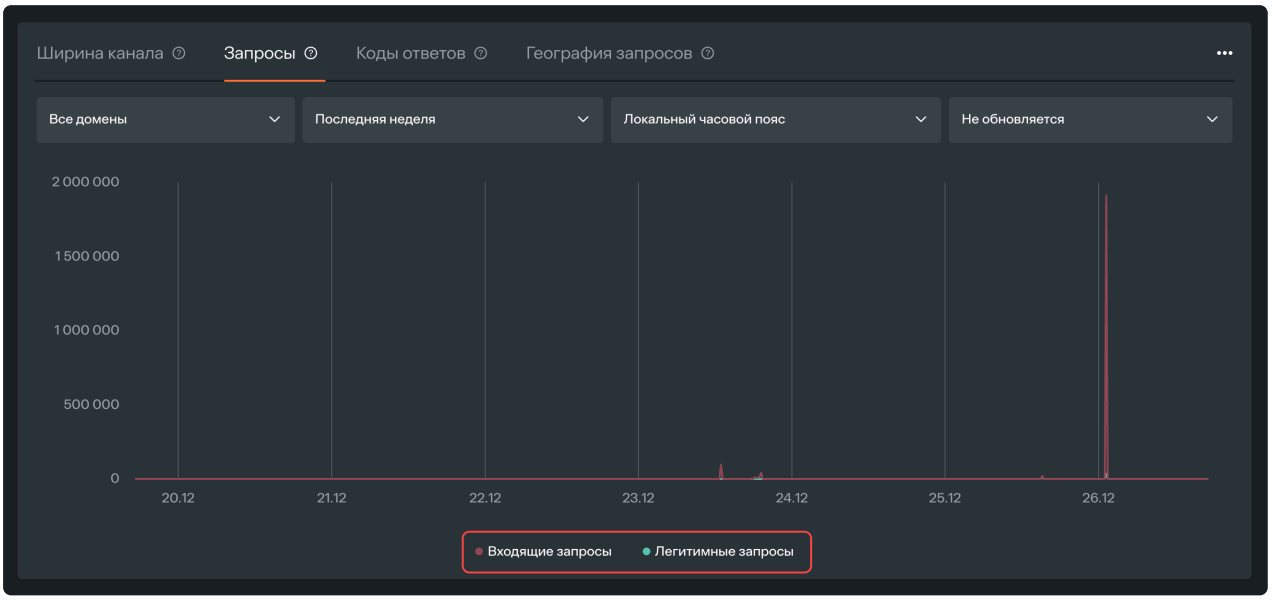
Запросы

Здесь отображается количество запросов ко всем вашим ресурсам. В верхней части над графиком можно выбрать домены, установить период отображения отчета, часовой пояс и частоту обновления.



Под графиком обозначено 2 типа запросов:

- **Входящие** — все запросы до фильтрации
- **Легитимные** — все запросы после фильтрации, соответствующие поведению реальных пользователей

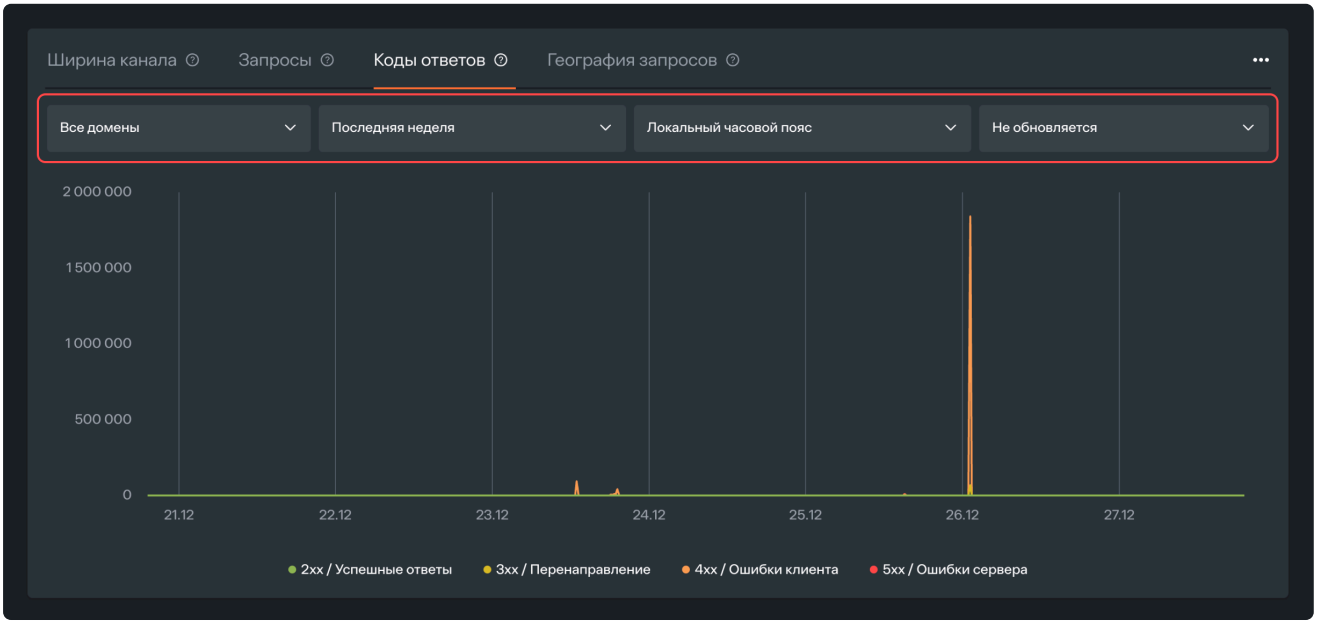


Нажимая на название типа запроса, вы можете исключить его из графика. В этом случае его название станет серым. Чтобы этот тип запроса снова отображался в отчете, повторно

нажмите на его название.

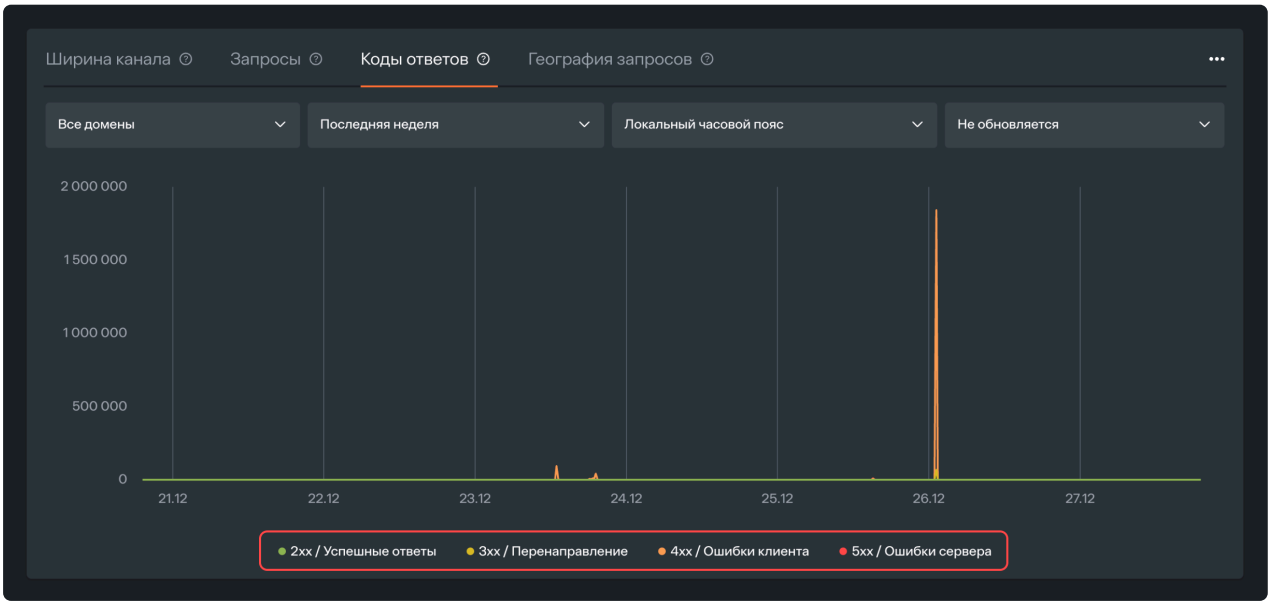
Коды ответов

Здесь обозначен результат взаимодействия пользователей с сервером. Параметры в верхней части можно изменять, аналогично вкладкам Ширина канала, Запросы и География запросов.



Под графиком обозначены 4 типа кодов ответов:

- **2xx/Успешные ответы** — этот код обозначает, что пользователь сразу перешел на ваш сайт
- **3xx/Перенаправление** — этот код обозначает, что пользователь перешел на ваш сайт через настроенный вами редирект
- **4xx/Ошибки клиента** — этот код обозначает, что у пользователя возникла проблема при взаимодействии с вашим сайтом (например, он перешел по сохраненной ссылке на страницу, которую вы удалили)
- **5xx/Ошибки сервера** — этот код обозначает проблемы на стороне сервера, возможно, он перегружен или временно недоступен



Нажимая на название кода ответа, вы можете исключить его из графика. В этом случае его название станет серым. Чтобы этот тип кода ответа снова отображался в отчете, повторно нажмите на его название.

География запросов

Здесь вы увидите, из каких стран приходят запросы к вашим ресурсам. В верхней части над графиком можно выбрать домены, установить период отображения отчета, часовой пояс и частоту обновления.

На карте вы можете навести на страну и увидеть количество запросов оттуда. Чем насыщеннее оттенок оранжевого, тем больше запросов пришло из этой страны. Белым цветом на карте обозначены страны, из которых не было обращений к ресурсу.

В этом разделе представлена подробная информация о тарифах и условиях оплаты наших услуг. Включает в себя:

- Тарификация и оплата
- Тарифы на веб-защиту
- Пополнение баланса
- Изменение тарифа
  - Добавление нового сервиса
  - Отключение сервисов
  - Изменение параметров тарифа

Тарификация и оплата

Расчетный период и оплата

Расчетный период составляет 30 дней. Для пользования сервисами необходимо положить на баланс в личном кабинете сумму в зависимости от выбранного тарифа.

Внести средства на баланс можно двумя способами:

- Онлайн с карты для типов контрагента "Физическое лицо" и "Самозанятый"
- Для типов контрагента "Юридическое лицо" и "Индивидуальный предприниматель" через поддержку Solar Space по электронной почте support@solarspace.pro

Списание с баланса происходит в формате предоплаты на 30 дней вперед, аналогично оплате интернета или онлайн-кинотеатров.

Отключение за неоплату

Если на балансе не хватает средств для списания за следующий месяц, вам придет уведомление о необходимости оплаты на электронную почту, указанную при регистрации.

В течение 5 дней после этого уведомления сервисы защиты продолжат работать даже при недостатке средств на балансе. После этого ресурс со всеми активными сервисами будет отключен.

Как измеряется тарифицируемый трафик для оплаты веб-защиты

Чтобы объяснить алгоритм расчета, обозначим основные виды трафика:

- **Тарифицируемый** — определяется объемом полосы пропускания, зафиксированной в тарифах на веб-защиту
- **Исходящий** — трафик, который ваш сервер отправил посетителям вашего сайта
- **Входящий** — весь трафик, который платформа фильтрации принимает и проверяет на предмет подозрительной активности. Включает в себя и реальных пользователей и паразитный трафик: DDoS-атаки, фишинг и спам, вредоносные файлы и коды, автоматические программы для сканирования на уязвимости
- **Входящий легитимный** — трафик после очистки нашей системой защиты и фильтрации вредоносных запросов, то есть только реальные пользователи и полезные роботы

поисковых систем

Для расчета тарифицируемого трафика используется **алгоритм 95-го перцентиля по исходящему и входящему легитимному трафику**. Это означает, что в течение 30-дневного расчетного периода исходящий и входящий легитимный трафик измеряются и фиксируются каждые 5 минут. Из этих замеров в конце месяца исключаются 5% пиковых значений, и из оставшихся 95% выбирается максимальный показатель. Это и есть 95-й перцентиль. Система сравнивает 95-й перцентиль исходящего трафика и 95-й перцентиль входящего легитимного трафика. Из этих двух значений выбирается наибольшее, которое используется для расчета оплаты.

Получается, что в течение 30-дневного расчетного периода исходящий или входящий легитимный трафик на вашем сайте может 36 часов (5% от 30 дней) превышать установленную тарифом полосу пропускания.

У большинства сайтов 95-й перцентиль входящего легитимного трафика будет превышать 95-й перцентиль исходящего трафика. Исключение могут составлять лишь веб-ресурсы, которые, к примеру, ведут трансляции и стримы, то есть "отдают" много трафика. У них 95-й перцентиль исходящего трафика может быть выше.

Пример измерения тарифицируемого трафика для оплаты веб-защиты

Дано:

- Количество доменов — 1 домен
- Уровень защиты — оптимальный (AntiDDoS + Antibot)
- Выбранный тариф — с полосой пропускания трафика 10 Мбит/с
- Трансляции с сайта — не предполагается

Решение: платформа в течение 30-дневного расчетного периода измеряет объем входящего легитимного и исходящего трафика каждые 5 минут. Объем исходящего трафика низкий, поскольку сайт не ведет трансляции и "отдает" мало трафика. Объем входящего легитимного трафика во время замеров не превышает 10 Мбит/с. Однако в конце месяца сайт подвергся атаке: она длилась почти сутки и объем входящего трафика достигал 300 Мбит/с. После окончания расчетного периода платформа проанализировала результаты всех замеров. В период атаки объем трафика превысил установленную тарифом полосу пропускания в 10 Мбит/с. Превышение фиксировалось на протяжении 14 часов.

Согласно правилам расчета 95-го перцентиля, трафик может превышать установленную тарифом полосу пропускания в общей сложности 36 часов в течение 30-дневного расчетного периода (5% от 30 дней). Поскольку превышение фиксировалось на протяжении 14 часов,

значение 95-го перцентиля "уместилось" в полосу пропускания 10 Мбит/с в выбранном тарифе.

Ответ: в этом случае оплачивается только фиксированная стоимость тарифа с параметром полосы 10 Мбит/с. Для оптимального уровня защиты, включающего AntiDDoS и Antibot, оплата составит 1500 рублей в месяц (без НДС). Список всех тарифов можно посмотреть на странице Тарифы на веб-защиту.

Как рассчитать свой уровень RPS для оплаты продвинутой защиты

RPS — это максимальное количество запросов в секунду, которое может обработать сайт. Этот показатель используется для расчета оплаты за сервис WAF Lite.

Для вычисления RPS нужно узнать пиковое количество посетителей сайта в сутки и разделить его на количество секунд в сутки, то есть на 86 400. Количество посетителей можно посмотреть в сервисах веб-аналитики, например, в Яндекс.Метрике.

Для сайта с максимальной посещаемостью 50 000 человек в сутки RPS составит 50 000/86 400 = 0,57 запросов в секунду. Это значит, что при подключении продвинутой защиты достаточно будет минимального тарифа для 5 RPS. Список всех тарифов можно посмотреть на странице Тарифы на веб-защиту.

Как оплачивается превышение

В тарифах на веб-защиту закреплено конкретное значение полосы пропускания или количества RPS (запросов к сайту в секунду). Если по итогам расчетного периода 95-й перцентиль превышает установленное в тарифе значение, вы получите счет за превышение параметров тарифа на электронную почту, указанную при регистрации на платформе.

Превышение 1 Мбит/с	200 ₽
Превышение 1 RPS	200 ₽

Превышение оплачивается как и фиксированный платеж — через внесение средств на баланс в личном кабинете.

⚠ Важно

Платежи за превышение, как правило, приходят из-за неверного выбора тарифа. Если в течение нескольких месяцев подряд вам поступают уведомления о превышении, выберите корректный тариф, который соответствует реальному трафику на вашем сайте

Тарифы на веб-защиту

Полный список тарифов доступен в личном кабинете. Если вам нужен тариф, который отличается от стандартной линейки, напишите на почту solarspace@rt-solar.ru. С вами свяжется менеджер.

Тарифы на базовый уровень веб-защиты — AntiDDoS

Подключение — 0 рублей.

Ежемесячный платеж за **базовую защиту** складывается из следующих компонентов:

- Фиксированная абонентская плата за тарифицируемый трафик (Мбит/с) — ширину канала
- Динамическая плата в случае превышения тарифицируемого трафика

Правила измерения и подсчета тарифицируемого трафика описаны в статье "Тарификация и оплата".

Тарифы на оптимальный уровень веб-защиты — AntiDDoS + Antibot

Подключение — 0 рублей.

Ежемесячный платеж за **оптимальную защиту** складывается из следующих компонентов:

- Фиксированная абонентская плата за тарифицируемый трафик (Мбит/с) — ширину канала
- Динамическая плата в случае превышения тарифицируемого трафика

Правила измерения и подсчета тарифицируемого трафика описаны в статье "Тарификация и оплата".

Тарифы на продвинутый уровень веб-защиты — AntiDDoS + Antibot + WAF Lite

Подключение — 0 рублей.

Ежемесячный платеж за **продвинутую защиту** складывается из следующих компонентов:

- Фиксированная абонентская плата за тарифицируемый трафик (Мбит/с) — ширину канала
- Фиксированная плата за количество запросов к сайту в секунду (RPS)
- Динамическая плата в случае превышения тарифицируемого трафика или количества RPS

Правила измерения и подсчета тарифицируемого трафика, а также рекомендации по расчету RPS (количества запросов к сайту в секунду) описаны в статье "Тарификация и оплата".

> Обратите внимание
>
> В личном кабинете важно выбрать тариф, параметры которого будут соответствовать реальному трафику на вашем сайте. Если по итогам 30-дневного расчетного периода фактический трафик будет выше параметров, установленных тарифом, вам придет уведомление об оплате превышения.

Если такие уведомления поступают в течение нескольких месяцев подряд, рекомендуем изменить тариф, чтобы он соответствовал реальному объему трафика и запросов на вашем сайте.

Как подобрать тариф

На что ориентироваться в личном кабинете при подборе тарифа:

- **1-5 Мбит/с, 5-10 RPS** — для простого сайта-визитки с контактами
- **10-30 Мбит/с, 20-50 RPS** — для каталога товаров и услуг без возможности онлайн-покупки
- **От 50 Мбит/с, более 50 RPS** — для интернет-магазинов и крупных сайтов
- **Более 100 Мбит/с, более 90 RPS** — по запросу через почту solarspace@rt-solar.ru

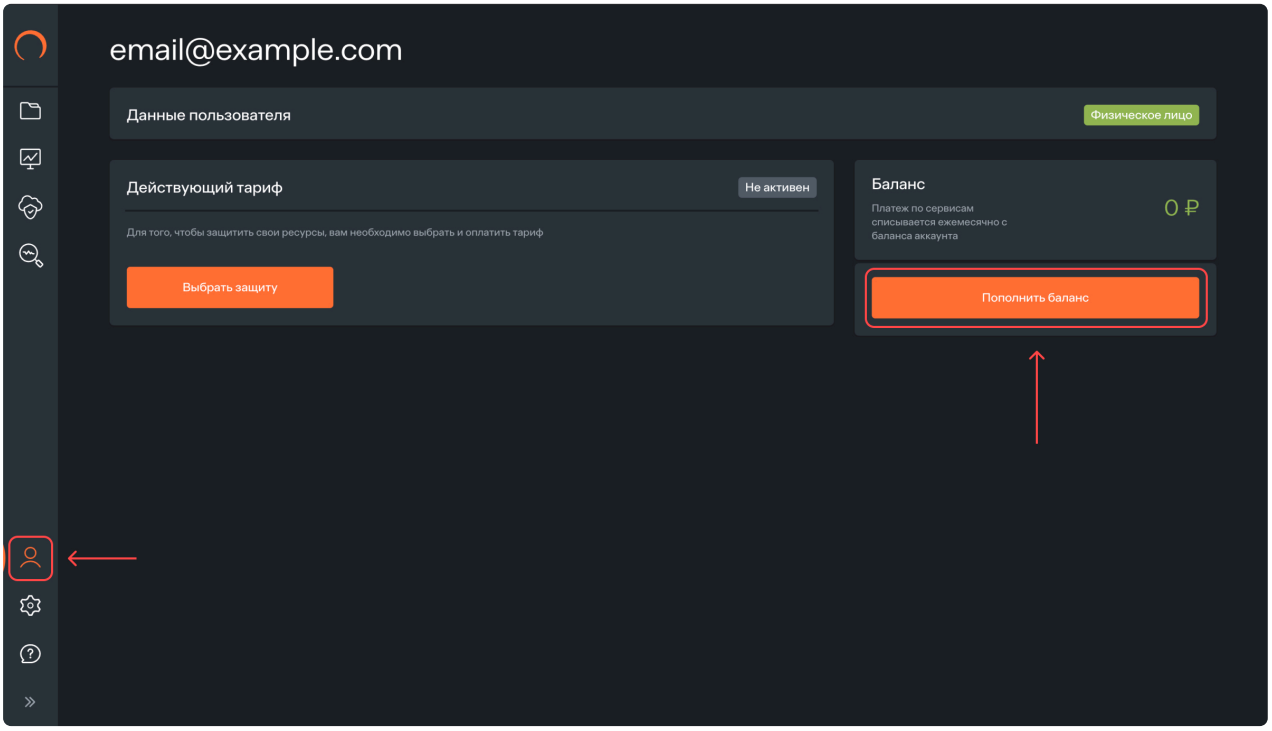
Эта рекомендация позволит приблизительно определить тариф, если у вас нет данных веб-аналитики. Для каждого конкретного сайта ситуация может отличаться. Кроме того, возможны всплески трафика, к примеру, в период проведения рекламных кампаний, которые привлекают на сайт больше посетителей, чем обычно.

Можно выбрать тариф по этой рекомендации, а далее на основе данных об использовании платформы Solar Space за 2-3 месяца при необходимости скорректировать его. Как изменить тариф, описано здесь.

Пополнение баланса

Для пополнения баланса выполните следующие действия:

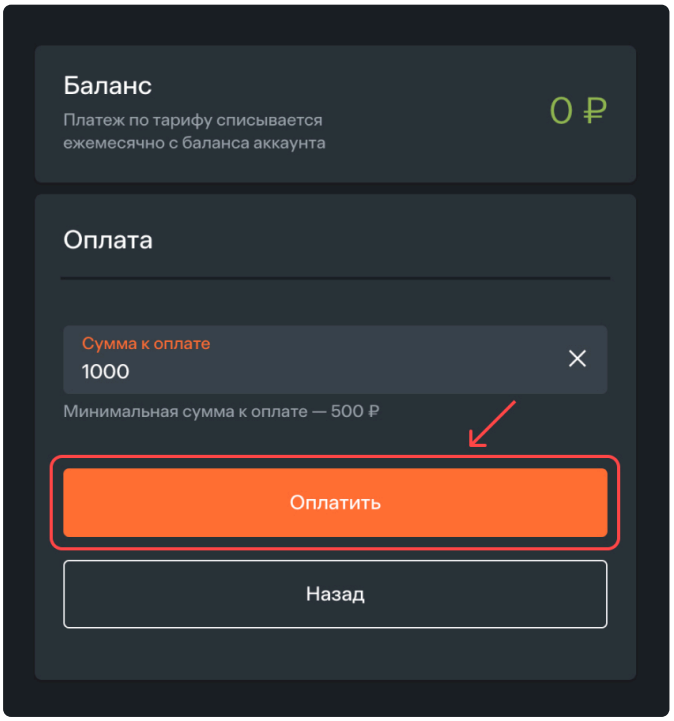
1. Перейдите на страницу профиля.
2. Нажмите на кнопку "Пополнить баланс".



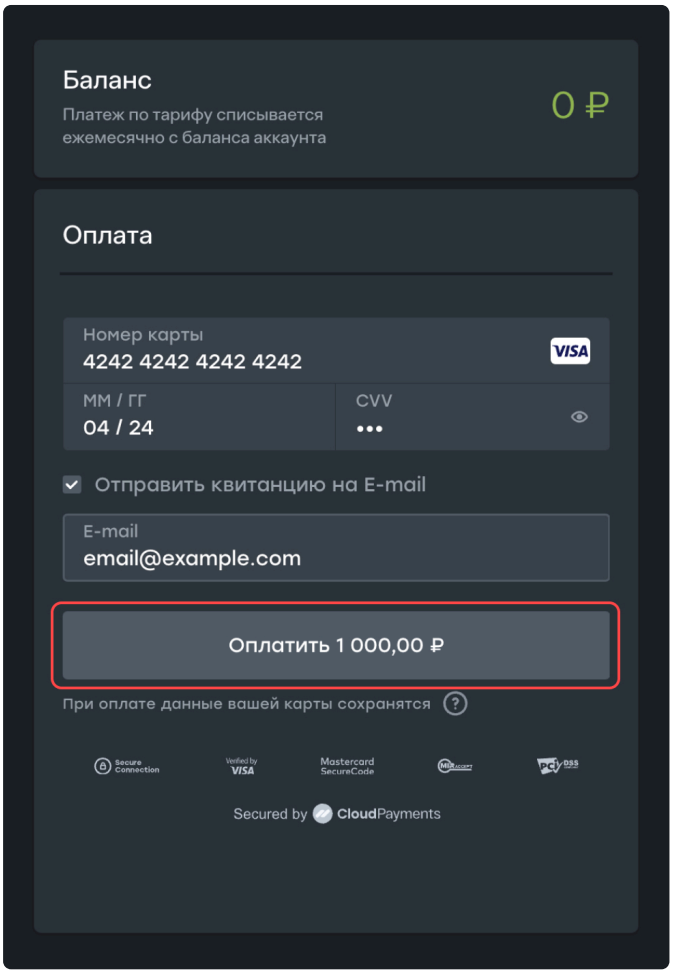
> **Обратите внимание**
>
> Оплата по карте доступна для типов контрагента "Физическое лицо" и "Самозанятый". Для типов контрагента "Индивидуальный предприниматель" и "Юридическое лицо" доступна оплата по счету

Тип контрагента "Физическое лицо" и "Самозанятый"

1. В разделе оплаты введите сумму для пополнения баланса (минимальная сумма 500 рублей) и нажмите на кнопку "Оплатить".



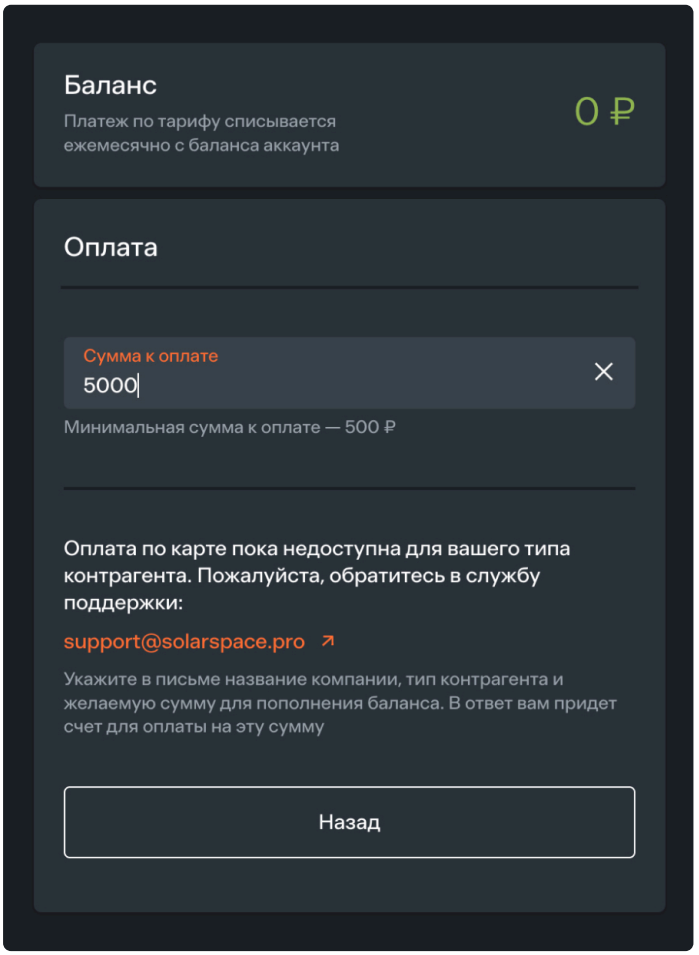
2. Введите данные карты в форму оплаты и нажмите на кнопку "Оплатить".



Тип контрагента "Индивидуальный предприниматель" и "Юридическое лицо"

Пользователям с этими типами контрагентов доступна оплата по счету.

Свяжитесь с поддержкой Solar Space support@solarspace.pro и укажите в письме название компании, тип контрагента и сумму, которую вы хотите положить на баланс.



Изменение тарифа

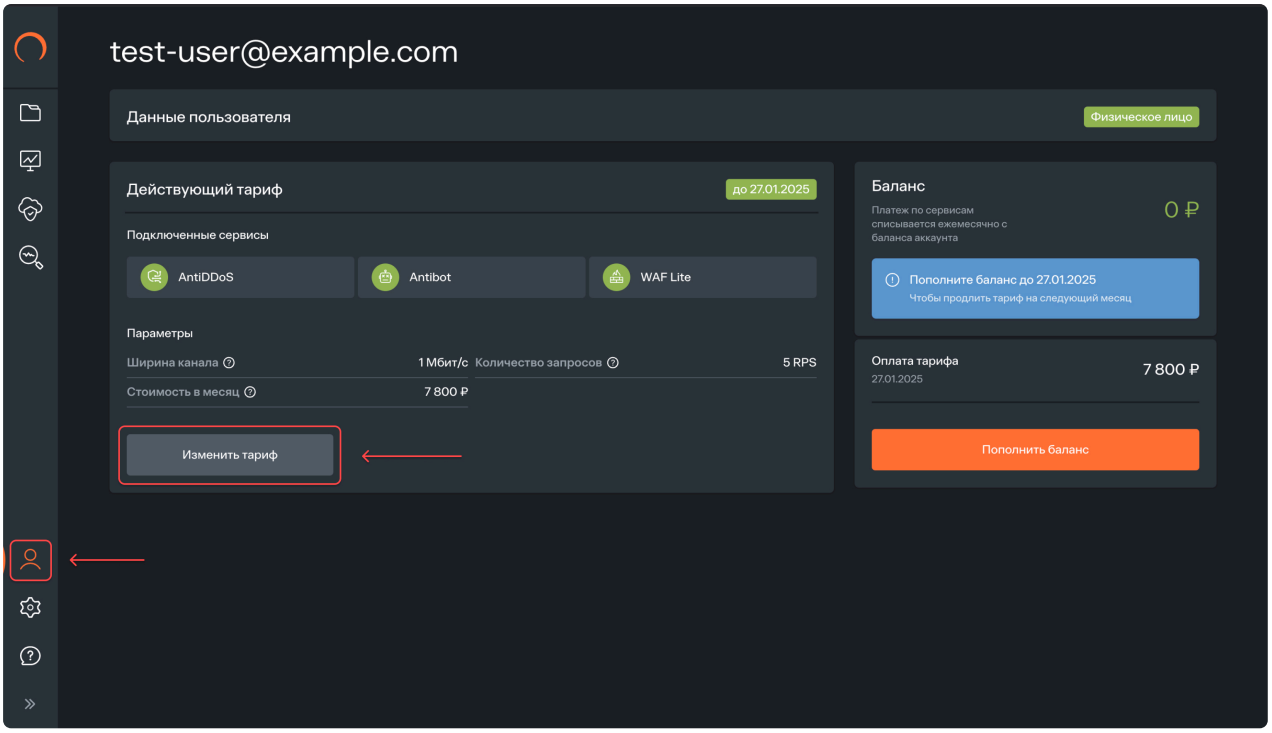
> **Обратите внимание**
>
> Изменение тарифа доступно только для пользователей с активным оплаченным тарифом

В рамках изменения тарифа вам доступны следующие действия:

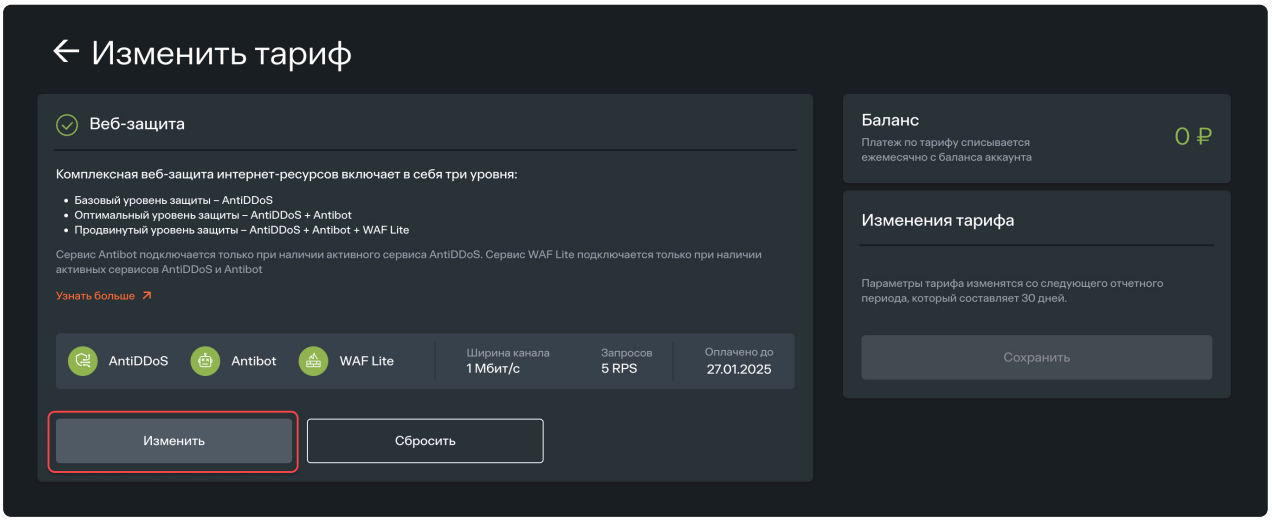
- Добавление нового сервиса
- Отключение сервисов
- Изменение параметров тарифа

Для того, чтобы изменить тариф, необходимо выполнить следующие действия:

1. Перейдите на страницу профиля в личном кабинете.
2. Нажмите на кнопку "Изменить тариф".



3. На странице изменения тарифа нажмите на кнопку "Изменить".



4. Выполните нужное действие: добавьте новый сервис, измените параметры тарифа или отключите сервис.

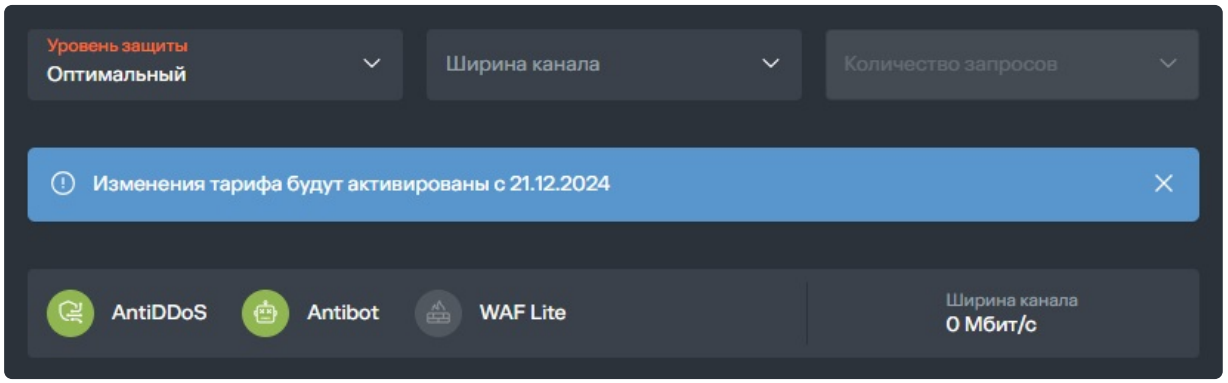
Добавление нового сервиса

Добавление нового сервиса заключается в изменении уровня защиты:

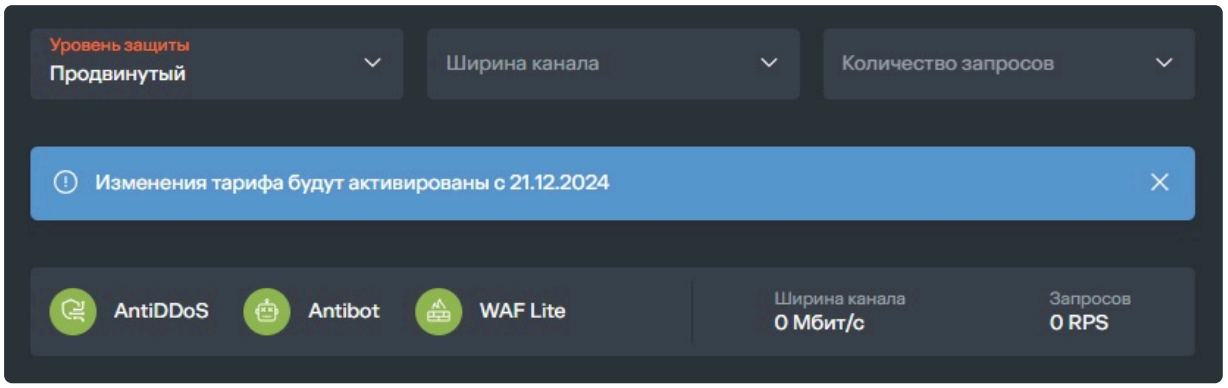
- Для добавления сервиса Antibot необходимо изменить уровень защиты с **базового** на **оптимальный**
- Для добавления сервиса WAF Lite необходимо изменить уровень защиты с **базового** или **оптимального** на **продвинутый** и установить значение для поля "Количество запросов"

Для того, чтобы добавить новый сервис, выполните следующие действия:

1. Измените уровень защиты.
   - Для добавления нового сервиса **Antibot** выберите из выпадающего списка уровней защиты **"Оптимальный"**



   - Для добавления нового сервиса **WAF Lite** выберите из выпадающего списка уровней защиты **"Продвинутый"**



2. В поле "Ширина канала" выберите нужное значение из выпадающего списка. Для продвинутого уровня защиты в поле "Количество запросов" также выберите значение из списка. Далее нажмите кнопку "Применить".

Добавление нового сервиса можно активировать:

- **Со следующего месяца**, если вы не только добавили новые сервисы, но и изменили параметры текущего тарифа — ширину канала

- **Сразу**, если не редактируются параметры текущего тарифа

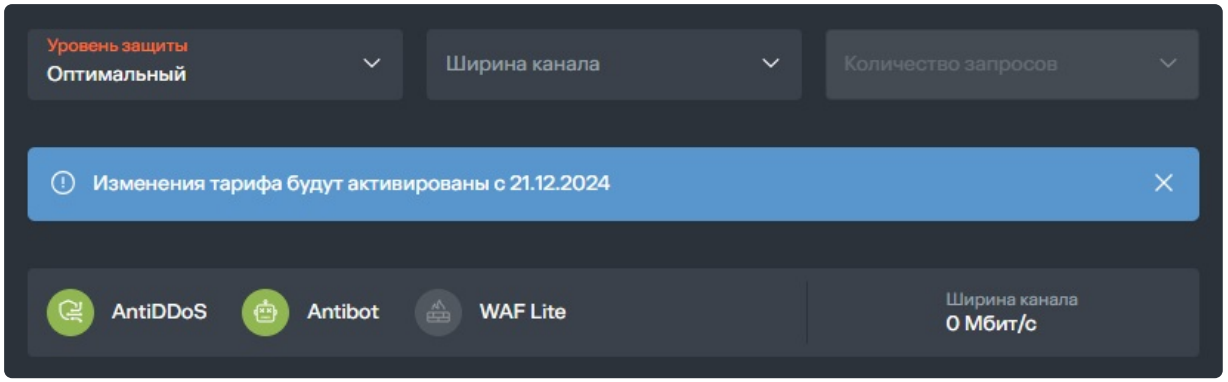
Активация сервиса сразу

Активация сервиса сразу доступна только в случае, если не изменяются текущие параметры тарифа (ширина канала).

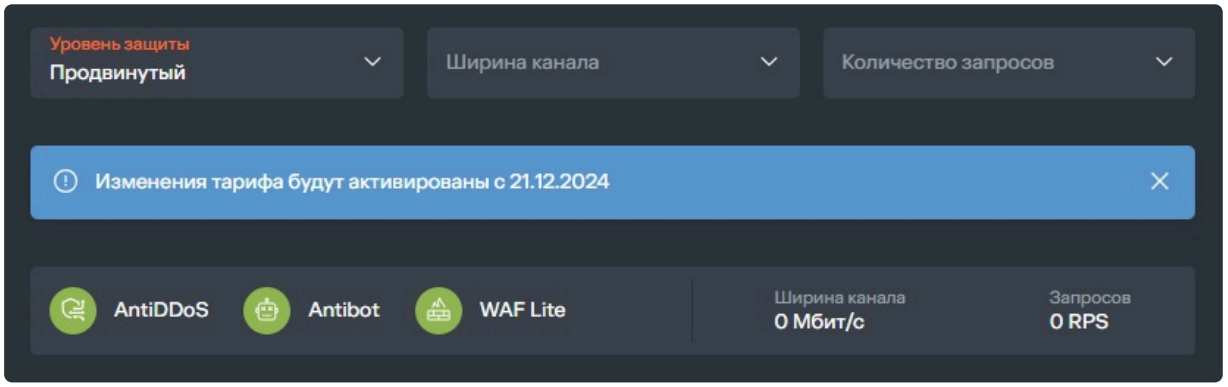
Пример.
У вас подключен базовый уровень (т.е услуга AntiDDoS) с шириной защищаемого канала 5 Мбит/с. Вы хотите увеличить ширину канала до 10 Мбит/с и одновременно перейти на оптимальный уровень защиты, добавив новый сервис Antibot с шириной канала 10 Мбит/с. Новый сервис будет активирован только с начала следующего расчетного периода, поскольку вы меняете параметр текущего тарифа — ширину канала в сервисе AntiDDoS. Чтобы активировать Antibot сразу, оставьте ширину канала на значении 5 Мбит/с, как в текущем тарифе, и оплатите Antibot только за дни, оставшиеся до начала следующего расчетного периода.

Для активации нового сервиса сразу выполните следующие действия:

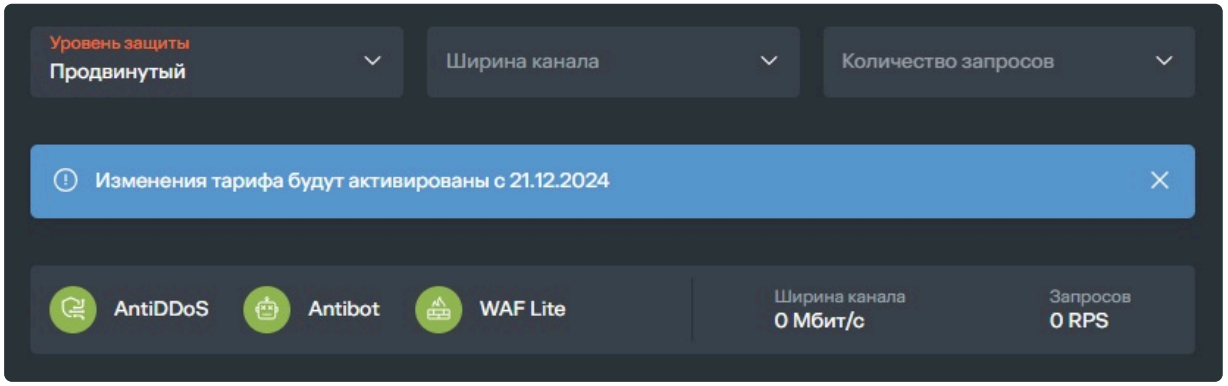
1. Добавьте новый сервис:
   - Если у вас подключен **базовый** уровень защиты, то вы можете выбрать **оптимальный**, добавив сервис **Antibot**



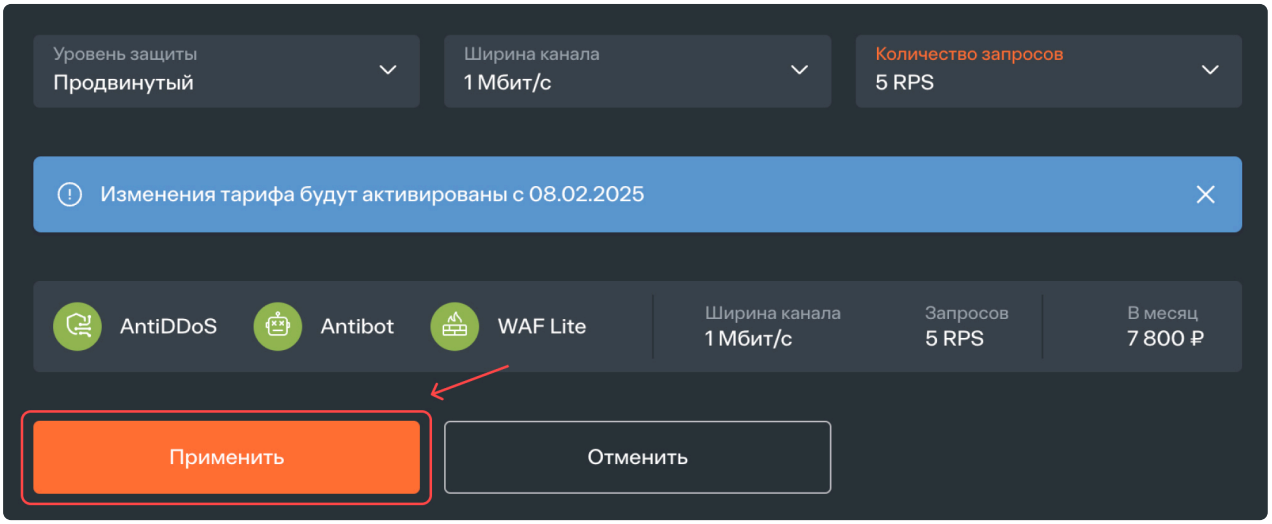
   - Если у вас подключен **базовый** уровень защиты, то вы также можете выбрать **продвинутый**, добавив сервисы **Antibot + WAF Lite**



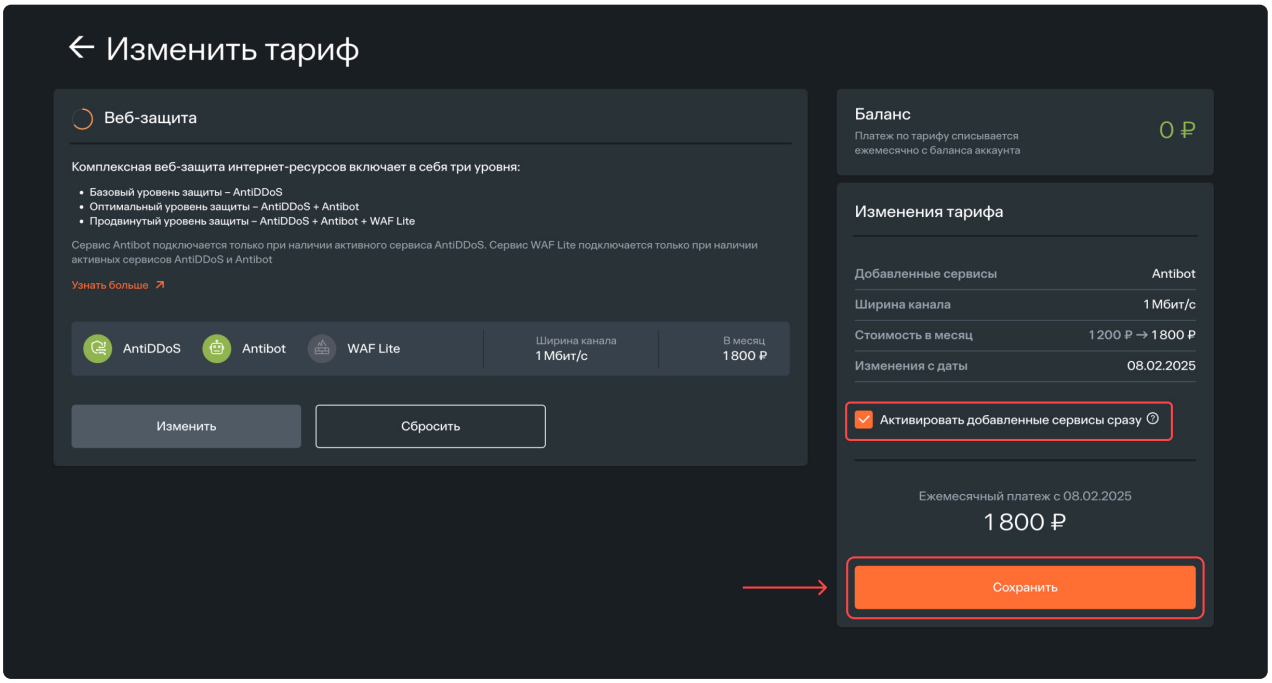
- Если у вас подключен **оптимальный** уровень защиты, то вы можете выбрать **продвинутый**, добавив сервис **WAF Lite**



2. В поле "Ширина канала" установите значение, **которое было выбрано в текущем тарифе**, и нажмите на кнопку "Применить". Если вы повышаете уровень защиты до продвинутого, добавляя сервис WAF Lite, укажите значение для поля "Количество запросов".

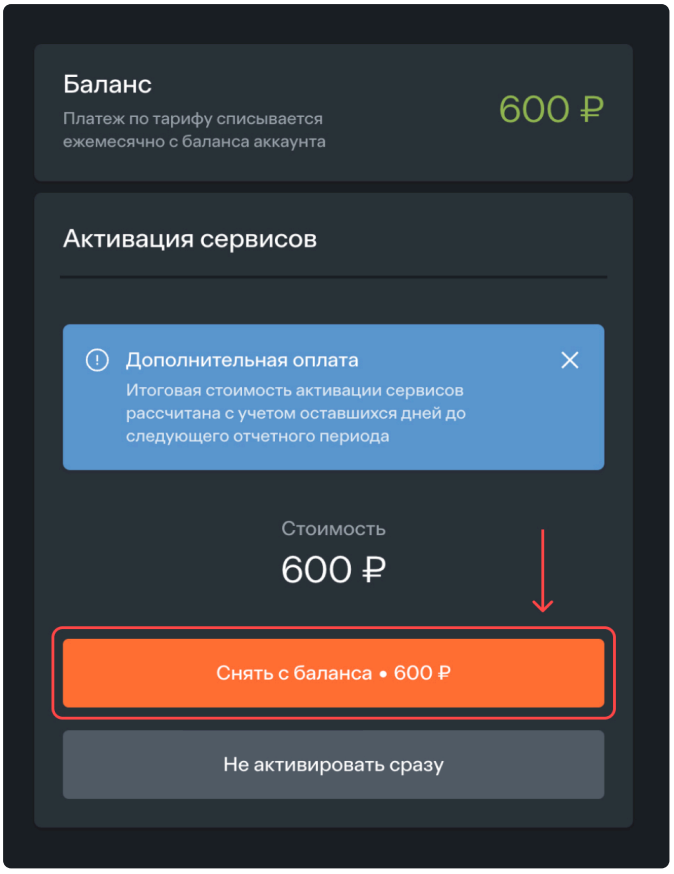


3. Проверьте информацию в блоке "Изменения тарифа", поставьте галочку "Активировать добавленные сервисы сразу" и нажмите на кнопку "Сохранить".

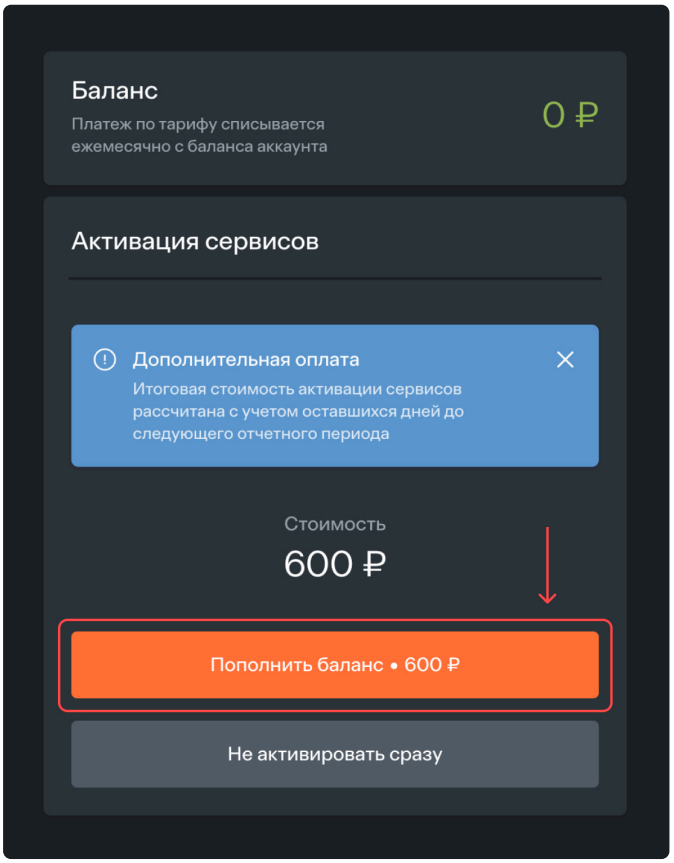


> **Обратите внимание**
>
> Стоимость нового сервиса при активации сразу рассчитывается исходя из количества дней, оставшихся до следующего расчетного периода

4. Если на вашем балансе достаточно средств, нажмите кнопку "Снять с баланса". Система автоматически спишет с него нужную сумму.



5. Если на балансе недостаточно средств, нажмите кнопку "Пополнить баланс" и далее оплатите новые сервисы



Если вы не готовы снимать с баланса или пополнять его сейчас, нажмите на кнопку "Не активировать сразу". В этом случае система автоматически спишет сумму ежемесячного платежа с учетом новых добавленных сервисов в начале следующего расчетного периода.

Отключение сервисов

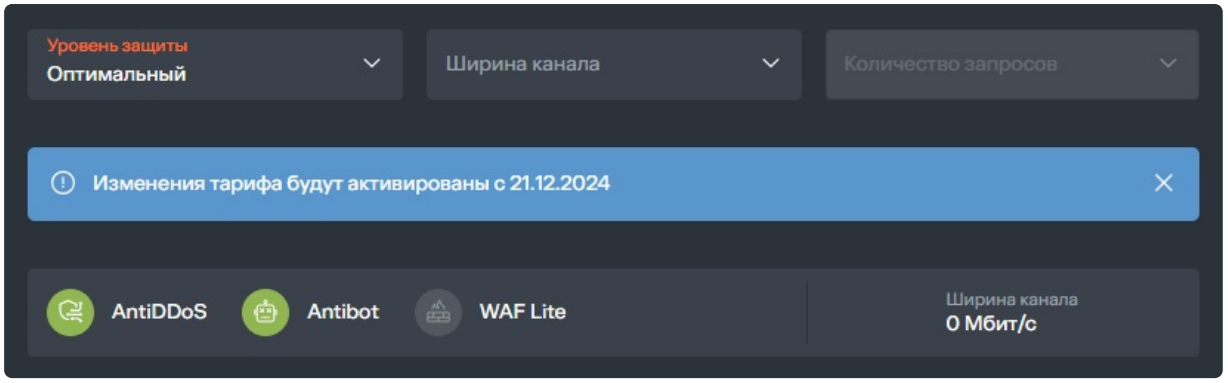
При отключении активного сервиса изменения вступят в силу со следующего расчетного периода.

Отключение сервисов означает понижение уровня защиты: с продвинутого на базовый или оптимальный, либо с оптимального на базовый.

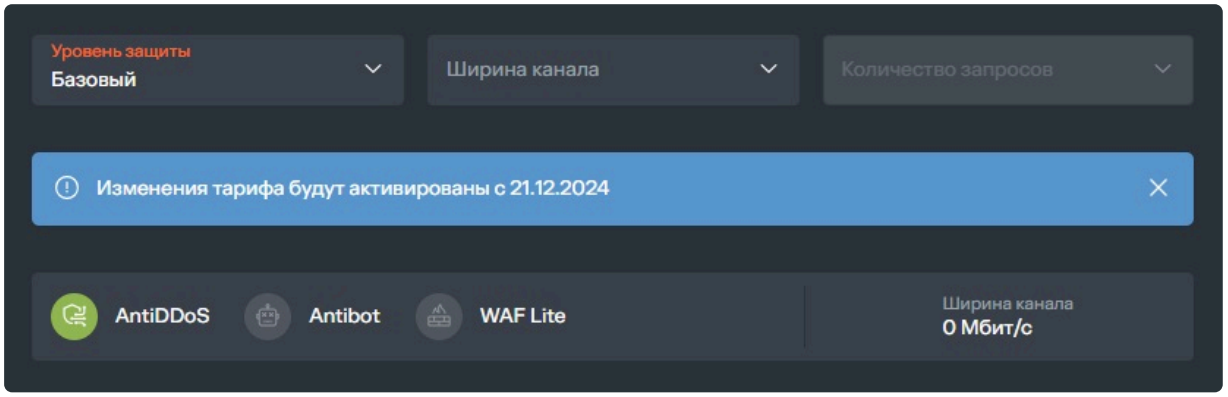
> ⚠ Важно
>
> При удалении сервиса AntiDDoS защита веб-ресурса полностью отключается

Для отключения сервисов выполните следующие действия:

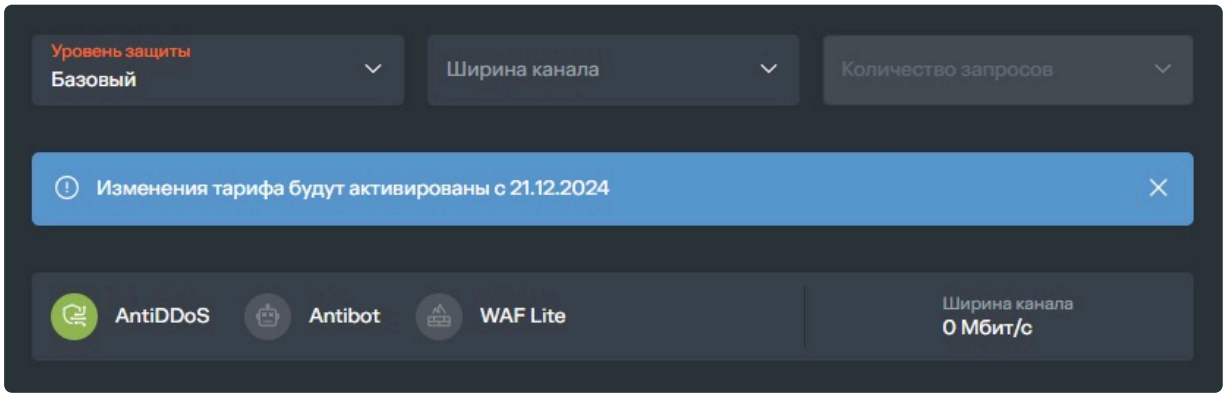
1. Измените уровень защиты:
   - С **продвинутого** на **оптимальный** — для отключения сервиса WAF Lite. Активными останутся сервисы **AntiBot** и **AntiDDoS**



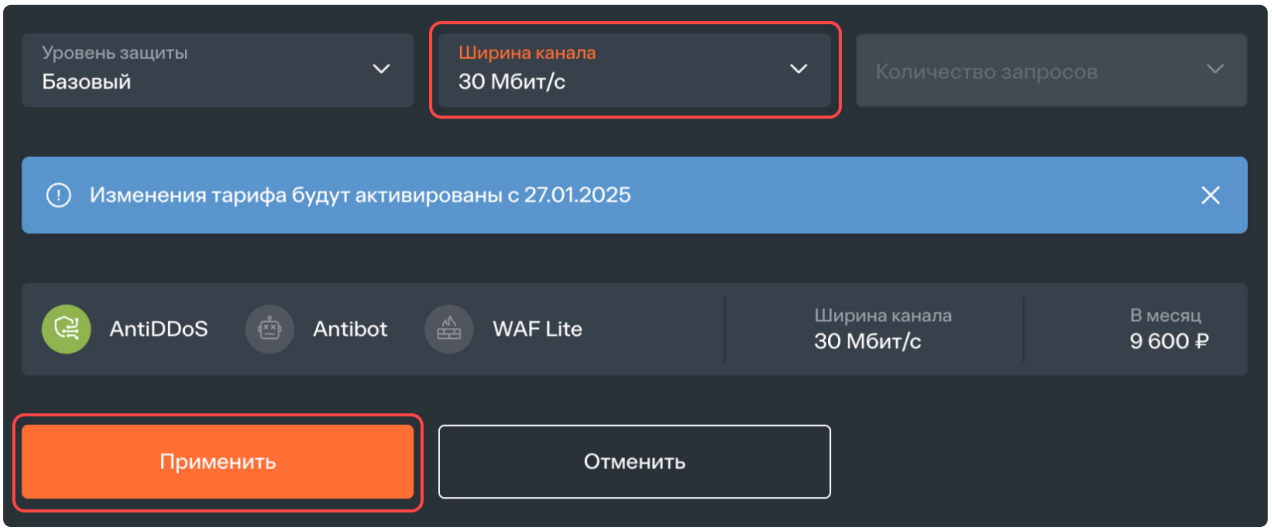
   - С **продвинутого** на **базовый** — для отключения сервисов WAF Lite и Antibot. Активным останется сервис **AntiDDoS**



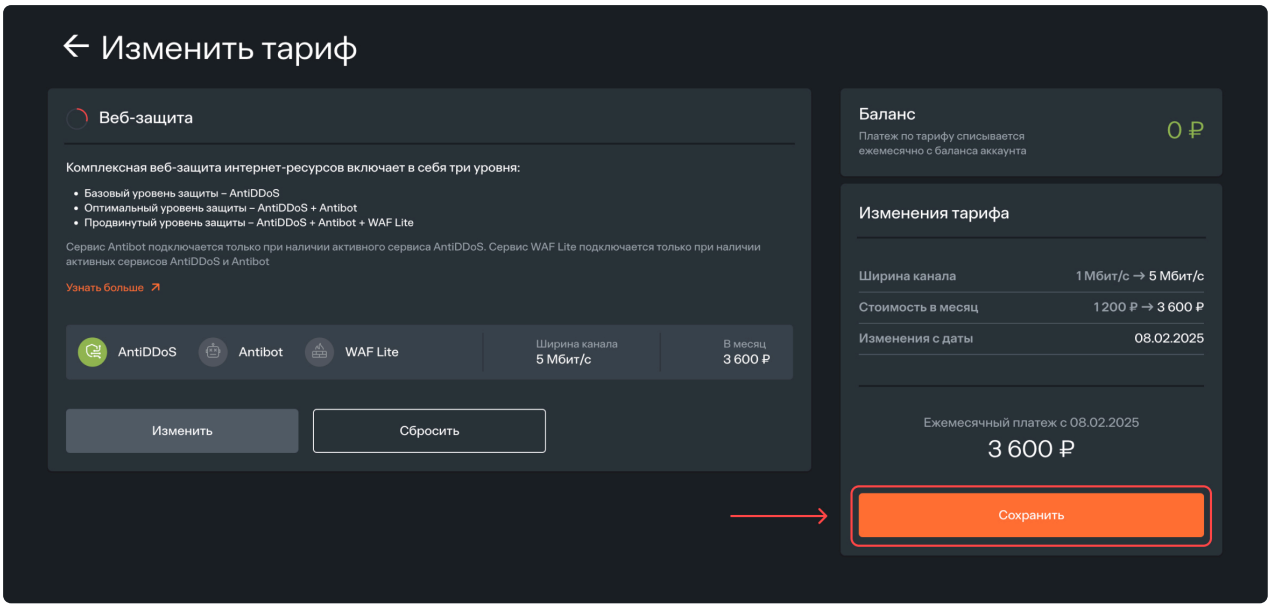
   - С **оптимального** на **базовый** — для отключения сервиса Antibot. Активным останется сервис AntiDDoS



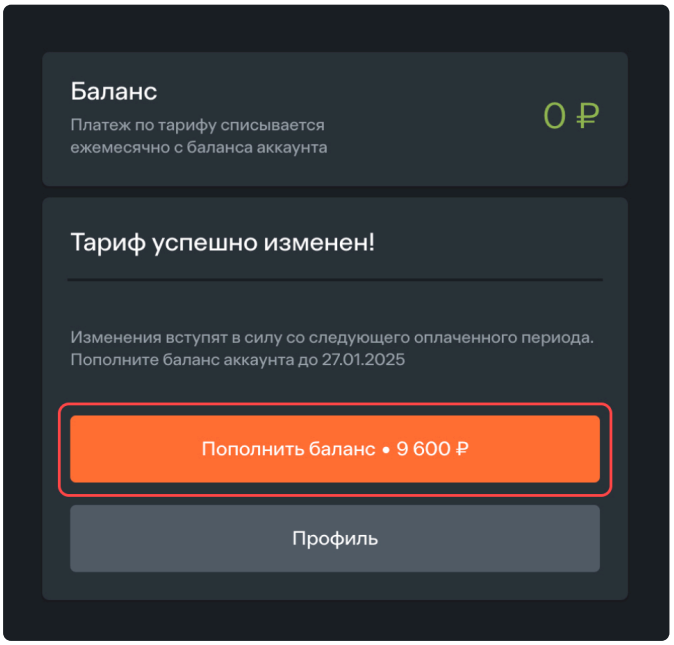
2. Укажите значение для поля "Ширина канала" и нажмите на кнопку "Применить".



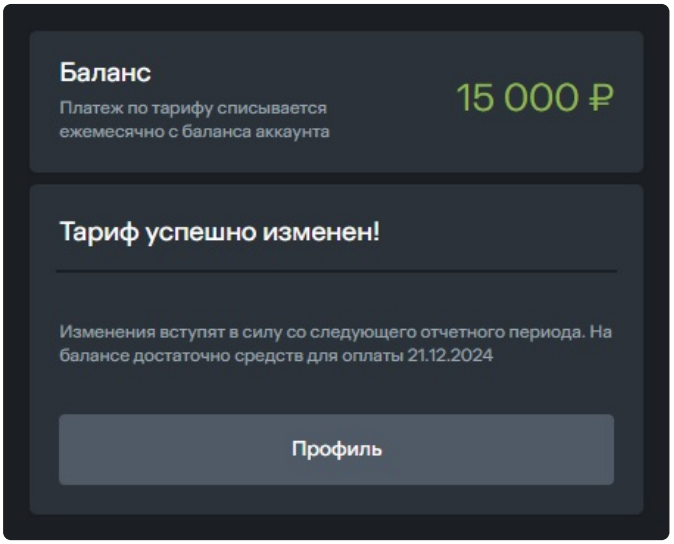
3. Проверьте информацию в блоке "Изменения тарифа" и нажмите на кнопку "Сохранить".



4. Если на балансе недостаточно средств, нажмите кнопку "Пополнить баланс".



5. Если на вашем счете достаточно средств, появится сообщение об успешном изменении тарифа. Изменения вступят в силу со следующего расчетного периода.



Изменение параметров тарифа

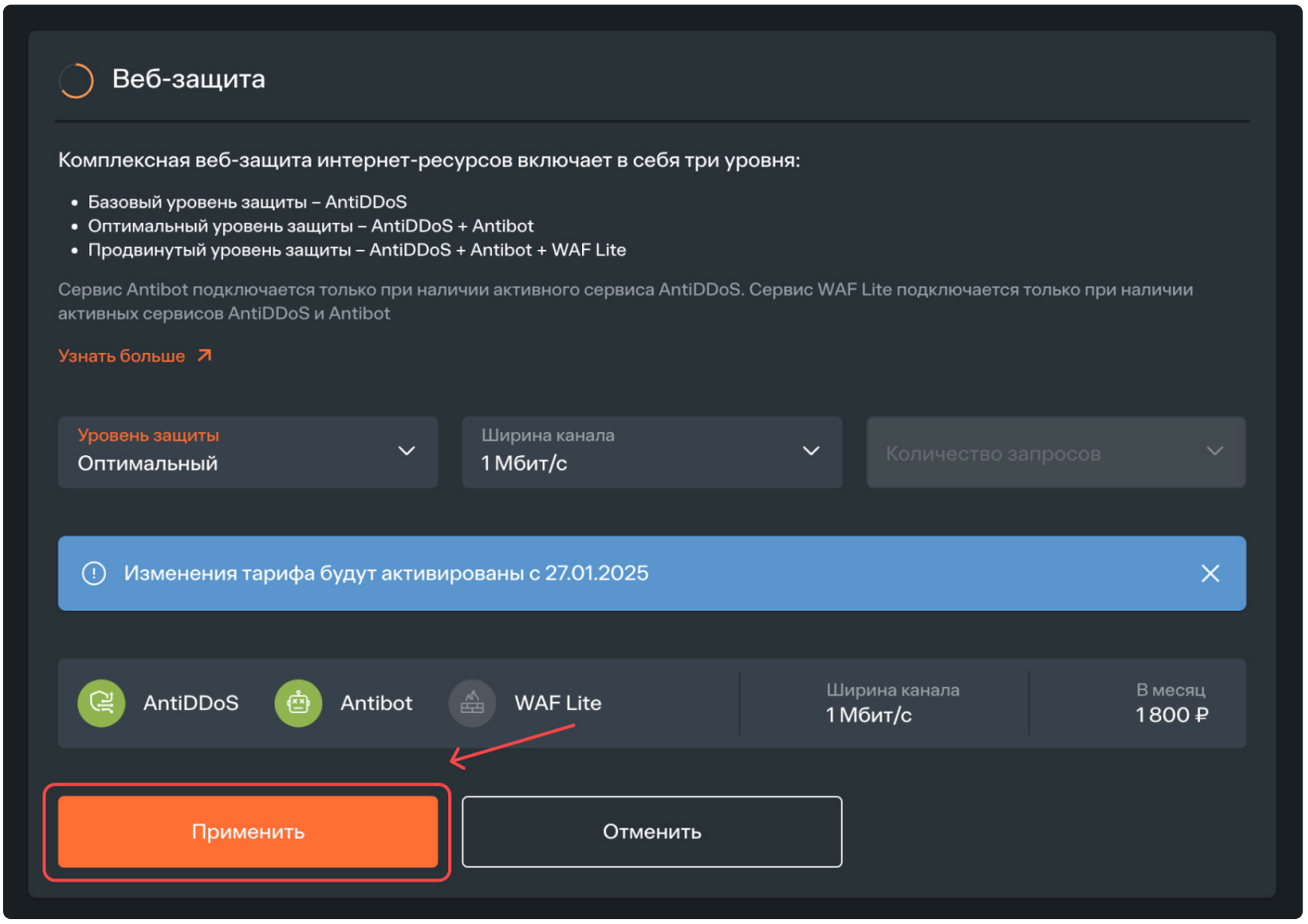
> Обратите внимание
>
> При редактировании параметров тарифа изменения вступят в силу со следующего отчетного периода

Параметры тарифа — это поля "Ширина канала" и "Количество запросов", которые редактируются вручную.

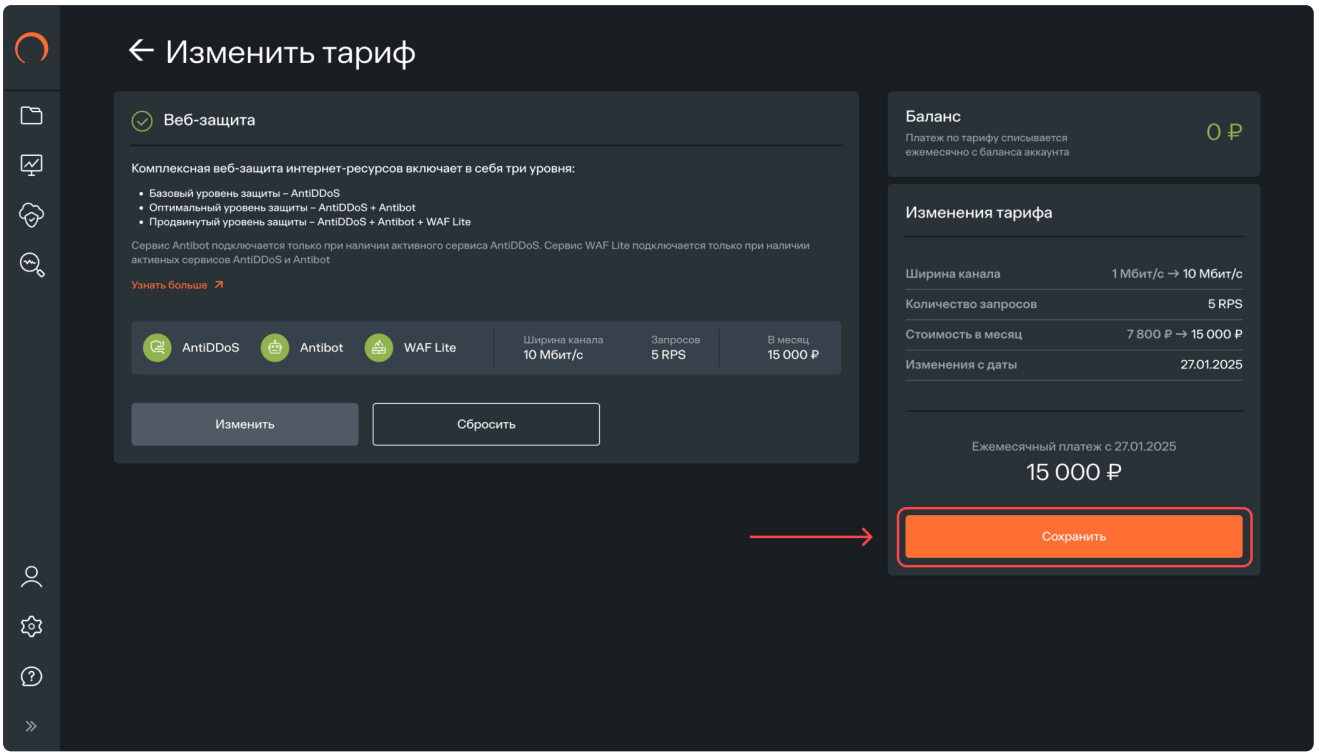
Для того, чтобы изменить параметры тарифа, выполните следующие действия:

1. Отредактируйте значения нужных полей. В редактирование параметров тарифа входят:
    - Изменение ширины канала для любого уровня защиты (например, с 5 Мбит/с на 20 Мбит/с)
    - Изменение количества запросов для продвинутого уровня защиты (например, с 10 RPS на 20 RPS)

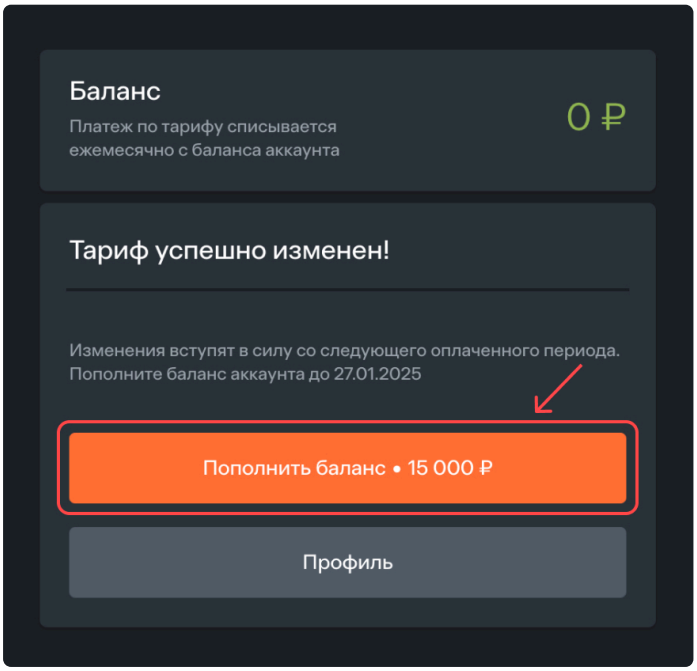
Если вы редактируете параметры тарифа и одновременно добавляете новый сервис, то все эти изменения вступят в силу со следующего отчетного периода. 2. После редактирования параметров тарифа нажмите на кнопку "Применить".



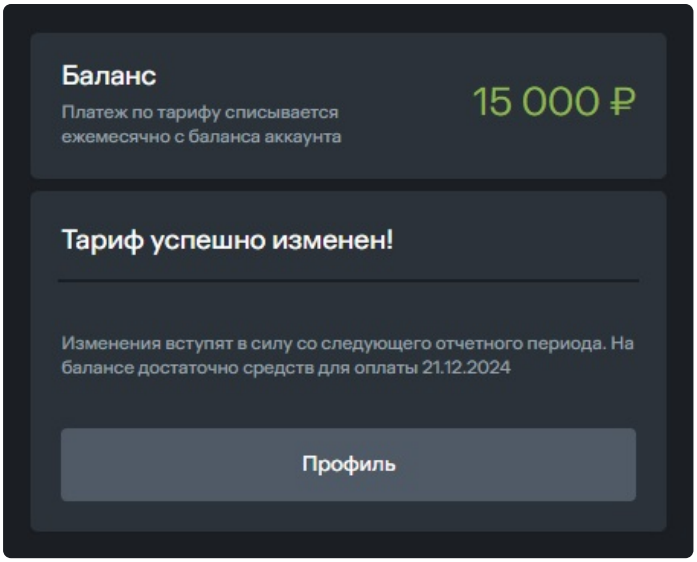
3. Проверьте информацию в блоке "Изменения тарифа" и нажмите на кнопку "Сохранить". Сумма к оплате в следующем месяце будет изменена.



4. Если на балансе недостаточно средств, нажмите кнопку "Пополнить баланс".



5. Если на вашем счете достаточно средств, то появится сообщение об успешном изменении тарифа. Изменения вступят в силу со следующего расчетного периода.



FAQ

В данном разделе вы найдете нужную информацию, которая поможет ответить на ваши вопросы.

- Как восстановить пароль?
- Как удалить ресурс?
- Какие могут возникнуть ошибки при верификации и перенаправлении трафика?

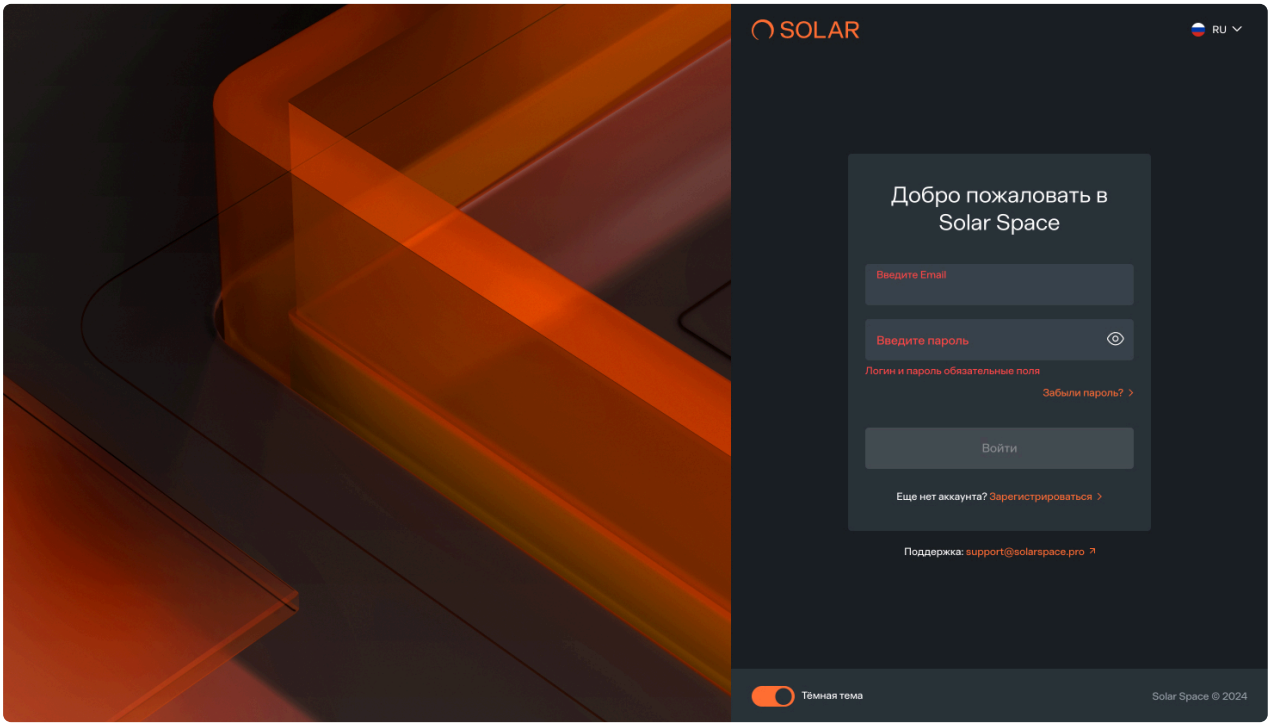
Авторизация

Если у вас еще нет аккаунта, вы можете зарегистрироваться.

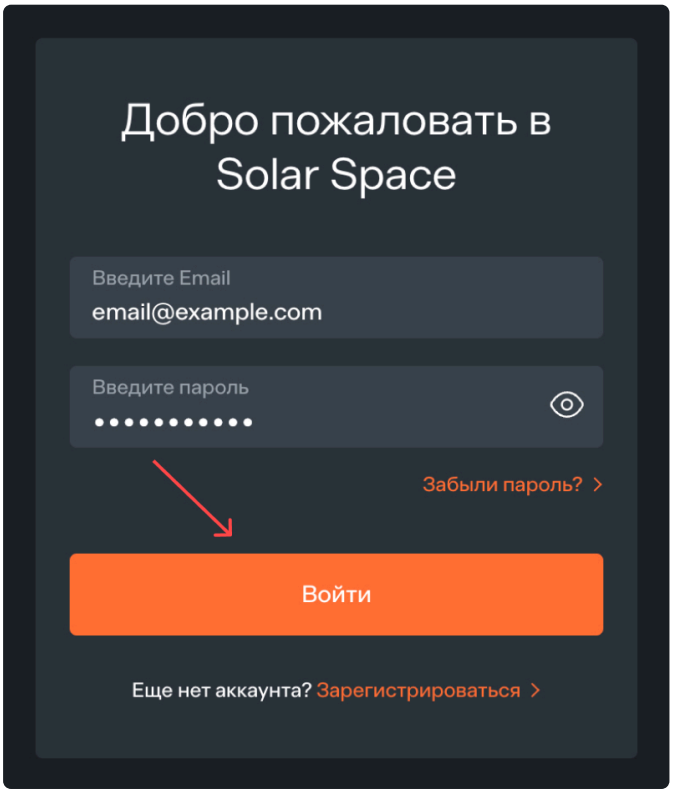
Если вы забыли пароль, у вас есть возможность его восстановить.

Для авторизации в личном кабинете выполните следующие действия:

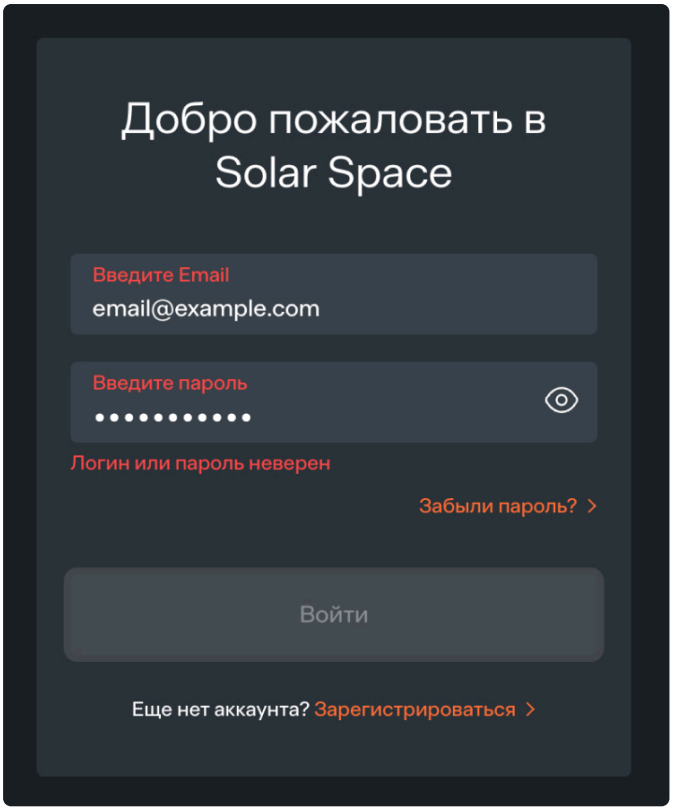
1. Введите в адресной строке браузера адрес – https://my.solarspace.pro. Откроется страница авторизации.



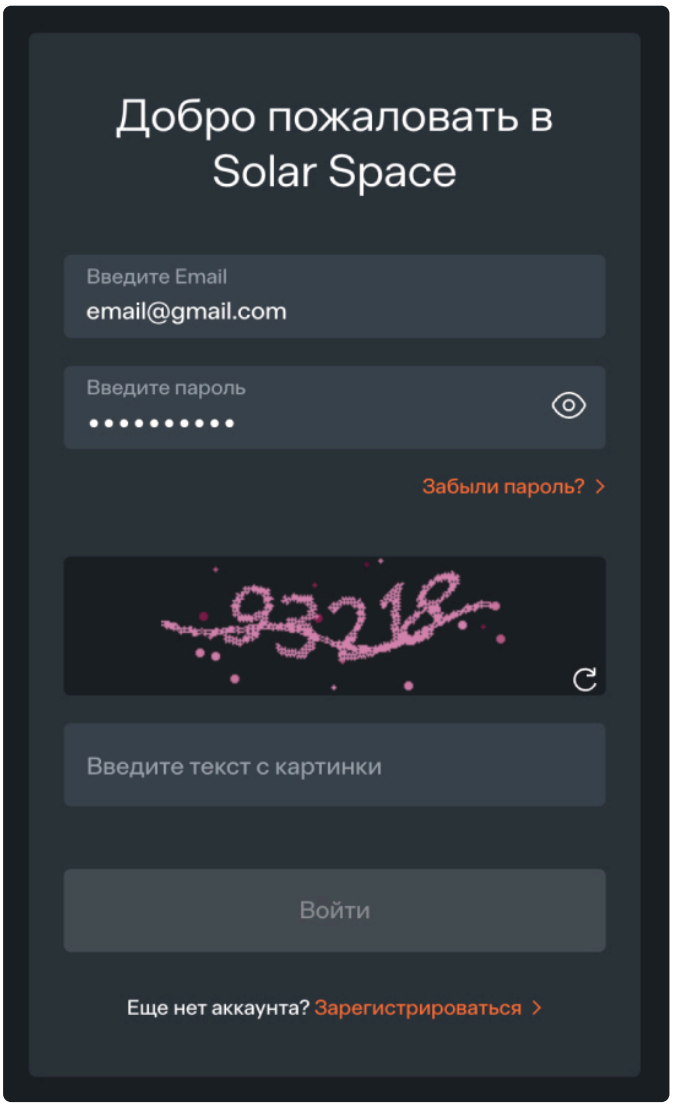
2. Введите email и пароль, которые вы указывали при регистрации и нажмите на кнопку "Войти" для входа в личный кабинет.



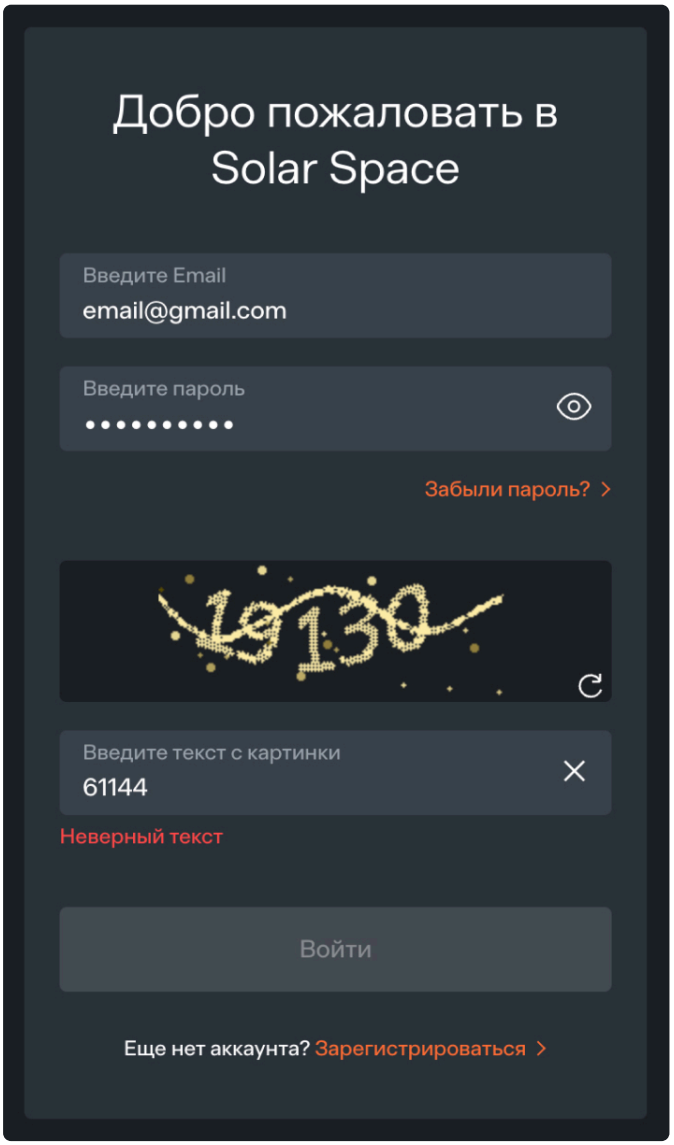
При вводе некорректных данных вы увидите сообщение "Логин или пароль неверен".



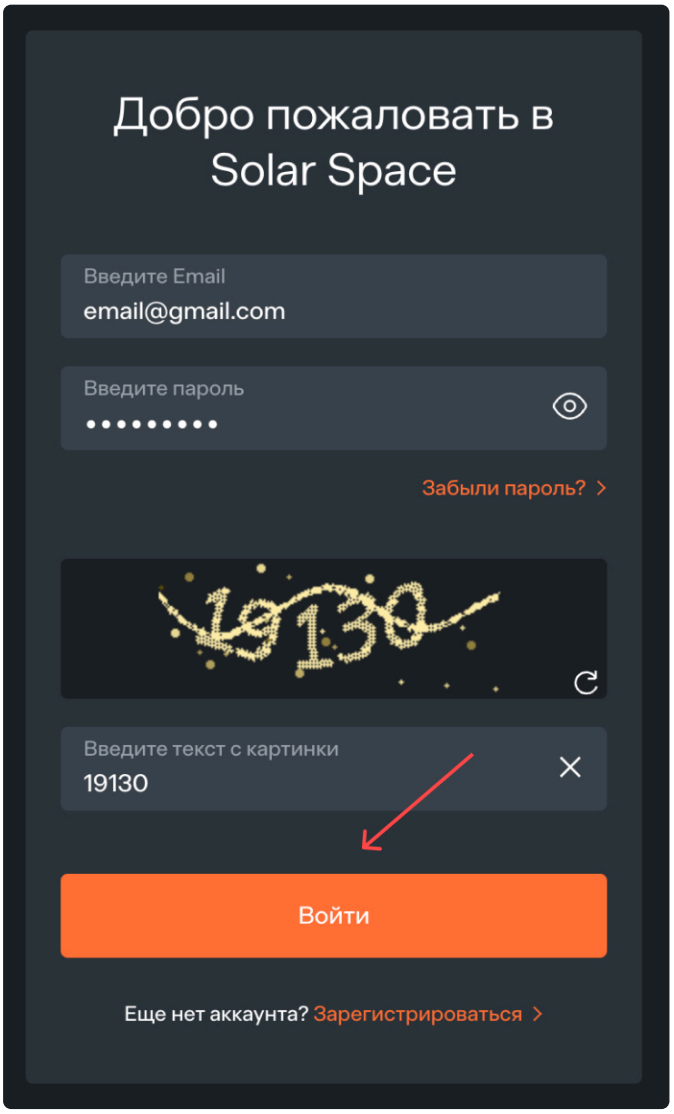
После 5 неудачных попыток авторизации с неверным паролем вам потребуется ввести капчу. Так система убедится, что форму заполняет реальный пользователь.



При отправке формы с некорректным кодом вы увидите сообщение "Неверный текст", и капча обновится. Количество попыток прохождения капчи неограничено.



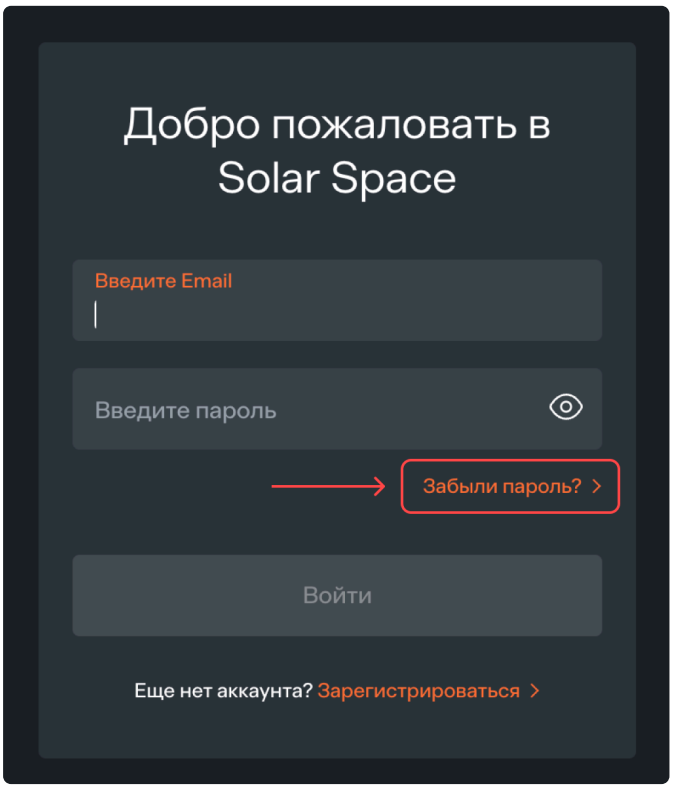
Когда капча пройдена, и поля "Логин" и "Пароль" заполнены корректно, кнопка "Войти" станет активной. Нажмите на нее для входа в личный кабинет.


Добро пожаловать в Solar Space
Введите Email
email@gmail.com
Введите пароль
Забыли пароль?
19130
Введите текст с картинки
19130
Войти
Еще нет аккаунта? Зарегистрироваться

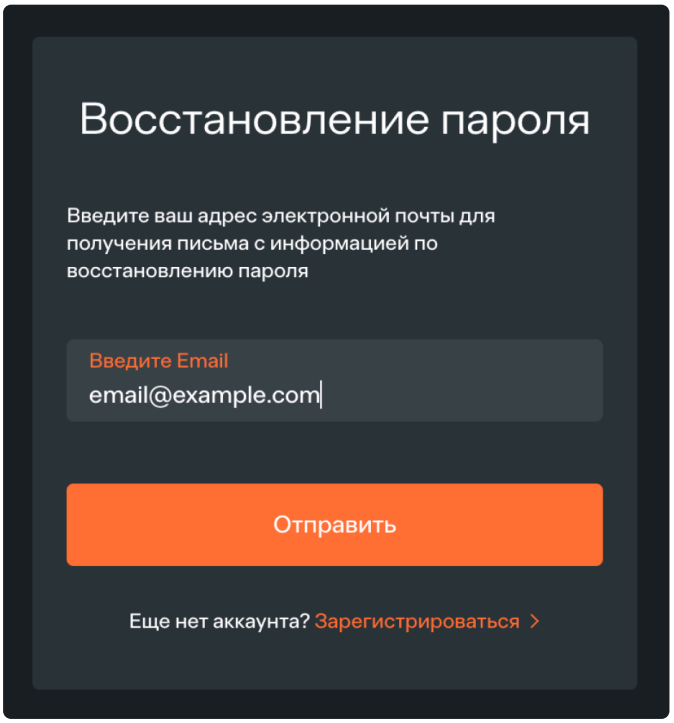
Восстановление пароля

Для восстановления пароля выполните следующие действия:

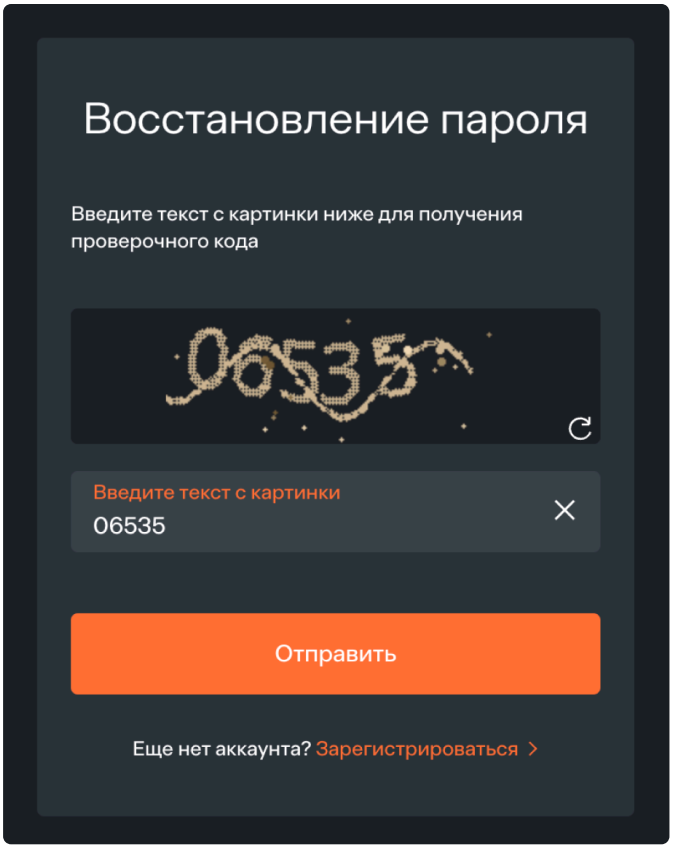
1. Откройте страницу авторизации https://my.solarspace.pro/sign-in
2. Для перехода на страницу восстановления пароля нажмите на ссылку "Забыли пароль?".



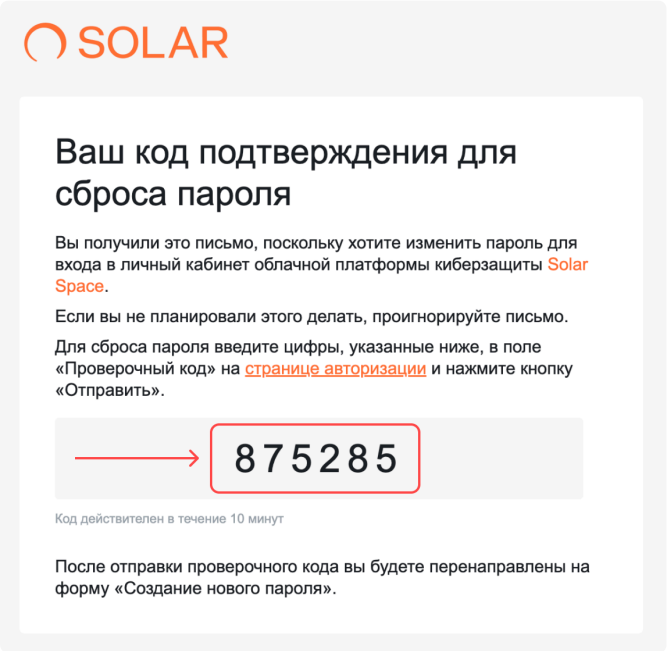
3. В поле "Email" введите электронную почту, которую вы использовали при регистрации и нажмите на кнопку "Отправить".



4. Далее вам необходимо пройти капчу. Так система убедится, что форму заполняет реальный пользователь. Для этого введите текст с картинки в соответствующее поле и нажмите кнопку "Отправить".

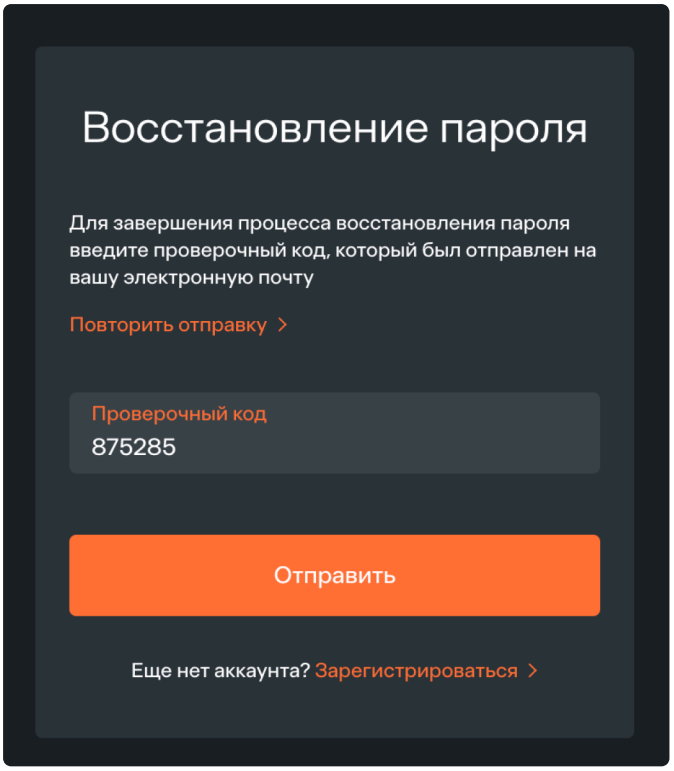


5. На ваш адрес электронной почты, указанный на шаге 3, придет письмо по восстановлению пароля. Откройте его и скопируйте 6-значный код из сообщения.

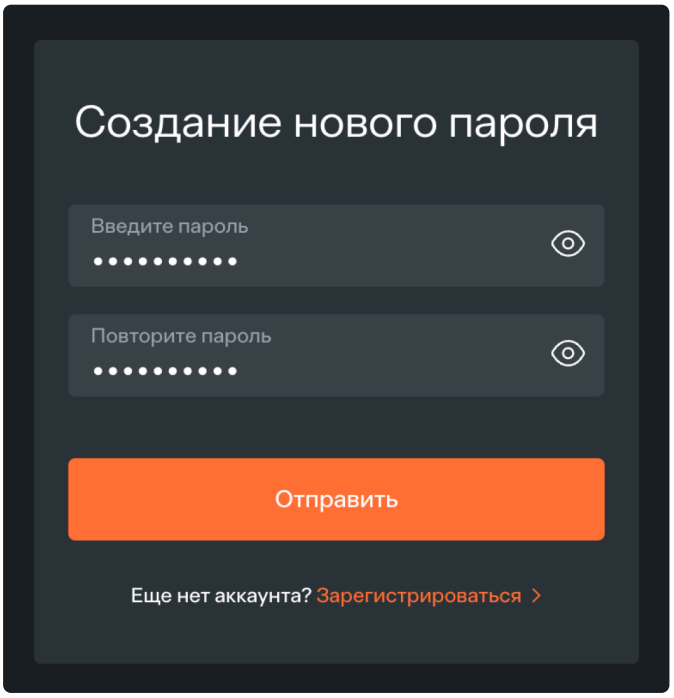


Если данного письма нет в папке "Входящие", проверьте папку "Спам". В случае, если письмо не пришло, перепроверьте введенную электронную почту и отправьте код повторно, нажав на кнопку "Повторить отправку". Запросить повторный код можно 1 раз в 60 секунд. Код действителен в течение 10 минут.

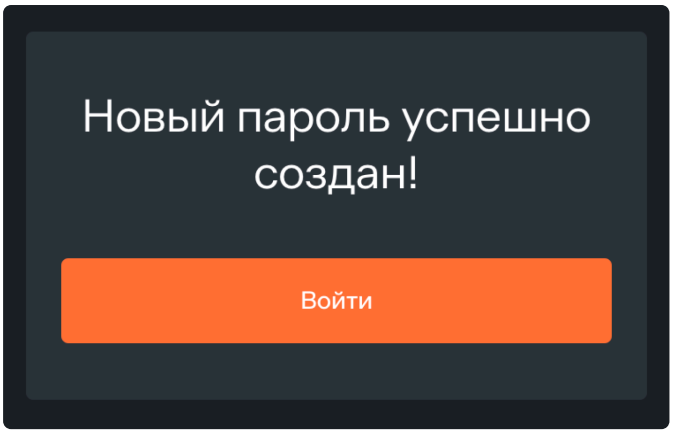
6. Вставьте 6-значный проверочный код в соответствующее поле и нажмите на кнопку "Отправить".



7. После успешного подтверждения кода появится форма для создания нового пароля. Введите новый пароль и повторите его (пароль должен содержать не менее 8 символов и включать как минимум одну цифру и буквы разных регистров). Нажмите на кнопку "Отправить".



8. При успешном сохранении пароля появится сообщение "Новый пароль успешно создан!". При нажатии на кнопку "Войти" откроется страница с авторизацией. Используйте свой email и новый пароль для входа в личный кабинет.



Возможные ошибки при верификации и перенаправлении трафика

При изменении DNS-A и DNS-TXT-записи в регистраторе или хостинг-провайдере возможны ошибки. Они приведут к проблемам при постановке домена под защиту.

Если вы отправили запрос на верификацию или перенаправление трафика, но статус домена не изменился на успешный, возможно, причина в одной из этих ошибок.

Неправильный формат записи

Текст в кавычках или лишние символы DNS-TXT-записи приведут к тому, что запись не будет распознана, а неправильный формат IP-адреса в DNS-A-записи (например, лишние цифры или символы) сделает запись недействительной. Убедитесь, что добавленные записи в настройках регистратора или хостинг-провайдера полностью соответствуют тем, которые вы скопировали из настроек своего ресурса в личном кабинете Solar Space, домен которого вы хотите верифицировать.

Опечатки в доменных именах

Ошибки могут быть допущены в доменном имени при создании ресурса или добавлении нового домена в личном кабинете Solar Space. Проверьте правильность введенного доменного имени — в нем не должно быть пропущенных или лишних символов.

Несохраненное изменение IP-адреса сервера

Отсутствие IP-адреса Solar Space в DNS-A-записи приведет к тому, что запросы от посетителей сайта не будут проходить через узел защиты, вследствие чего ваш сайт не будет защищен. Убедитесь, что в вашем регистраторе или хостинг-провайдере DNS-A-запись содержит IP-адрес, скопированный из настроек своего ресурса на странице Веб-защиты в личном кабинете Solar Space, домен которого вы хотите поставить под защиту.

Большое значение для параметра TTL

Если параметр Time to Live (TTL) в настройках регистратора или хостинг-провайдера слишком велик, изменения могут не вступить в силу сразу, так как DNS-записи будут обновляться

значительно дольше, чем обычно.

Конфликты записей

Наличие нескольких A или AAAA-записей для одного домена с разными IP-адресами вызовут проблемы с перенаправлением трафика. Проверьте, чтобы в настройках регистратора или хостинг-провайдера была только одна A-запись, содержащая IP-адрес узла защиты Solar Space. Это гарантирует, что весь входящий трафик будет обрабатываться сервисами защиты.

Кэширование

Локальные или промежуточные DNS-серверы могут кэшировать старые записи, что увеличит время обновленияй DNS- записей. Чтобы ускорить процесс, попробуйте очистить кэш DNS. Для этого обратитесь в поддержку регистратора или хостинг-провайдера.

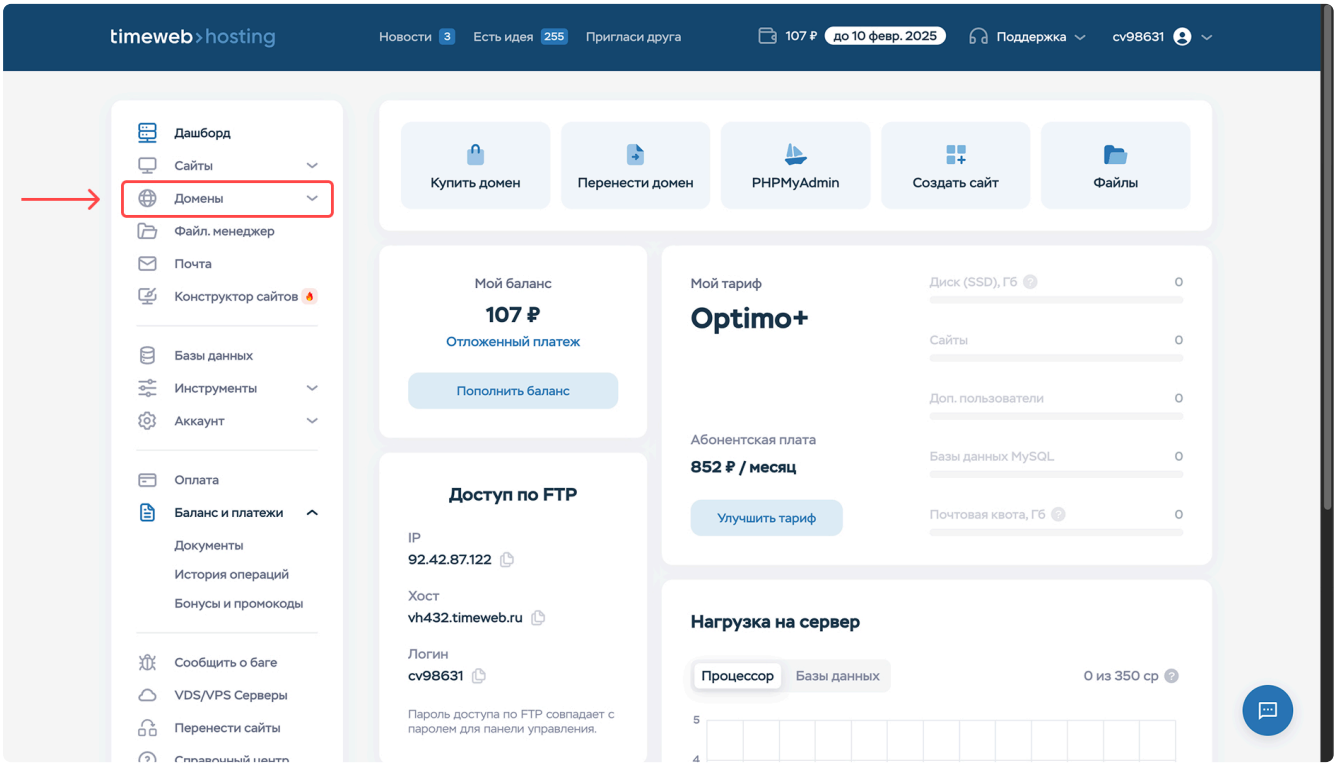
Технические проблемы

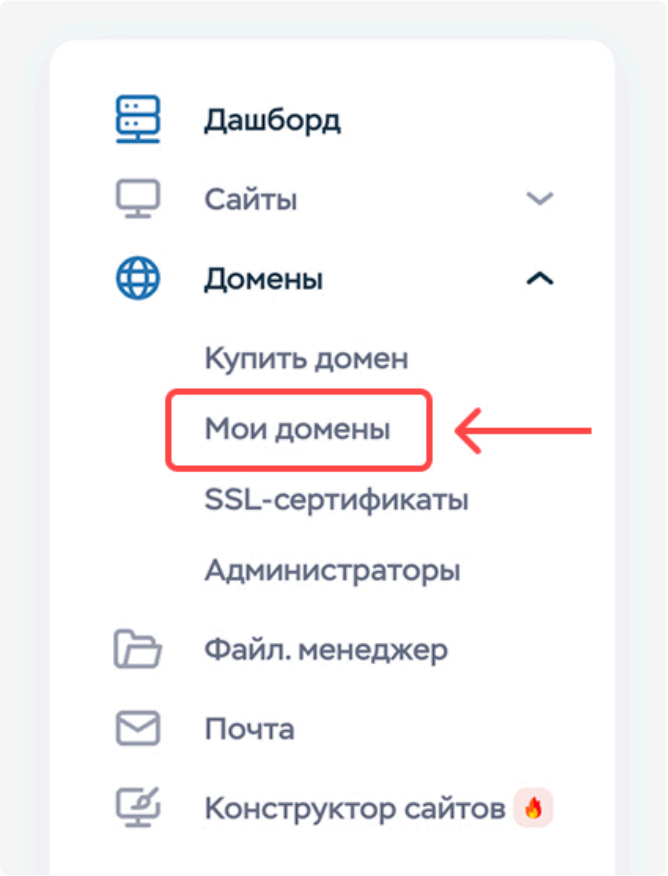
В некоторых случаях долгое обновление записей может быть связано с техническими проблемами на стороне DNS-сервера. Обратитесь в поддержку регистратора или хостинг-провайдера.

Добавление TXT-записи для Timeweb

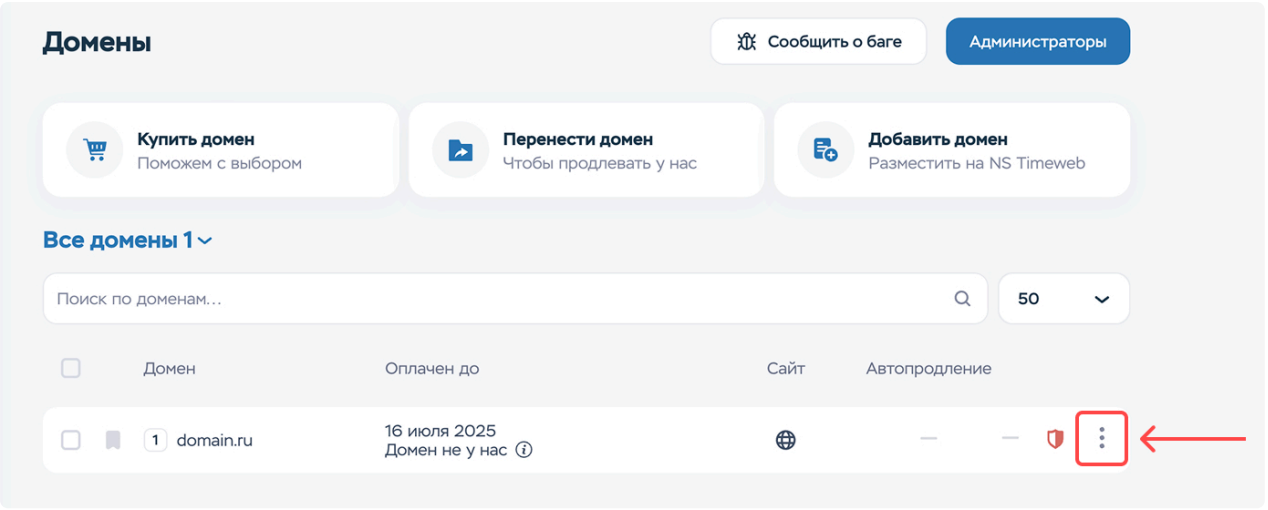
По инструкции ниже вы можете верифицировать ваш домен на примере хостинг-провайдера Timeweb. Добавление TXT-записи у других регистраторов или хостинг-провайдеров аналогично.

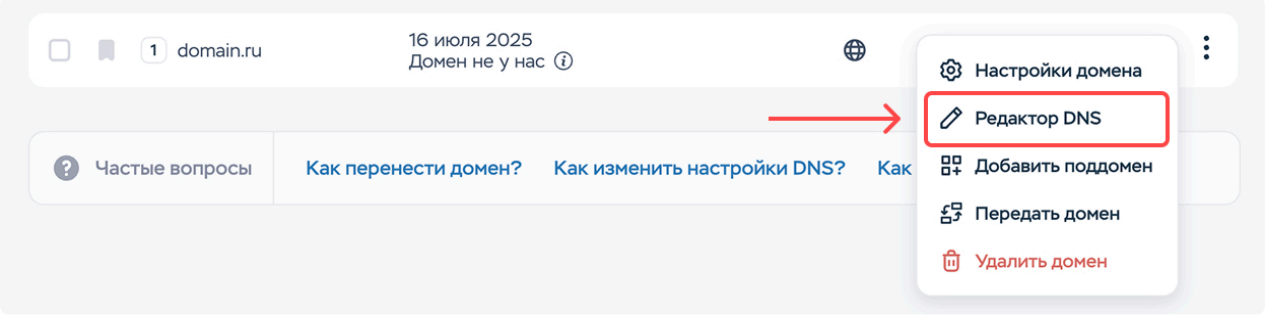
1. Откройте раздел "Домены", а затем "Мои домены".



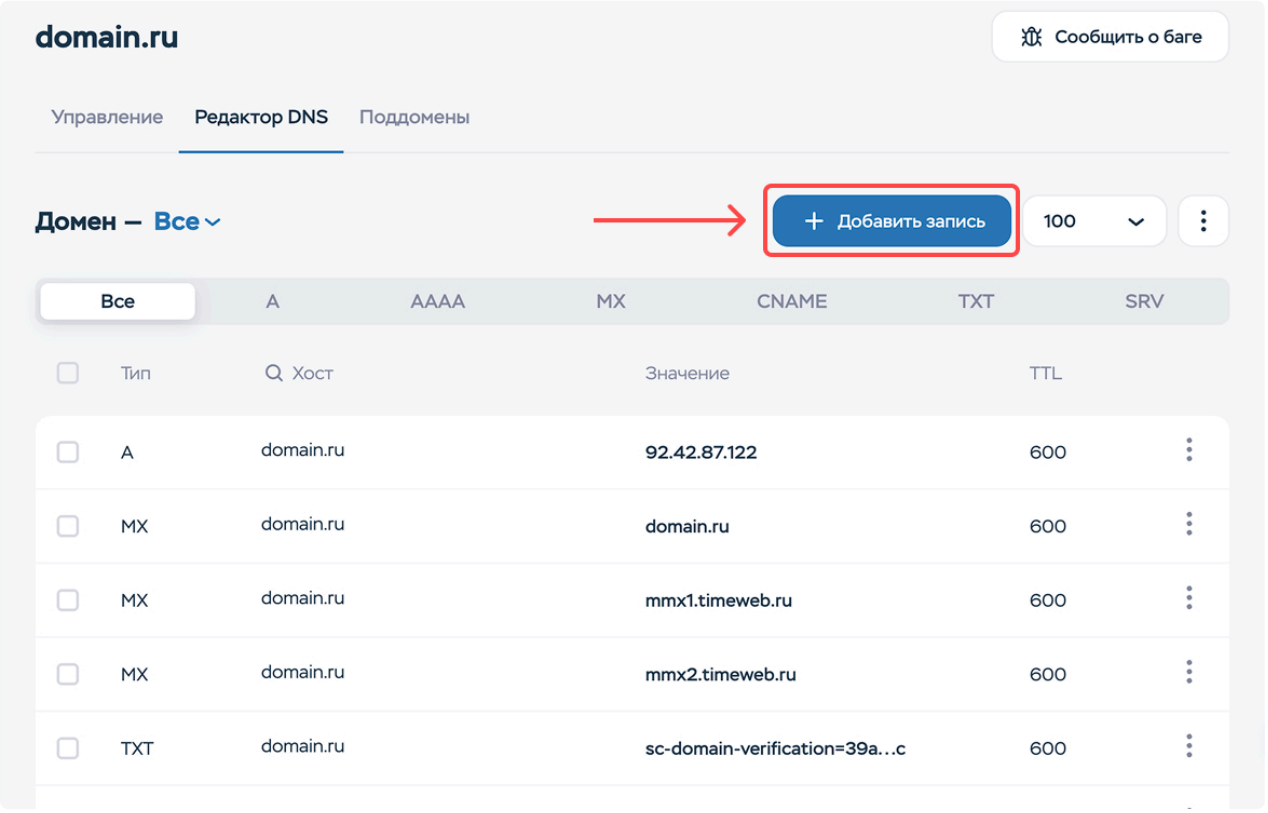


2. Выберите нужный домен и в правой части строки, нажав на три точки, выберите из выпадающего списка пункт "Редактор DNS". Откроется страница с записями.

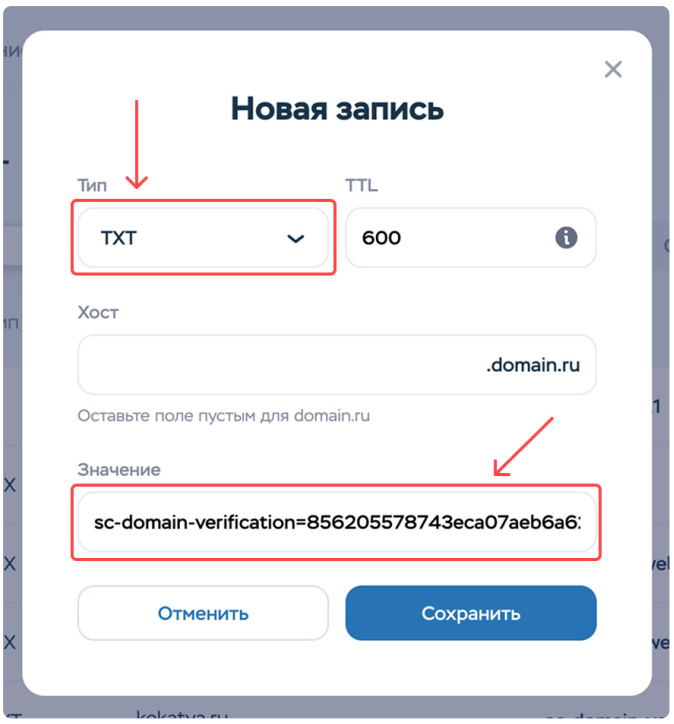




3. Нажмите на кнопку "Добавить запись".



4. В окне "Новая запись" выберите тип записи "TXT", в поле "Значение" введите TXT-запись, скопированную из личного кабинета Solar Space. Нажмите кнопку "Сохранить".



5. Вернитесь в личный кабинет Solar Space и нажмите на кнопку "Верифицировать".

Что такое TTL?

TTL (Time To Live) в контексте DNS (Domain Name System) — это параметр, определяющий время, в течение которого DNS-записи хранятся в кэше на серверах и клиентских устройствах. Он измеряется в секундах и влияет на то, как часто обновляются данные о доменах.

Как работает TTL?

Когда вы обновляете DNS-записи в настройках своего регистратора или хостинг-провайдера, это изменение не вступает в силу сразу. DNS-записи обновляются только после того, как истекает TTL (время жизни) предыдущих записей в кэше каждого DNS-сервера. При большом значении параметра TTL информация будет храниться дольше, следовательно, обновление DNS-TXT и DNS-A записей в рамках личного кабинета Solar Space займет больше времени.

> ⓘ Обратите внимание
>
> Уменьшение TTL перед внесенными изменениями ускорит процесс обновления DNS-TXT и DNS-A записей, но увеличит нагрузку на DNS-серверы. Это происходит потому, что при малом значении TTL устройства будут чаще запрашивать актуальную информацию у DNS-серверов

На что влияет TTL?

- **Снижение нагрузки на DNS-серверы**: благодаря кэшированию DNS-записей устройства могут использовать сохраненные данные, что снижает нагрузку на DNS-серверы
- **Ускорение загрузки страниц**: кэширование DNS-записей позволяет устройствам быстрее получать необходимую информацию о доменах, что может ускорить загрузку страниц
- **Обеспечение стабильности работы сети**: если установлено слишком низкое значение параметра TTL, то частые обновления DNS-записей могут привести к перегрузке сети и снижению ее стабильности из-за большого колиичества запросов к серверу

Как изменить TTL?

1. Войдите в панель управления вашего регистратора или хостинг-провайдера.

2. Перейдите в раздел с DNS-записями.
3. Выберите запись, для которой хотите изменить TTL.
4. Укажите новое значение TTL (в секундах).
5. Сохраните изменения.

> ⚠ Важно
>
> Даже после изменения TTL старые записи могут оставаться в кэше до истечения их предыдущего времени жизни

Оптимальный TTL

Небольшие значения TTL (например, 300 секунд) обеспечивают более частое обновление DNS-записей, но могут увеличить нагрузку на DNS-серверы и сеть. Такие значения рекомендуется устанавливать для высоконагруженных сайтов, когда частые обновления записей действительно необходимы. Большие значения TTL (например, 86400 секунд) уменьшают нагрузку на сеть, но могут замедлить процесс обновления DNS-записей.

При выборе оптимального значения TTL учитывайте следующие факторы:

- Частоту изменений DNS-записей
- Размер вашей сети и количество DNS-серверов
- Требования к скорости обновления DNS-записей в вашей организации

Рекомендуется провести тестирование и мониторинг производительности сети при различных значениях TTL для определения оптимального значения.

Когда в системе происходят какие-то изменения, например, смена IP-адреса или переезд на новый хостинг, то нужно заранее уменьшить TTL, чтобы изменения распространились быстрее. Чтобы TXT- и A-записи при настройке защиты Solar Space обновились быстрее, также рекомендуется уменьшить значение TTL. После завершения настройки можно вернуть параметр к прежнему значению.

Если у вас есть вопросы или проблемы с изменением значения TTL, обратитесь в техническую поддержку вашего регистратора DNS или хостинг-провайдера. Они смогут помочь вам настроить TTL правильно и безопасно.

Solar Space — альтернатива Cloudflare?

Ответ не такой однозначный, как может показаться — и да, и нет. Давайте разберемся почему.

По состоянию на 2025 год полного аналога Cloudflare в мире, в том числе в России, не существует. Однако масштабные кибератаки, которым подвергается российский бизнес с 2022 года, серьезно ускорили развитие отечественных решений в области информационной безопасности.

Почему Cloudflare может быть недостаточно надежен в России?

Практика показывает, что сайты на Cloudflare не всегда доступны российским пользователям из-за блокировок отдельных типов шифрования на уровне российских операторов и регуляторов.

Причина проста: каждое государство в целях собственной безопасности стремится обеспечить хранение и обработку данных в пределах своей территории, что ведет к ограничениям и блокировкам зарубежных сервисов. Наша задача — помочь бизнесу адаптироваться к текущей ситуации и обеспечить надежную защиту веб-ресурсов.

Используя Cloudflare, компании передают данные под юрисдикцию другой страны, что может быть неприемлемым для объектов критической информационной инфраструктуры, государственных учреждений, а также организаций, работающих с госструктурами или персональными данными. Solar Space хранит и обрабатывает данные исключительно на территории России, что соответствует требованиям российского законодательства.

Что не так с бесплатным тарифом Cloudflare?

Бесплатный тариф Cloudflare имеет существенные ограничения:

- Минимальная защита от DDoS-атак и ботов, которой недостаточно для защиты от мощных и сложных атак
- Ограниченное число правил фильтрации трафика
- Коммерческое использование вашего трафика и данных

> **Важно помнить**
>
> Бесплатные сервисы редко бывают действительно бесплатными — обычно продуктом становитесь вы сами. Ваши данные компания может анализировать, хранить и использовать по своему усмотрению

Solar Space предлагает расширенные возможности настройки и усиленную защиту уже в базовом пакете по доступной цене. Это достойная альтернатива международным решениям, если вам важна надежность и безопасность. Мы стремимся привлечь внимание к качественным отечественным решениям, учитывающим специфику российского рынка. Это не значит, что Cloudflare плохой продукт. Это значит, что наше решение адаптировано к реалиям отечественного бизнеса и законодательства.

Создавая сервис Solar Space, мы взяли лучшее от мировых аналогов, дополнили собственными инновациями и сделали максимально удобным и безопасным для российских пользователей. Команда продолжает совершенствовать продукт, чтобы он стал еще более функциональным и эффективным решением для защиты отечественного бизнеса.