

ДОКУМЕНТАЦИЯ SOLAR SPACE



Оглавление

1. ОПИСАНИЕ ПЛАТФОРМЫ	5
2. АККАУНТ И ПРОФИЛЬ	7
3. РЕГИСТРАЦИЯ	8
4. ПОДТВЕРЖДЕНИЕ АККАУНТА	13
5. ПОДКЛЮЧЕНИЕ СЕРВИСОВ	17
6. ОПЛАТА	27
7. ПРОФИЛЬ	30
8. ИМПОРТ ИЗ CLOUDFLARE	33
9. БЫСТРЫЙ СТАРТ	39
10. СЕРВИСЫ	52
11. ВЕБ-ЗАЩИТА	53
12. ANTIDDOS	61
13. ANTIBOT	65
14. WAF LITE	69
15. РАЗРЕШЕННЫЕ ПУТИ WAF LITE	77
16. НАСТРОЙКИ	82
17. ДОМЕН И SSL	83
18. ЦЕЛЕВОЙ IP	93
19. HTTP-ЗАГОЛОВКИ	100
20. ОГРАНИЧЕНИЯ ДОСТУПА	107
21. ДОСТУП К РЕСУРСУ ИЗ СТРАН	109
22. НАСТРОЙКИ BLACK LIST	110
23. НАСТРОЙКИ WHITE LIST	118
24. ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ БЕЗОПАСНОСТИ	120
25. ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ СЕРВЕРА	122
26. СКАНИРОВАНИЕ УЯЗВИМОСТЕЙ	126
27. СКАНЕР ВЕБ-СЕРВЕРА	127
28. AURA	132
29. ZERO DAY	136

30. SECURITY AWARENESS	137
31. SEC DNS	138
32. STRESSTEST	139
33. SEG	140
34. МОИ САЙТЫ	141
35. НАСТРОЙКИ	143
36. СТАТИСТИКА	149
37. СЕРВИСЫ	155
38. СТАТИСТИКА	168
39. ШИРИНА КАНАЛА	170
40. ЗАПРОСЫ	172
41. КОДЫ	174
42. ГЕОГРАФИЯ ЗАПРОСОВ	176
43. СТАТИСТИКА ANTIVOT	177
44. СТАТИСТИКА WAF LITE	182
45. ТАРИФЫ И ОПЛАТА	184
46. ТАРИФИКАЦИЯ И ОПЛАТА	185
47. ТАРИФЫ НА ВЕБ-ЗАЩИТУ	189
48. ПОПОЛНЕНИЕ БАЛАНСА	192
49. ИЗМЕНЕНИЕ ТАРИФА	195
50. ДОБАВЛЕНИЕ НОВОГО СЕРВИСА	197
51. ОТКЛЮЧЕНИЕ СЕРВИСОВ	202
52. ИЗМЕНЕНИЕ ПАРАМЕТРОВ ТАРИФА	205
53. FAQ	208
54. КАК АВТОРИЗОВАТЬСЯ?	209
55. КАК ВОССТАНОВИТЬ ПАРОЛЬ?	214
56. КАКИЕ МОГУТ ВОЗНИКНУТЬ ОШИБКИ?	218
57. КАК ДОБАВИТЬ TXT-ЗАПИСЬ ДЛЯ TIMEWEB?	220
58. ЧТО ТАКОЕ TTL?	223
59. SOLAR SPACE — АЛЬТЕРНАТИВА CLOUDFLARE?	225
60. КАК ДОБАВИТЬ СВОЙ SSL-СЕРТИФИКАТ?	227
61. КАК ДОБАВИТЬ DNS-ЗАПИСИ В РЕГИСТРАТОРЕ NIC.RU?	237
62. КАК ДОБАВИТЬ DNS-ЗАПИСИ В РЕГИСТРАТОРЕ REG.RU?	244

63. ПОЧЕМУ МОЖЕТ СРАБОТАТЬ КАПЧА ИЛИ АНТИБОТ 251

64. КАК ПОДОБРАТЬ ПАРАМЕТРЫ ТАРИФА ВЕБ-ЗАЩИТЫ 254

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 Awareness** 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.rt-solar.ru> 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**

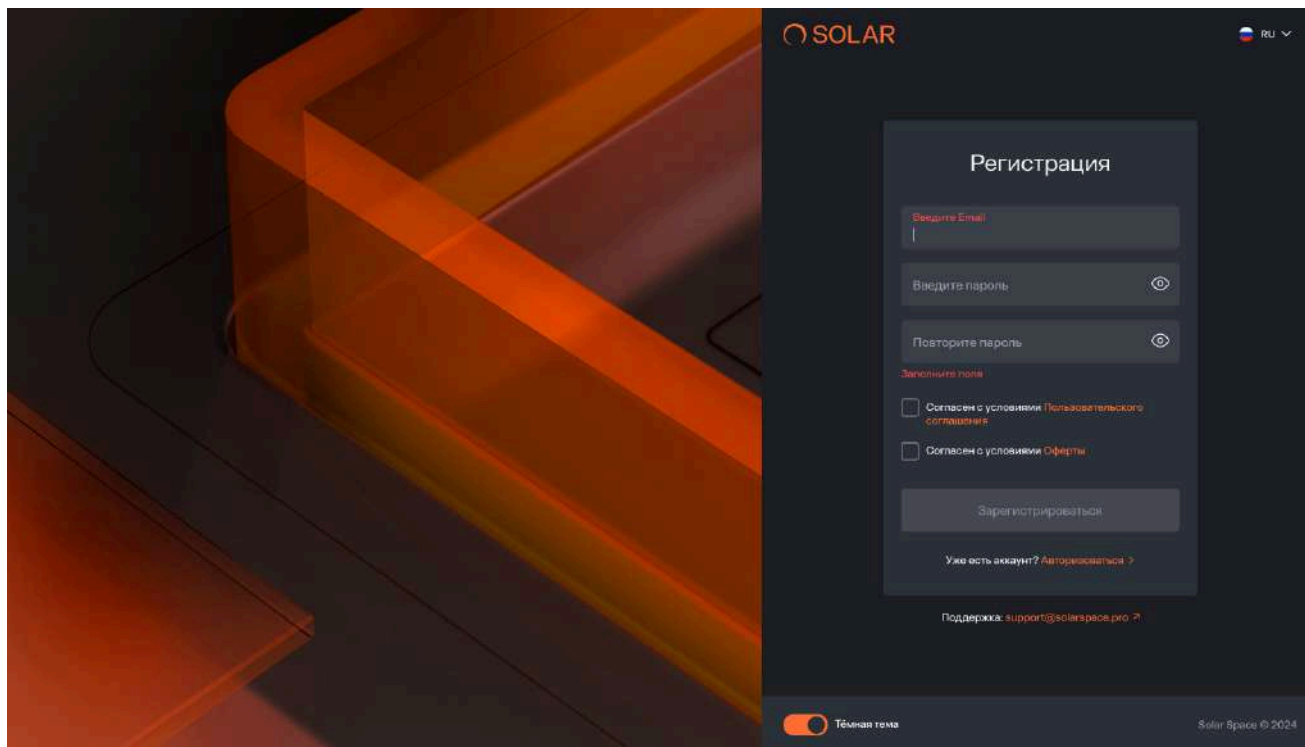
Регистрация

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](#)

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

Регистрация

Введите Email
email@example.com

Введите пароль
..... 

Повторите пароль
..... 

☐ Согласен с условиями Пользовательского соглашения

☐ Согласен с условиями Оферты

Зарегистрироваться

Уже есть аккаунт? [Авторизоваться >](#)

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

Регистрация

Введите Email
email@example.com

Введите пароль
.....

Повторите пароль
.....

☒ Согласен с условиями [Пользовательского соглашения](#)

☒ Согласен с условиями [Оферты](#)

Зарегистрироваться

Уже есть аккаунт? [Авторизоваться >](#)

2. 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".

Регистрация

Введите текст с картинки ниже для получения проверочного кода

95654

Введите текст с картинки
95654

Зарегистрироваться

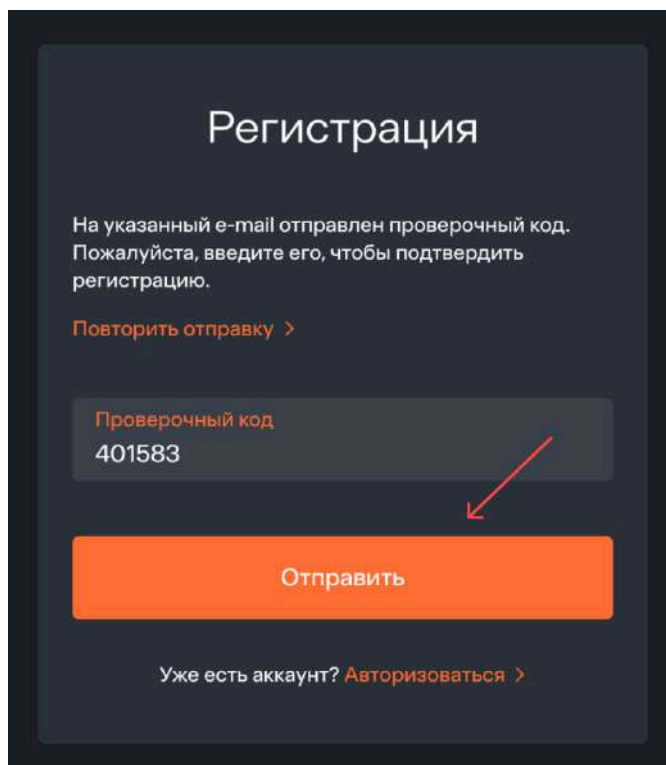
Уже есть аккаунт? [Авторизоваться >](#)

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

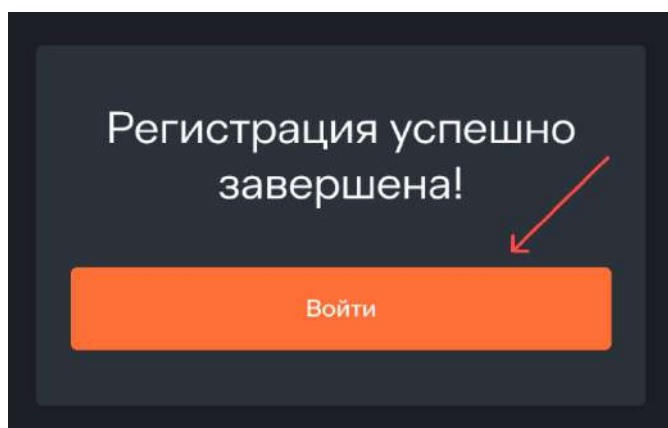


Если данного письма нет в папке "Входящие", проверьте папку "Спам". В случае, если письмо не пришло, перепроверьте введенную электронную почту и отправьте код повторно, нажав на кнопку "Повторить отправку". Запросить повторный код можно 1 раз в 60 секунд. Код действителен в течение 10 минут.

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



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



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

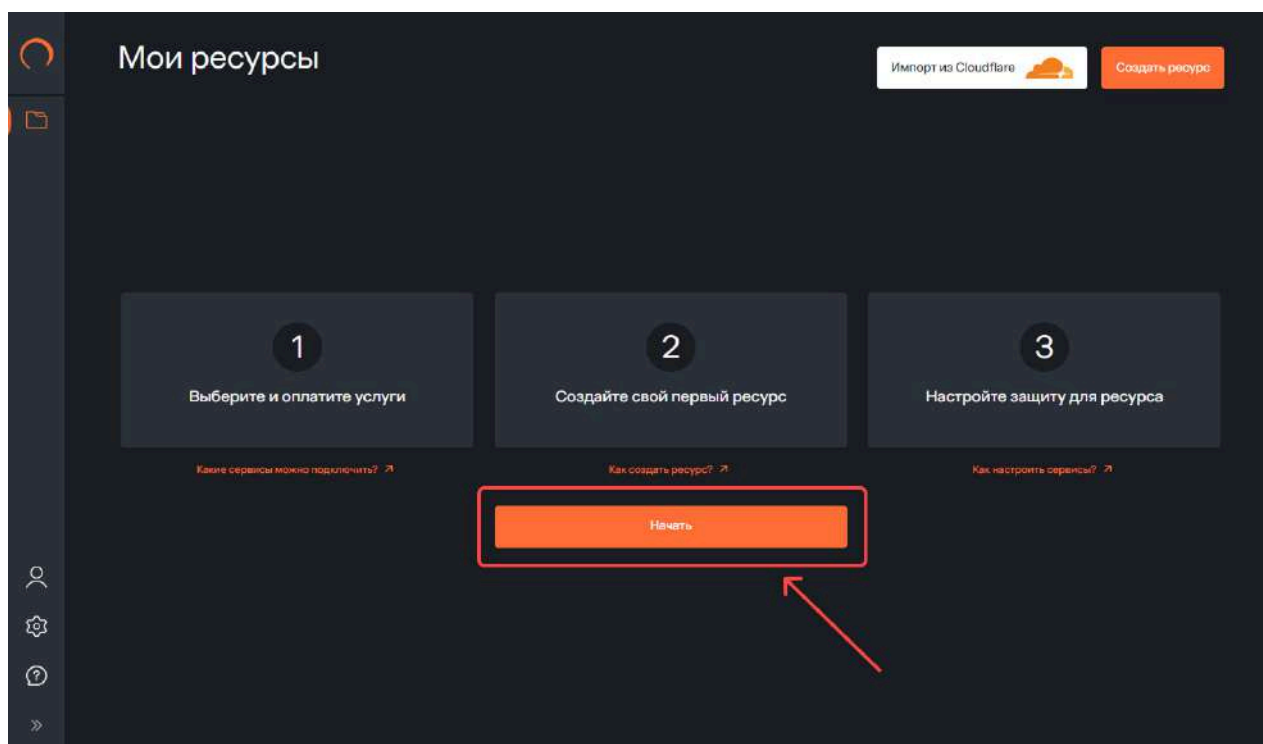
Подтверждение аккаунта

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 solar@rt-solar.ru

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



2. Выберите тип контрагента:

- **Физическое лицо**
- **Самозанятый**
- **Индивидуальный предприниматель**
- **Юридическое лицо**

← Данные пользователя

Тип контрагента

Выберите тип контрагента. От этого зависит документооборот и способ оплаты

- ☒ 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".

← 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

ФИО	Дата рождения	Проверить
Иванов Иван Иванович	10.10.1995	

Самозанятый

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

← 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

ФИО Иванов Иван Иванович	Дата рождения 10.10.1995	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.

← 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 123123123123	Проверить
---------------------	-----------

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 зависят 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 один из доступных тарифов веб-защиты:

- **Бесплатный тариф** — сервис **AntiDDoS** (ограничение: до 1 Мбит/с, один ресурс)
 - **Базовый тариф** — сервис **AntiDDoS**
 - **Оптимальный тариф** — сервисы **AntiDDoS** + **Antibot**
 - **Продвинутый тариф** — сервисы **AntiDDoS** + **Antibot** + **WAF Lite**
 - **Демо-тариф на 14 дней** — сервисы **AntiDDoS** + **Antibot** + **WAF Lite**, полный функционал без ограничений
-

Подключение сервиса

1. Нажмите на кнопку «Подключить» в тарифе «Веб-защита» после **подтверждения аккаунта**.
Откроется форма выбора уровня защиты.

← Выберите уровень защиты

☒ Веб-защита

Комплексная веб-защита интернет-ресурсов

Если вы уже знаете, какая защита вам нужна, выберите ее и переходите к настройке параметров тарифа

Бесплатный тариф

- Только один ресурс
- Ширина канала 1 Мбит/с



AntiDDoS



Antibot



WAF Lite



0 ₽

бессрочно

Подключить

Базовая защита

Подавление DDoS-атак на сайты и веб-приложения



AntiDDoS



Antibot



WAF Lite



от 1 200 ₽

в месяц

Подключить

Оптимальная защита

Базовая защита + блокировка ботов на сайте



AntiDDoS



Antibot



WAF Lite



от 1 800 ₽

в месяц

Подключить

Продвинутая защита

Оптимальная защита + предотвращение взлома



AntiDDoS



Antibot



WAF Lite



от 7 800 ₽

в месяц

Подключить

Демо на 14 дней

Вы сможете пользоваться **всеми сервисами** в течение 14 дней бесплатно. После этого наши специалисты порекомендуют вам оптимальный тариф на основе показателей вашего сайта. Предложение доступно только для новых пользователей

Бесплатно

на 14 дней

Подключить

2. Укажите желаемый тариф:

- Бесплатный тариф** — только **AntiDDoS**, ограничение по каналу 1 Мбит/с и один ресурс.

← Выберите уровень защиты

Веб-защита

Бесплатный тариф

Уровень защиты

Бесплатный

Базовый

Оптимальный

Продвинутый

Защита от DDoS-атак для одного сайта с объемом трафика до 1 Мбит/с и примерным количеством посетителей до 5000 в месяц

 AntiDDoS

 Antibot

 WAF Lite

Ширина канала
1 Мбит/с

Под защитой
1 ресурс

В месяц
0 Р

Применить

Отменить

Демо на 14 дней

Вы сможете пользоваться **всеми сервисами** в течение 14 дней бесплатно. После этого наши специалисты порекомендуют вам оптимальный тариф на основе показателей вашего сайта. Предложение доступно только для новых пользователей

Бесплатно
на 14 дней

Подключить

- Базовый тариф — только AntiDDoS.

← Выберите уровень защиты

Веб-защита

Уровень защиты

Бесплатный

Базовый

Оптимальный

Продвинутый

Защита от DDoS-атак, направленных на перегрузку серверов. Для блокировки вредоносных ботов подключите Antibot

Ширина канала

1 Мбит/с — до 5 000 посетителей в месяц

Запросы в секунду

Ширина канала — объем очищенного трафика без учета трафика атак. Соотносится с количеством посетителей сайта ?

Запросы в секунду (RPS) — количество обращений к вашему сайту за 1 секунду ?



AntiDDoS



Antibot



WAF Lite

Ширина канала
1 Мбит/с

В месяц
1200 ₽

Применить

Отменить

Демо на 14 дней

Вы сможете пользоваться **всеми сервисами** в течение 14 дней бесплатно. После этого наши специалисты порекомендуют вам оптимальный тариф на основе показателей вашего сайта. Предложение доступно только для новых пользователей

Бесплатно
на 14 дней

Подключить

- Оптимальный тариф — AntiDDoS + Antibot.

← Выберите уровень защиты

Веб-защита

Уровень защиты

Бесплатный

Базовый

Оптимальный

Продвинутый

Защита от DDoS-атак и вредоносных ботов. Для блокировки попыток взлома сайта подключите WAF Lite

Ширина канала

1 Мбит/с — до 5 000 посетителей в месяц

Запросы в секунду

Ширина канала — объем очищенного трафика без учета трафика атак. Соотносится с количеством посетителей сайта

Запросы в секунду (RPS) — количество обращений к вашему сайту за 1 секунду



AntiDDoS



Antibot



WAF Lite

Ширина канала
1 Мбит/с

В месяц
1800 Р

Применить

Отменить

Демо на 14 дней

Вы сможете пользоваться **всеми сервисами** в течение 14 дней бесплатно. После этого наши специалисты порекомендуют вам оптимальный тариф на основе показателей вашего сайта. Предложение доступно только для новых пользователей

Бесплатно
на 14 дней

Подключить

- Продвинутый тариф — AntiDDoS + Antibot + WAF Lite.

← Выберите уровень защиты

✓ Веб-защита

Уровень защиты

Бесплатный

Базовый

Оптимальный

Продвинутый

Защита от DDoS-атак и вредоносных ботов. Для блокировки попыток взлома сайта подключите WAF Lite

Ширина канала

1 Мбит/с — до 5 000 посетителей в месяц

Запросы в секунду

Ширина канала — объем очищенного трафика без учета трафика атак. Соотносится с количеством посетителей сайта

Запросы в секунду (RPS) — количество обращений к вашему сайту за 1 секунду



AntiDDoS



Antibot



WAF Lite

Ширина канала
1 Мбит/с

Запросов
5 RPS

В месяц
7 800 Р

Применить

Отменить

Демо на 14 дней

Вы сможете пользоваться **всеми сервисами** в течение 14 дней бесплатно. После этого наши специалисты порекомендуют вам оптимальный тариф на основе показателей вашего сайта. Предложение доступно только для новых пользователей

Бесплатно
на 14 дней

Подключить

3. После выбора тарифа появятся поля для настройки параметров:

- **Ширина канала** — определяет объём трафика, проходящий через защиту. Для простого сайта-визитки обычно достаточно 10–30 Мбит/с. В бесплатном тарифе значение фиксировано (1 Мбит/с).
- **Количество запросов в секунду (RPS)** — отражает нагрузку на сайт. Этот параметр нужен только в продвинутом тарифе (с WAF Lite). Например, визитке хватает 5–10 RPS, интернет-магазину — от 50 RPS и выше.

4. Проверьте параметры тарифа и нажмите кнопку «Применить».

←

Выберите уровень защиты

✓ Веб-защита

Уровень защиты

Бесплатный

Базовый

Оптимальный

Продвинутый

Комплексная защита от DDoS-атак, вредоносных ботов и попыток взлома сайта

Ширина канала
1 Мбит/с — до 5 000 посетителей в месяц

Запросы в секунду
5 RPS

Ширина канала — объем очищенного трафика без учета трафика атак. Соотносится с количеством посетителей сайта ⓘ
Запросы в секунду (RPS) — количество обращений к вашему сайту за 1 секунду ⓘ

AntiDDoS

Antibot

WAF Lite

Ширина канала
1 Мбит/с

Запросов
5 RPS

В месяц
7 800 Р

Применить

Отменить

Демо на 14 дней

Вы сможете пользоваться **всеми сервисами** в течение 14 дней бесплатно. После этого наши специалисты порекомендуют вам оптимальный тариф на основе показателей вашего сайта. Предложение доступно только для новых пользователей

Бесплатно
на 14 дней

Подключить

5. В форме «Настройки тарифа» укажите оплачиваемый период (от 1 до 12 месяцев) и нажмите кнопку «Оформить».

←

Выберите уровень защиты

✓ Веб-защита

Уровень защиты

Бесплатный

Базовый

Оптимальный

Продвинутый

Комплексная защита от DDoS-атак, вредоносных ботов и попыток взлома сайта

Ширина канала
1 Мбит/с — до 5 000 посетителей в месяц

Запросы в секунду
5 RPS

Ширина канала — объем очищенного трафика без учета трафика атак. Соотносится с количеством посетителей сайта ⓘ
Запросы в секунду (RPS) — количество обращений к вашему сайту за 1 секунду ⓘ

AntiDDoS

Antibot

WAF Lite

Ширина канала
1 Мбит/с

Запросов
5 RPS

В месяц
7 800 Р

Изменить

Настройки тарифа

Оплачиваемый период ⓘ
Вы можете оплатить тариф сразу на несколько месяцев вперед. Сумма тарифа будет автоматически списываться с вашего баланса ежемесячно.

1 месяц

Итоговая стоимость
7 800 Р

Оформить

6. После выбора сервисов перейдите к шагу **оплаты**.

Демо-тариф

Демо-тариф даёт возможность протестировать весь функционал веб-защиты бесплатно в течение 14 дней.

В этот период доступны **AntiDDoS**, **Antibot** и **WAF Lite** без ограничений по каналу и количеству запросов. Можно подключать любое количество ресурсов — так, как если бы у вас был полноценный платный тариф.

← Выберите уровень защиты

Веб-защита

Комплексная веб-защита интернет-ресурсов

Если вы уже знаете, какая защита вам нужна, выберите ее и переходите к настройке параметров тарифа

Бесплатный тариф

Только один ресурс
Ширина канала 1 Мбит/с

AntiDDoS
Antibot
WAF Lite

0 Р
бессрочно

Подключить

Базовая защита

Подавление DDoS-атак на сайты и веб-приложения

AntiDDoS
Antibot
WAF Lite

от 1 200 Р
в месяц

Подключить

Оптимальная защита

Базовая защита + блокировка ботов на сайте

AntiDDoS
Antibot
WAF Lite

от 1 800 Р
в месяц

Подключить

Продвинутая защита

Оптимальная защита + предотвращение взлома

AntiDDoS
Antibot
WAF Lite

от 7 800 Р
в месяц

Подключить

Демо на 14 дней

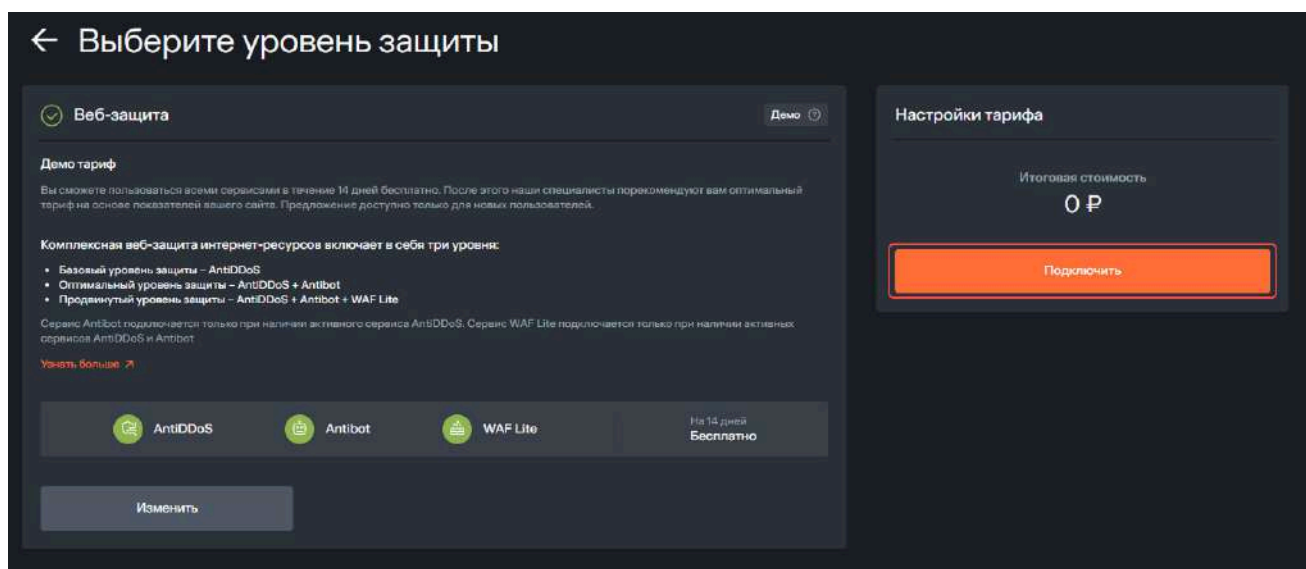
Вы сможете пользоваться **всеми сервисами** в течение 14 дней бесплатно. После этого наши специалисты порекомендуют вам оптимальный тариф на основе показателей вашего сайта. Предложение доступно только для новых пользователей

Бесплатно на 14 дней

Подключить

Особенности подключения

- Демо можно активировать только один раз для аккаунта.
- Доступен пользователям, у которых ранее не было активных тарифов с сервисами, входящими в демо.
- После активации весь функционал работает в полном объёме.



Рекомендации тарифа

По окончании демо система автоматически формирует **персональные предложения платных тарифов** на основе статистики использования.

← Выберите уровень защиты

Веб-защита

Демо ?

Рекомендованные тарифы

Учитывая данные собранные за время работы демо тарифа, мы подготовили для вас несколько вариантов защиты с подходящими параметрами. Выберите один из платных уровней или используйте бесплатный тариф, чтобы обеспечить безопасность ресурсов

Базовая защита

Подавление DDoS-атак на сайты и веб-приложения



AntiDDoS



Antibot



WAF Lite

Ширина канала
1 Мбит/с

1 200 ₽
в месяц

Подключить

Оптимальная защита

Базовая защита +
блокировка ботов на сайте



AntiDDoS



Antibot



WAF Lite

Ширина канала
1 Мбит/с

1 800 ₽
в месяц

Подключить

Продвинутая защита

Оптимальная защита
+ предотвращение взлома



AntiDDoS



Antibot



WAF Lite

Ширина канала
1 Мбит/с

Запросов
50 RPS

22 200 ₽
в месяц

Подключить

Статистика за 14 дней использования

Тарифицируемый трафик ?

26.81 Мбит/с

Входящий легитимный трафик ?

392 Мбит/с

Тарифицируемый RPS ?

50 RPS

[Подробная статистика >](#)

Бесплатный тариф

Защита от DDoS-атак для сайтов с объемом трафика до 1 Мбит/с
и примерным количеством посетителей до 5000 в месяц

Подключить

- Если нагрузка не превышала 1 Мбит/с и RPS оставался низким — система предложит базовые варианты (например, 2 Мбит/с и 5 RPS).
- Если нагрузка была выше — будут предложены более мощные тарифы (например, 30 Мбит/с и 20 RPS).
- Варианты подбираются из трёх уровней: **Базовый**, **Оптимальный**, **Продвинутый**, с указанием рекомендуемой ширины канала и количества запросов.

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.

Оплатываемый тариф

Подключенные сервисы

- AntiDDoS
- Antibot

Параметры

Ширина канала	5 Мбит/с	Стоимость в месяц	5 400 Р
Оплатываемый период	1 месяц		

Оплата

Итоговая стоимость

5 400 Р

Оплатить

Назад

ⓘ Обратите внимание

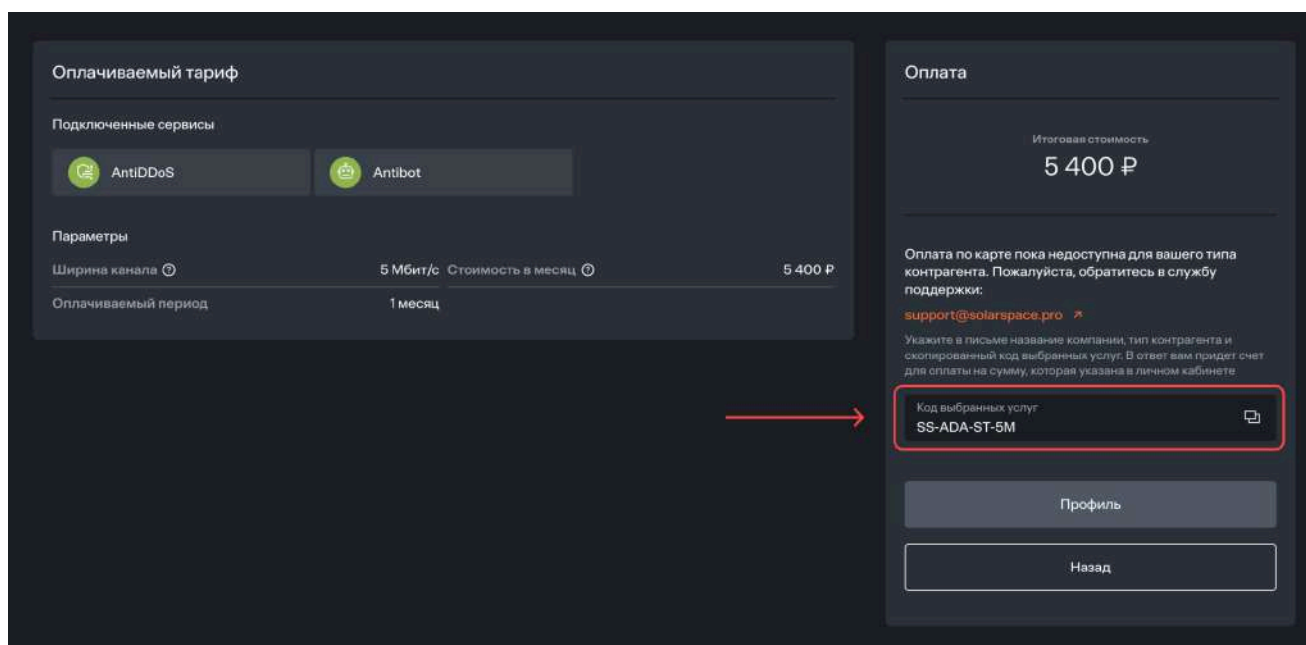
Способ оплаты зависит от выбранного типа контрагента

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

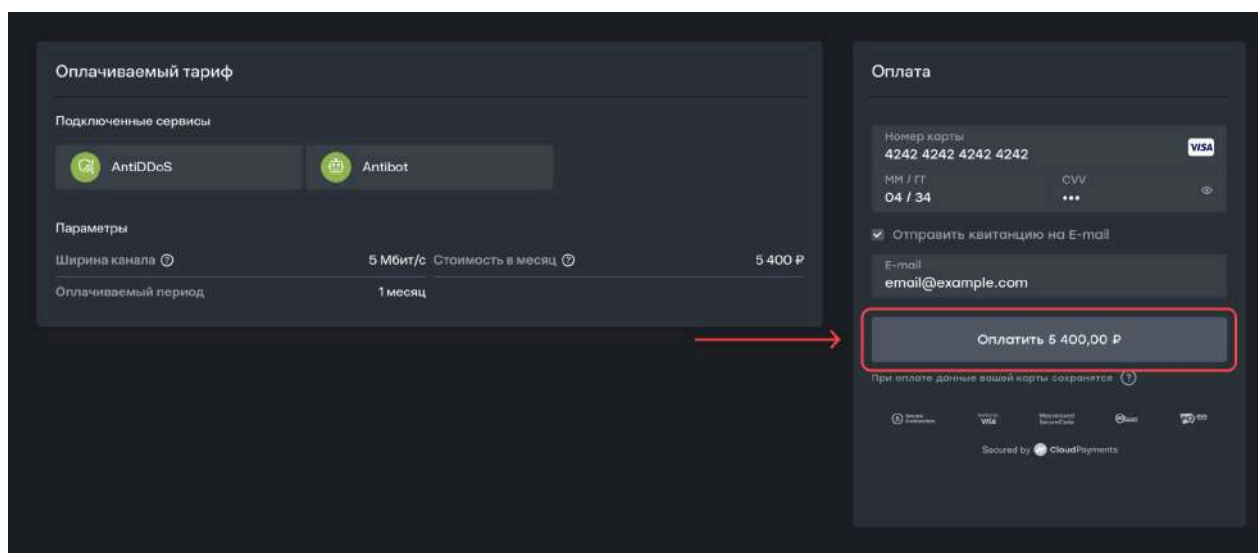
В ответ вам придет счет для оплаты на сумму, которая указана в личном кабинете при оформлении Веб-защиты.



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 вашим адресом электронной почты, указанным при регистрации).
2. После ввода данных нажмите на кнопку "Оплатить".



3. Актуальный баланс будет отображаться на верхней панели рядом с профилем.
4. 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

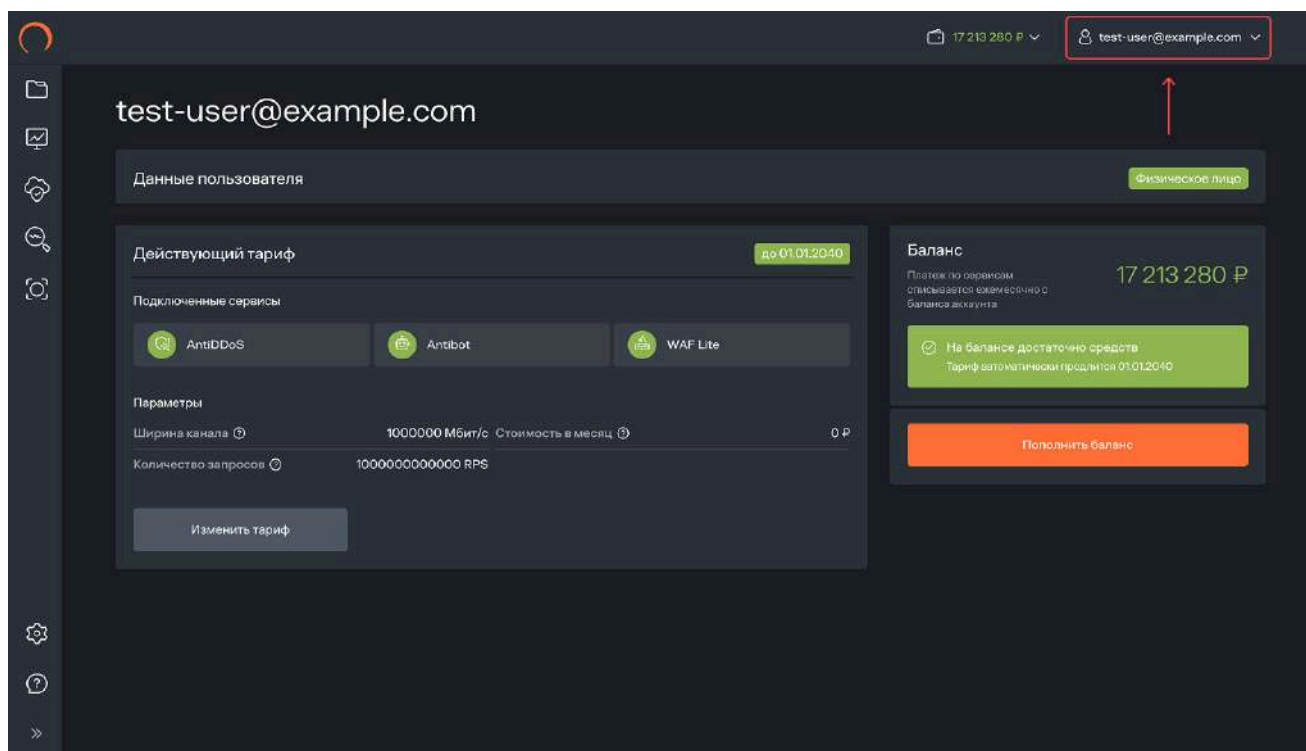
Настрою позже

Профиль

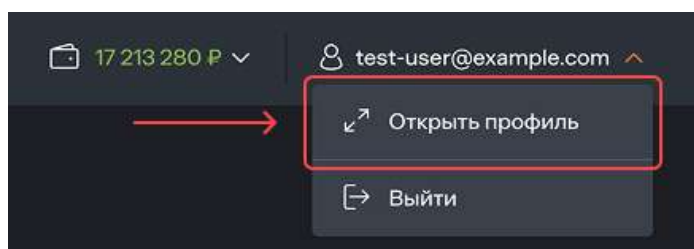
На странице профиля вы можете:

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

Для того, чтобы попасть на страницу профиля из любого раздела, нажмите на имя вашего домена в верхнем меню страницы.



Откроется выпадающий список. Нажмите "Открыть профиль".



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".

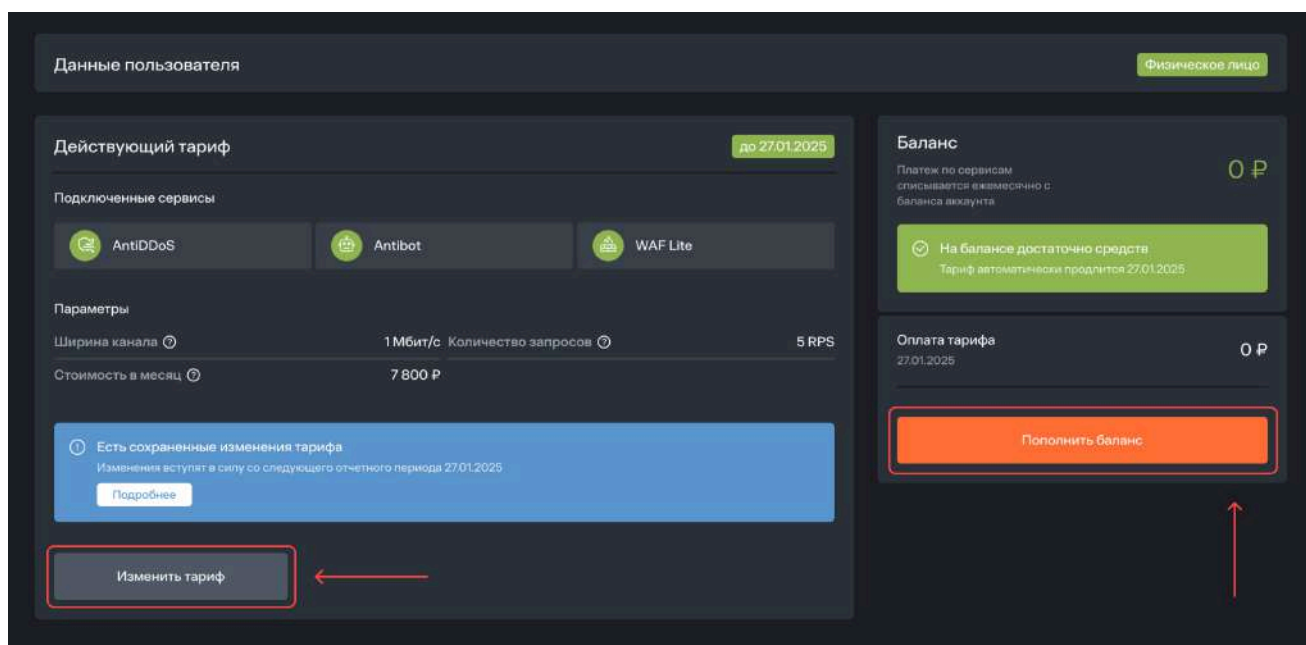
На странице профиля вы можете:

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

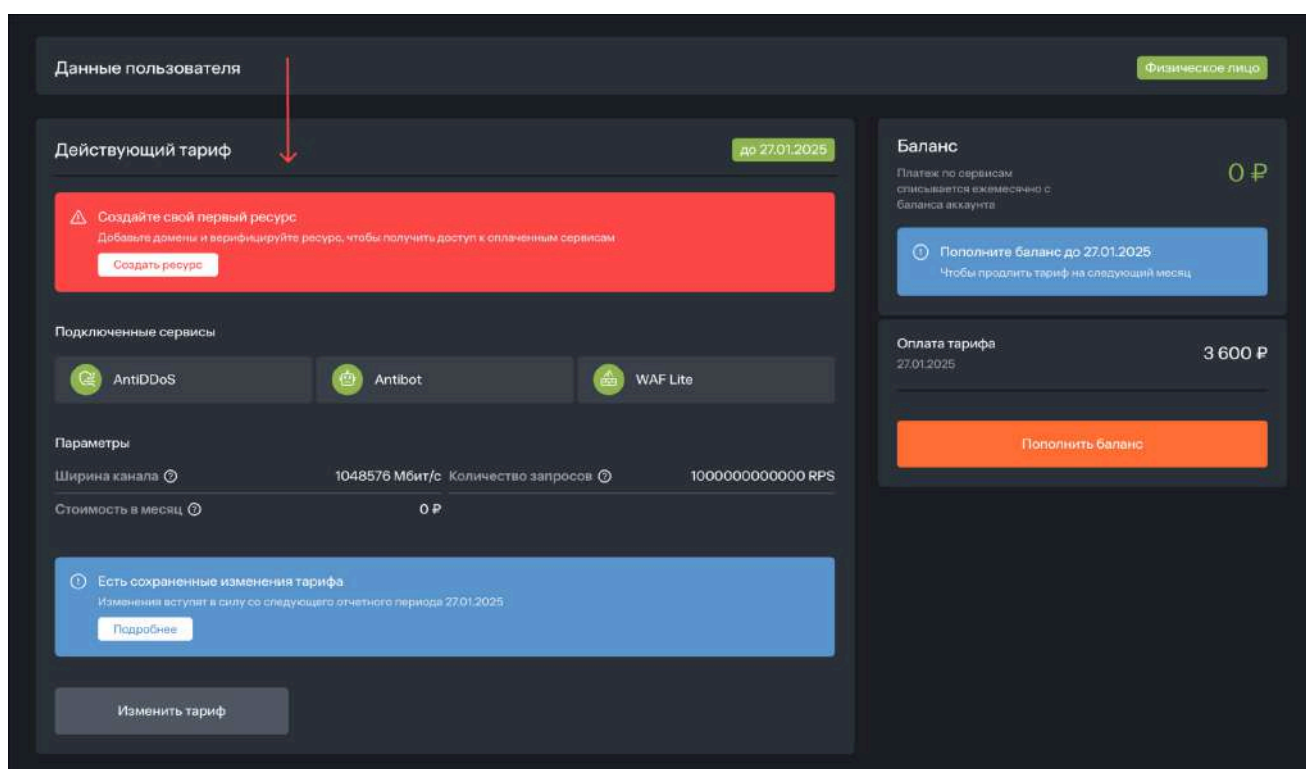
Подтвержденный пользователь с активными услугами

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

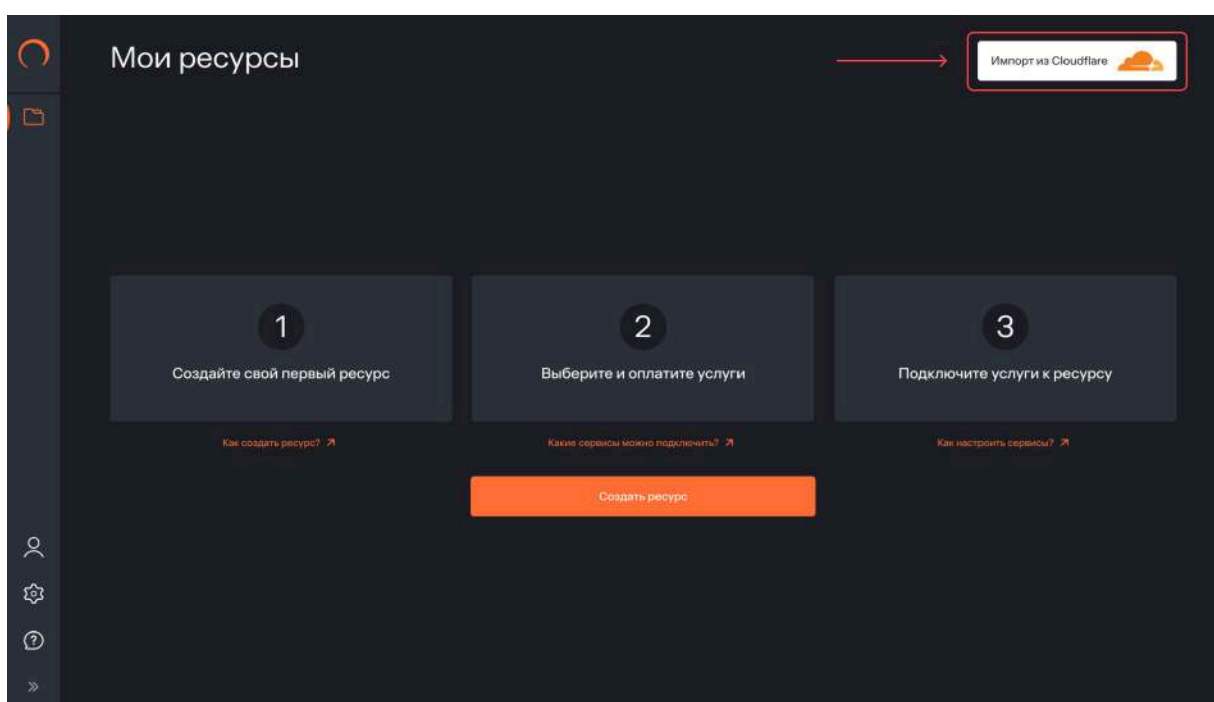
Функция импорта из CloudFlare предназначена для быстрого автоматического переноса ресурсов со всеми доменами в личный кабинет Solar Space.

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

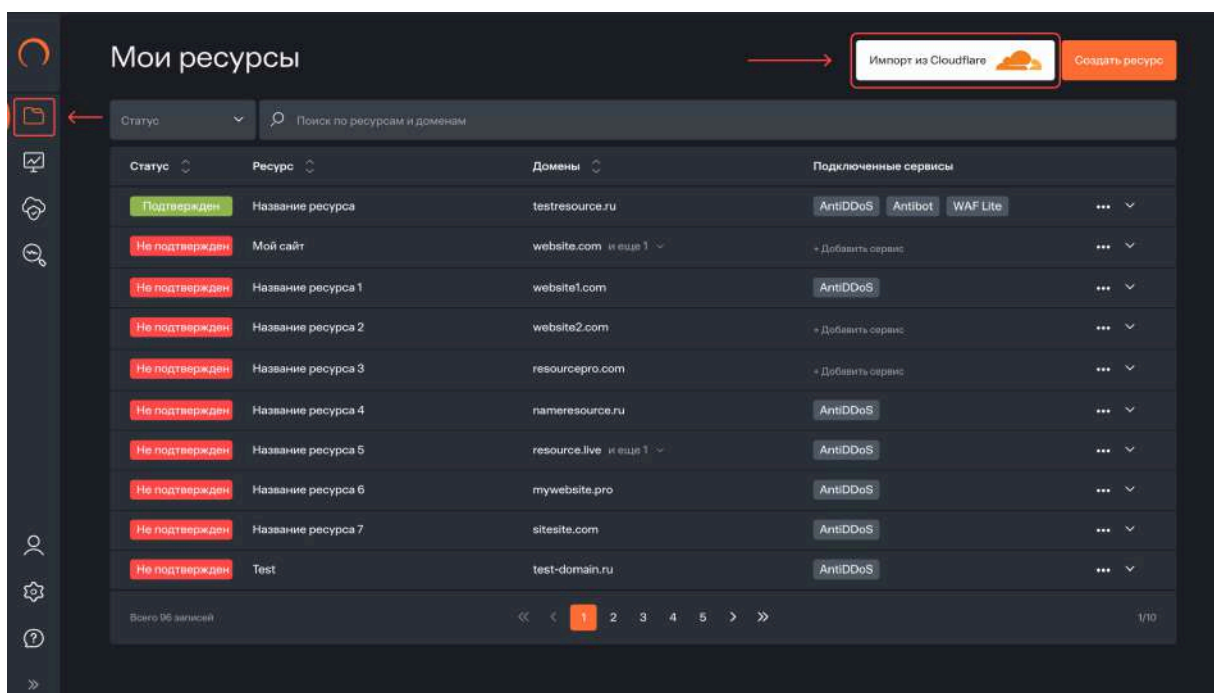
Для импорта ресурсов из CloudFlare выполните следующие действия:

1. Нажмите на кнопку "Импорт из CloudFlare" в правом верхнем углу экрана:

- Если вы новый пользователь без ресурсов

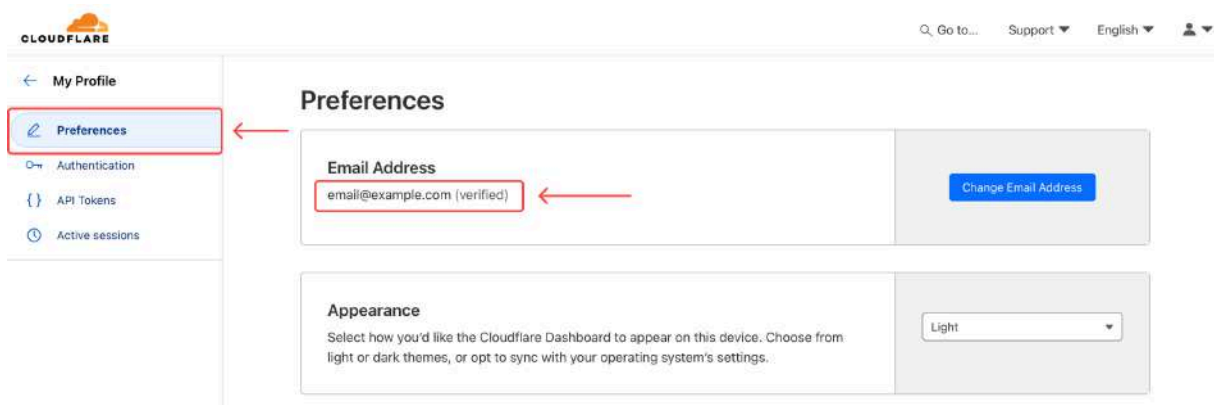


- Если у вас уже есть аккаунт с созданными ресурсами на странице "Мои ресурсы"

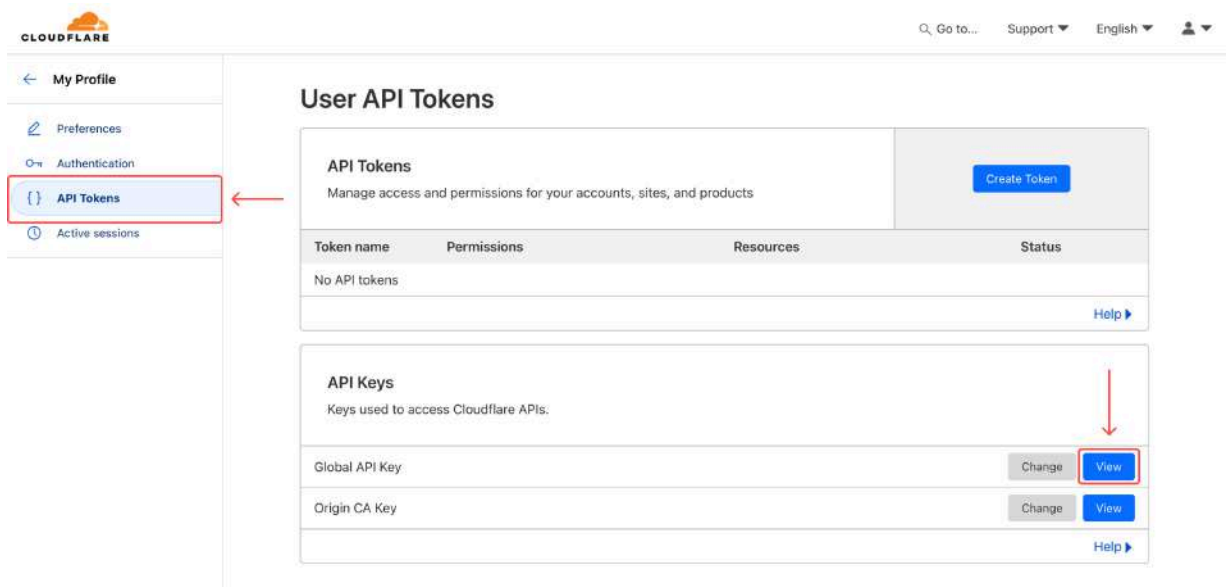


2. Перейдите в личный кабинет CloudFlare и скопируйте значения из полей:

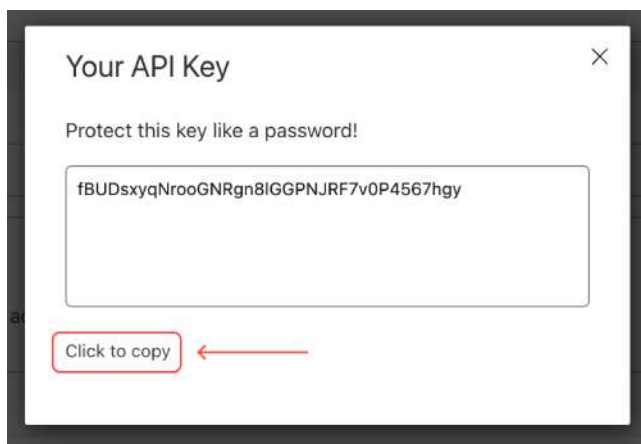
- **Email Address** — это поле находится **на этой странице** в разделе "Preferences" сервиса CloudFlare



- **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".

← Импорт ресурсов из Cloudflare

Подключение к Cloudflare

Для импорта ресурсов зайдите в личный кабинет Cloudflare и скопируйте параметры из настроек профиля

[Узнать больше ↗](#)

Email Address
email@example.com

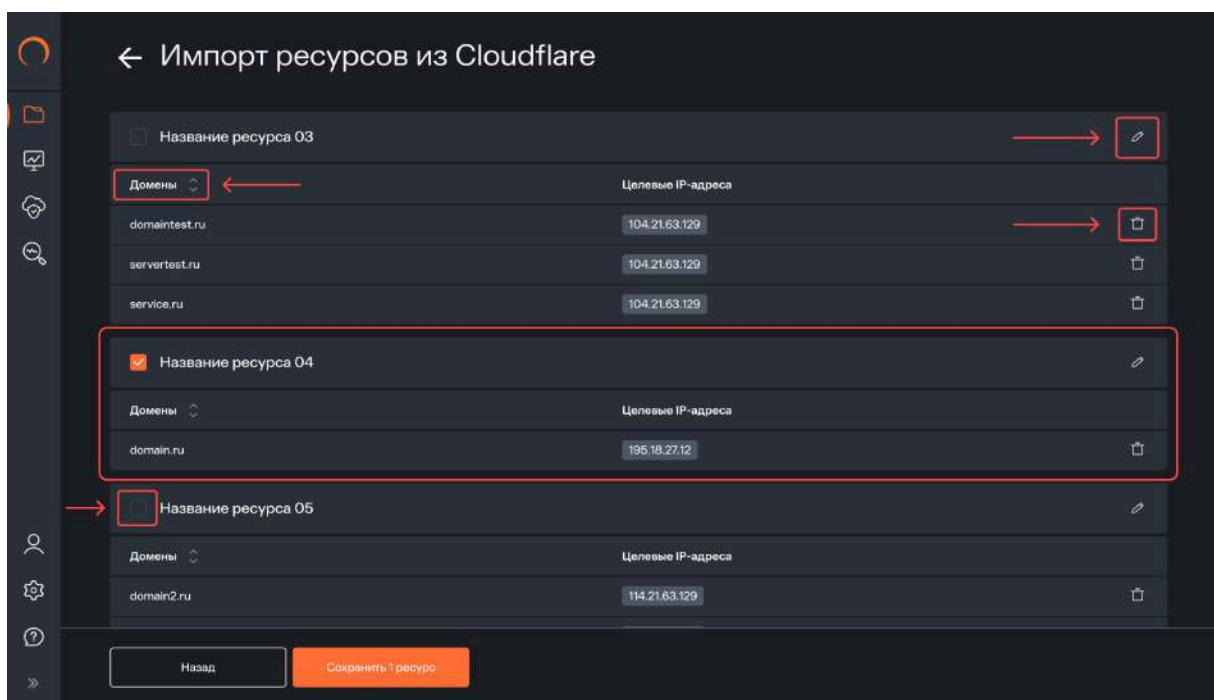
Global API key
fBUDsxyqNrooGNRgn8IGGPNJRF7v0P4567hgy

Назад

Импортировать

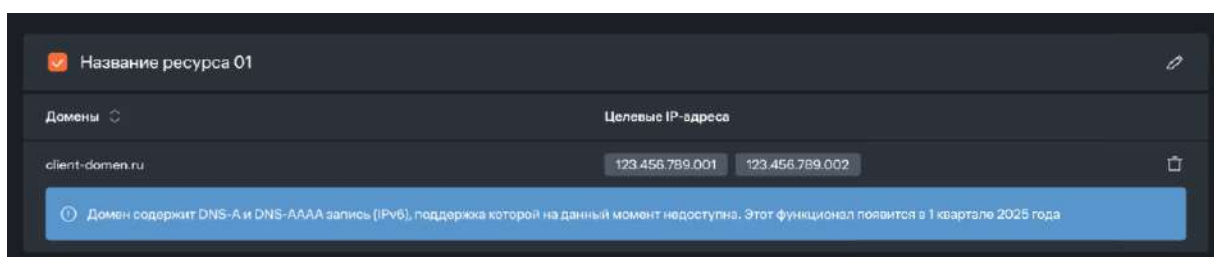
5. Импорт ресурсов займет не более 1 минуты. После этого появится список перенесенных ресурсов со всеми доменами. Успешно импортированные ресурсы отмечены по умолчанию "галочкой". Вы можете:

- **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

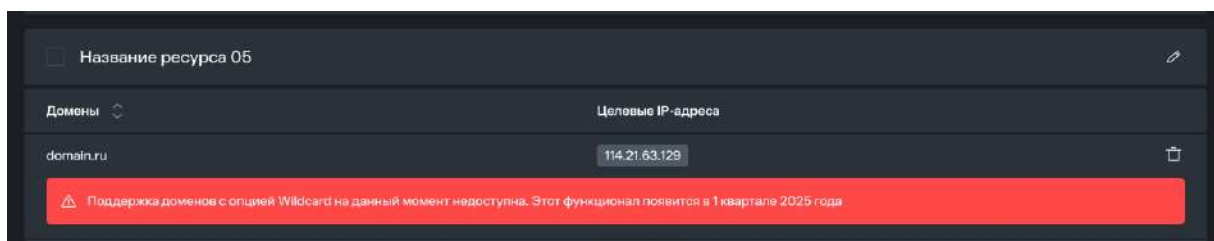


6. В 2025 году появится возможность поддержки ресурсов с IPv6 и SSL-сертификатами WildCard, которые обеспечивают защиту всех поддоменов. Пока при импорте таких ресурсов появляются предупреждающие сообщения:

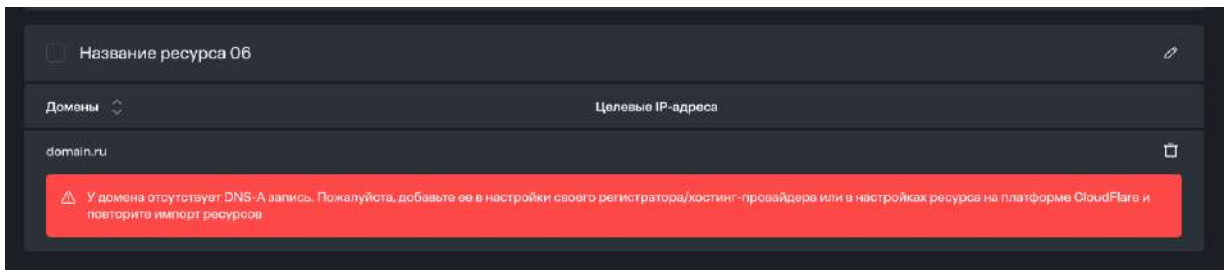
- **Для доменов в формате IPv6:** "Домен содержит DNS-A и DNS-AAAA запись (IPv6), поддержка которой на данный момент недоступна. Этот функционал появится в 1 квартале 2025 года"



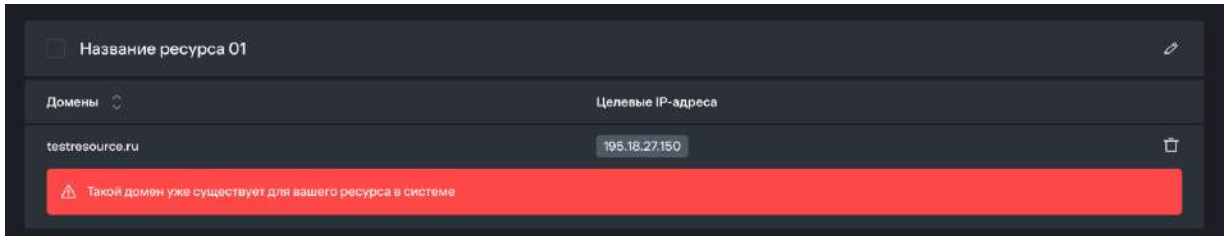
- **Для доменов с WildCard-сертификатом:** "Поддержка доменов с опцией Wildcard на данный момент недоступна. Этот функционал появится в 1 квартале 2025 года"



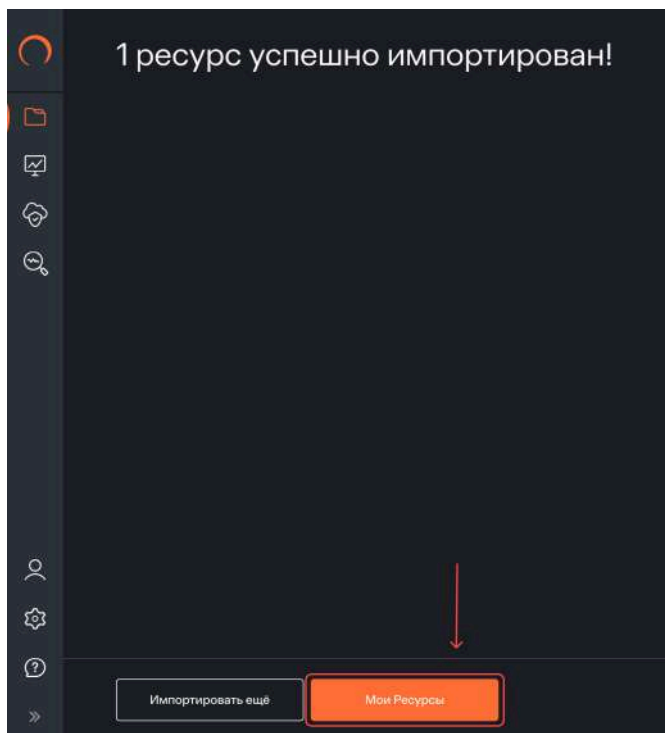
- **Для доменов, у которых отсутствует A запись:** "У домена отсутствует DNS-A запись. Пожалуйста, добавьте ее в настройки своего регистратора/хостинг-провайдера или в настройках ресурса на платформе CloudFlare и повторите импорт ресурсов"



- 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.



Быстрый старт

Добро пожаловать. Ниже — пошаговая инструкция, которая поможет быстро и безопасно подключить ваш сайт к защите Solar Space.

Следуя этим шагам, вы:

- Подтвердите, что домен принадлежит вам
 - Настроите безопасную маршрутизацию трафика
 - Выпустите SSL-сертификат
 - Активируете защиту платформы
-

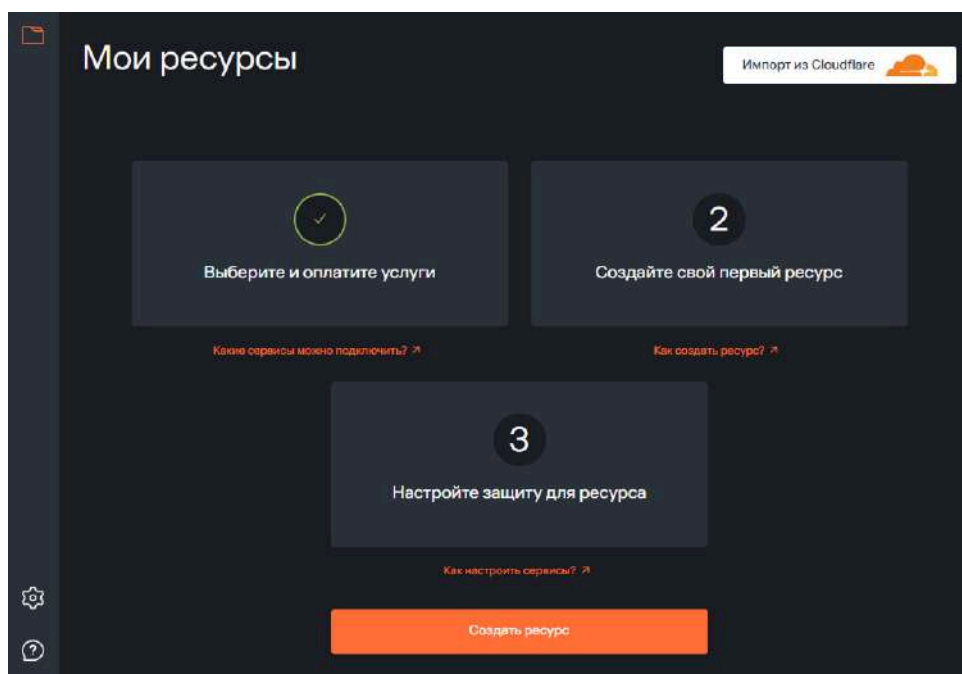
Подготовка к подключению

Перед началом убедитесь, что у вас есть:

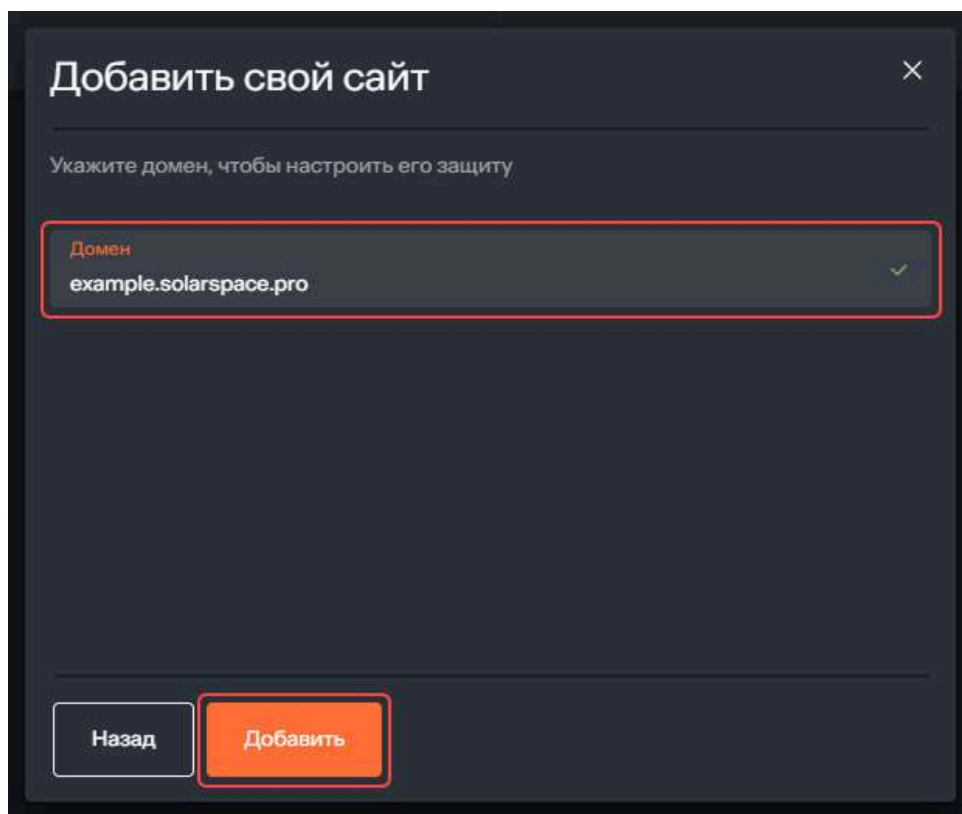
- Зарегистрированный домен, который нужно защитить
 - Хостинг или панель управления с доступом к DNS-записям
 - [Аккаунт в Solar Space](#)
-

Создание ресурса

После выбора и оплаты тарифа вы попадёте на страницу «**Мои ресурсы**». Если у вас ещё нет ни одного ресурса, интерфейс отобразит последовательность из трёх шагов и предложит создать первый ресурс.



Чтобы подключить домен к защите, сначала необходимо создать ресурс. Ресурс — это объект, к которому будут привязаны настройки фильтрации, SSL-сертификат и другие параметры защиты.

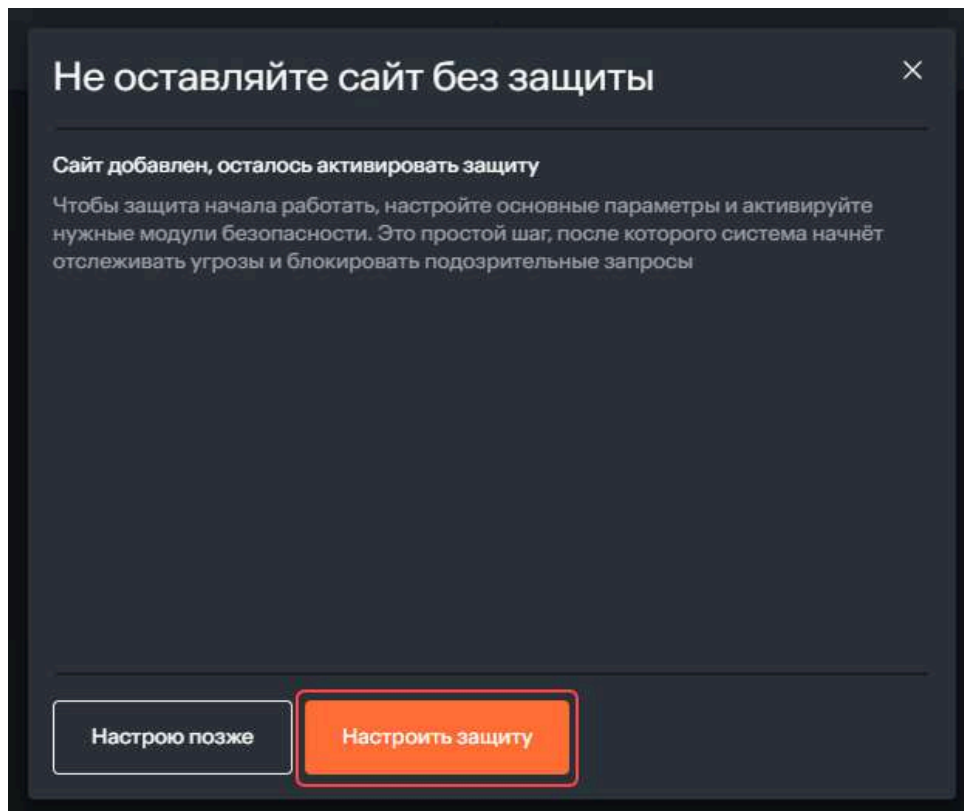


1. Перейдите в **личный кабинет Solar Space**
2. Нажмите кнопку **«Создать ресурс»**
3. Укажите **название ресурса** — для вашего удобства. Например: «Основной сайт» или «Интернет-магазин»

4. Укажите **домен**, который хотите защитить (например: `example.ru`) В этой инструкции используется `example.solarspace.pro` как демонстрационный пример

5. Нажмите «**Добавить**»

После добавления домена появится окно с предложением настроить защиту. На этом этапе ресурс создан, и вы можете перейти к дальнейшей настройке.

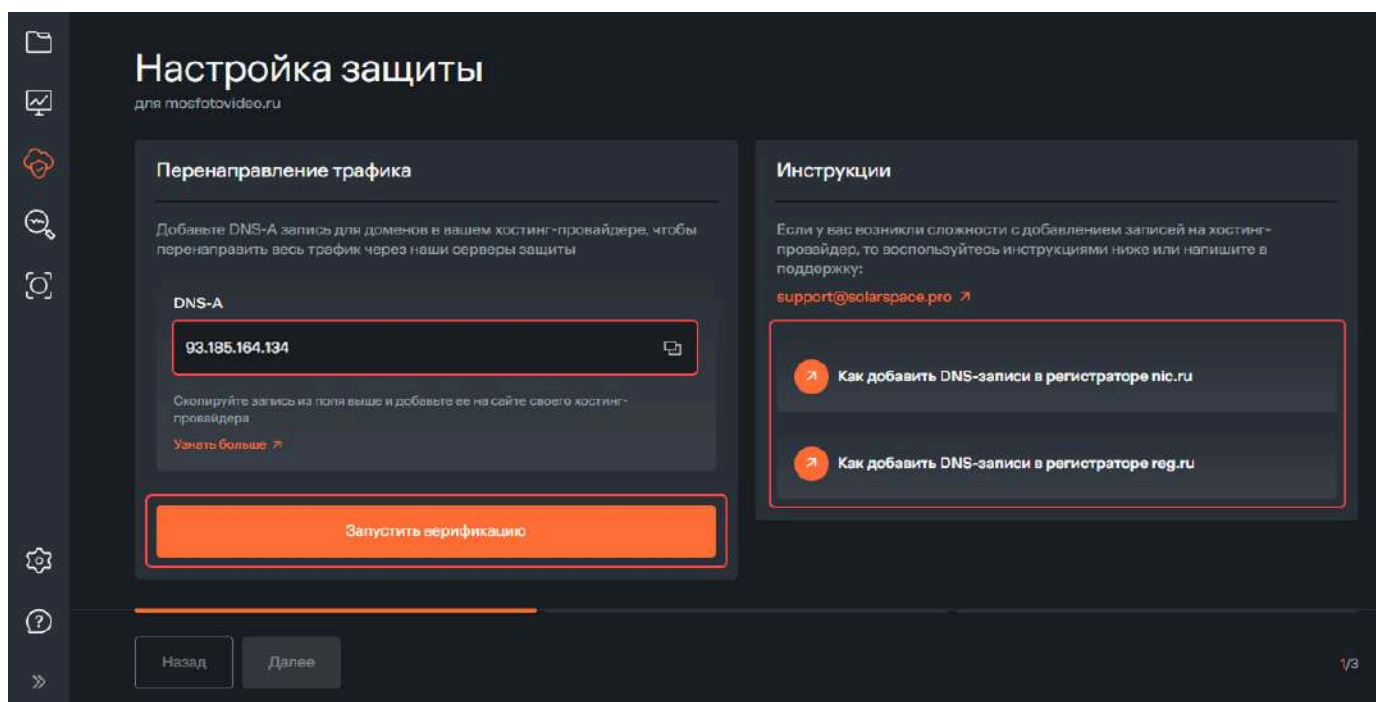


Нажмите «**Настроить защиту**», чтобы продолжить.

❗ Если вы ранее использовали Cloudflare, вы можете воспользоваться встроенной функцией импорта — это упростит добавление домена и сократит первичную настройку. Подробнее — в [инструкции по импорту из Cloudflare](#)

Перенаправление трафика (А-запись)

На этом этапе, после прохождения верификации, необходимо направить трафик домена через инфраструктуру Solar Space.



Для этого используется **А-запись**, которая указывает, на какой IP-адрес должны приходить запросы к вашему сайту.

- ❗ Символ "@" в DNS обозначает корневой домен — основной адрес сайта (например, example.ru). В некоторых интерфейсах он может отображаться как полное имя домена — это одно и то же. Поддомены (www, mail, ftp и т.п.) остаются без изменений и не участвуют в этом подключении.

Что нужно сделать

1. Откройте DNS-панель у вашего регистратора или хостинг-провайдера.
2. Найдите А-запись для @ или имени домена без поддоменов.
3. Замените существующий IP-адрес на значение, указанное в кабинете в блоке **DNS-A**. В этом примере это: 93.185.164.134.
4. Сохраните изменения у провайдера.
5. Вернитесь в кабинет и нажмите кнопку «**Запустить верификацию**» — это позволит системе проверить обновления DNS и активировать кнопку «**Далее**».

+ Добавить новую запись

Хост	Тип	Значение	TTL	Дата	- фильтр
example					
example	A	93.185.164.134		2025-10-31 14:17:16	

Всего записей 42 . Показывать по 50

⚠ Изменять нужно только запись с именем "@" или полным именем вашего домена. Все поддомены ("www", "mail", "ftp" и т.п.) остаются на текущем IP, их конфигурацию следует оставить без изменений. **Удалите все AAAA-записи** (IPv6), если они есть — они могут мешать корректной маршрутизации трафика.

⚠ Если вы используете CDN (поддомены вида cdn.example.com, static.example.com, img.example.com и т.п.), не изменяйте DNS-записи этих поддоменов. Они должны продолжать указывать на вашего CDN-провайдера. Перевод CDN-поддоменов на сервис защиты может привести к недоступности изображений и других статических файлов сайта.

Дополнительные инструкции

Если не уверены, как именно внести изменения — воспользуйтесь инструкцией по работе с DNS у популярных регистраторов:

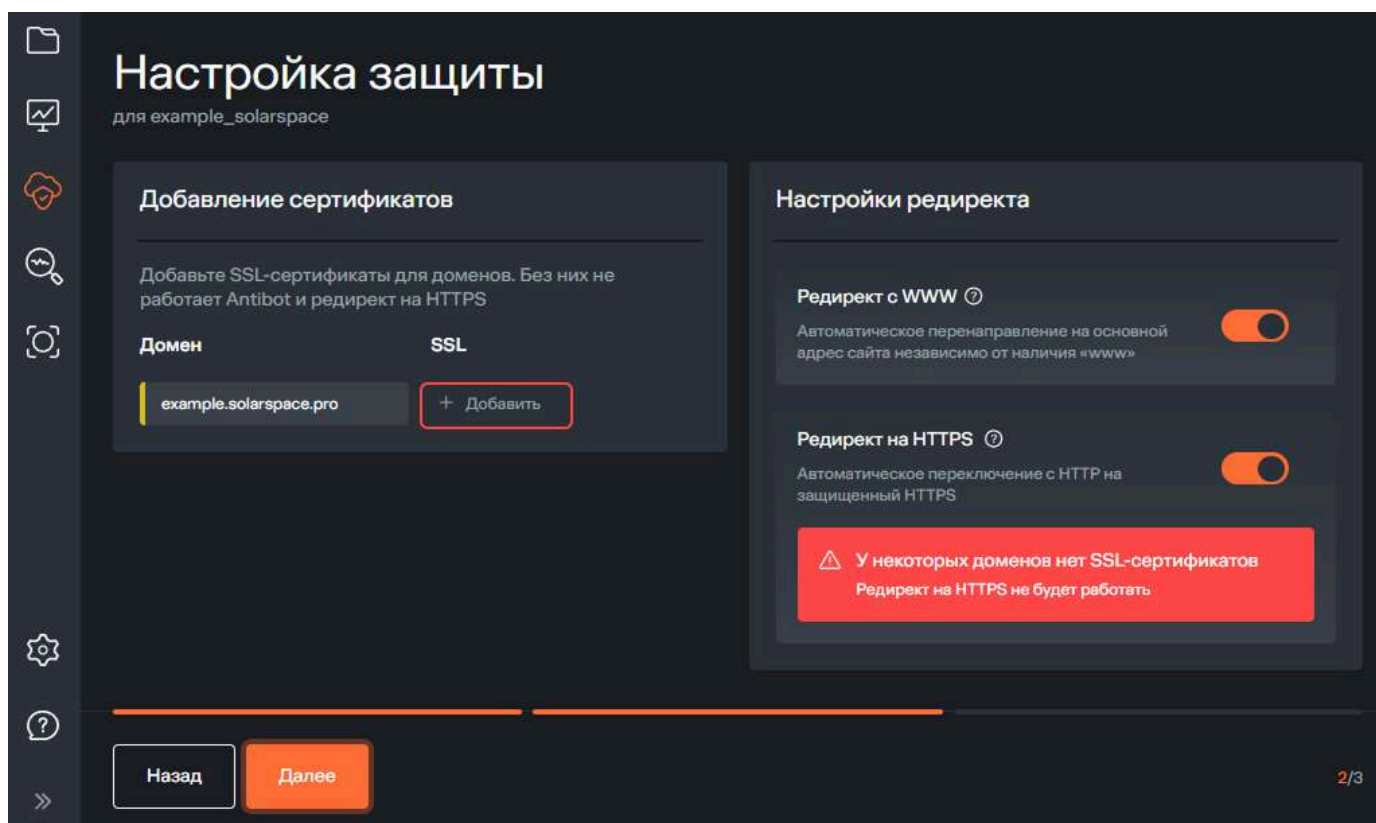
- [Как добавить DNS-записи в NIC.RU](#)
- [Как добавить DNS-записи в REG.RU](#)

После успешной проверки вы сможете перейти к следующему шагу.

Установка SSL-сертификата

После подтверждения подключения необходимо настроить SSL-сертификат. Без него не работает фильтрация **Antibot** и невозможен редирект на **HTTPS**.

Общая справка по **SSL-сертификатам**, а также по редиректам (с **WWW**, на **HTTPS**) — в разделе [SSL и редирект](#).



На этапе настройки вы можете выбрать один из вариантов:

- **Бесплатный сертификат Let's Encrypt (LE)**
- **Собственный сертификат**

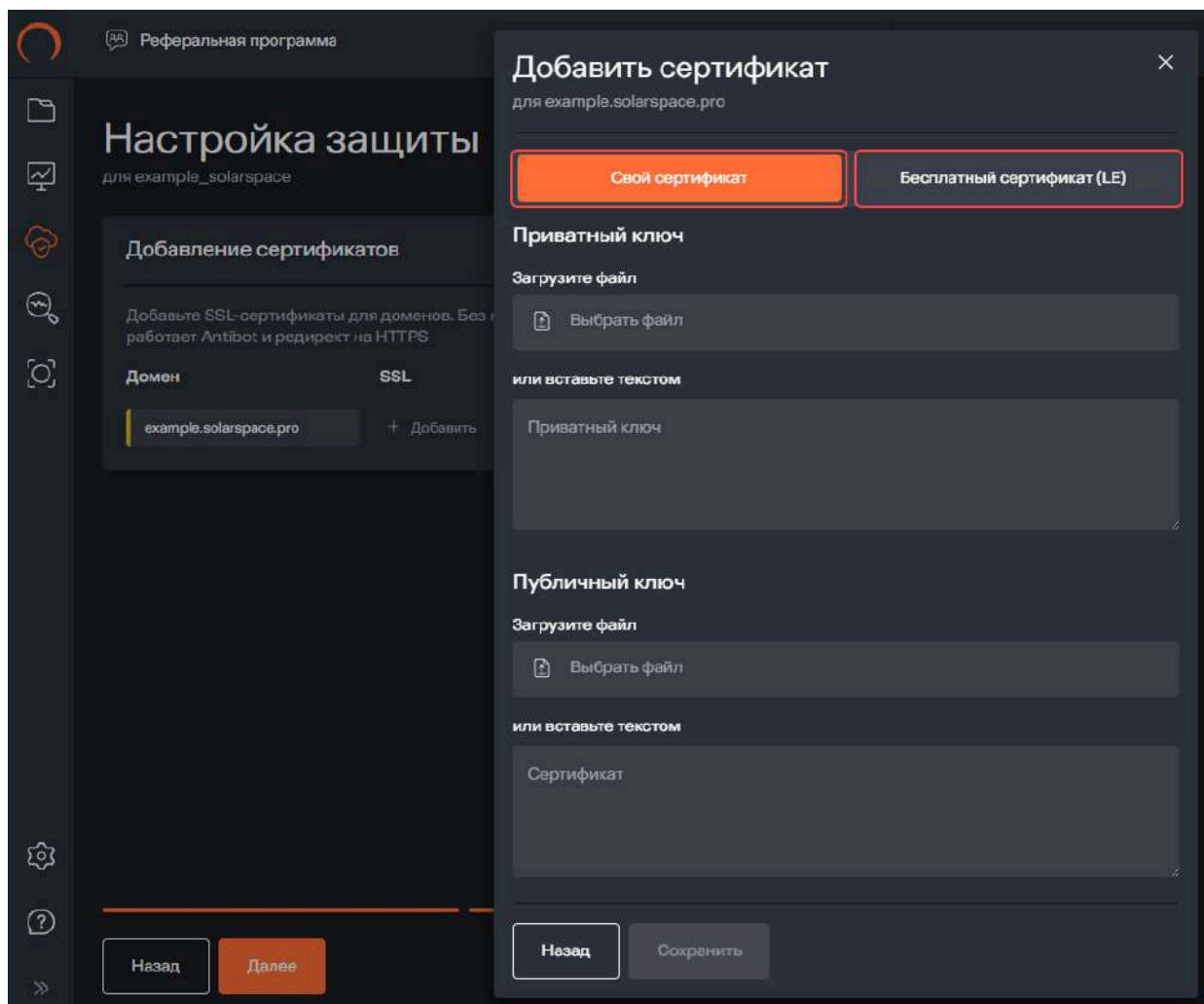
Как добавить сертификат

1. Нажмите «**Добавить**» напротив нужного домена.

2. Выберите способ:

- «**Бесплатный сертификат (Let's Encrypt)**», если нужен автоматический выпуск.
- «**Свой сертификат**», если у вас есть собственная пара ключ/сертификат.

1. При выборе собственного сертификата загрузите **приватный ключ** и **публичный сертификат** (файлами или текстом). Подробная инструкция по загрузке собственного сертификата — [Как добавить локальный SSL-сертификат](#)



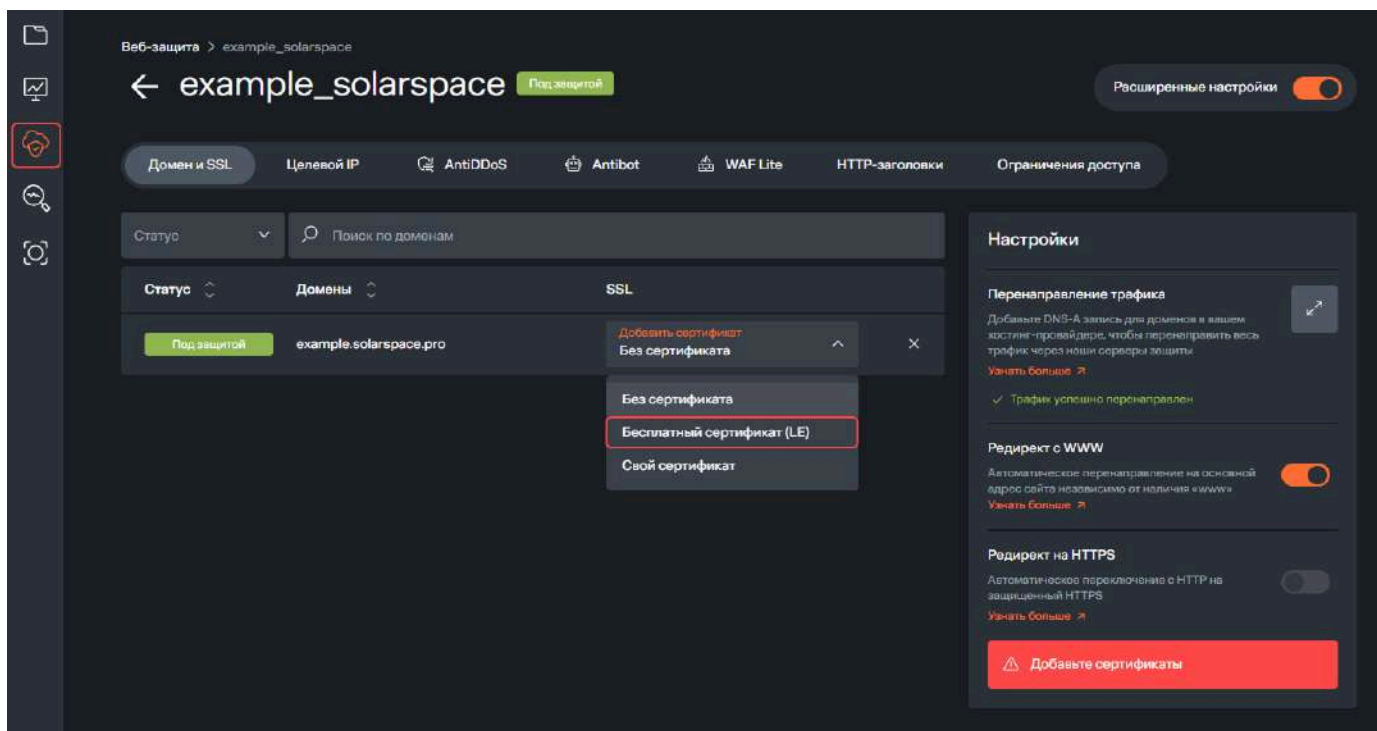
Выпуск бесплатного сертификата (LE)

LE-сертификат можно выпустить **двумя способами** — сразу на этапе настройки или позже через «WEB-защиту».

Способ 1. Выпуск сразу (рекомендуется)

1. Выберите «**Бесплатный сертификат (LE)**» в всплывающем окне панели SSL. Платформа автоматически выполнит выпуск и установку сертификата.
2. Убедитесь, что включён параметр «**Редирект на HTTPS**».

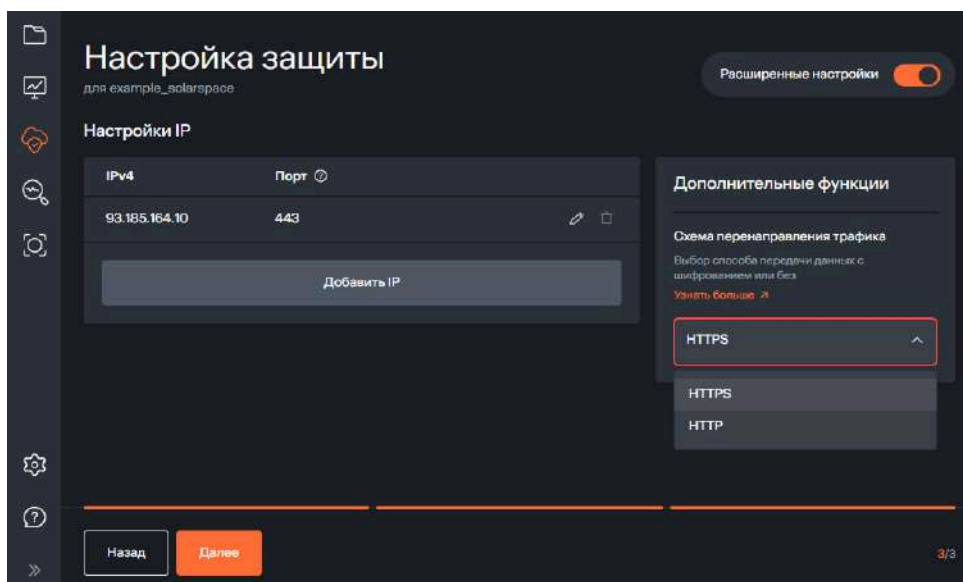
Способ 2. Выпуск позже, через раздел «WEB-защита»



1. Перейдите в раздел «WEB-защита».
2. Откройте настройки нужного ресурса.
3. Нажмите «Выпустить сертификат».
4. Выберите «Бесплатный сертификат (LE)»
5. Включите Редирект на HTTPS .
6. Сохраните изменения.

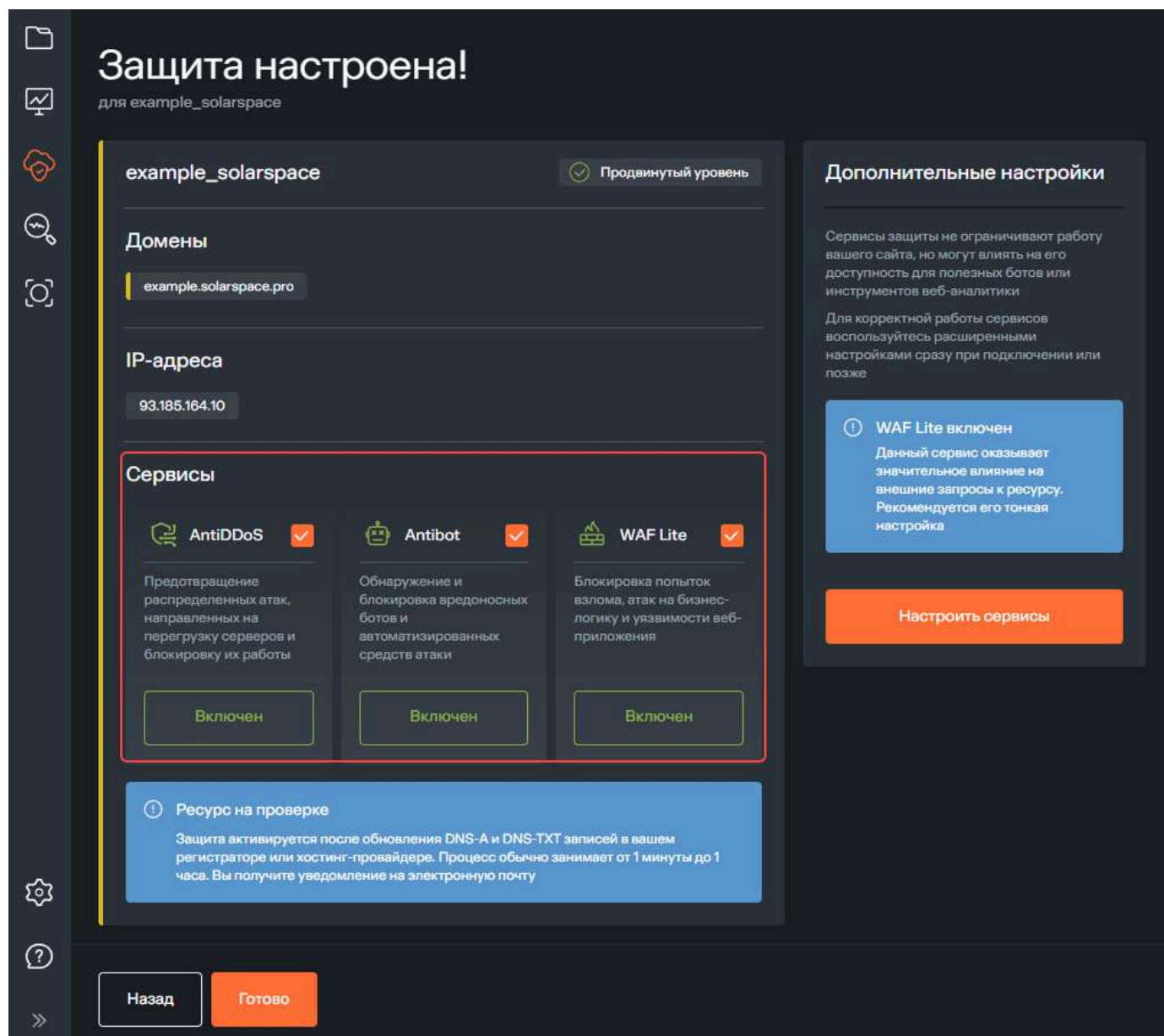
Включение защитных функций

На финальном шаге включите нужные сервисы и задайте схему перенаправления трафика.



Откройте блок «**Дополнительные функции**» и в поле «**Схема перенаправления трафика**» выберите режим. Рекомендуем **HTTPS** — весь трафик шифруется между платформой и вашим сервером.

Подробное описание режимов, их назначение и кейсы применения — в разделе «**Целевой IP**» .



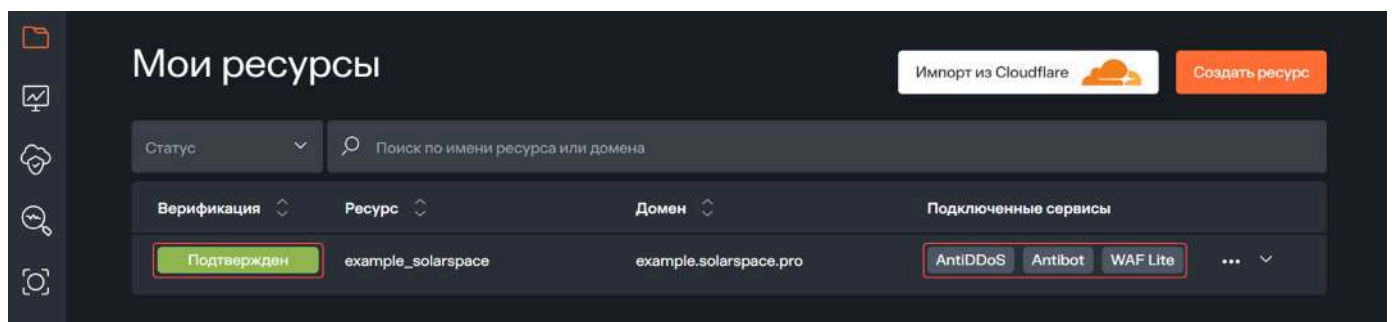
1. Включите необходимые модули защиты, доступные в вашем тарифе: **AntiDDoS**, **Antibot**, **WAF Lite**.
2. При необходимости перейдите к тонкой настройке по кнопке «**Настроить сервисы**».
3. Проверьте состав активных сервисов и нажмите «**Готово**».

- ❗ Доступность и предварительное состояние сервисов зависят от выбранного тарифа: часть модулей может быть включена автоматически. Настроить или изменить состав сервисов можно как сейчас, так и позже в разделе *Веб-защита*.

- ⚠ Сервис **AntiDDoS** является базовым. Его отключение приведёт к отключению **Antibot** и **WAF Lite**.

Финальная проверка защиты

Если все шаги успешно выполнены, вы получите активный ресурс с включёнными фильтрами и действующим SSL-сертификатом.

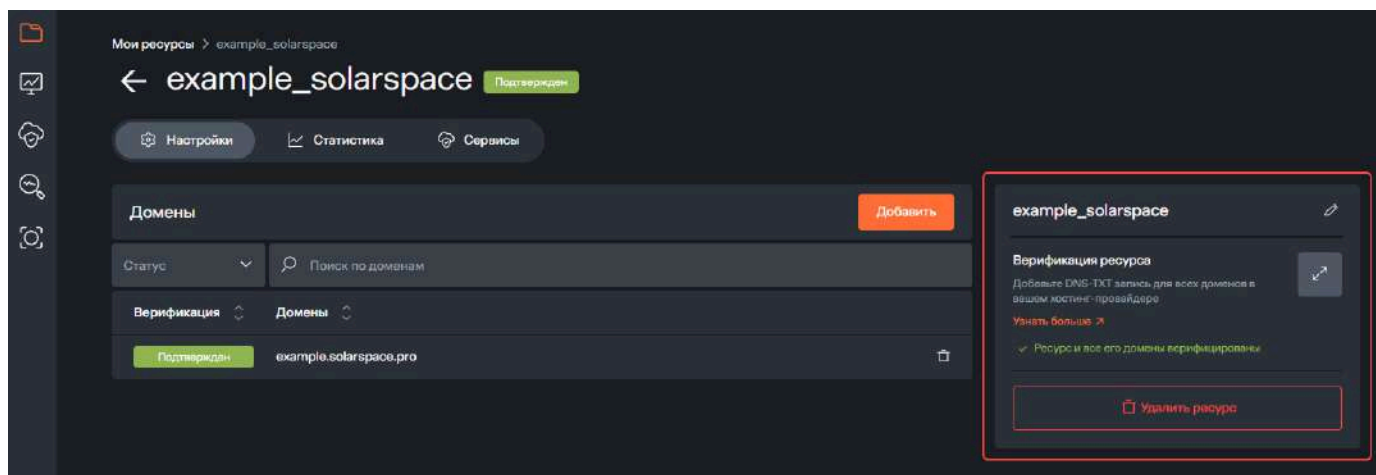


- ✅ Базовая защита активна. Остальные возможности доступны через интерфейс Solar Space. Подробнее — [в документации](#).

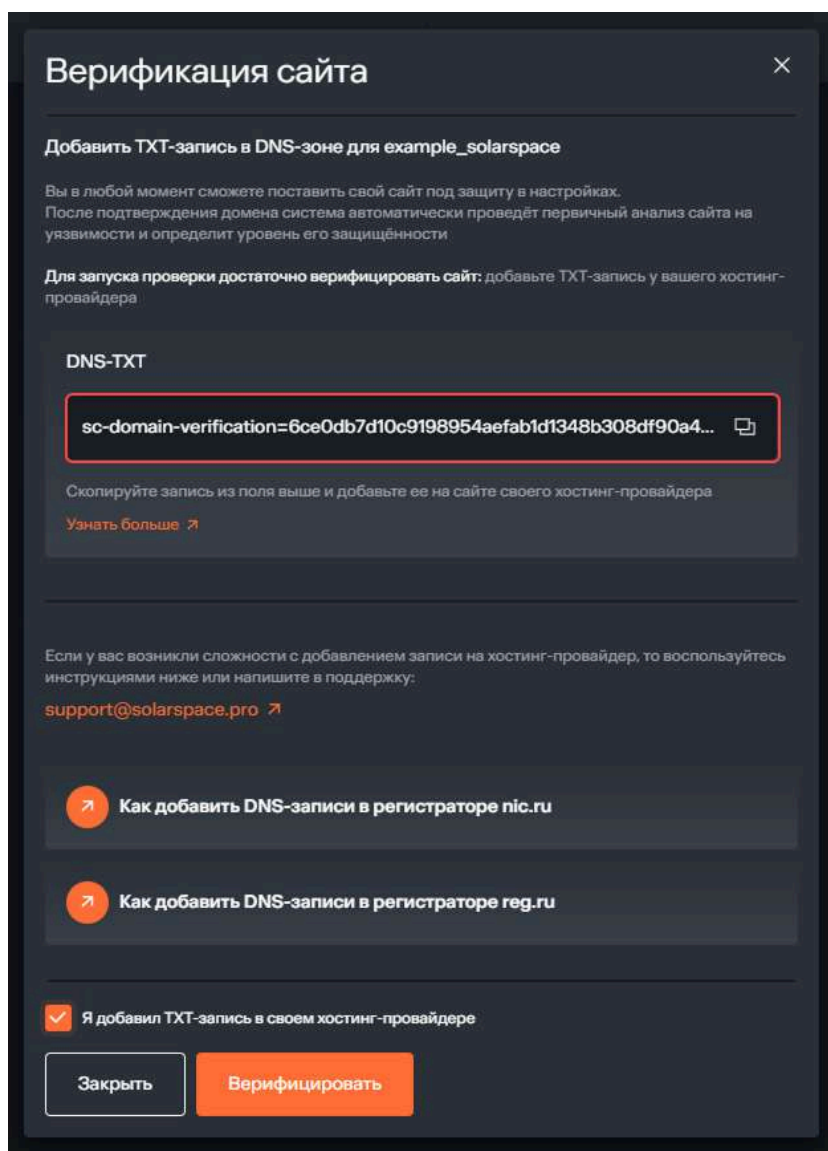
Верификация домена (TXT-запись)

- ❗ Этот шаг необязателен.

В большинстве случаев достаточно изменить A-запись у регистратора — этого хватает для подключения защиты и подтверждения домена. TXT-запись используется для подтверждения домена и позволяет использовать сервисы сканирования без изменения DNS A-записей и перевода трафика.



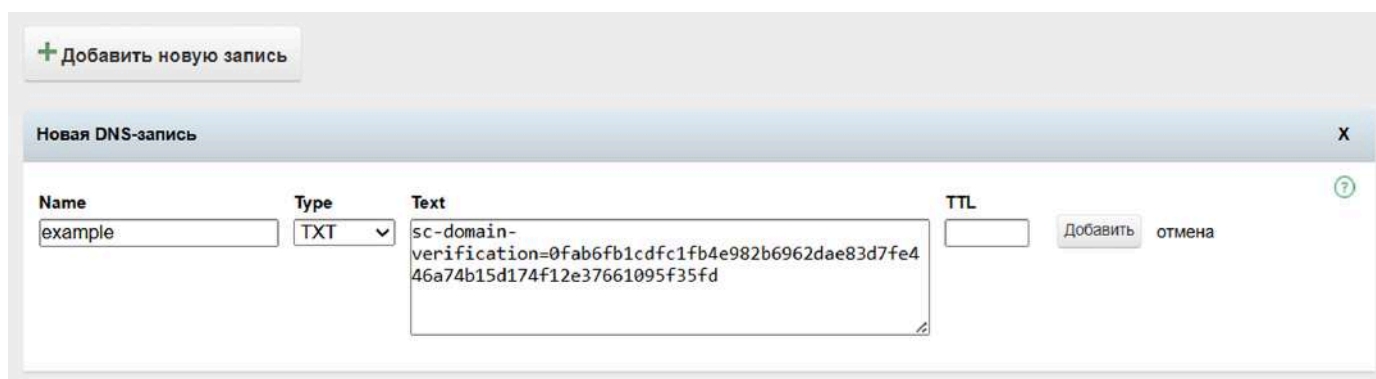
Верификация через DNS-TXT используется только при необходимости. Если в настройках ресурса отображается блок DNS-TXT или вам рекомендовали добавить TXT-запись, выполните действия ниже.



1. Откройте DNS-настройки у вашего DNS-провайдера или DNS-регистратора

2. Найдите раздел управления записями (например: «DNS», «Zone Editor», «Редактировать записи»)
3. Нажмите «**Добавить запись**», выберите тип **TXT**
4. Заполните поля новой **TXT** записи:
 - **Имя (Host):** @ (в DNS это означает корневой домен — например, @ = example.ru)
 - **Тип (Type):** TXT
 - **Значение (Value):** скопированный код из графы DNS-TXT в настройках ресурса
 - **TTL:** оставьте значение по умолчанию

Сохраните запись. Ознакомьтесь с примером готовой TXT-записи:



❗ Если у вас уже есть другие TXT-записи (например, для почты или верификации других сервисов), просто добавьте новую запись для. Это **не повлияет** на работу остальных сервисов — TXT-записи могут сосуществовать независимо друг от друга.

Запуск проверки

После того как вы добавили TXT-запись у регистратора, **вернитесь в кабинет и нажмите кнопку «Верифицировать»** — это необходимо для запуска процесса подтверждения.

❗ Проверка занимает от 1 минуты до 1 часа — зависит от скорости обновления DNS у вашего провайдера. Когда домен будет верифицирован, вы получите письмо на e-mail.

Возможные ошибки и их решение

Домен не подтверждается (TXT)

- TXT-запись создана в корне зоны ([@](#)), значение скопировано **целиком**.
- Нажата кнопка «**Верифицировать**» в кабинете.
- Прошло менее 60 минут на обновление DNS.
- Инструкции у регистраторов: [NIC.RU](#), [REG.RU](#).

Сайт не открывается

- Изменена только **A-запись** для [@](#) , поддомены не трогались.
- Удалены **AAAA (IPv6)** для корня домена.
- IP из поля **DNS-A** указан без ошибок.
- В *Целевом IP* выбран корректный [порт/схема][215#additional-features]).

LE-сертификат не выпускается

- Домен подтверждён по TXT и трафик направлен A-записью.
- В *WEB-защите* в поле **SSL** выбран «**Бесплатный сертификат (LE)**».
- Подождите 5–15 минут и повторите.
- Для своего сертификата: [Как добавить локальный SSL](#).

Antibot / WAF Lite не включаются

- Включите базовый сервис **AntiDDoS**.

Статус «Ресурс на проверке»

- Подождите до 1 часа и снова нажмите «**Верифицировать**».

Дополнительно: краткие разборы — в [FAQ](#).

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:

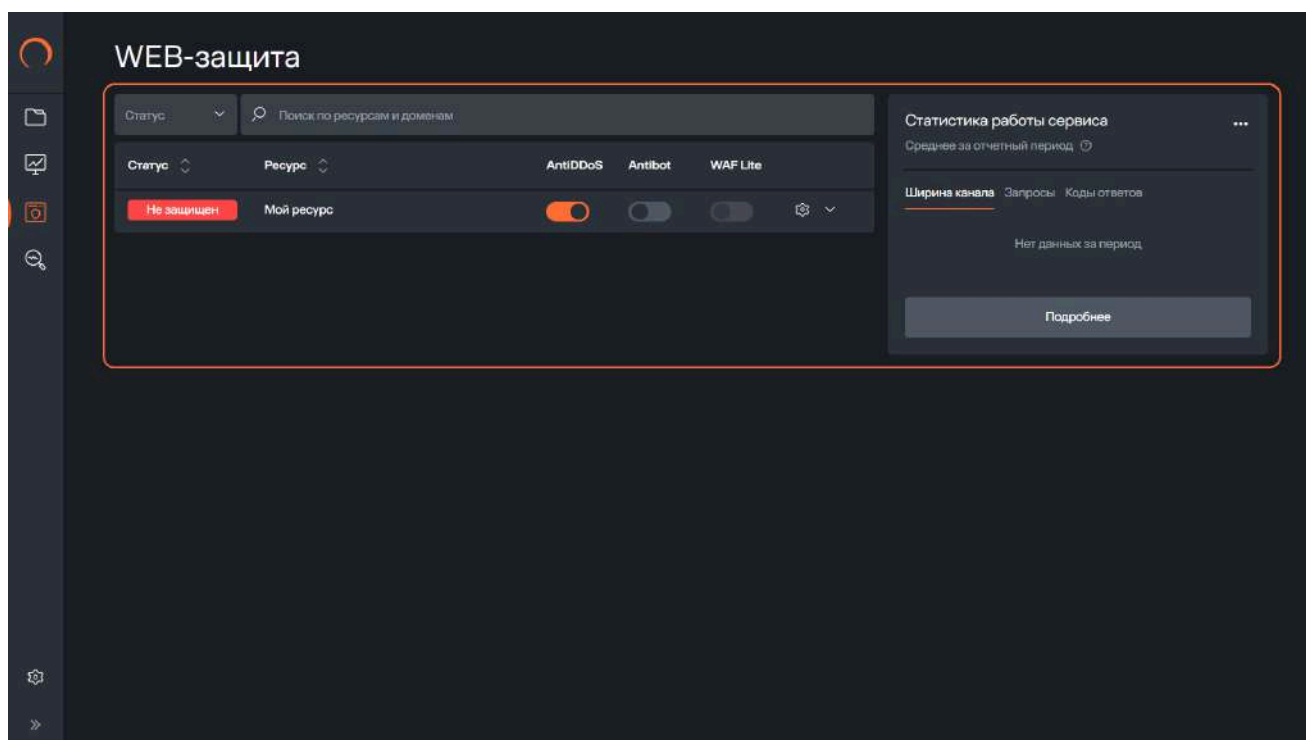
- **WEB AntiDDoS**
- **WEB Antibot**
- **WAF Lite**

В основе работы веб-защиты от Solar Space лежит механизм reverse proxy – обратного прокси-сервера. Это означает, что для постановки веб-ресурса под защиту нужно заменить его IP-адрес на IP-адрес нашего сервера. Таким образом весь входящий трафик сначала перенаправится на сервер защиты Solar Space. Сервисы проанализируют и очистят его, после чего "пропустят" к сайту только легитимные запросы.

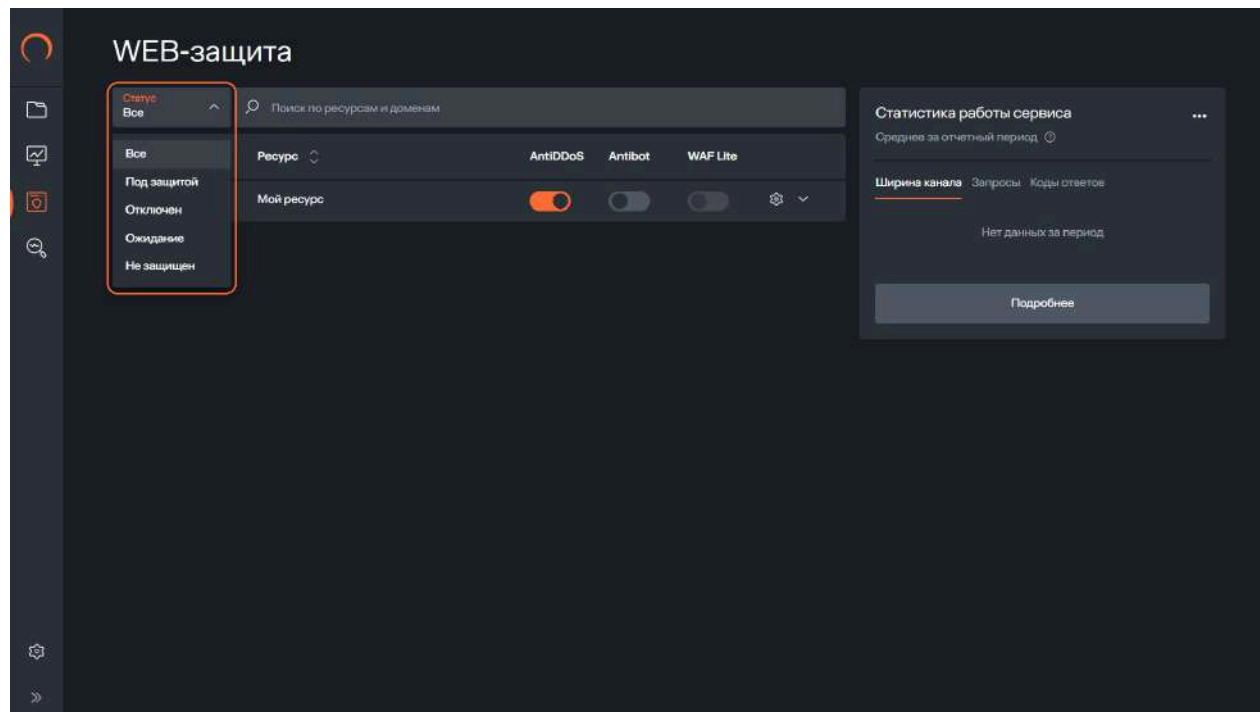
Вы можете выбрать один из 3 уровней защиты:

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

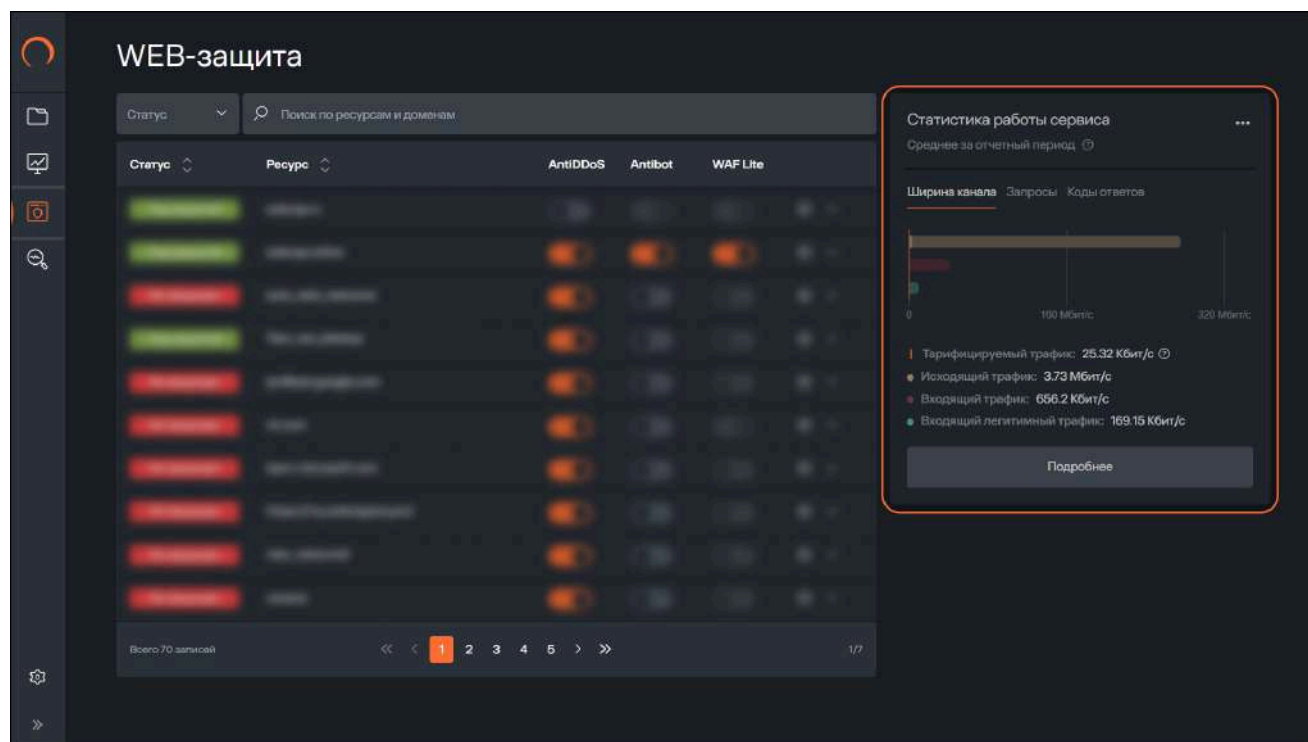


⚠ Обратите внимание

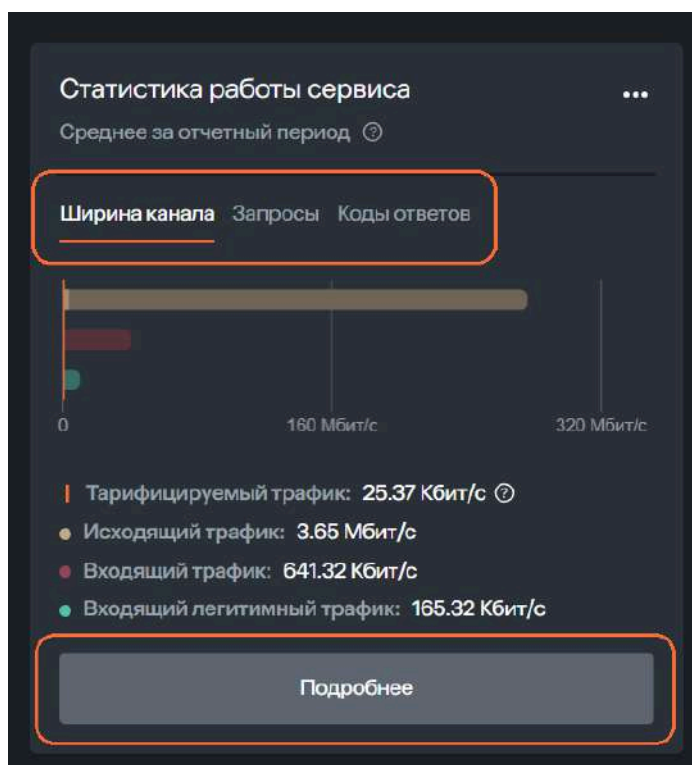
Для наиболее эффективной защиты веб-ресурсов рекомендуется подключать все три сервиса. Они отражают разные виды атак и в комплексе обеспечивают эшелонированную (многоуровневую) защиту

Статистика

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

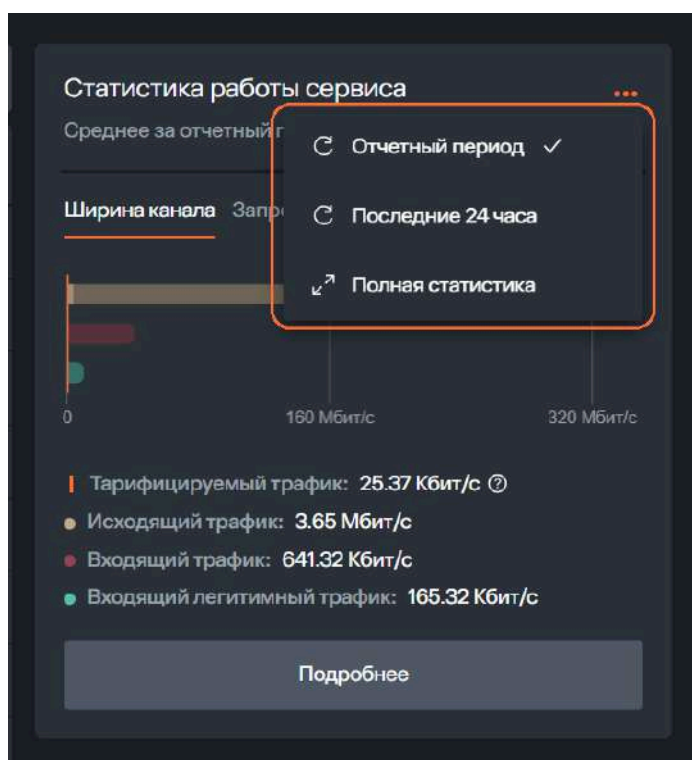


В блоке отображается три вкладки: "Ширина канала", "Запросы" и "Коды ответов". На каждой из них есть кнопка "Подробнее".

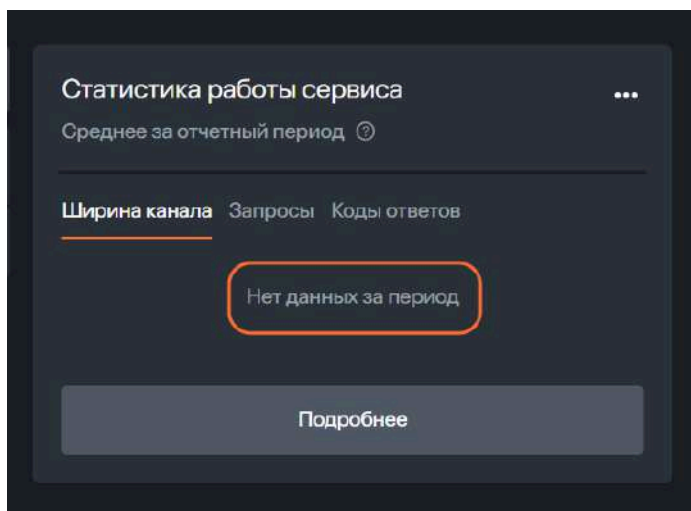


При нажатии на кнопку "Подробнее" вы перейдете на аналогичную вкладку страницы **Статистика** с подробным отчетом по этому параметру – ширине канала, запросам или кодам ответов.

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.

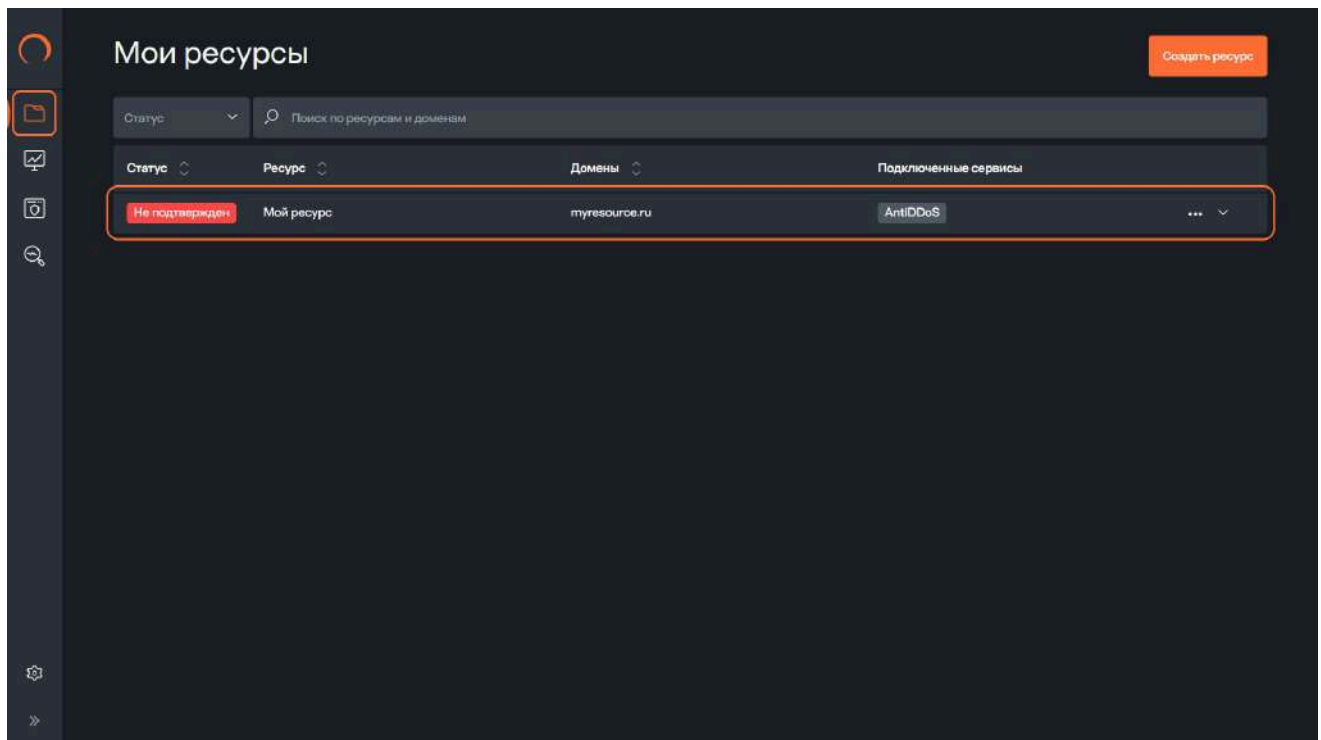
Полная статистика — переход на страницу "[Статистика](#)" с подробными отчетами.

Настройки сервисов

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

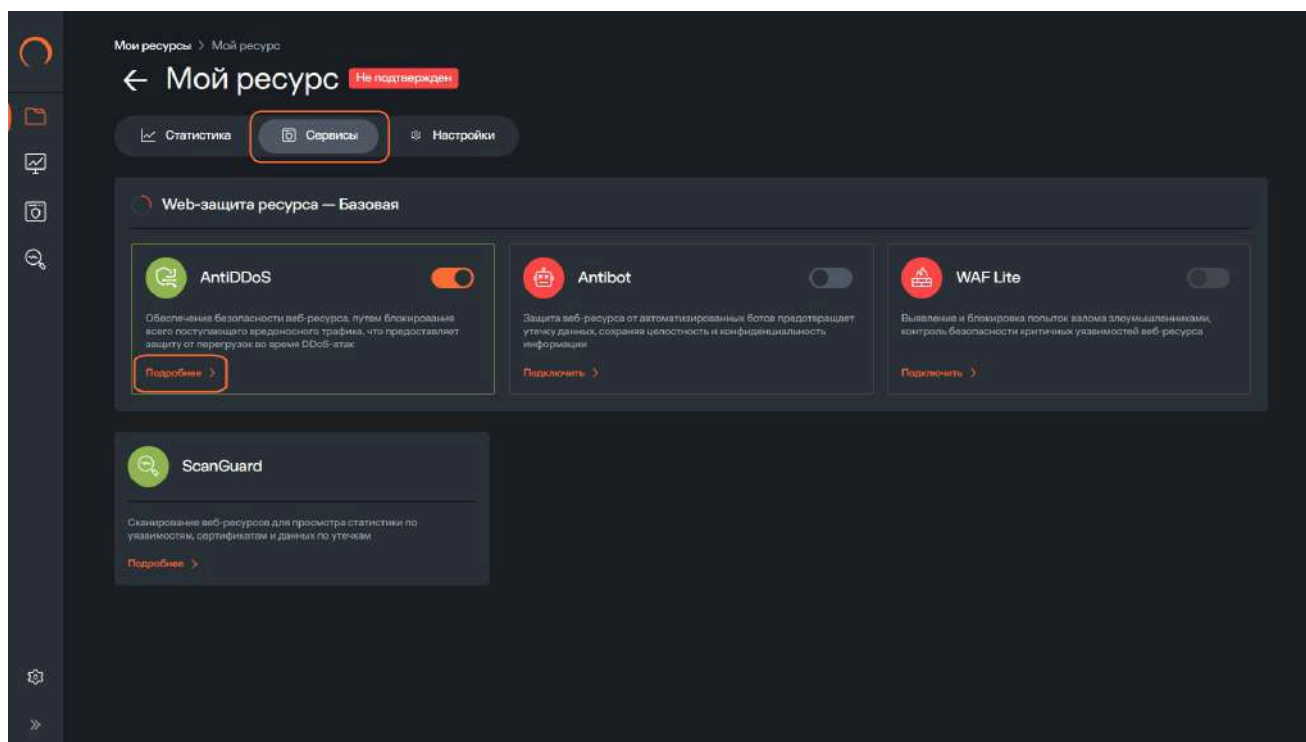
1 способ

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



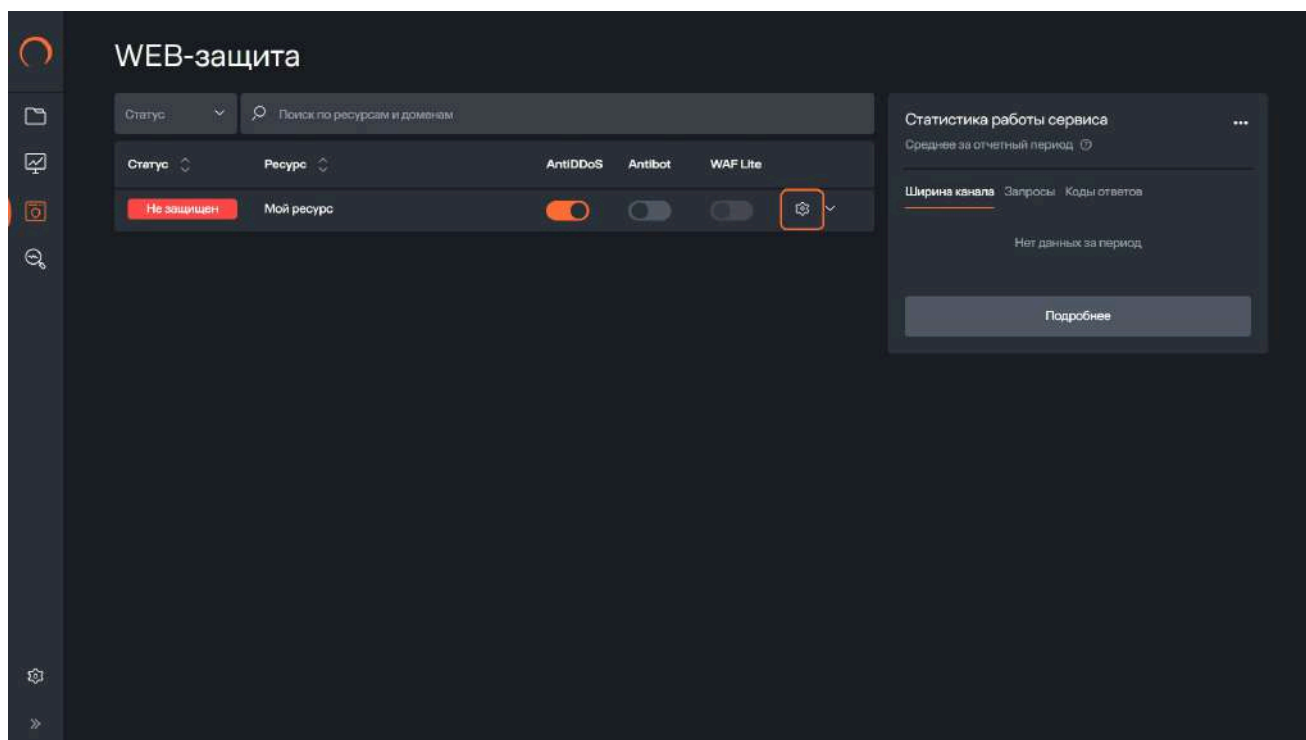
Вы перейдете на страницу ресурса, где вам нужно открыть вкладку "Сервисы". На вкладке "Сервисы" нажмите на кнопку "Подробнее" в блоке активного сервиса, чтобы перейти на

страницу настроек защиты.



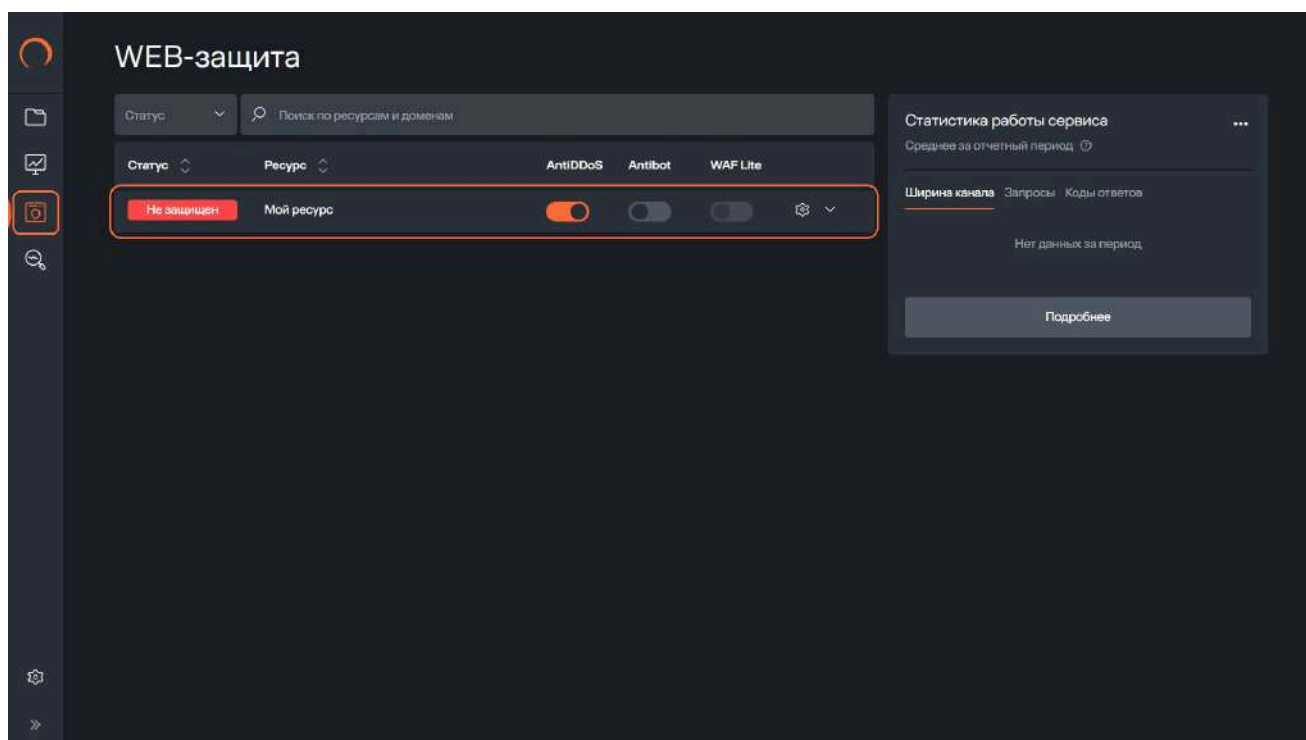
2 способ

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



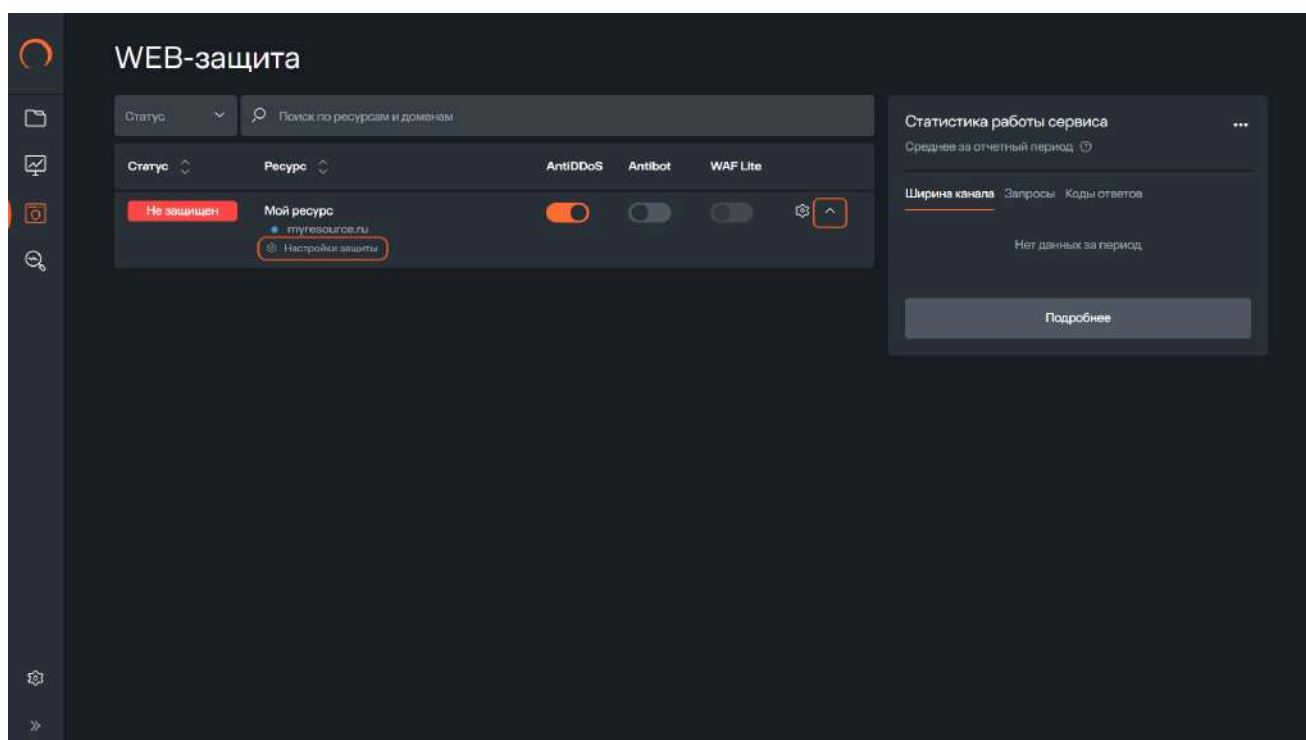
3 способ

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

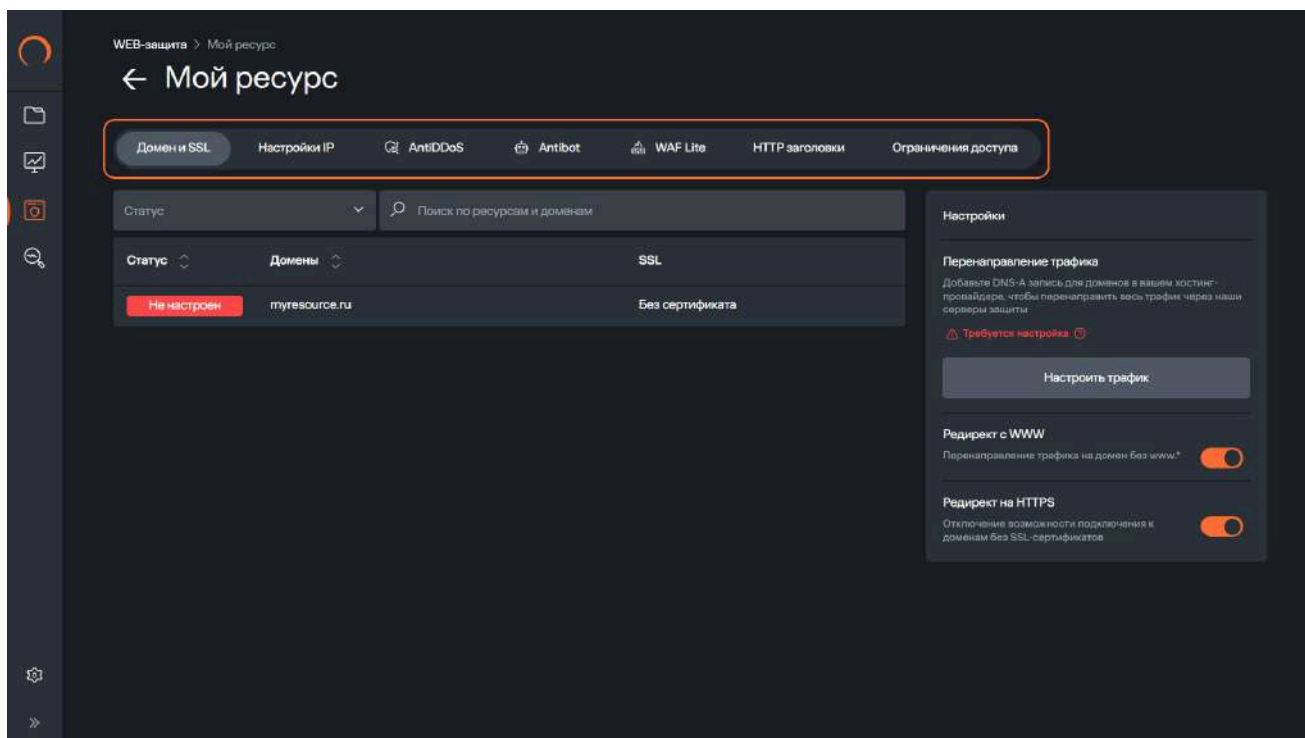


4 способ

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 отражает атаки массовыми запросами на уровне L7 модели OSI и формирует «первую линию обороны» для Antibot и WAF Lite.

DDoS-атака — это попытка вывести сайт из строя за счёт массовой отправки запросов. Злоумышленник использует большое количество устройств (ботнет), чтобы перегрузить ресурс, занять его каналы связи или исчерпать вычислительные мощности.

Типичные проявления DDoS-атаки:

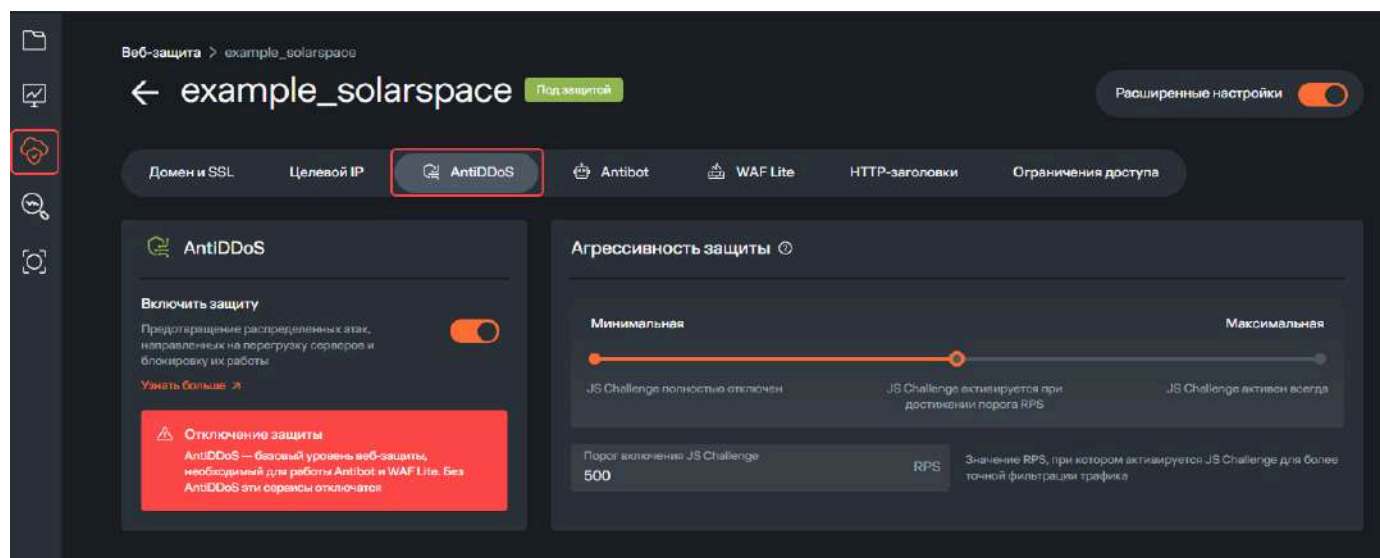
- сайт начинает работать медленнее обычного;
- страницы загружаются с задержкой или не открываются вовсе;
- сервер утилизирует ресурсы на обработку вредоносного трафика, а не реальных пользователей.

AntiDDoS анализирует входящий трафик в реальном времени, определяет подозрительные запросы и блокирует их, поддерживая стабильную работу ресурса. трафик в реальном времени, определяет подозрительные запросы и блокирует их.

⚠ Важно

AntiDDoS — обязательный уровень защиты. Без него недоступны [WEB Antibot](#) и [WAF Lite](#).

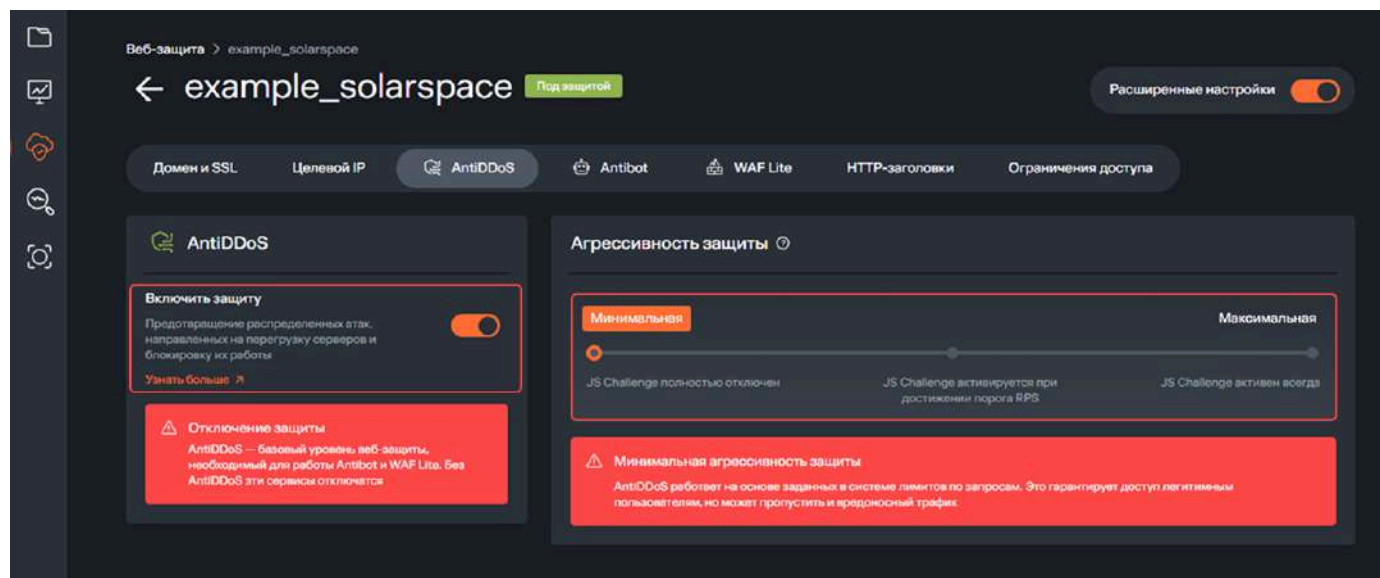
На вкладке **AntiDDoS** отображаются ключевые элементы управления сервисом: переключатель активации, статус защиты и блок «**Агрессивность защиты**».



После активации AntiDDoS начинает отслеживать входящий трафик и применять выбранный уровень реагирования.

Включение защиты

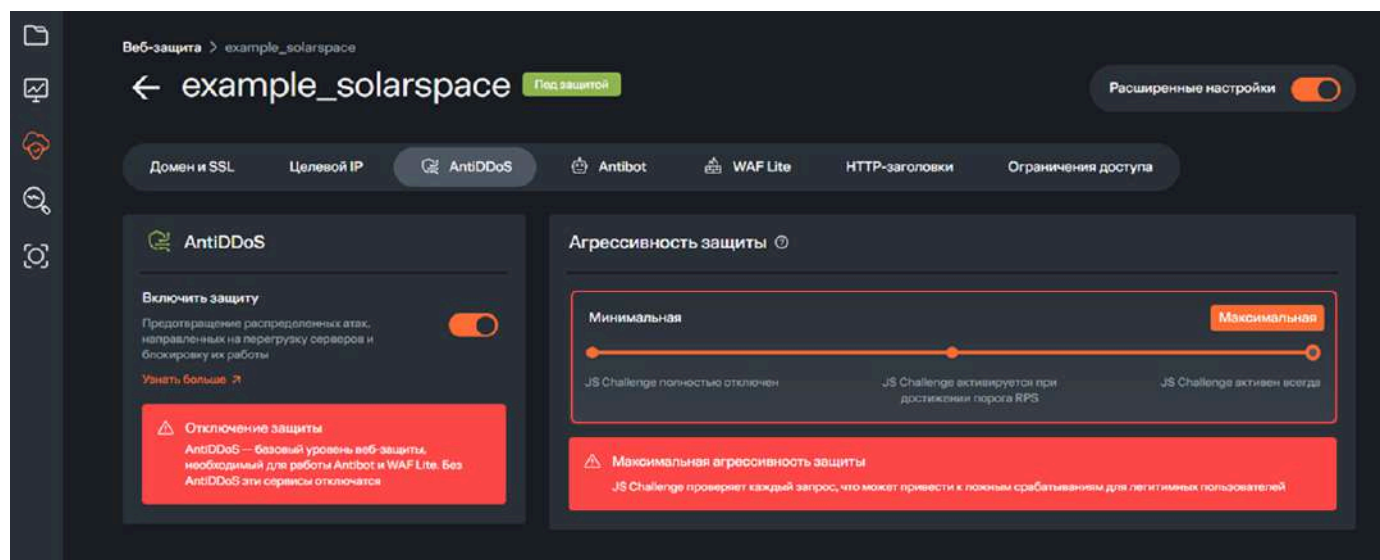
AntiDDoS можно активировать тумблером в левой части интерфейса.



После включения:

- сервис начинает анализ запросов в режиме реального времени;
- фильтруется трафик, который превышает допустимую частоту обращений;
- доступные модули зависят от состояния защиты.

Если AntiDDoS отключить, появится предупреждение о невозможности работы других сервисов:



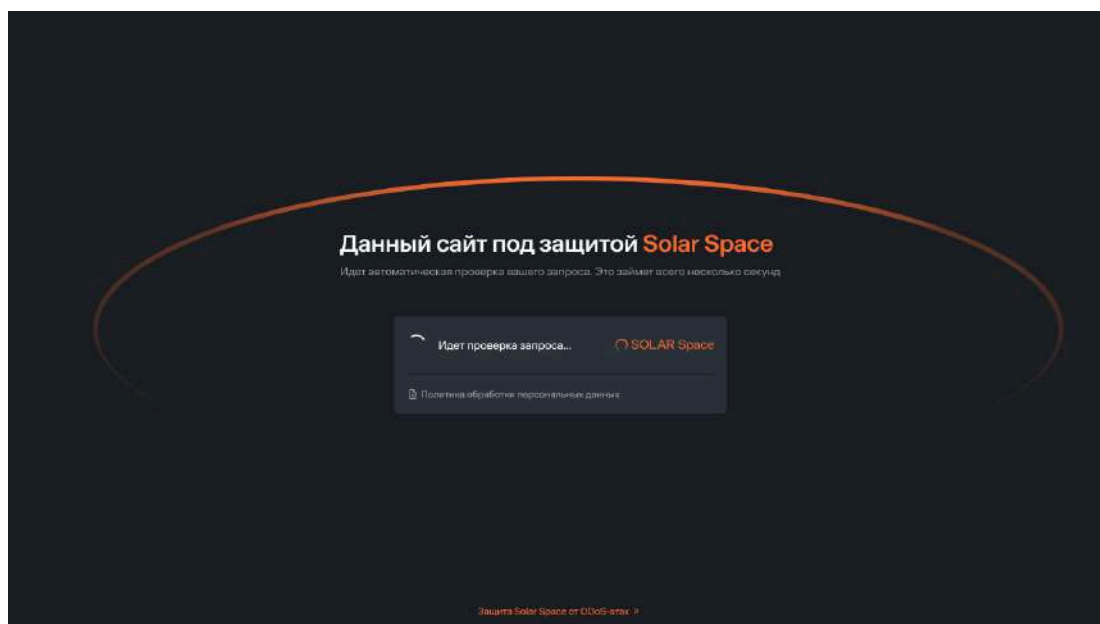
Механизмы защиты

AntiDDoS использует единую логику фильтрации трафика, которая состоит из трёх уровней реакции. Механизмы не работают по отдельности — они дополняют друг друга и включаются в зависимости от нагрузки и поведения трафика.

1. Лимиты запросов Сервис контролирует связку «IP-адрес + путь». Если частота запросов превышает допустимое значение, источник получает `429 Too Many Requests`. Лимит обновляется каждую секунду, поэтому честный пользователь не сталкивается с длительными блокировками, а флудеры — отсеиваются сразу.

2. Интерактивная проверка (JS Challenge) Когда нагрузка выходит за рамки нормальной или поведение выглядит подозрительно, AntiDDoS включает JS-Challenge — браузер выполняет проверочный JavaScript-код. Если код выполнен — пользователь проходит. Если нет — доступ блокируется.

Пример страницы проверки:



3. Агрессивность защиты и порог RPS Эти настройки задают, *когда именно* AntiDDoS будет подключать JS Challenge и как часто.

Уровни агрессивности:

- **Минимальная** — работает только базовый уровень (лимиты запросов).
- **Средняя (по умолчанию)** — JS Challenge включается, если текущий RPS превышает установленный порог.
- **Максимальная** — JS Challenge применяется ко всем запросам.

Порог включения JS Challenge (RPS) используется для средней агрессивности и определяет, при какой нагрузке включается интерактивная проверка. Корректно подобранный порог обеспечивает баланс между удобством для пользователей и эффективностью фильтрации.

Работа AntiDDoS в цепочке защиты

AntiDDoS — первый фильтр в общей системе веб-защиты. На его работу опираются:

- **WEB Antibot** — анализ поведения и фильтрация ботов.
- **WAF Lite** — защита от вредоносных запросов и попыток взлома.

Без активного AntiDDoS последующие уровни защиты недоступны.

Перенаправление трафика

Для включения защиты необходимо поставить домен под **защиту**, обновить **DNS-A запись**, направив домен на защитный IP. Пока трафик не перенаправлён — защита не работает.

Фильтрация выполняется за доли секунды и не влияет на скорость загрузки сайта.

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, сканируют страницы, замедляют работу сайта, спамят в комментариях и формах, а также негативно влияют на поведенческие показатели, оцениваемые поисковыми системами.

WEB Antibot анализирует трафик, прошедший через фильтрацию WEB AntiDDoS, и определяет, отправил запрос человек или бот. При каждом обращении к сайту пользователь передаёт определённый набор параметров, который анализируется алгоритмами машинного обучения для вычисления вероятности того, что запрос отправлен роботом.

- Если вероятность ниже порогового значения — запрос определяется как человеческий и пропускается к сайту.
- Если вероятность выше порогового значения — сервис предполагает, что запрос отправил бот, и предлагает пройти капчу. Если капча пройдена, запрос пропускается, если нет — блокируется.

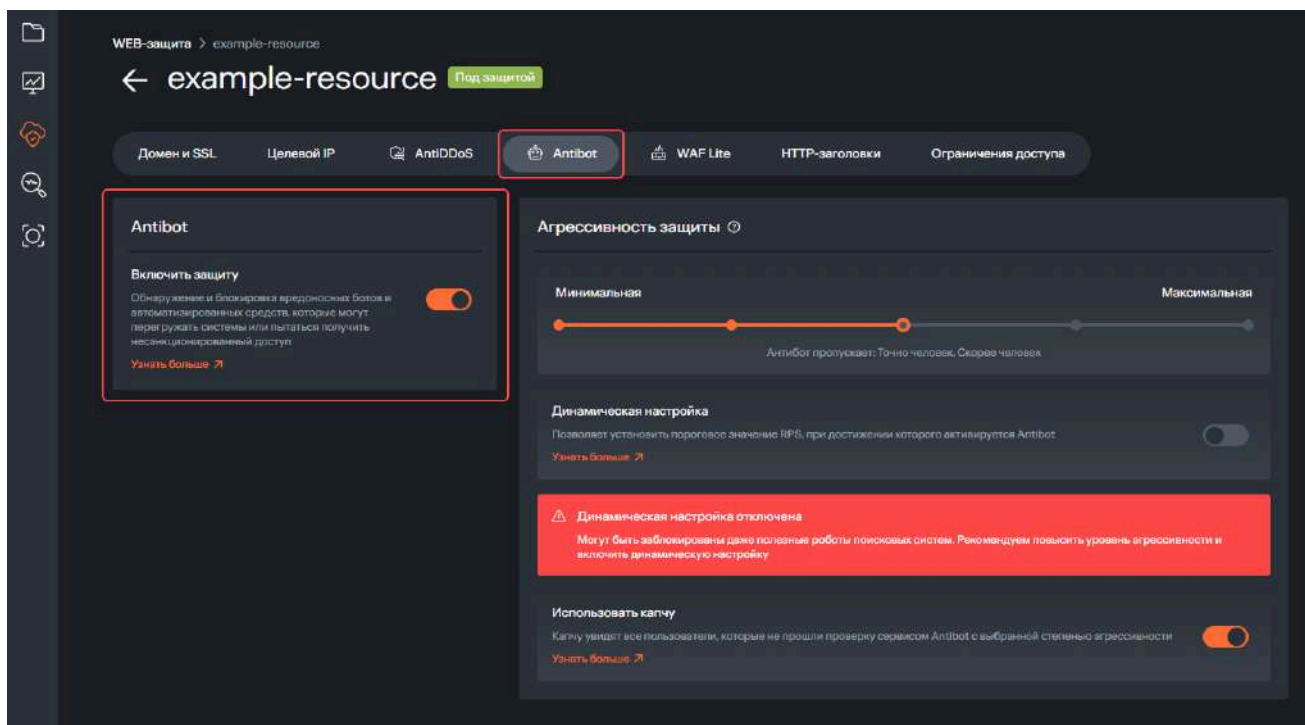
Платформа распознаёт трафик поисковых роботов Yandex и при подтверждённой идентификации источника не предъявляет им интерактивные проверки (например, капча). Идентификация выполняется по FCrDNS: проверяется обратное разрешение имени (rDNS/PTR) и подтверждается прямым разрешением этого же имени на тот же адрес. Из-за ротации адресов поисковых систем фиксировать публичные IP-списки нецелесообразно; приоритет отдаётся DNS-верификации.

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

WEB Antibot не защищает от таких атак, как SQL-инъекции или межсайтовый скриптинг (XSS). Эти атаки используют уязвимости веб-ресурса для кражи данных, подмены контента или взлома аккаунтов. Для защиты от них рекомендуется использовать **WAF Lite**.

На странице сервиса Antibot доступно краткое описание и переключатель для активации.

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



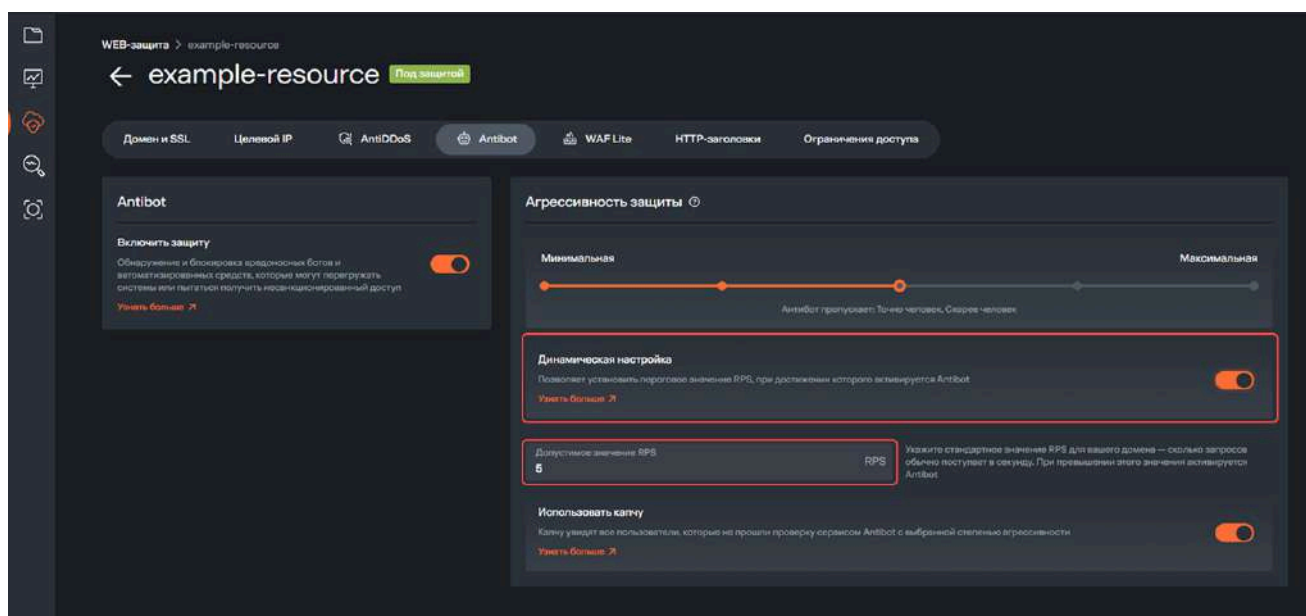
Чтобы активировать его вручную, передвиньте переключатель вправо при соблюдении следующих условий:

- Домены имеют статус «Под защитой» (ресурсы верифицированы и активирован сервис AntiDDoS)
- Для доменов добавлен SSL-сертификат (на вкладке «Домен и SSL»)
- Включён функционал «Редирект на HTTPS» (на вкладке «Домен и SSL»)

Динамическая настройка

Опция «**Динамическая настройка**» позволяет задать порог срабатывания Antibot по количеству запросов в секунду (RPS). Когда реальное число запросов превышает установленное значение, система активирует фильтрацию и начинает проверять трафик с повышенным вниманием.

После включения тумблера появляется дополнительное поле «**Допустимое значение RPS**», где можно указать стандартное количество запросов для вашего домена — сколько обращений обычно поступает в секунду. Рекомендуется установить значение, соответствующее средней нагрузке на сайт: слишком низкий порог приведёт к частым срабатываниям защиты, слишком высокий — снизит её эффективность.



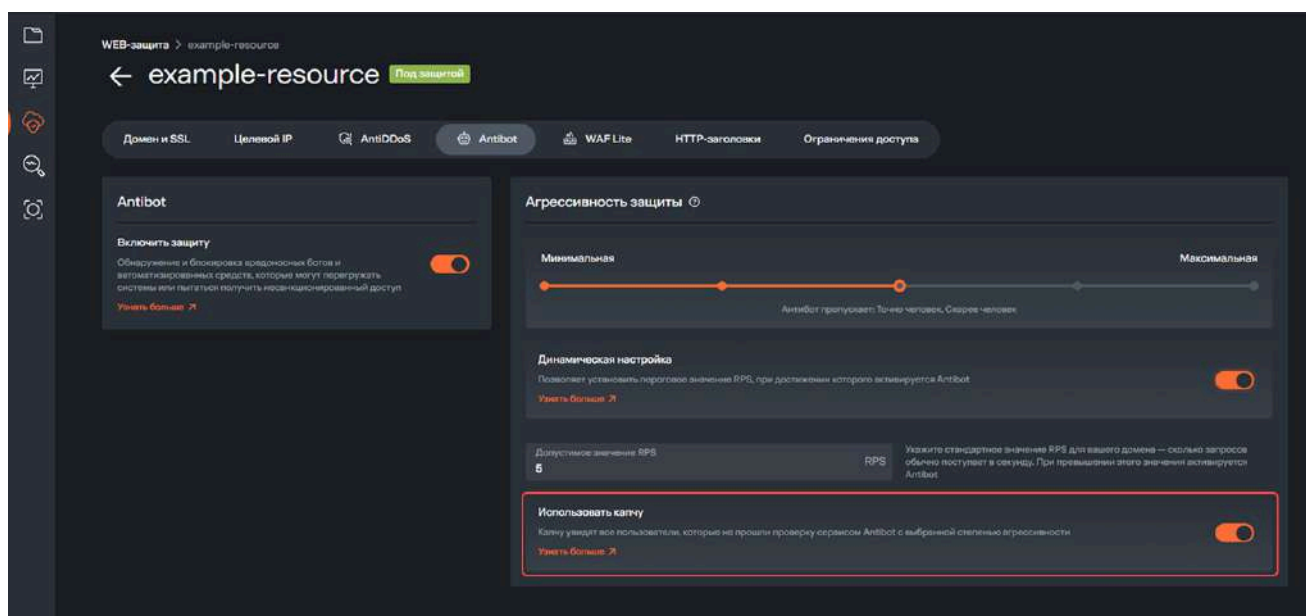
При активированной динамической настройке сервис анализирует поведение пользователей и автоматически корректирует уровень агрессивности защиты в зависимости от текущей нагрузки. Это помогает снизить ложные срабатывания и сохранить стабильную работу ресурса даже при всплесках активности.

После внесения изменений нажмите **«Сохранить изменения»**, чтобы применить новые параметры.

Использовать капчу

Функция **«Использовать капчу»** задаёт дополнительный уровень проверки при срабатывании антибот-фильтра. Когда вероятность того, что запрос отправлен ботом, превышает установленный порог, пользователю отображается капча.

Если капча пройдена — запрос пропускается, если нет — блокируется. Настройка позволяет снизить риск ошибочной блокировки реальных пользователей, сохранив высокий уровень защиты. Рекомендуется включать капчу на сайтах с открытыми формами, регистрацией или комментариями.



После изменения состояния тумблера обязательно нажмите **«Сохранить изменения»**, чтобы обновлённые настройки вступили в силу.

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

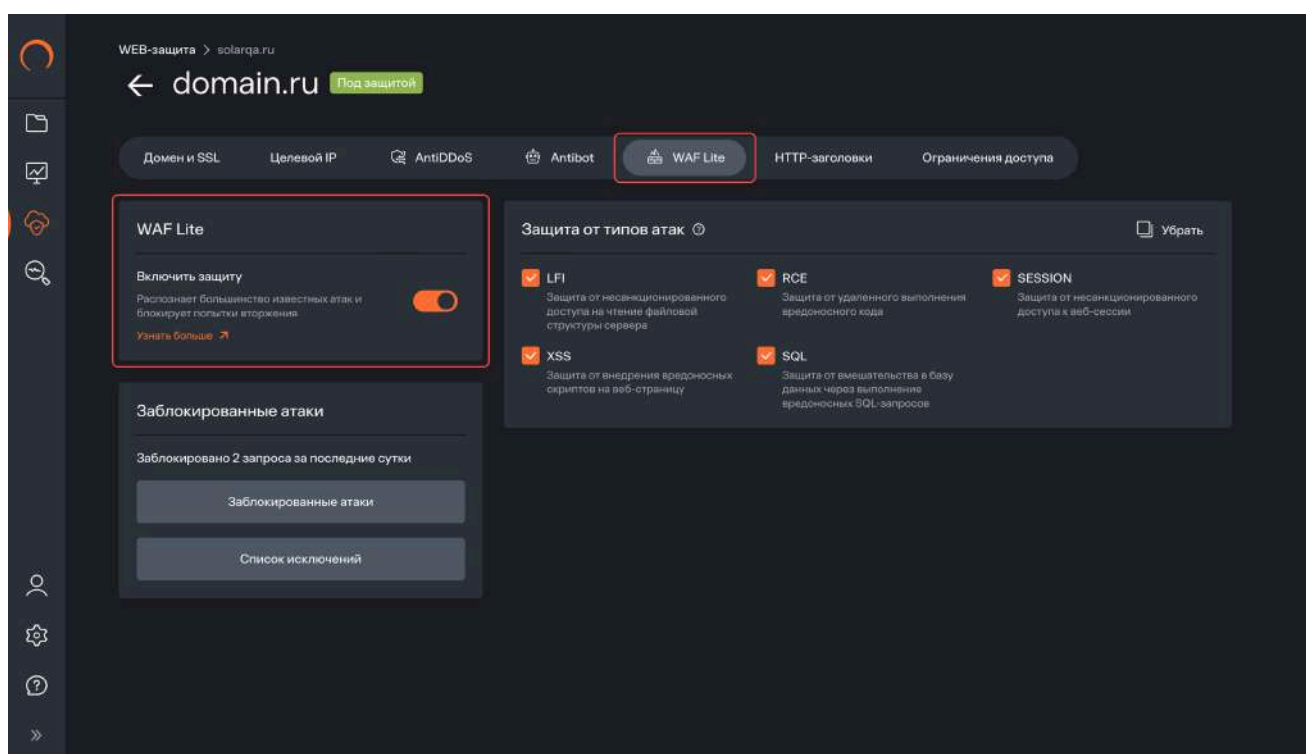
получение доступа к конфиденциальной информации. Для защиты от перехвата сессий используется шифрование сессионных данных и безопасное управление сроком их действия. Это исключает возможность их кражи и повторного использования.

- **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 параметризованные 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 обеспечивают максимальную эффективность комплексной защиты веб-ресурсов

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

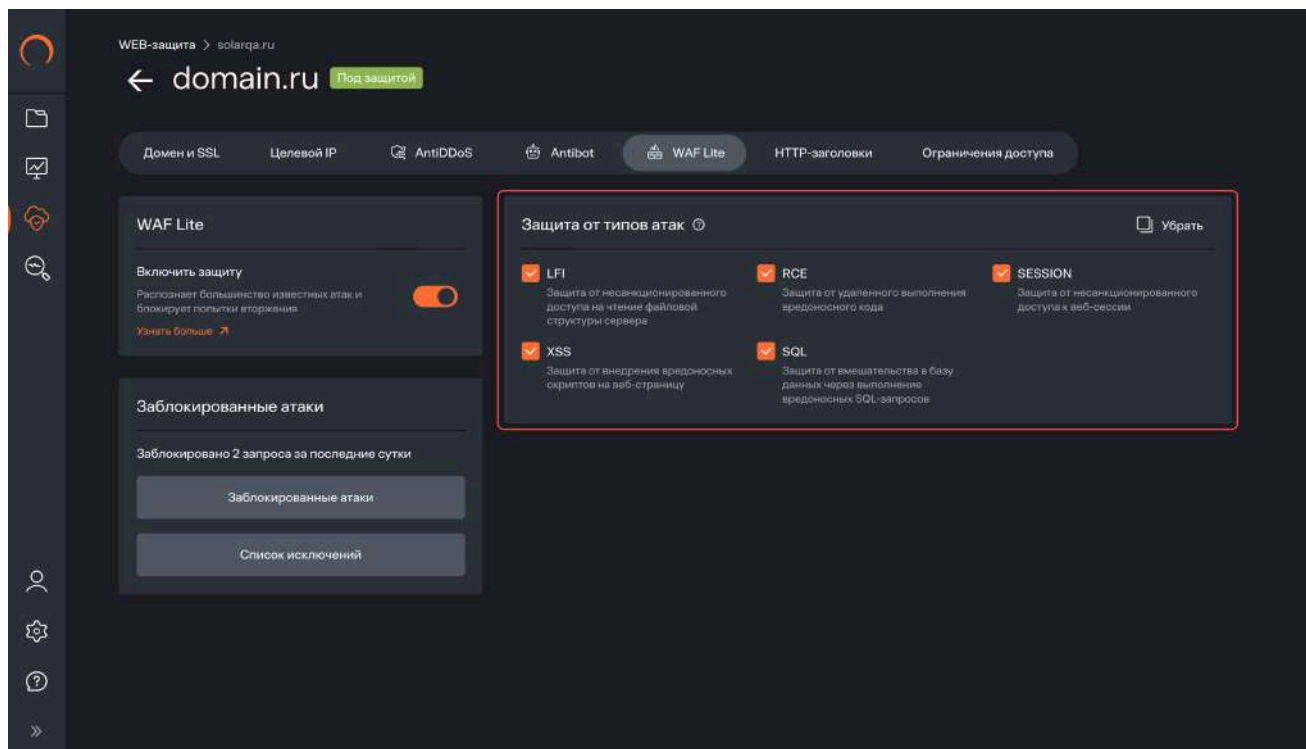


Если вы выбрали версию защиты, в состав которой входит WAF Lite, то ползунок на этой странице уже находится в состоянии "Подключено".

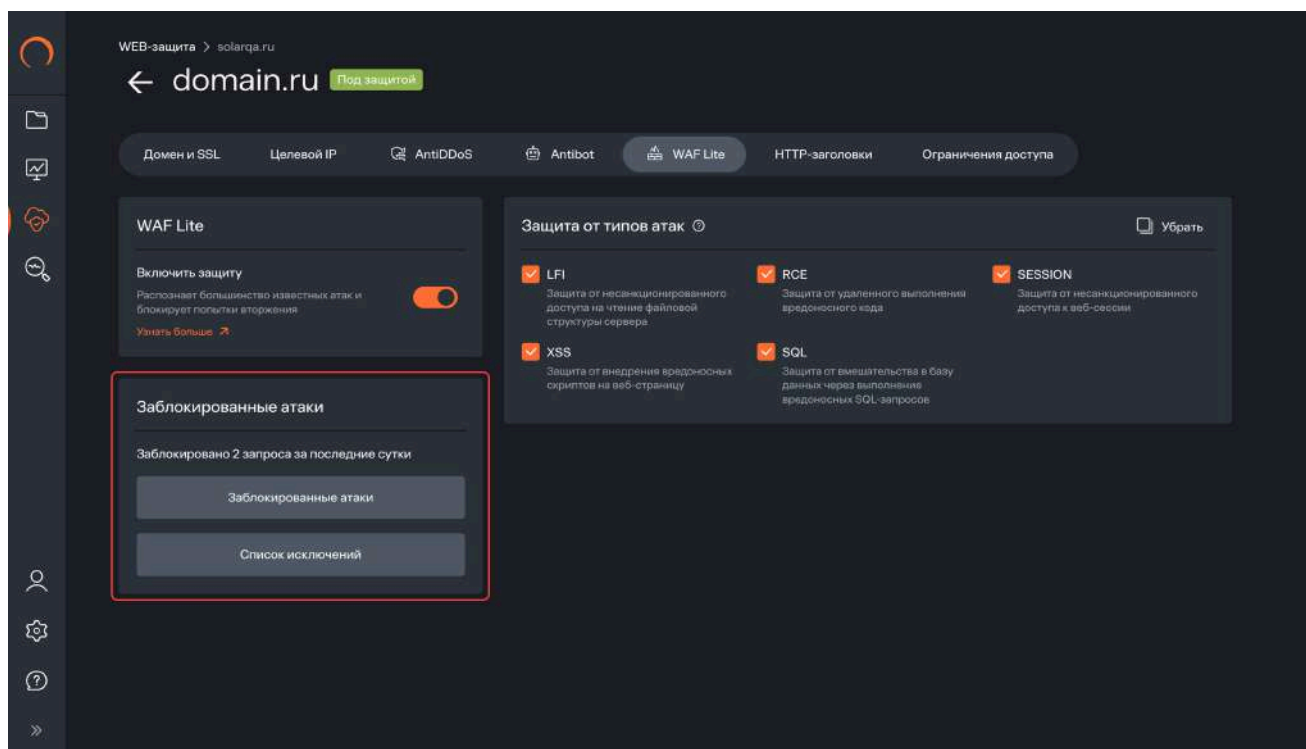
Вы можете активировать WAF Lite при условии, что у вас уже активированы сервисы AntiDDoS и Antibot.

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.

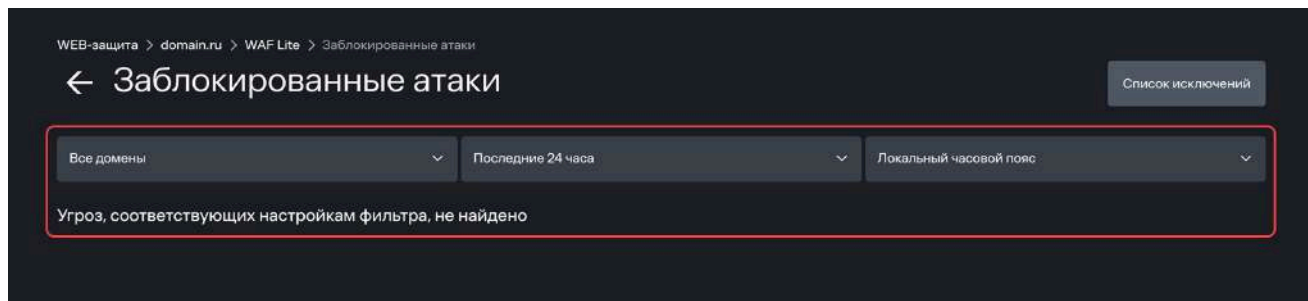


В блоке "Заблокированные атаки" расположены кнопки "Заблокированные атаки" и "Список исключений". При нажатии на них можно просмотреть подробную информацию.



Заблокированные атаки

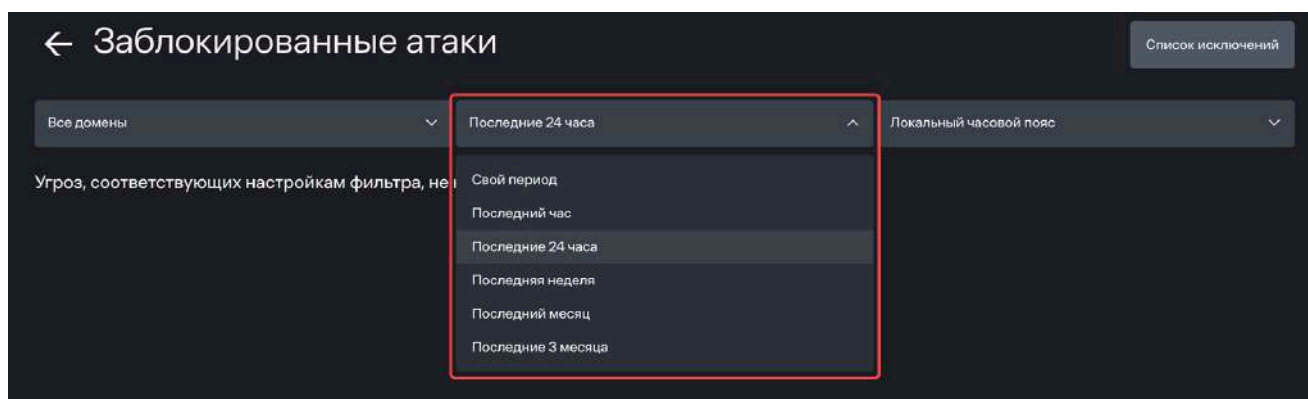
При нажатии на кнопку "Заблокированные атаки" вы перейдете на страницу заблокированных сервисом атак. По умолчанию откроется список за последние сутки, но период можно изменить. Если система не зафиксировала атак за этот период, вы увидите сообщение "Угроз, соответствующих настройкам фильтра, не найдено".



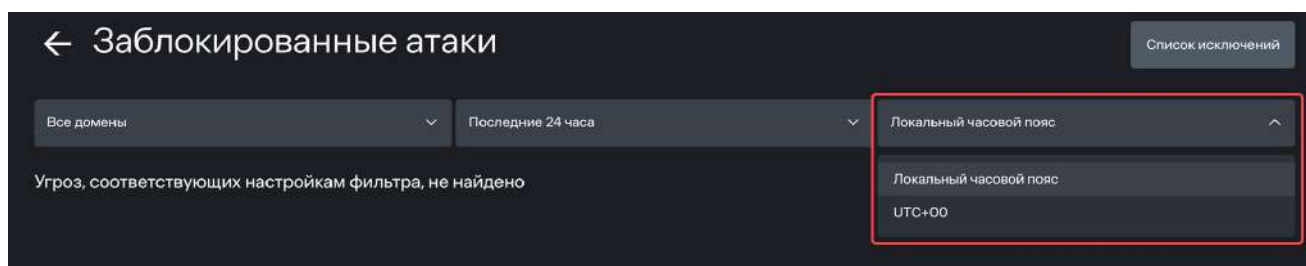
В первом поле можно выбрать ресурсы, для которых будет отображаться отчет.



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:

Дата	Домен	Путь	Сообщения об атаке	Код ответа	Тип запроса
05.03.2025, 04:40	domain.ru	/	HTTP header is restricte...	403	GET
04.03.2025, 20:26	domain.ru	/.env	.	403	GET
04.03.2025, 07:55	domain.ru	/admin/.env	.	403	GET
04.03.2025, 07:55	domain.ru	/.env.example	.	403	GET
04.03.2025, 07:55	domain.ru	/.env.example	.	403	GET
04.03.2025, 07:55	domain.ru	/.aws/credentials	.	403	GET
04.03.2025, 07:55	domain.ru	/.env	.	403	GET
04.03.2025, 07:55	domain.ru	/.env.production	.	403	GET
04.03.2025, 07:55	domain.ru	/.env	.	403	GET
04.03.2025, 07:55	domain.ru	/.aws/credentials	.	403	GET

Всего 135 записей

1 2 3 4 5 > >>

1/14

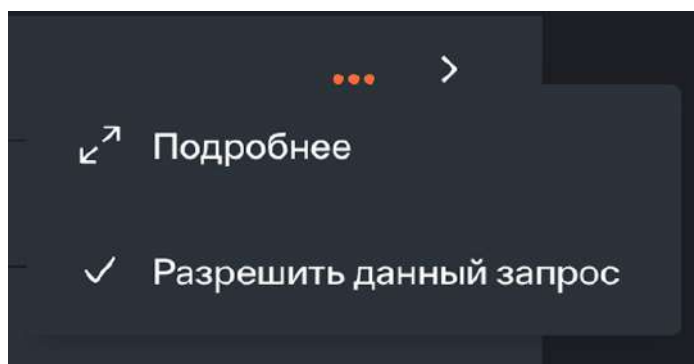
Краткая информация об атаке отражается в следующих полях:

- **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

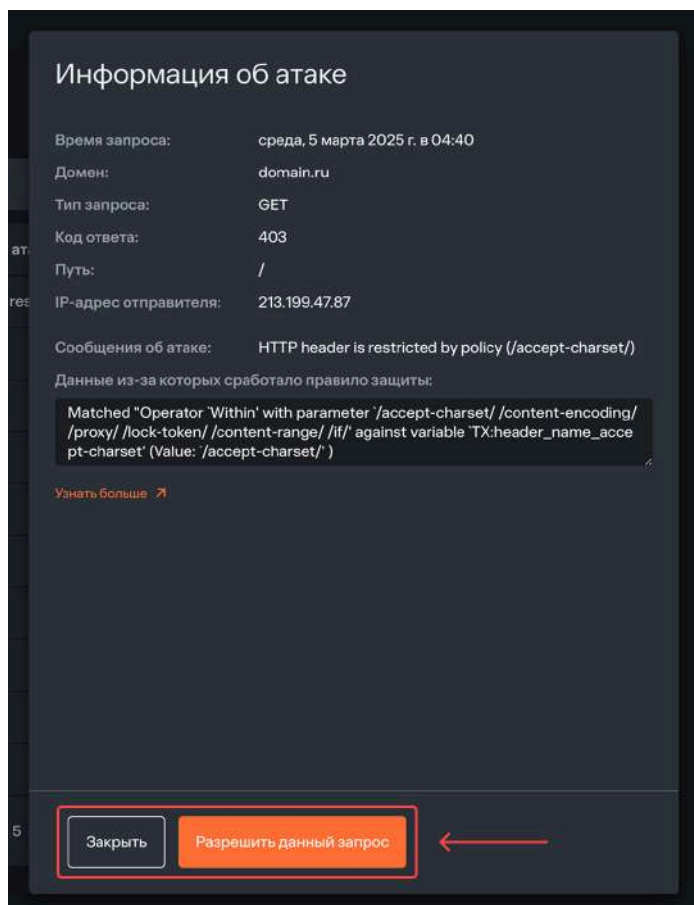
Для всех полей кроме "Сообщения об атаке" доступна сортировка по возрастанию/убыванию.

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

Дата	Домен	Путь	Сообщения об атаке	Код ответа	Тип запроса	
05.03.2025, 04:40	domain.ru	/	HTTP header is restricte...	403	GET	...
04.03.2025, 20:26	domain.ru	/env	.	403	GET	...
04.03.2025, 07:55	domain.ru	/admin/.env	.	403	GET	...



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

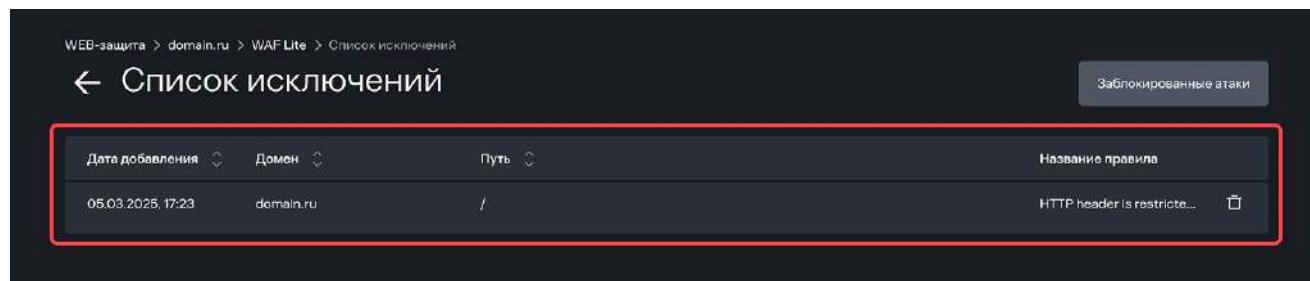


Если нажмете "Закрыть", окно закроется. Если нажмете "Разрешить данный запрос", он пропадет из списка заблокированных атак и в дальнейшем не будет блокироваться при условии, что придет по тому же пути. Также вы можете выбрать вариант "Разрешить данный"

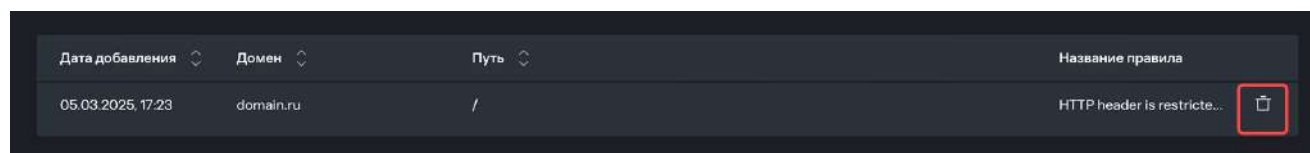
запрос", не открывая это окно. Достаточно нажать на три точки в строке атаки и кликнуть по второму пункту в появившемся меню.

Список исключений

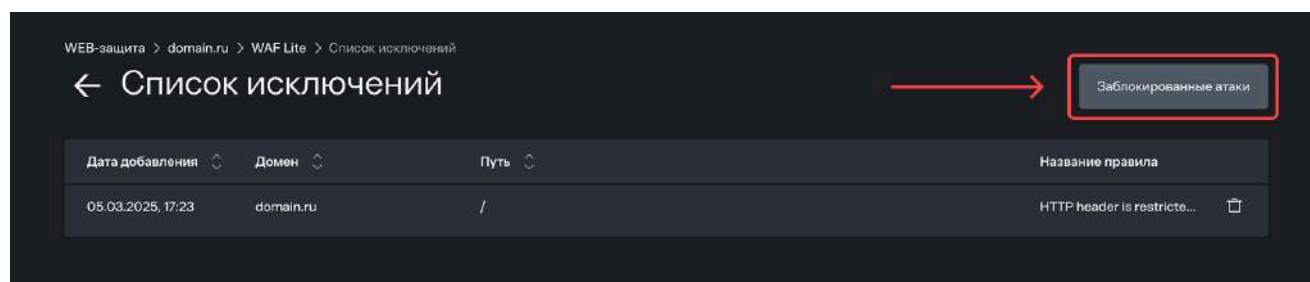
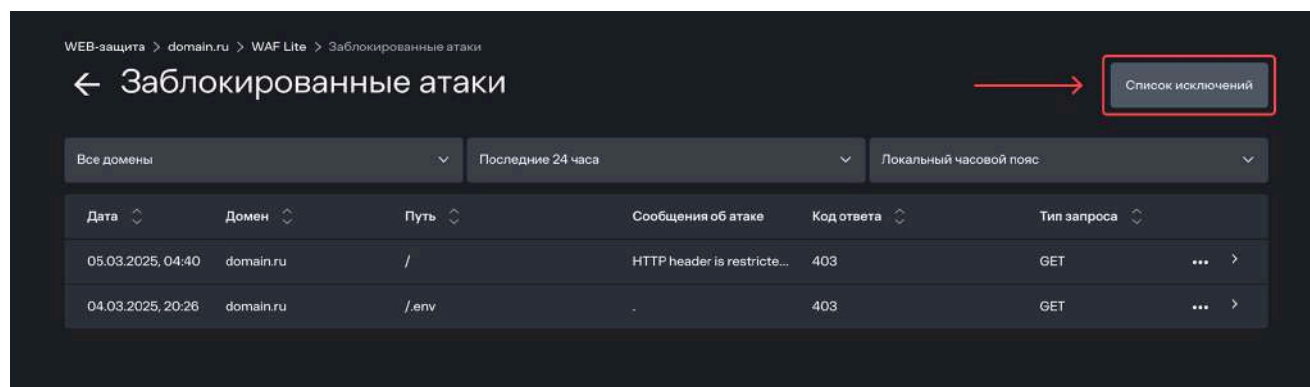
Список разрешенных запросов вы найдете в разделе "Список исключений" на вкладке WAF Lite.



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".



Разрешенные пути WAF Lite

Разрешенные пути — это список URI (адресов или маршрутов внутри веб-приложения), к которым WAF Lite разрешает доступ без проверки.

Как настроить разрешенные пути для WAF Lite

Как это работает:

1. Вы указываете в личном кабинете Solar Space домен и разрешенные пути для него.
2. WAF Lite анализирует путь (URI) входящих HTTP-запросов и сравнивает его с заранее заданным списком разрешенных путей.
3. Если путь входит в этот список, сервис пропускает запрос без проверки.

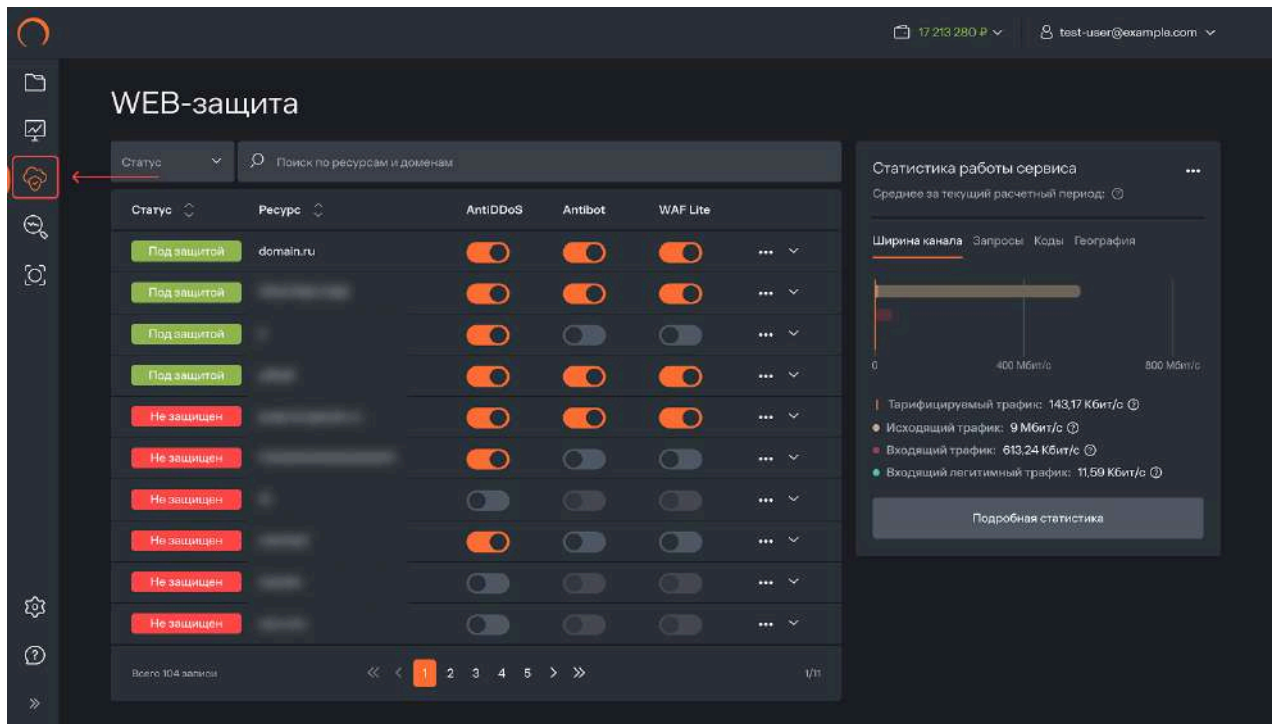
Разрешенные пути позволяют:

- Уменьшить нагрузку на сервер: если известно, что определенные пути безопасны, можно настроить их пропуск без дополнительной проверки, что снизит нагрузку на систему безопасности и ускорит обработку запросов
- Снизить количество ложных срабатываний, если легитимные действия пользователей или автоматизированных сервисов не вписываются в типовые шаблоны поведения

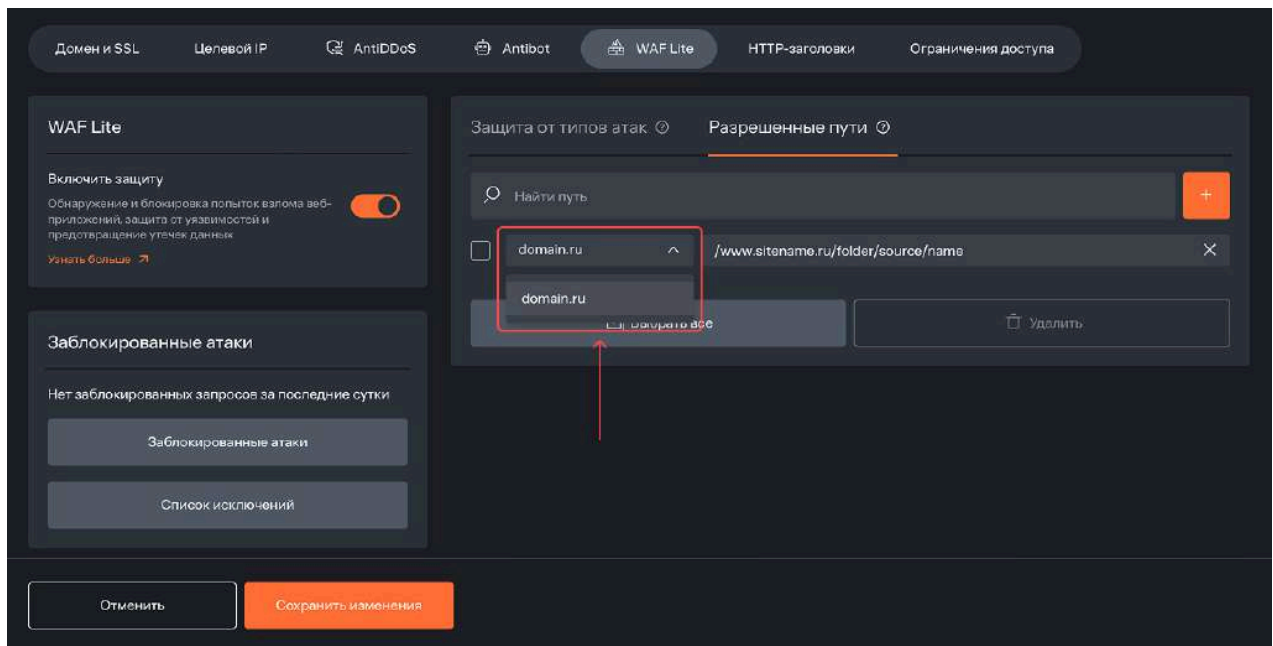
Как добавить разрешенные пути в личном кабинете

Для добавления разрешенных путей выполните следующие действия:

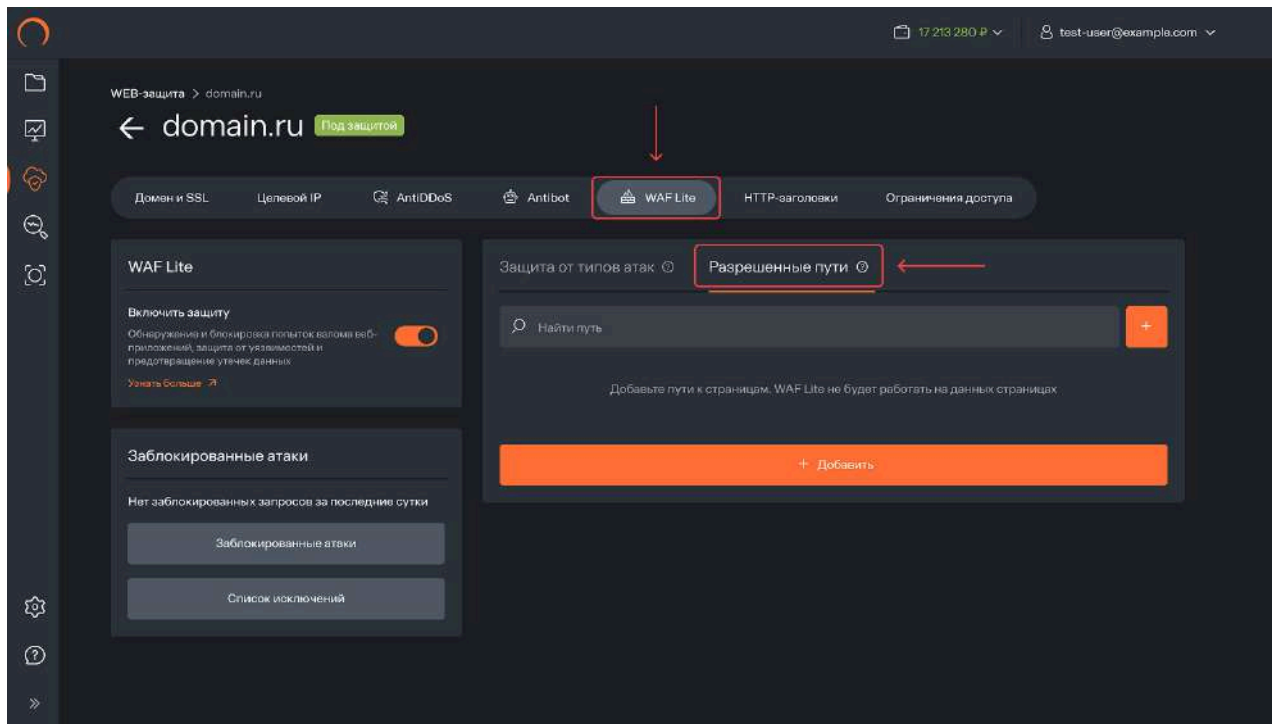
1. Перейдите на вкладку **Веб-защиты**.



2. Откройте нужный ресурс, нажав на его имя.

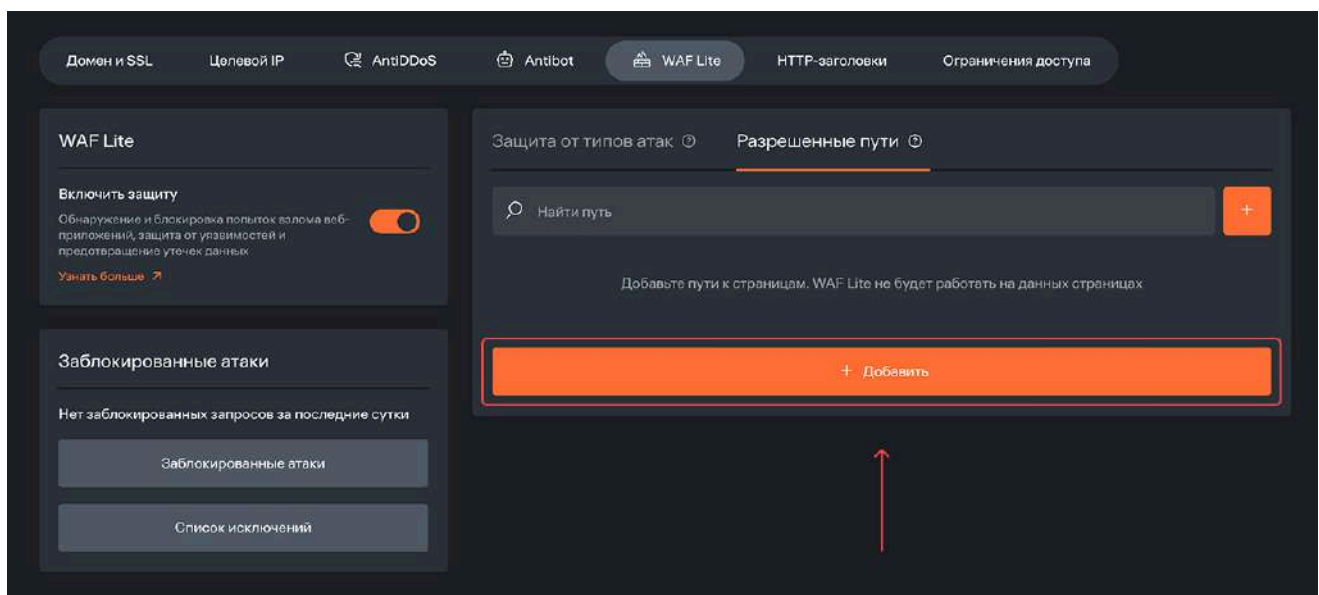


3. Перейдите на вкладку "WAF Lite" и выберите раздел "Разрешенные пути".

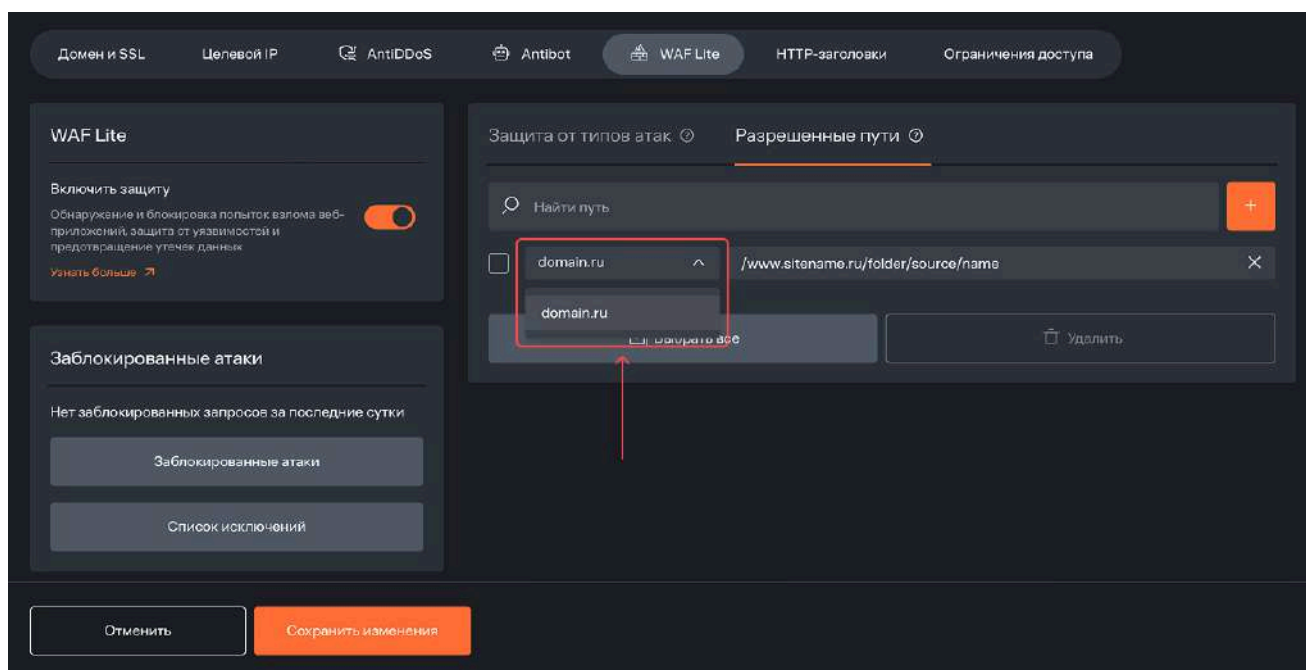


4. Добавьте разрешенные пути вручную:

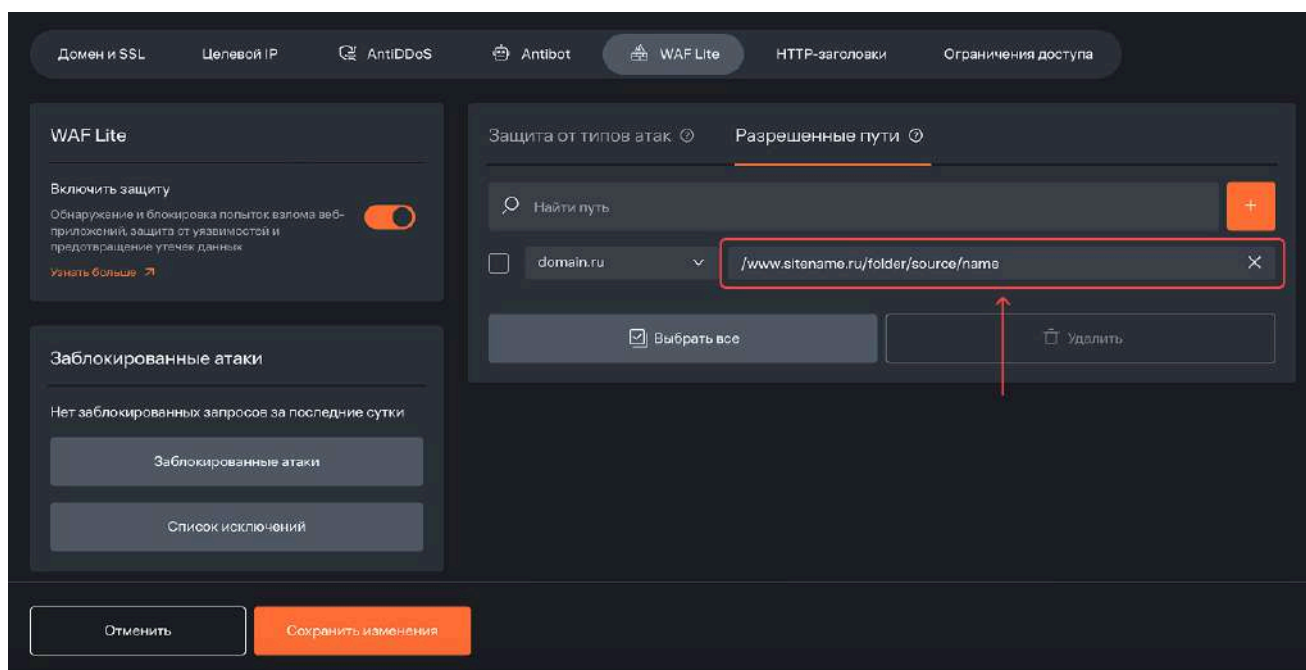
Нажмите на кнопку "Добавить".



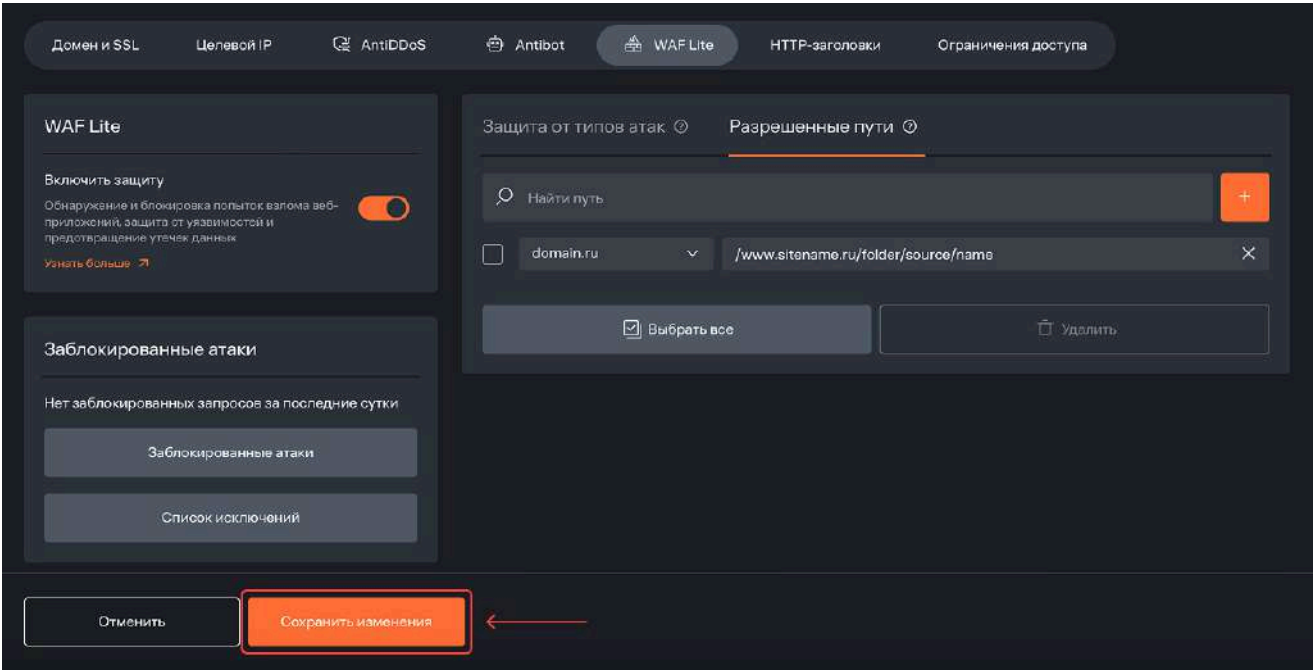
Выберите домен, для которого добавляете разрешенные пути.



Введите название пути в формате `https://www.sitename.ru/folder/source/name` .



Сохраните изменения.



Настройки

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

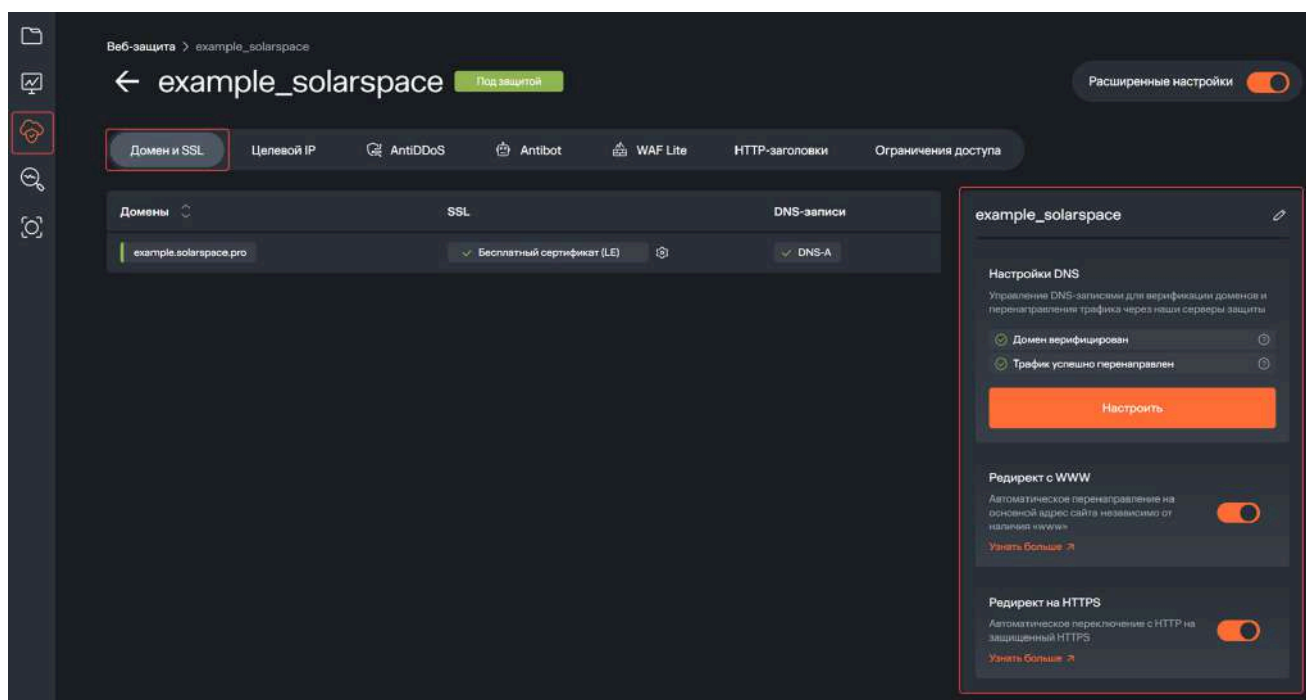
- Домен и SSL
- Целевой IP
- AntiDDoS
- Antibot
- WAF Lite
- HTTP-заголовки
- Ограничения доступа

Домен и SSL

Вкладка «Домен и SSL» предназначена для управления настройками домена: перенаправлением трафика на защиту, подтверждением владения доменом, выпуском и просмотром SSL-сертификата, а также настройками редиректов.

На этой вкладке вы можете:

- Настроить DNS-записи
- Посмотреть SSL-сертификат
- Включить дополнительные настройки

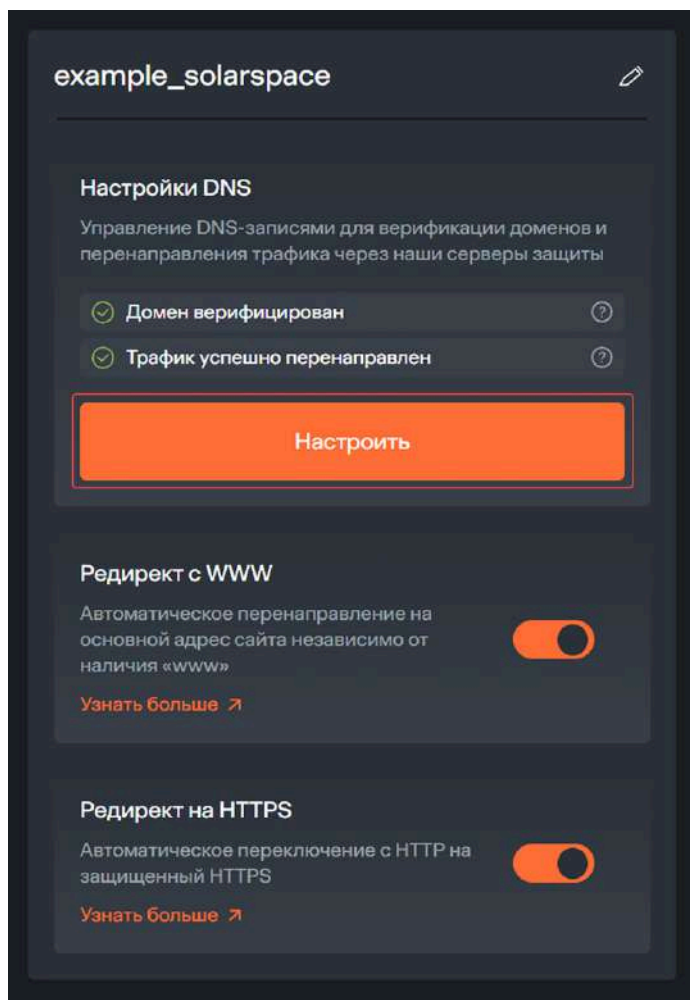


Настройки DNS

В блоке «**Настройки DNS**» выполняются два действия:

1. Перенаправление трафика на защиту — через DNS A-запись.
2. Подтверждение владения доменом — через DNS TXT-запись.

Нажмите кнопку «**Настроить**», чтобы открыть окно «Верификация домена».



В открывшемся окне доступны две вкладки:

Перенаправление трафика

Отображается значение DNS A-записи (IP-адрес сервера защиты), которое необходимо добавить у регистратора или хостинг-провайдера.

После обновления записи и проверки:

- домен получает статус «**Под защитой**»;
- появляется уведомление «**Трафик успешно перенаправлен**».

Верификация домена

Перенаправление трафика
для подключения защиты

Верификация домена
для подтверждения владения доменом

1 Автоматическая верификация
После обновления DNS-A записи и проверки, домен получит статус
«Верифицирован». TXT-запись добавлять не нужно

DNS-A

93.185.164.134

Скопируйте запись из поля и добавьте её в
настройках DNS у вашего регистратора или
хостинг-провайдера

Если возникли сложности с добавлением записи в настройках DNS у регистратора или хостинг-
провайдера, воспользуйтесь инструкциями ниже или напишите в поддержку:
support@solarspace.pro

Как добавить DNS-записи в регистраторе nic.ru

Как добавить DNS-записи в регистраторе reg.ru

☐ Я добавил A-запись в настройках DNS у своего регистратора или хостинг-провайдера

Заккрыть

Перенаправить трафик

Верификация домена

Отображается значение DNS TXT-записи для подтверждения владения доменом.

TXT-запись используется, если необходимо подтвердить владение без перенаправления трафика (например, для запуска сканирования уязвимостей без подключения защиты).

Верификация домена

Перенаправление трафика
для подключения защиты

Верификация домена
для подтверждения владения доменом

1

Доступ к сканированию на уязвимости

Верифицируйте домен через DNS-TXT, если подтверждение нужно без перенаправления трафика. После подтверждения система выполнит переченьный анализ и определит уровень защищённости. Подключить защиту можно в любой момент — в настройках сайта

DNS-TXT

sc-domain-verification=6ce...

Скопируйте запись из поля и добавьте её в настройках DNS у вашего регистратора или хостинг-провайдера

Если возникли сложности с добавлением записи в настройках DNS у регистратора или хостинг-провайдера, воспользуйтесь инструкциями ниже или напишите в поддержку:
support@solarspace.pro

Как добавить DNS-записи в регистраторе nic.ru

Как добавить DNS-записи в регистраторе reg.ru

☐ Я добавил TXT-запись в настройках DNS у своего регистратора или хостинг-провайдера

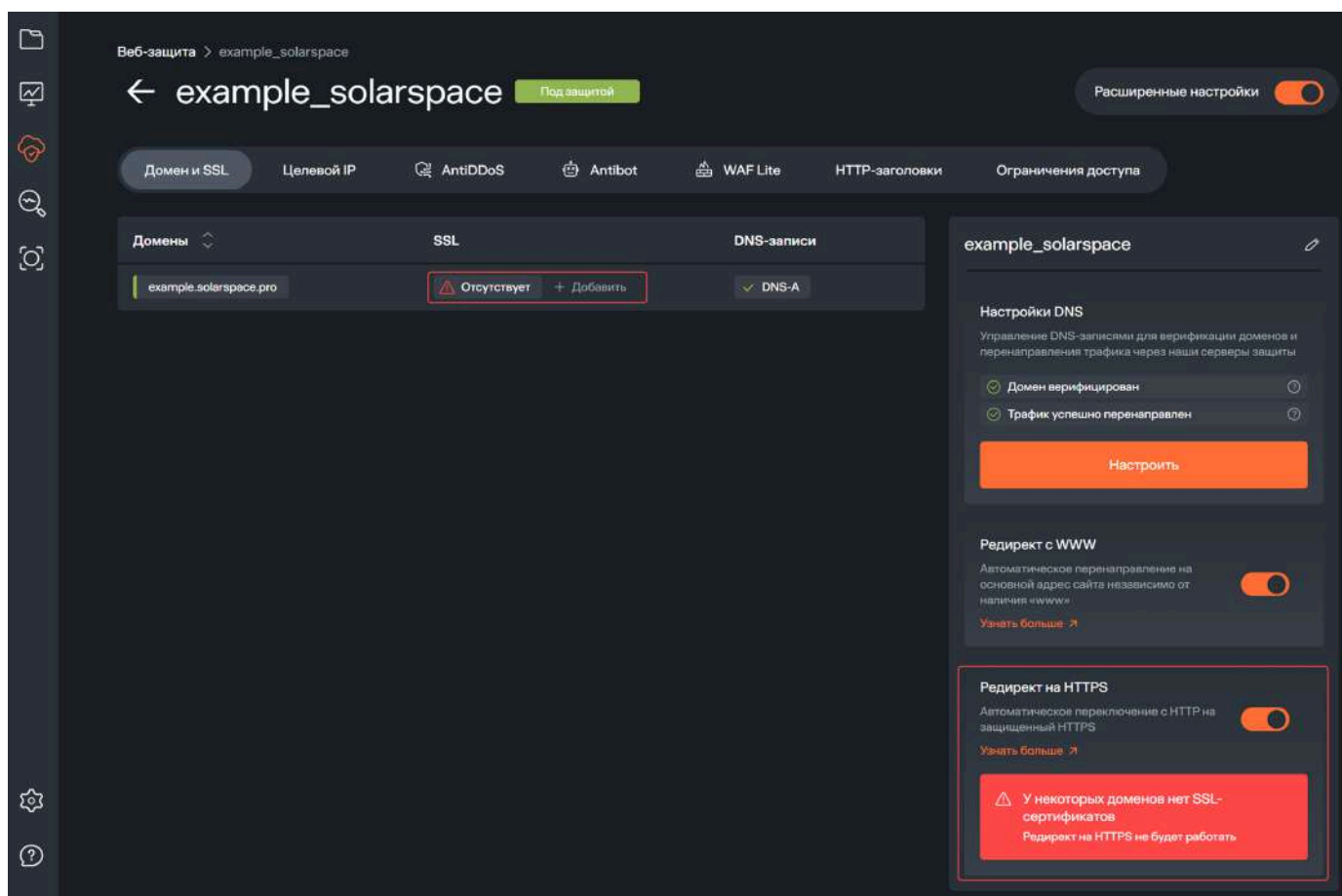
Закрыть

Верифицировать

❗ Если после обновления DNS сайт находится в статусе «Не подтвержден», проверьте корректность записи и дождитесь её распространения.

SSL-сертификат

SSL-сертификат используется для работы сайта по HTTPS и шифрования соединения между браузером посетителя и сайтом.



SSL-сертификат необходим для:

- работы сайта по HTTPS;
- корректной работы фильтрации **Antibot**;
- включения **Редиректа на HTTPS**.

Какой сертификат выбрать

Платформа поддерживает два варианта SSL-сертификата:

- **бесплатный сертификат Let's Encrypt (LE)** — платформа выпускает и устанавливает сертификат автоматически;
- **собственный сертификат** — загрузка сертификата и приватного ключа вручную.

Добавить сертификат

для example.solarspace.pro

Свой сертификат Бесплатный сертификат (LE)

Приватный ключ

Загрузите файл

Выбрать файл

или вставьте текстом

Приватный ключ

Публичный ключ

Загрузите файл

Выбрать файл

или вставьте текстом

Сертификат

Назад Сохранить

Бесплатный сертификат (LE) подходит в большинстве случаев и рекомендуется, если:

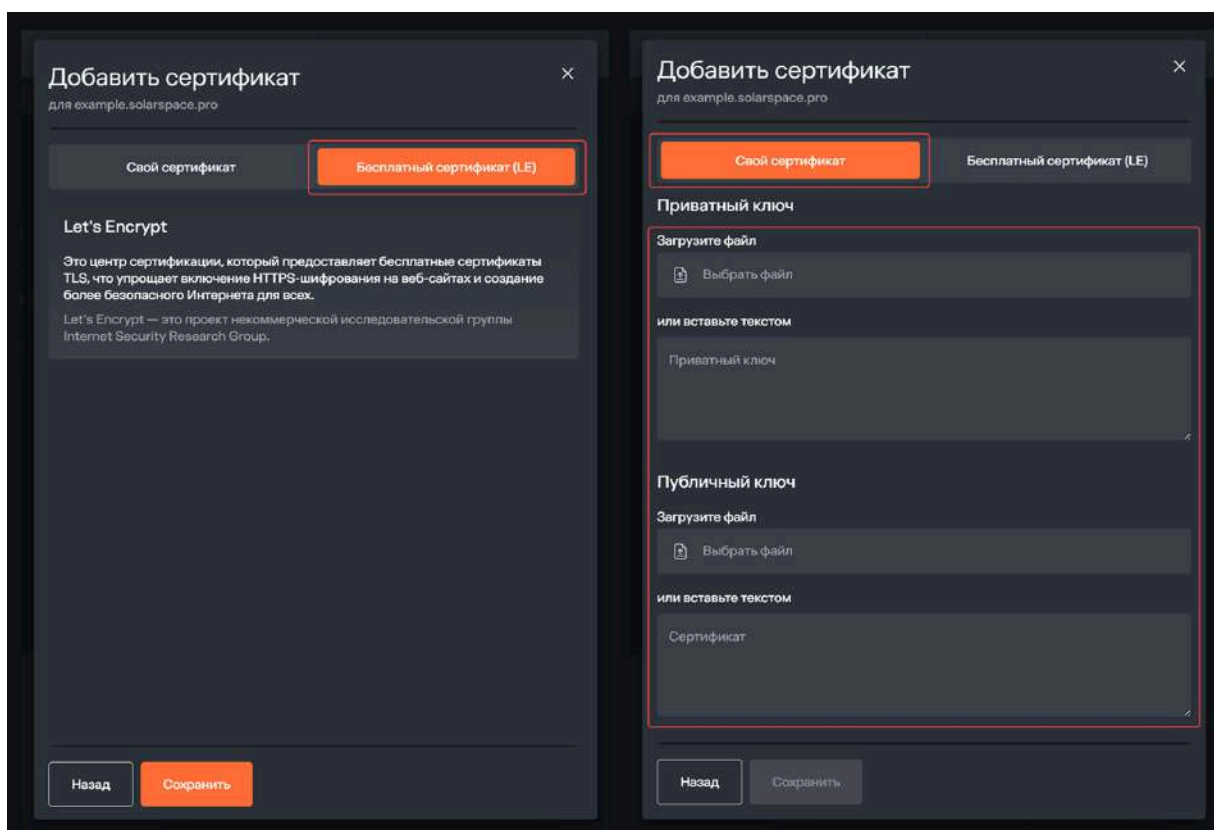
- сертификат требуется для стандартного HTTPS-сценария;
- не предъявляются дополнительные требования к типу сертификата и центру сертификации.

Собственный сертификат рекомендуется использовать, если:

- сертификат уже выпущен в другой инфраструктуре;
- требуется сертификат от определённого центра сертификации;
- используется сертификат с расширенной проверкой или корпоративными требованиями.

Как добавить сертификат

1. В строке нужного домена нажмите **«Добавить»**.
2. Выберите вариант:
 - **«Бесплатный сертификат (LE)»** — для автоматического выпуска и установки сертификата.
 - **«Свой сертификат»** — для загрузки собственного сертификата.



3. Если выбран вариант «**Свой сертификат**», загрузите:

- **приватный ключ**;
- **публичный сертификат**. Загрузку можно выполнить файлами или вставкой текста.

Добавление своего SSL-сертификата

SSL-сертификат состоит из публичного (открытого) и приватного (закрытого) ключей шифрования.

Публичный ключ шифрует данные при обращении пользователя к серверу. Он состоит из следующих элементов:

- сертификат;
- промежуточный сертификат;
- корневой сертификат.

Приватный ключ расшифровывает данные, которые пользователь отправил серверу.

Подробная инструкция по загрузке собственного сертификата приведена в статье [Как добавить локальный SSL-сертификат](#).

Выпуск бесплатного сертификата (LE)

Бесплатный сертификат Let's Encrypt можно выпустить:

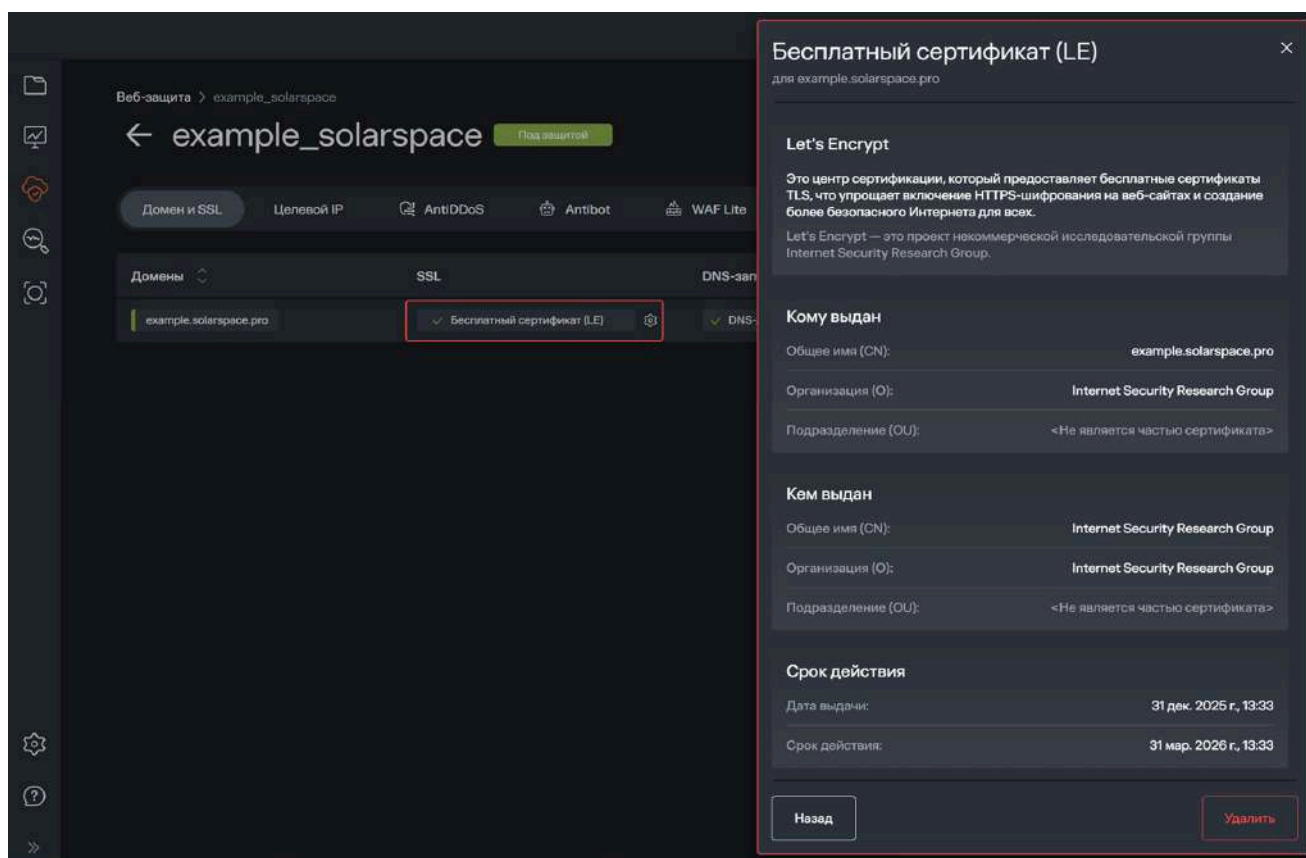
- при добавлении сертификата для домена;
- позже, в настройках сайта на вкладке «**Домен и SSL**».

После выбора варианта «**Бесплатный сертификат (LE)**» платформа выполняет выпуск и установку сертификата автоматически.

Просмотр информации о сертификате

Чтобы посмотреть сведения о сертификате:

1. Откройте вкладку «**Домен и SSL**».
2. В строке домена нажмите на иконку настроек рядом с полем **SSL**.



В окне отображаются основные сведения о сертификате и срок его действия.

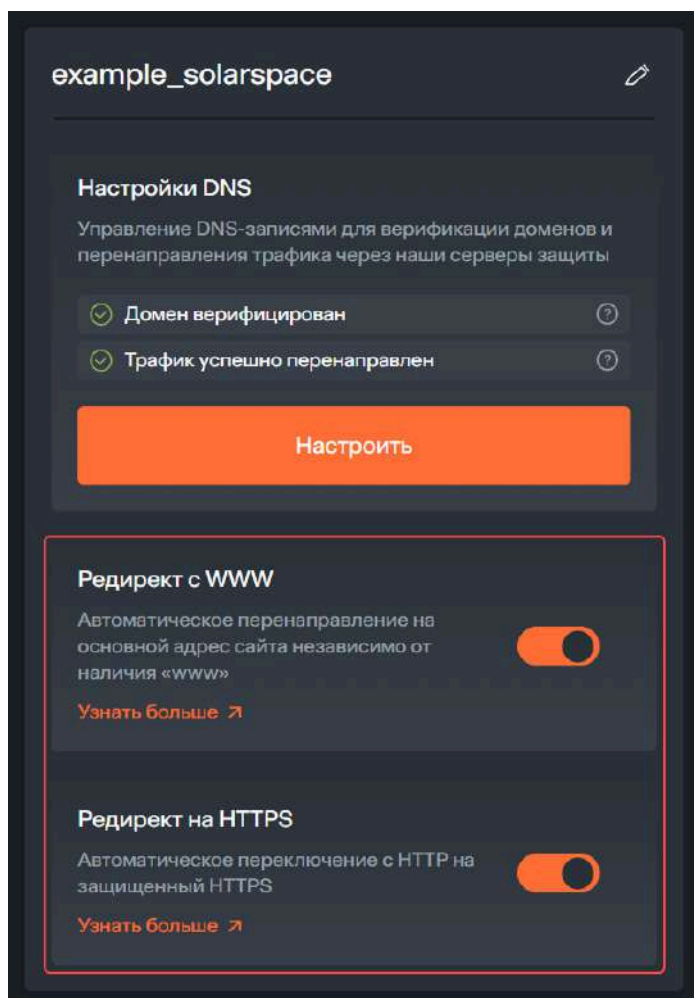
Продление сертификата

- **Let's Encrypt (LE)** продлевается автоматически.

- **Собственный сертификат** необходимо обновлять вручную. После обновления сертификата загрузите актуальную версию в личный кабинет.

Дополнительные настройки

В блоке «**Настройки**» на странице «**Домен и SSL**» можно включить параметры «**Редирект с WWW**» и «**Редирект на HTTPS**», отвечающие за корректное направление трафика и безопасность соединений.



Редирект с WWW

Перенаправляет обращения к сайту, введенные с префиксом `www` (например, `www.example.com`), на основной домен без `www` — `example.com`. Функция обеспечивает единый адрес сайта и предотвращает появление дублей страниц в поисковой выдаче. При отключённой настройке обращения с `www` могут завершаться ошибкой «Страница не найдена».

Рекомендуется включать редирект после настройки перенаправления трафика (DNS A-запись) в разделе [Постановка домена под защиту](#).

Редирект на HTTPS

Перенаправляет все запросы с небезопасного протокола HTTP на HTTPS. Редирект работает только при наличии SSL-сертификата. Если SSL-сертификат для домена не добавлен, перенаправление выполняться не будет.

После включения редиректа:

- запросы к `http://` будут автоматически перенаправляться на `https://`;
- сайт будет открываться только по защищённому протоколу.

Рекомендуется включать редирект на HTTPS после [добавления SSL-сертификата](#).

Целевой IP

Чтобы открыть целевой IP перейдите на страницу **Веб-защита**, нажав на иконку облака в левом меню с любой страницы личного кабинета.

WEB-защита

Статус: [выпадающий список] Поиск по ресурсам и доменам

Статус	Ресурс	AntiDDoS	Antibot	WAF Lite	
Не защищен		☒	☒	☐	...
Не защищен		☐	☐	☐	...
Не защищен		☐	☐	☐	...
Под защитой	domain.ru	☒	☒	☒	...
Под защитой		☒	☒	☒	...
Под защитой		☒	☐	☐	...
Не защищен		☒	☐	☒	...
Не защищен		☒	☐	☐	...
Не защищен		☐	☐	☐	...

Всего 107 записей << < 1 2 3 4 5 > >> 1/11

Статистика работы сервиса

Среднее за текущий расчетный период: ⓘ

Ширина канала Запросы Коды География

Тарифицируемый трафик: 158,86 Кбит/с ⓘ

Исходящий легитимный трафик: 2 Мбит/с ⓘ

Входящий трафик: 13,43 Кбит/с ⓘ

Входящий легитимный трафик: 13,09 Кбит/с ⓘ

Подробнее статистика

Откроется страница со списком ваших ресурсов. Выберите нужный вам ресурс, кликнув по нему.

Статус	Ресурс	AntiDDoS	Antibot	WAF Lite	
Не защищен		☒	☒	☐	...
Не защищен		☐	☐	☐	...
Не защищен		☐	☐	☐	...
Под защитой	domain.ru	☒	☒	☒	...
Под защитой		☒	☒	☒	...
Под защитой		☒	☐	☐	...
Не защищен		☒	☐	☒	...
Не защищен		☒	☐	☒	...
Не защищен		☒	☐	☐	...
Не защищен		☐	☐	☐	...

Всего 107 записей

<< < 1 2 3 4 5 > >>

1/11

Или нажмите на три точки в правой части строки ресурса.

Под защитой	domain.ru	☒	☒	☒	...
Под защитой		☒	☒	☒	...
Под защитой		☒	☐	☐	...

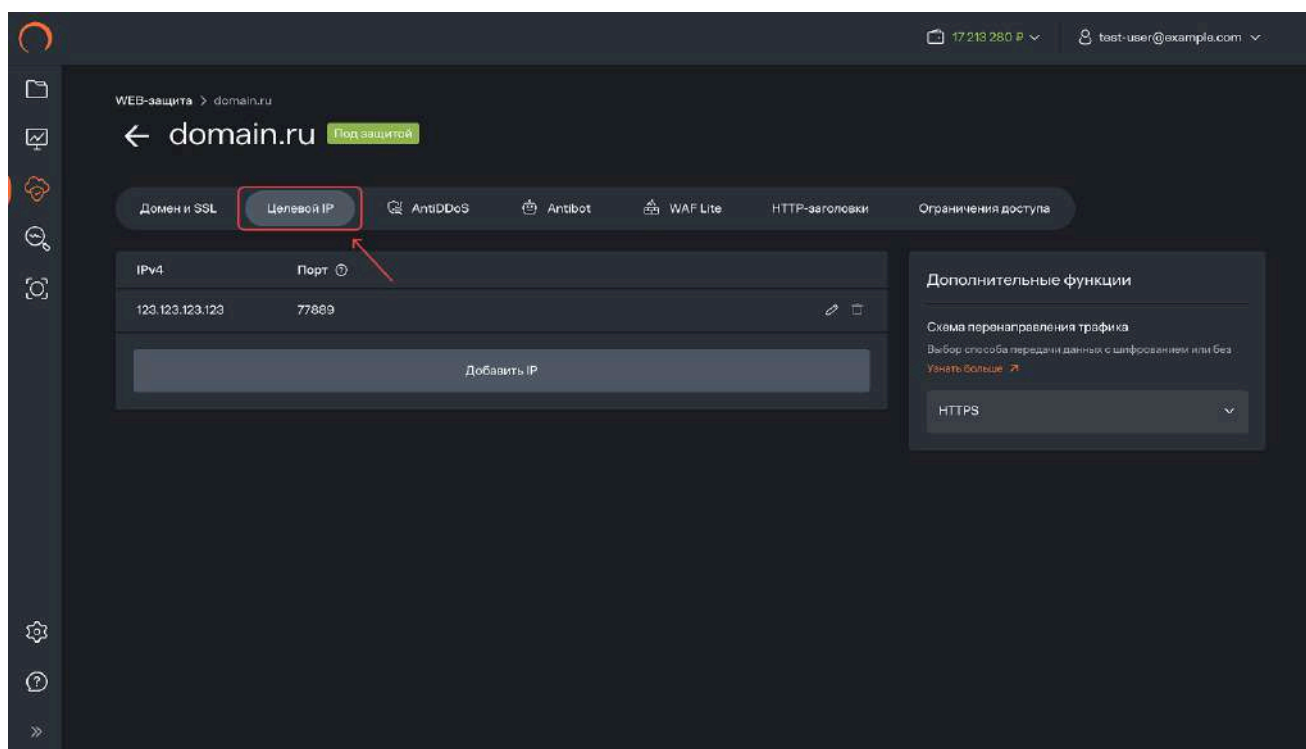
Выберите "Настройки".

Под защитой	domain.ru	☒	☒	☒	...
Под защитой		☒	☒		...
Под защитой		☒	☐		...

Настройки

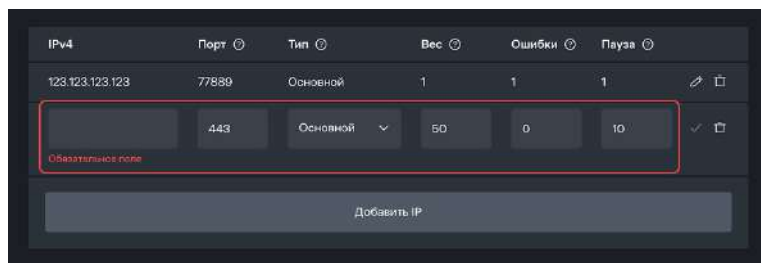
Статистика

Вы увидите страницу с открытой вкладкой "Домен и SSL". Нажмите на вкладку "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.

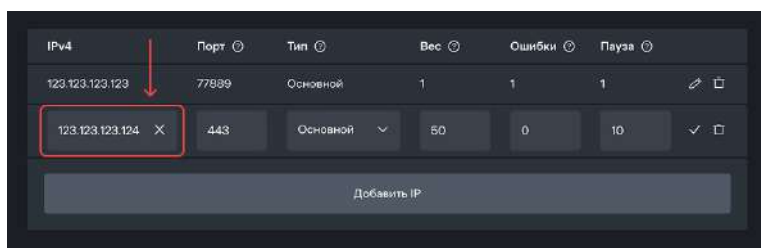


Все предзаполненные поля можно редактировать:

- **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"

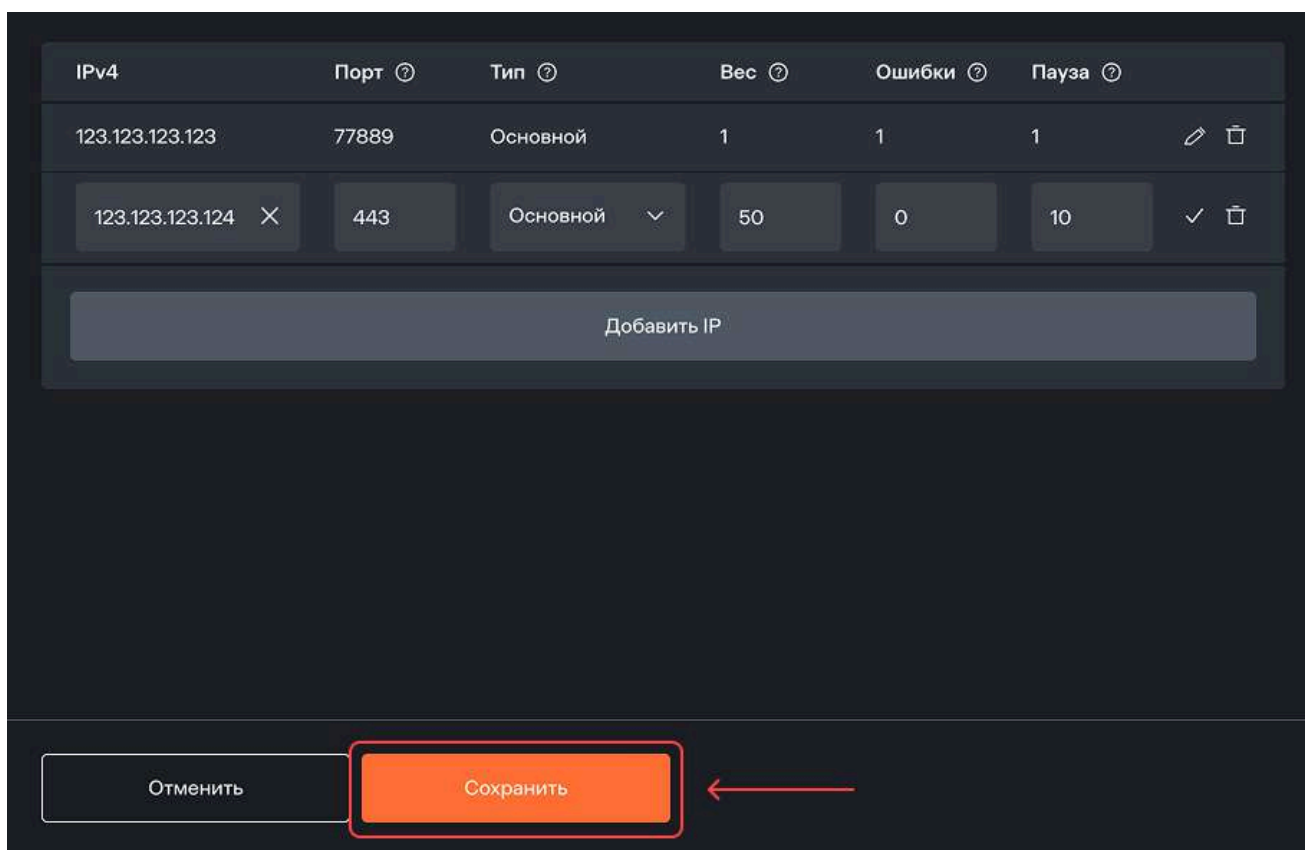
Введите IP-адрес в поле "IPv4", он должен отличаться от IP, который уже есть в списке.



IPv4	Порт	Тип	Вес	Ошибки	Пауза
123.123.123.123	77889	Основной	1	1	1
123.123.123.124	443	Основной	50	0	10

Добавить IP

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

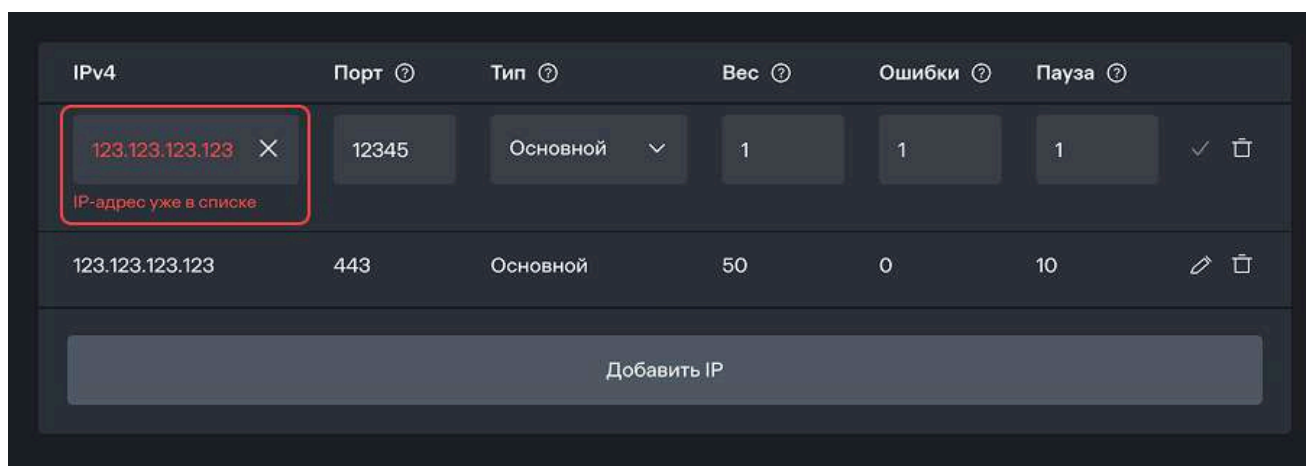


IPv4	Порт	Тип	Вес	Ошибки	Пауза
123.123.123.123	77889	Основной	1	1	1
123.123.123.124	443	Основной	50	0	10

Добавить IP

Отменить Сохранить

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



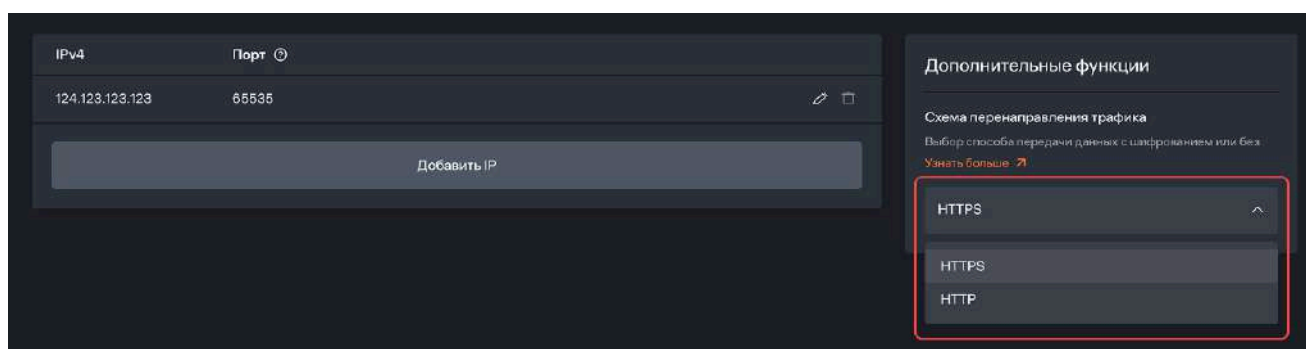
Дополнительные функции

Если у вас один IP-адрес, в правой части страницы будет раздел «**Дополнительные функции**», где можно выбрать схему перенаправления трафика и настроить порты IP-адресов.

Схема перенаправления трафика

Определяет, по какому протоколу будет передаваться трафик между серверами — с шифрованием (HTTPS) или без него (HTTP). Доступны три варианта:

- **По умолчанию** — система выбирает порт автоматически в зависимости от включения функции «*Редирект на HTTPS*» на вкладке «*Домен и SSL*».
- **HTTP (80)** — передача данных без шифрования, используется только для тестовых целей.
- **HTTPS (443)** — зашифрованный канал связи между браузером и сервером, рекомендуется для всех рабочих ресурсов.

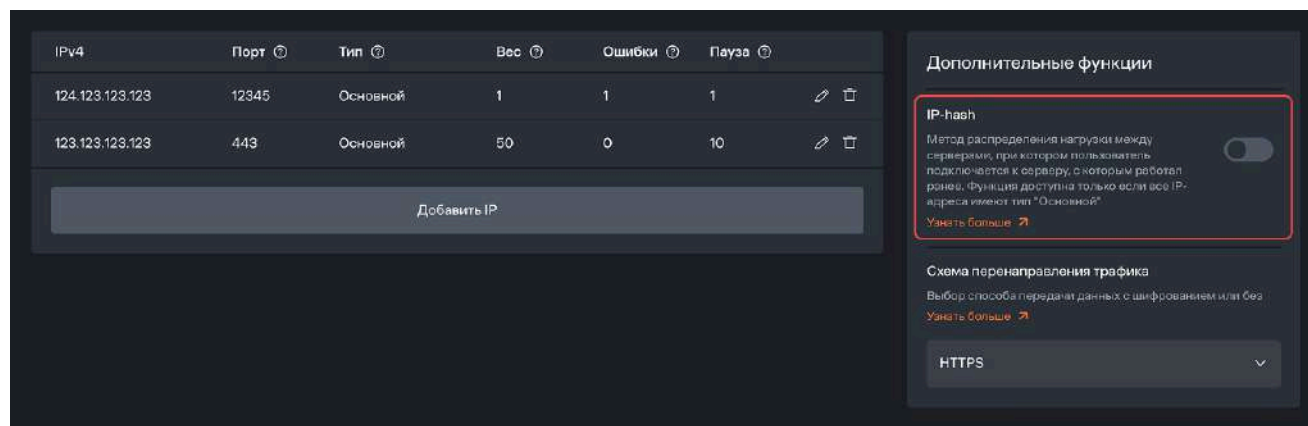


Если у вас несколько IP-адресов, в этом же блоке появится дополнительная опция **IP-hash**.

IP-hash

Метод распределения нагрузки между серверами, при котором пользователь всегда подключается к тому же серверу, с которым взаимодействовал ранее. Функция доступна, если все IP-адреса имеют тип «Основной».

Этот механизм особенно полезен для веб-приложений с пользовательскими сессиями — например, личных кабинетов или интернет-магазинов. При использовании IP-hash пользователь возвращается к активному сеансу, без необходимости повторного входа в систему.

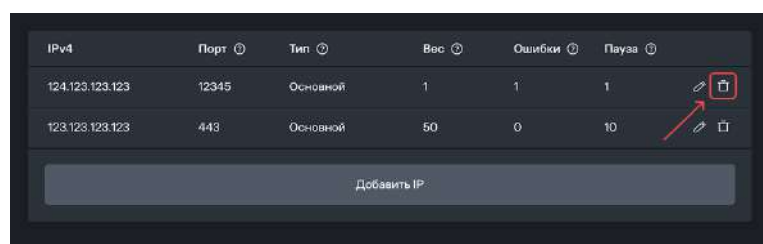


ⓘ Обратите внимание

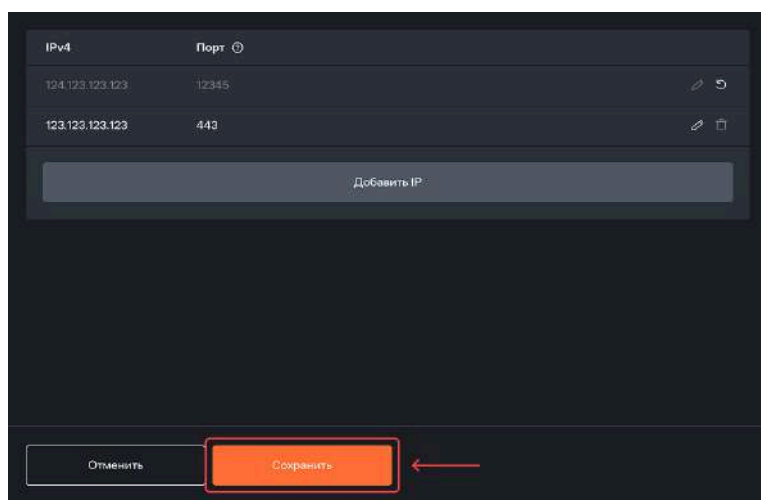
Функция IP-hash доступна, если все введенные IP-адреса имеют тип "Основной"

Удаление IP-адреса

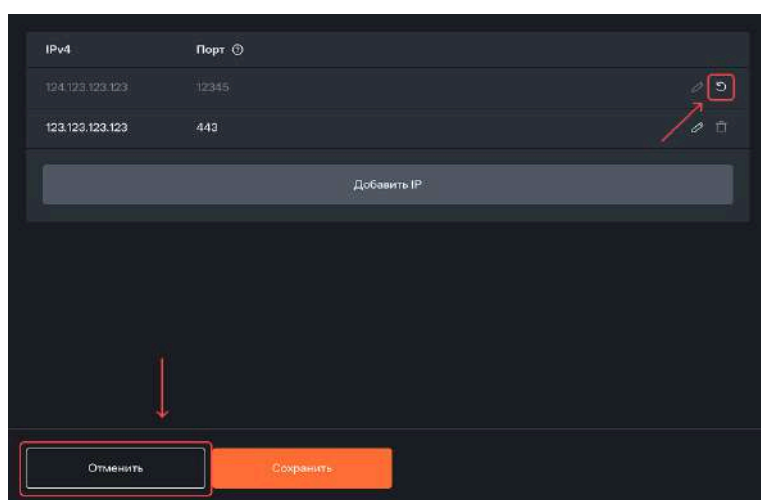
Для удаления IP нажмите на иконку корзины в строке с нужным адресом.



В обновленной странице нажмите кнопку "Сохранить".



Если необходимо вернуть удаленный ресурс, нажмите кнопку "Отменить" или нажмите на круговую стрелку в правой части строки.



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 закрывает 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.

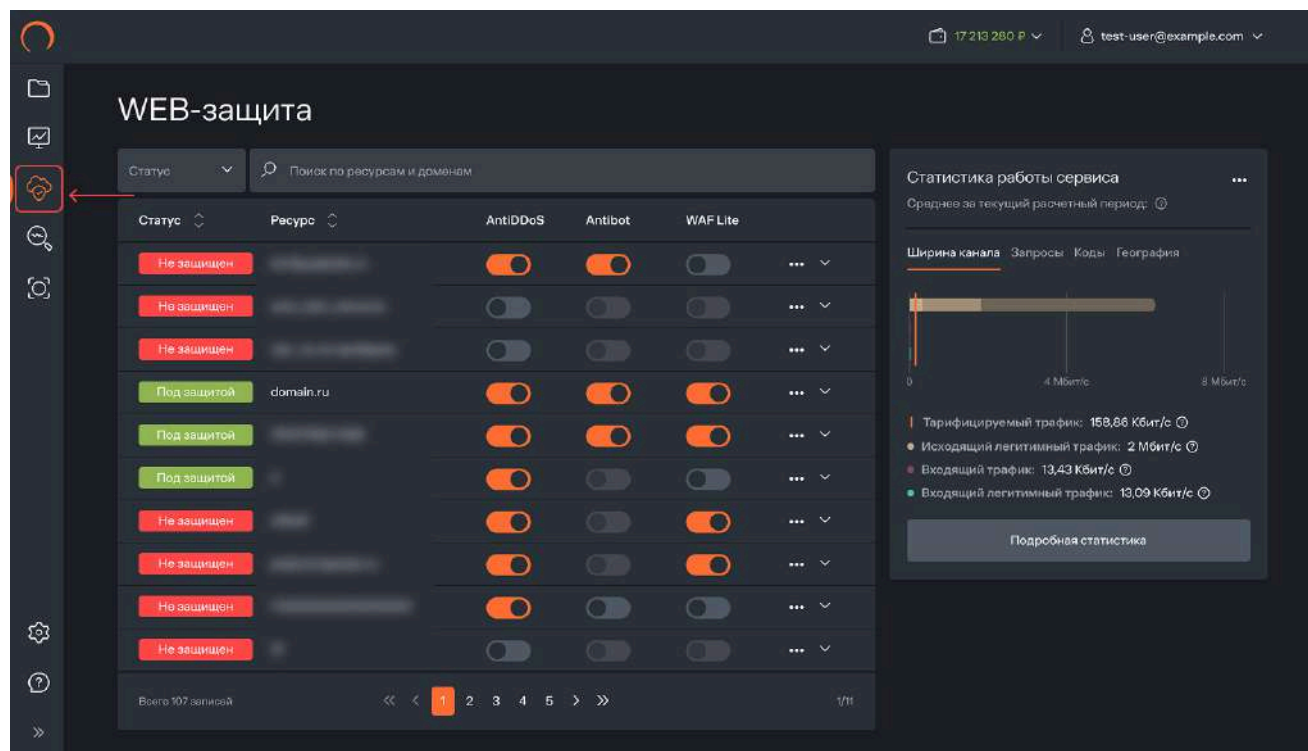
Повышение производительности

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.

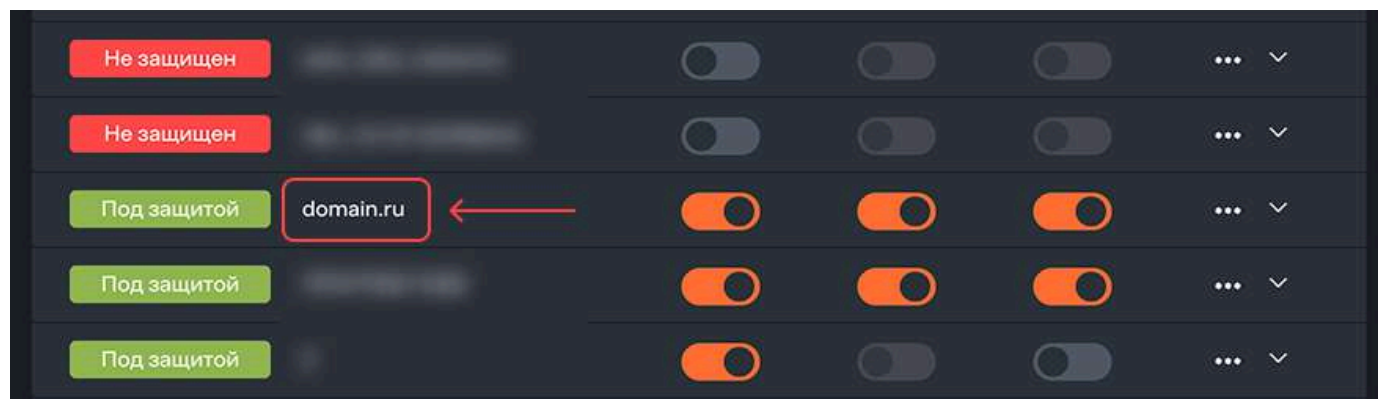
Добавьте эти заголовки в **личном кабинете** Solar Space, чтобы повысить эффективность и безопасность вашего сайта.

Как работать с HTTP-заголовками в личном кабинете

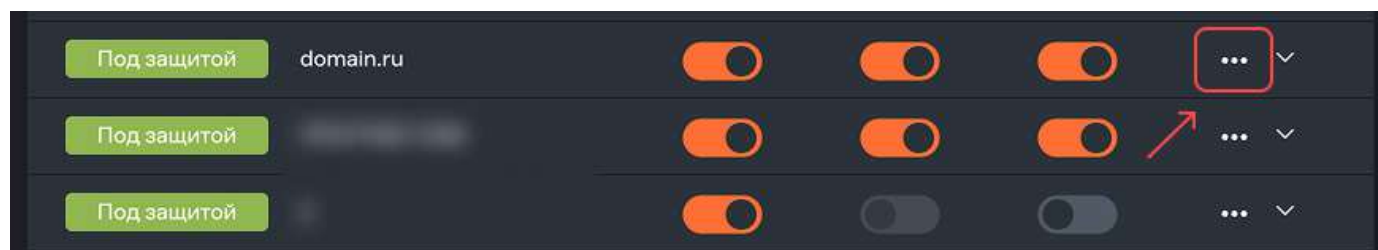
Чтобы открыть страницу "HTTP-заголовки" перейдите на страницу **Веб-защита**, нажав на иконку облака в левом меню с любой страницы личного кабинета.



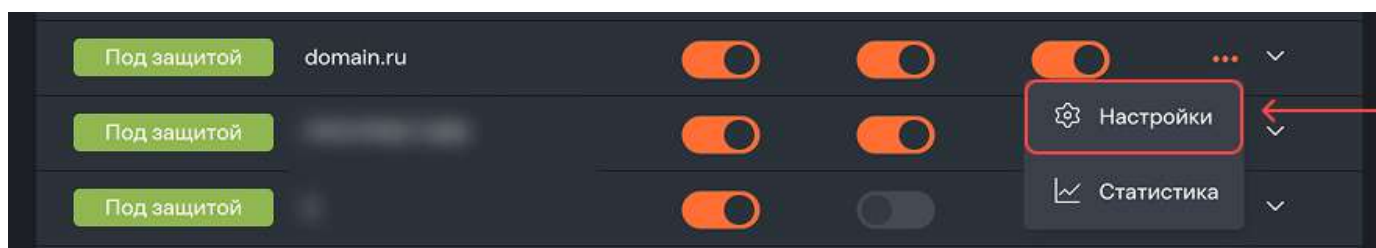
Откроется страница со списком ваших ресурсов. Выберите нужный вам ресурс, кликнув по нему.



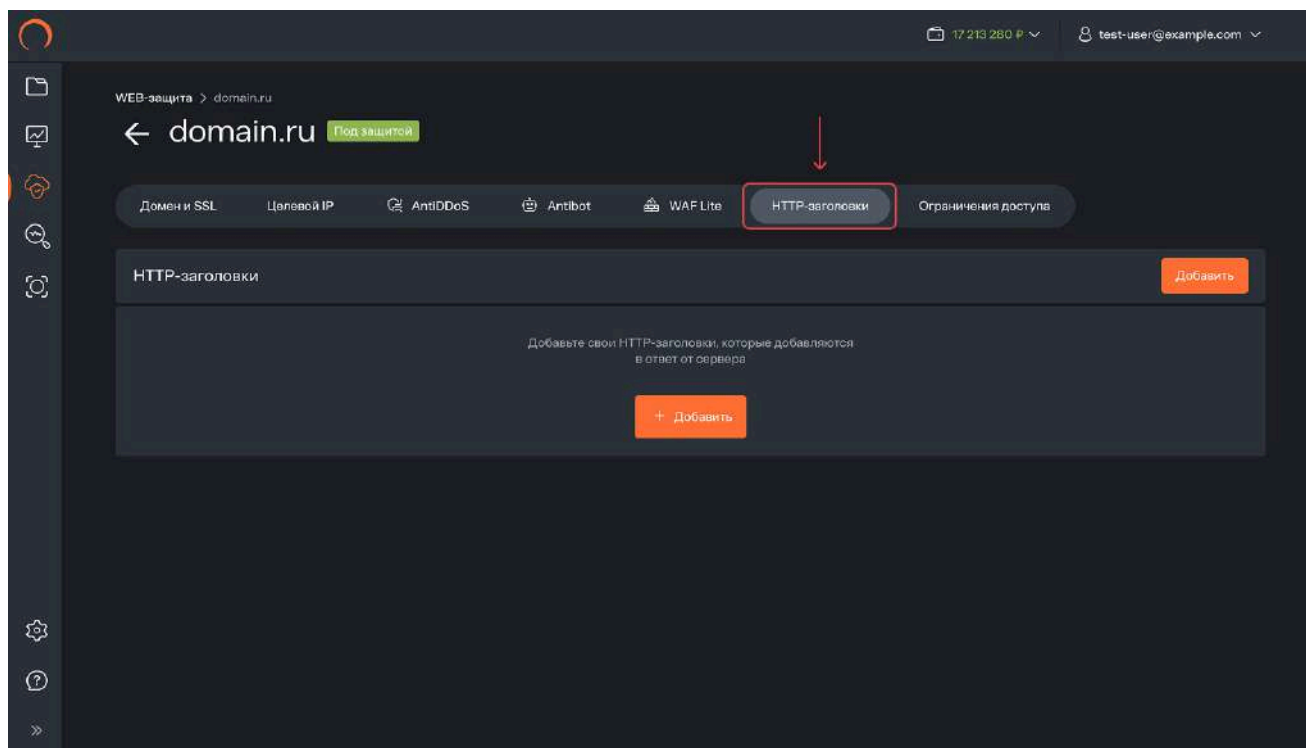
Или нажмите на три точки в правой части строки ресурса.



Выберите "Настройки".



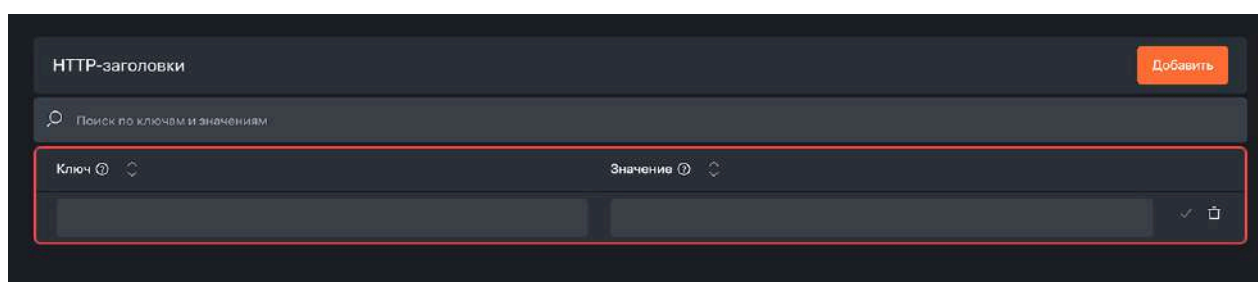
Вы увидите страницу со стартовой вкладкой "Домен и SSL". Нажмите на вкладку "HTTP-заголовки"



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.

The screenshot shows a dark-themed interface titled "HTTP-заголовки". At the top right is an orange "Добавить" button. Below the title is a search bar with the placeholder "Поиск по ключам и значениям". Underneath are two dropdown menus labeled "Ключ" and "Значение". A table contains one row with the key "hashed_keyABC" and the value "{username:john_doe}". Each cell has a small "X" icon to its right. To the right of the value cell are checkmark and delete icons. At the bottom, there are two buttons: "Отменить" and "Сохранить". The "Сохранить" button is orange and highlighted with a red rectangle and a red arrow pointing to it from the right.

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"**. Нужно поле выберите в выпадающем списке

This screenshot shows the same "HTTP-заголовки" interface. The search bar "Поиск по ключам и значениям" is highlighted with a red rectangle. The table below it is the same as in the previous screenshot, showing the header "hashed_keyABC" with value "{username:john_doe}". The "Сохранить" button is no longer highlighted.

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

HTTP-заголовки

Добавить

🔍 Поиск по ключам и значениям

Ключ 🔄

Значение 🔄

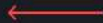
referer: jsuABQ

[безымянный_документ]



Отменить

Сохранить



Общее описание ограничений доступа

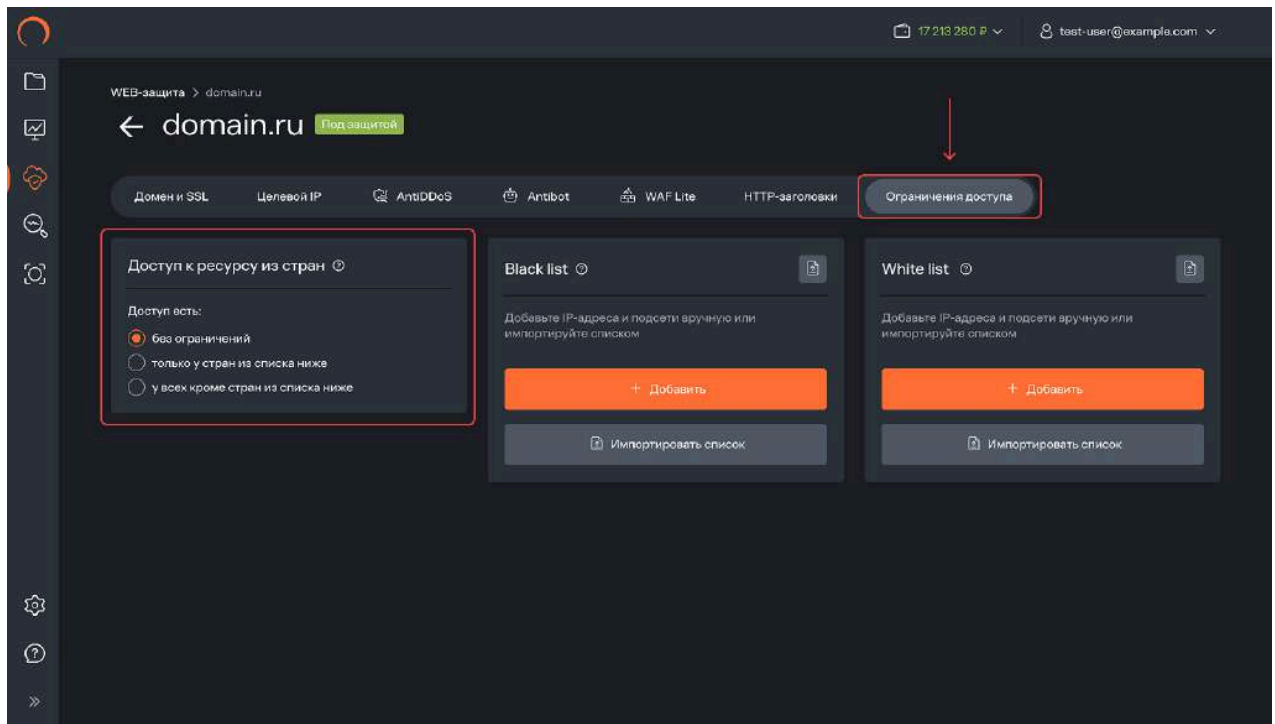
Ограничения доступа — это перечень настроек, которые позволяют управлять входящими запросами к вашему сайту.

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

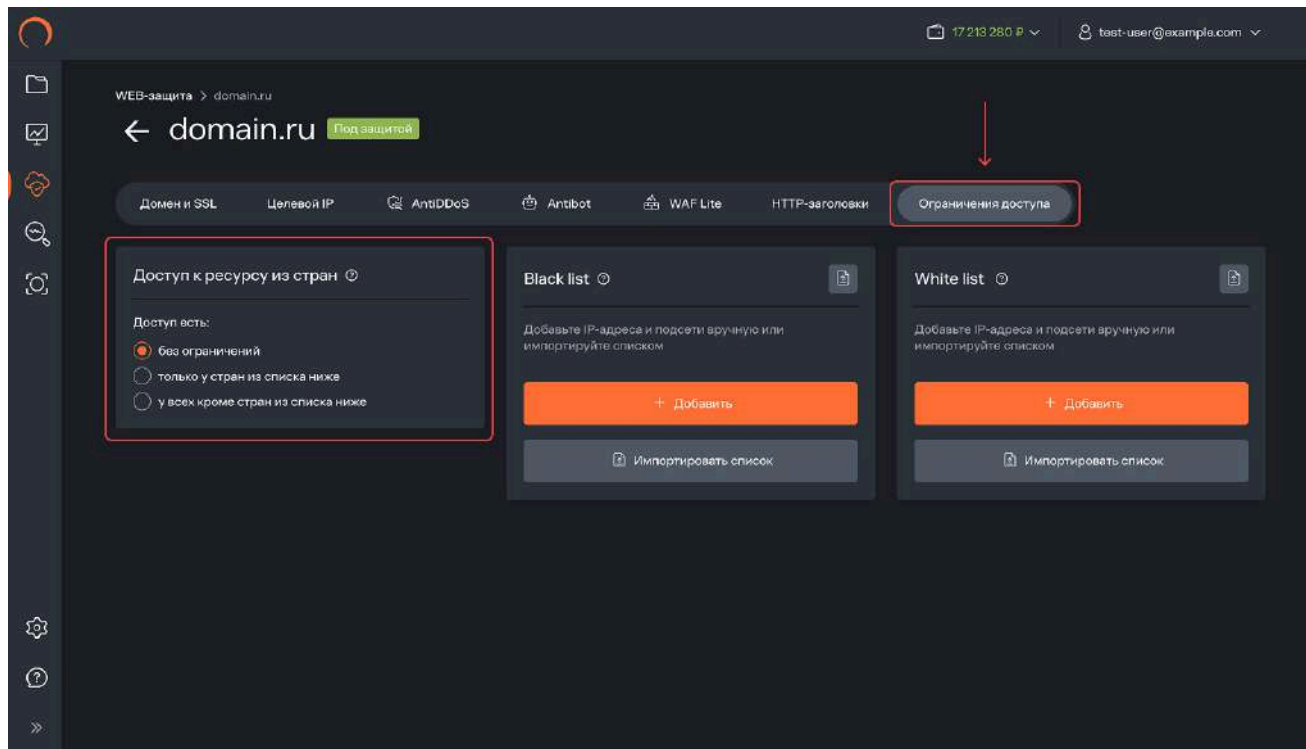
Каждое входящее обращение к сайту система обрабатывает в следующей последовательности:

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.



Доступ к ресурсу из стран

Перейдите на вкладку **Ограничения доступа**, чтобы задать географические ограничения для вашего ресурса. Здесь вы сможете определить, из каких стран разрешены или запрещены входящие запросы к вашему сайту.



Блок **«Доступ к ресурсу из стран»** позволяет управлять географией запросов, поступающих к вашему сайту. В нём можно выбрать один из трёх режимов работы:

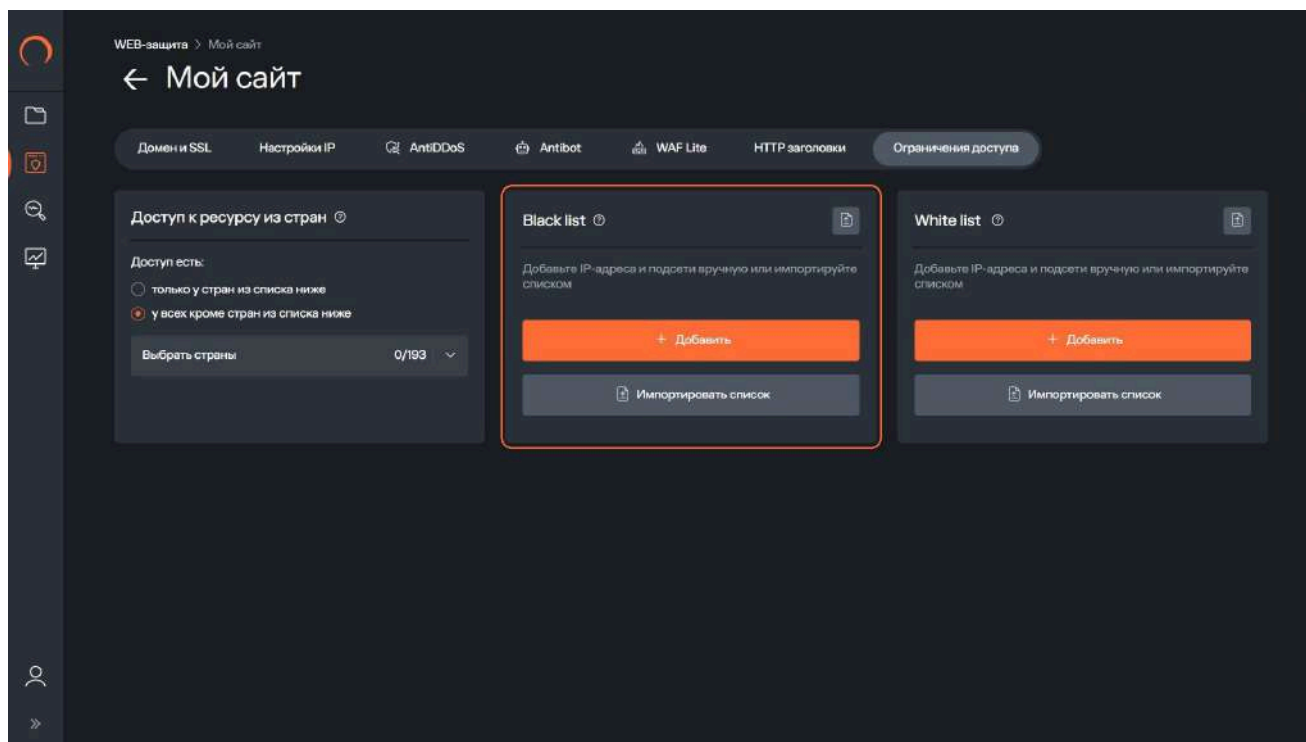
- **Без ограничений** — запросы разрешены для всех стран.
- **Только у стран из списка ниже** — выберите конкретные страны, из которых доступ разрешён.
- **У всех кроме стран из списка ниже (по умолчанию)** — выберите страны, из которых доступ будет запрещён.

После выбора нужного режима нажмите **«Сохранить изменения»**, чтобы применить настройки.

Black list

Функция **Black list** позволяет добавлять IP-адреса и подсети, запросы от которых будут блокироваться без дополнительных проверок.

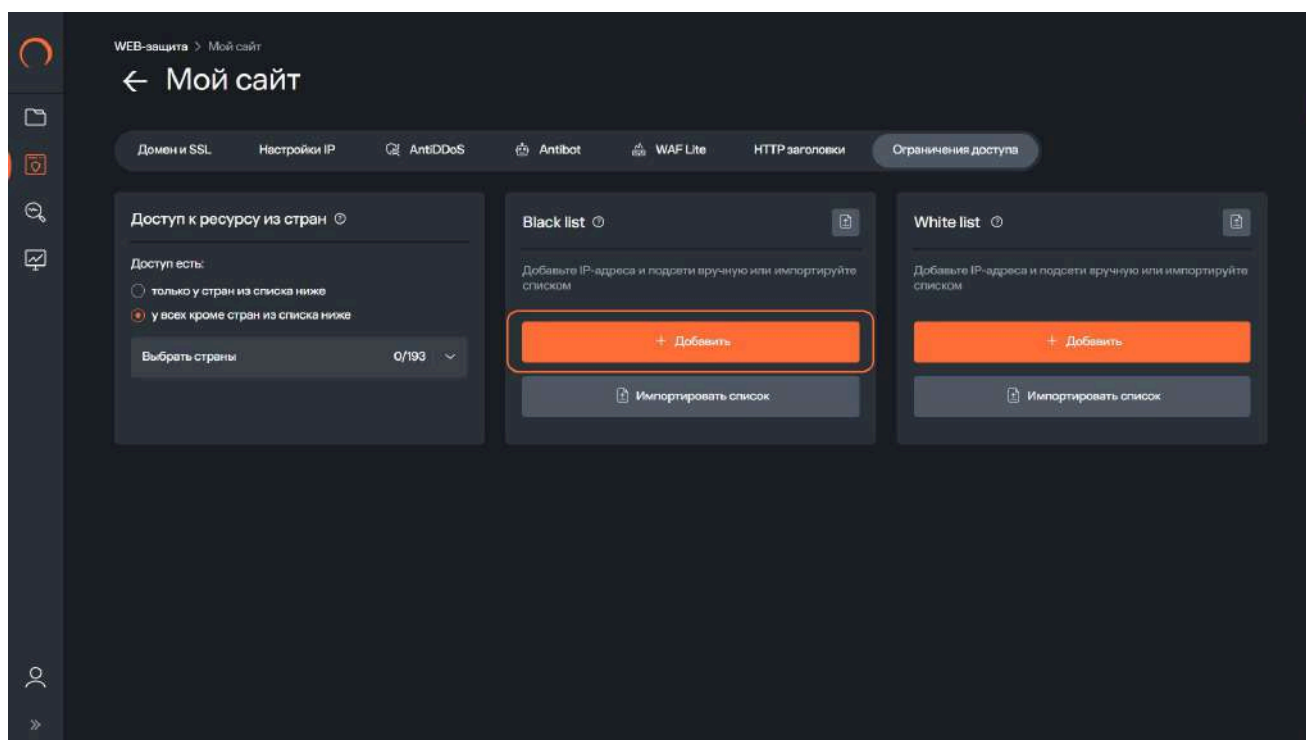
Чтобы открыть раздел, перейдите в панель управления и выберите вкладку «**Ограничения доступа**».



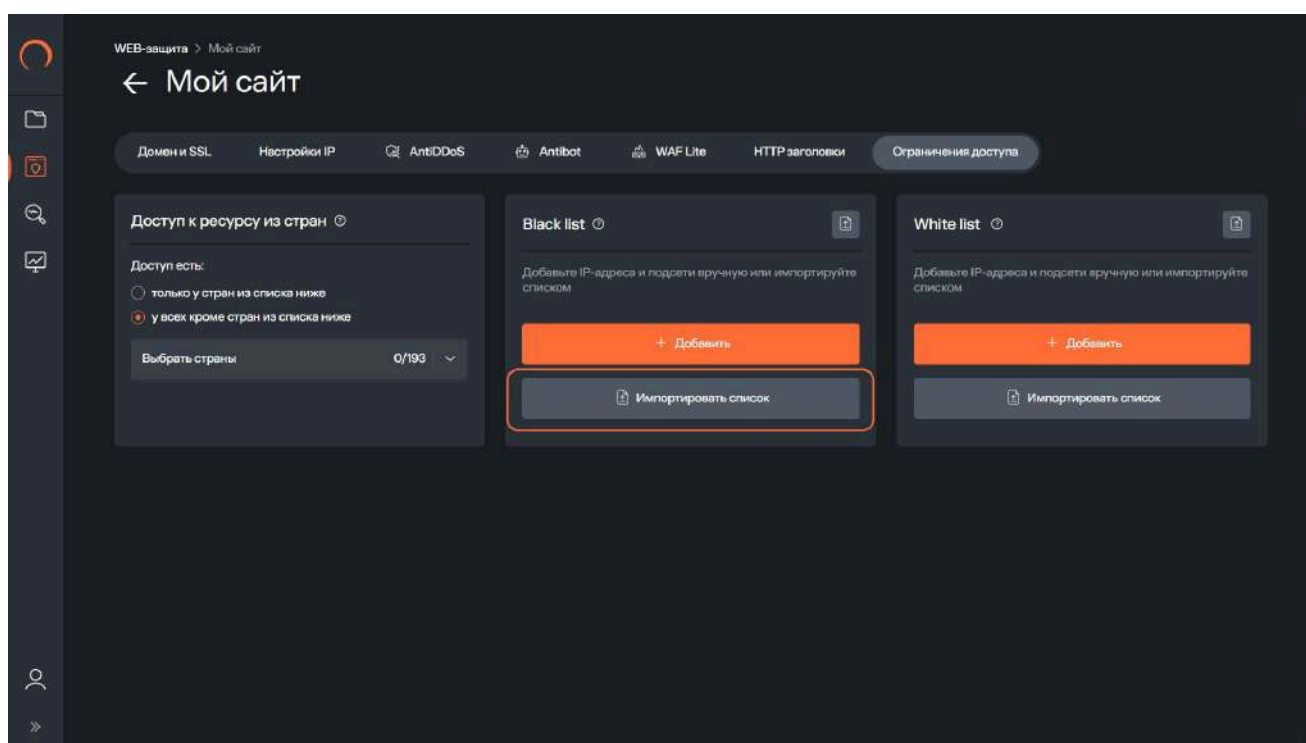
Добавление IP-адресов и подсети в Black list

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.

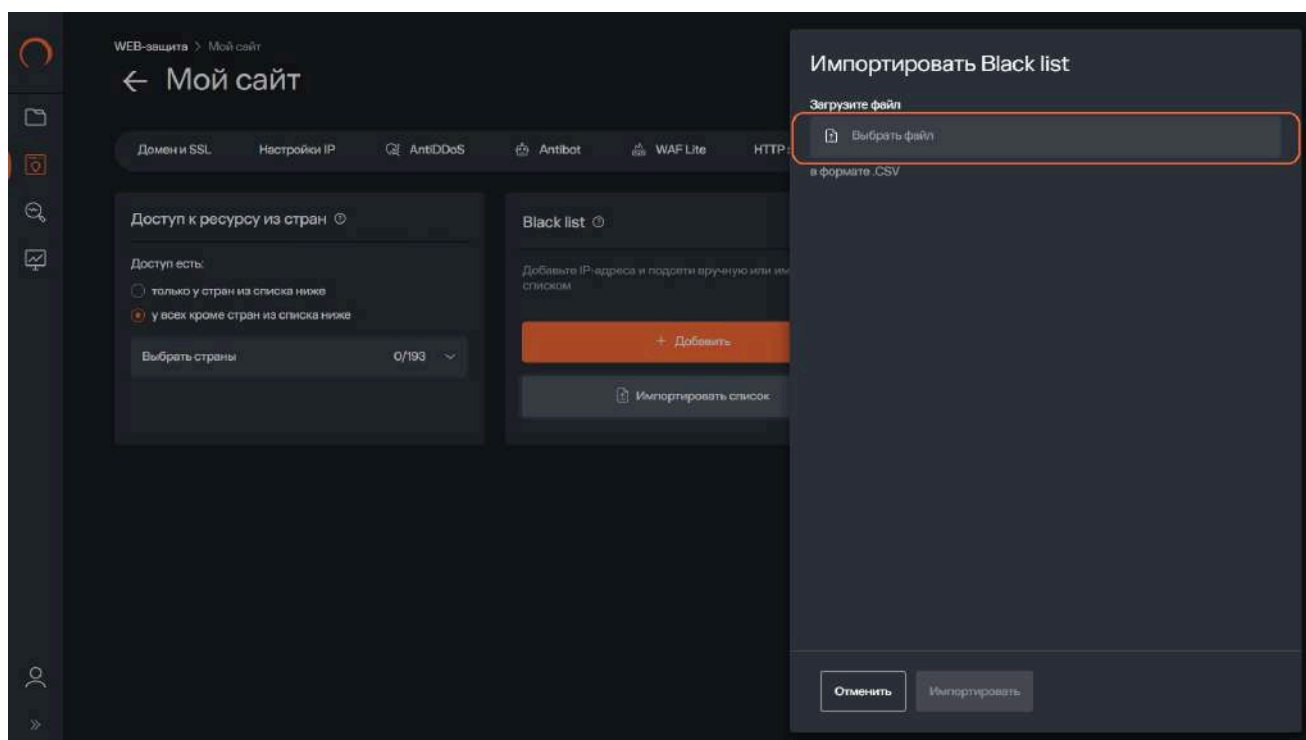
Если вы еще не добавили ни одного IP-адреса в Black list, то увидите кнопки "Добавить" (для добавления IP-адресов вручную).



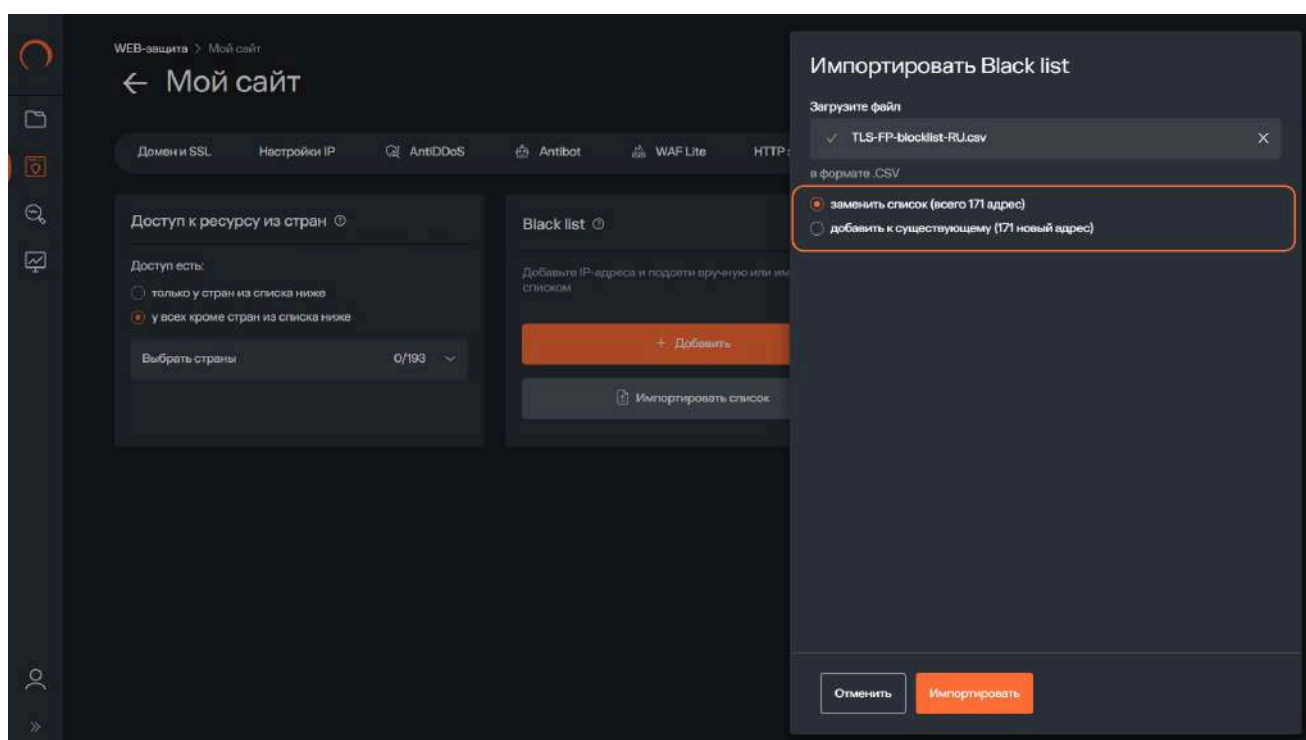
Также вы можете "Импортировать список" IP-адресов в Black list (для загрузки файла со списком).

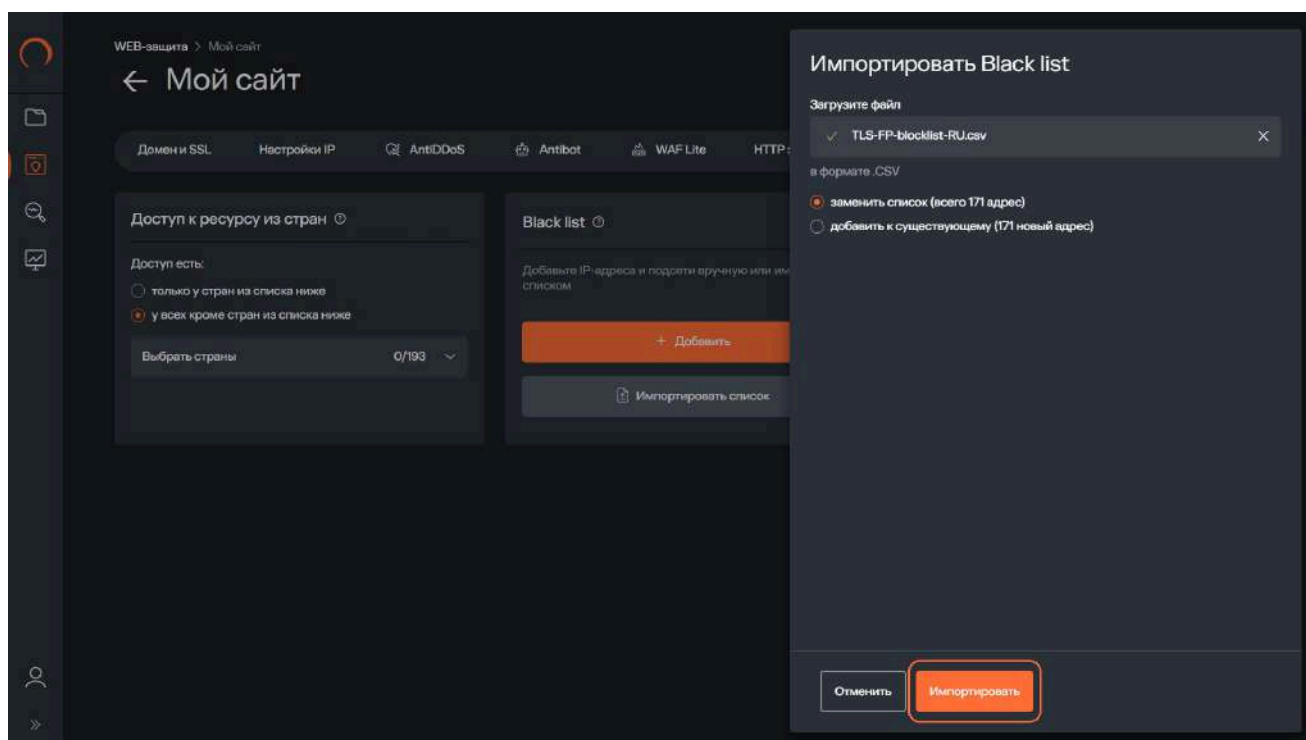


При нажатии на кнопку "Импортировать список" справа откроется окно для загрузки файла в формате .csv. Когда вы добавите файл, кнопка "Импортировать" в нижней части экрана станет активной.

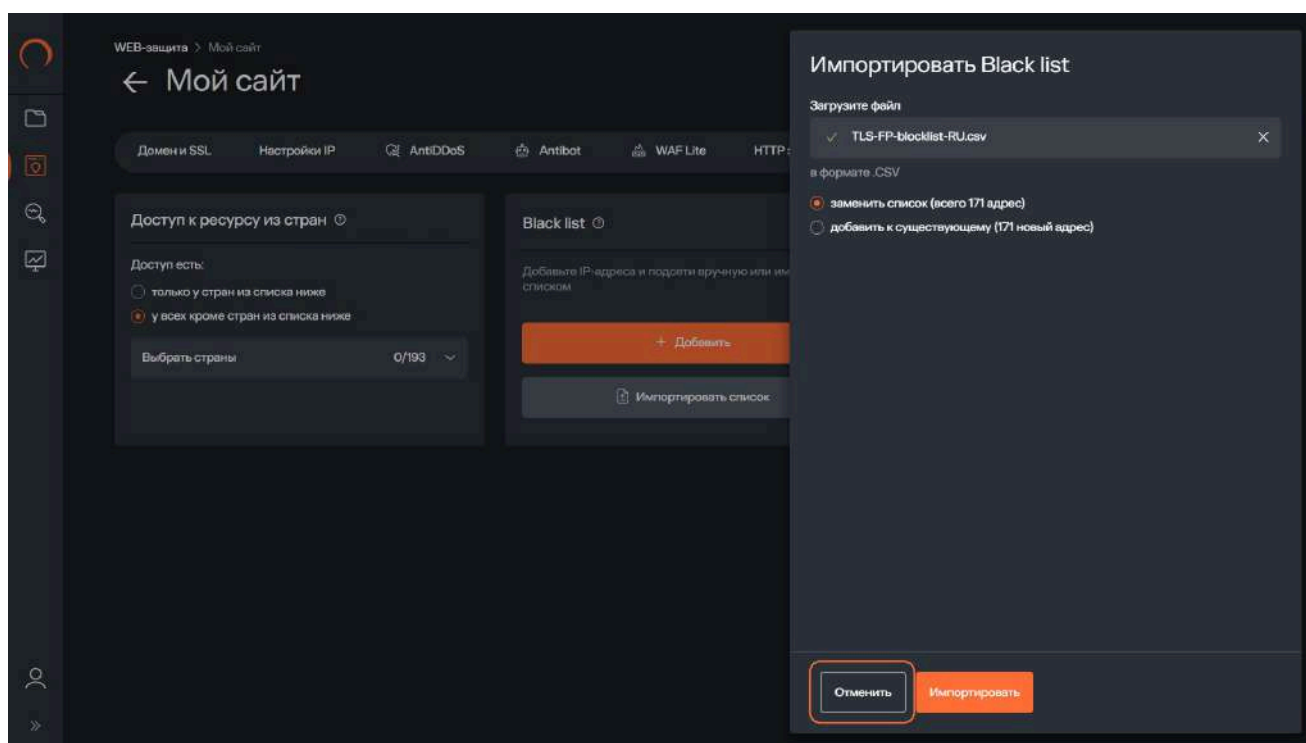


После загрузки файла, выберите один из способов его добавления в Black list и нажмите "Импортировать".





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

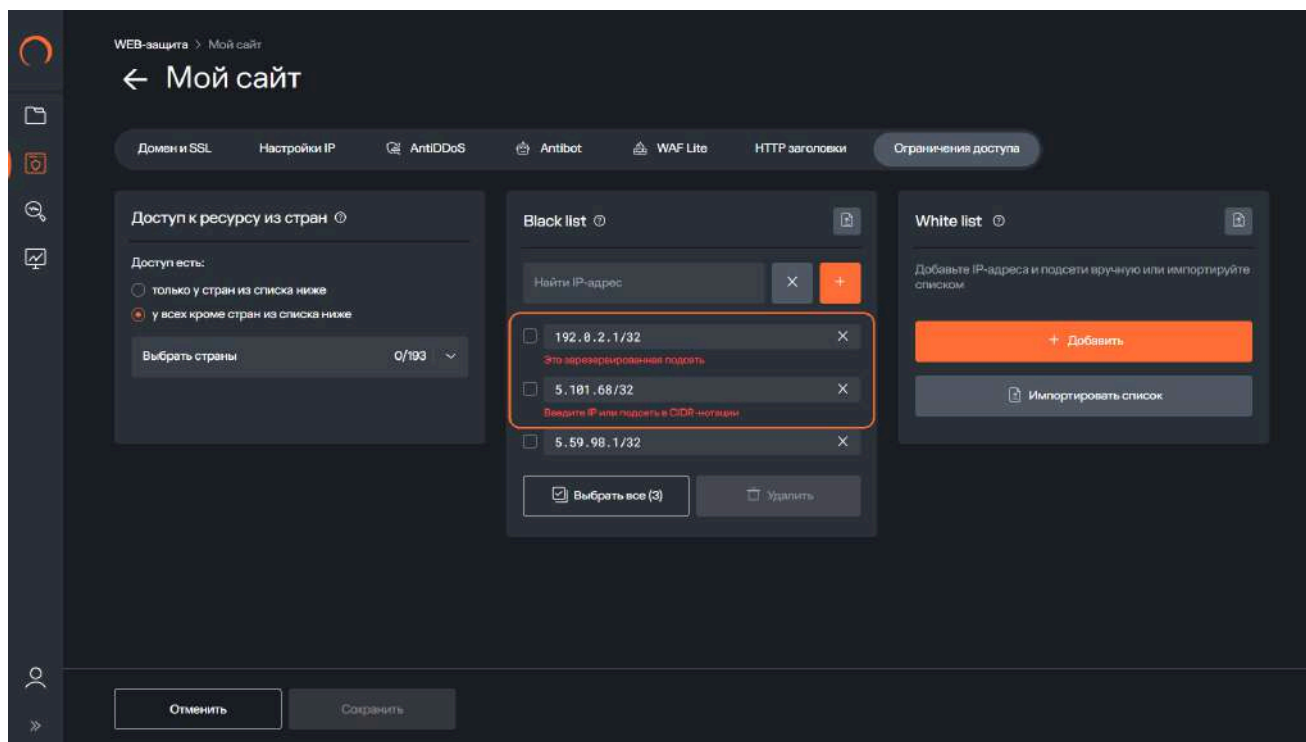


Если вы будете добавлять IP-адреса в Black list вручную, обратите внимание: IP-адрес должен состоять из уровней, разделенных точкой. Если ввести его в некорректном формате, система покажет сообщение "Введите IP или подсеть в CIDR-нотации".

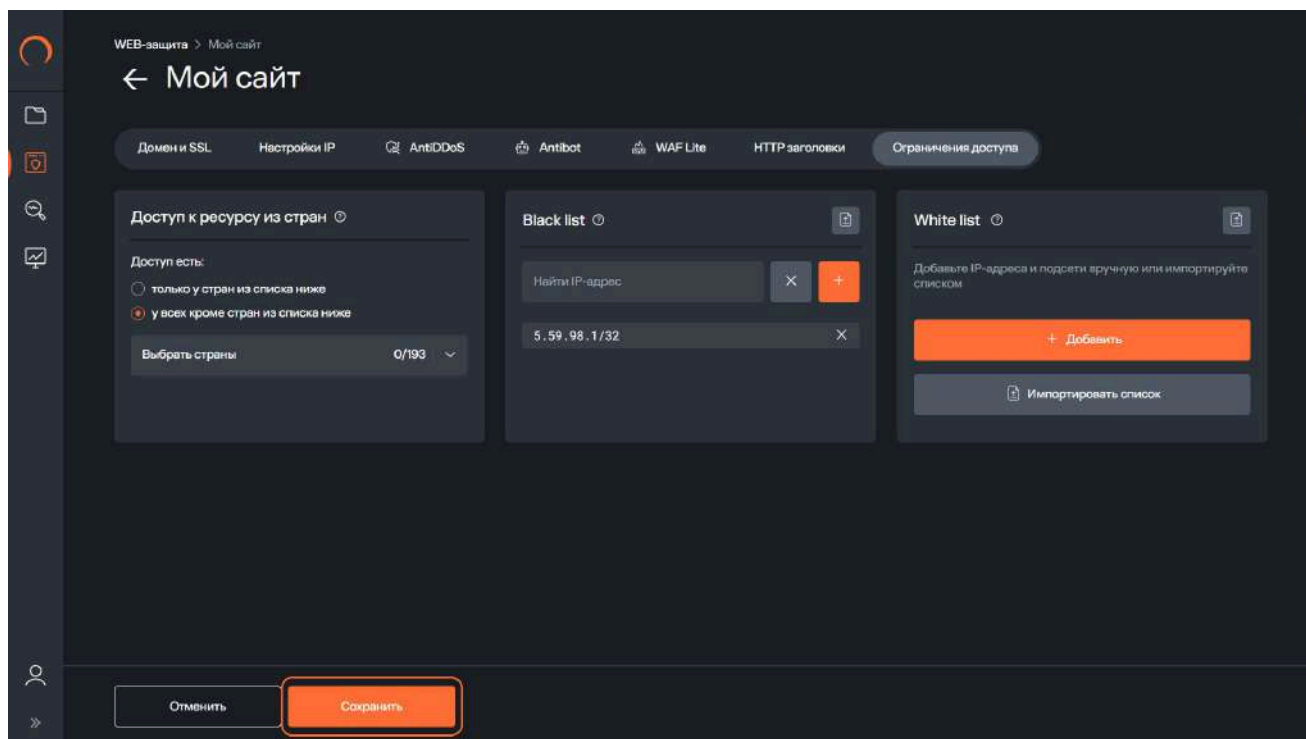
Если ввести IP-адрес сети которая не используется в сети Интернет и предназначена только для частного пользования, под этим полем появится текст "Это зарезервированная подсеть".

ⓘ Обратите внимание

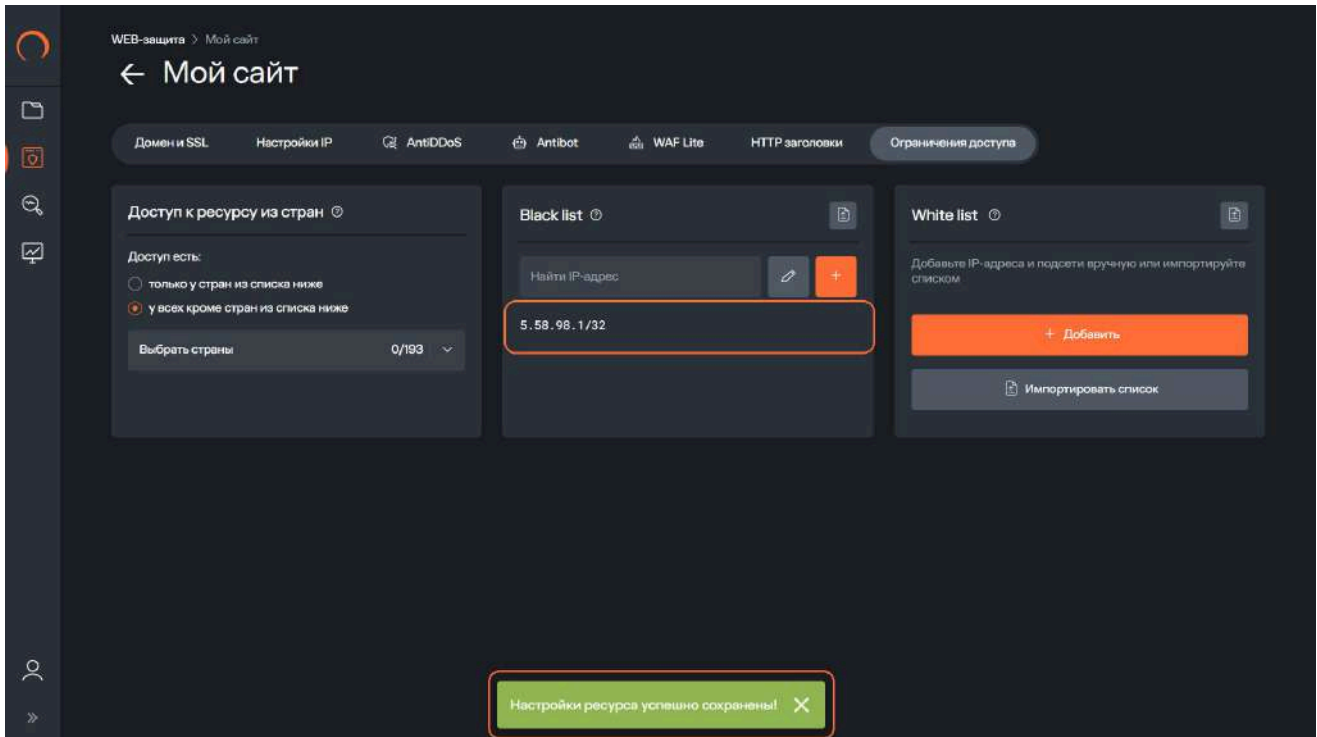
Слеш "/" и число "32" вводить не нужно. Система проставит их сама исходя из введенного вами IP-адреса.



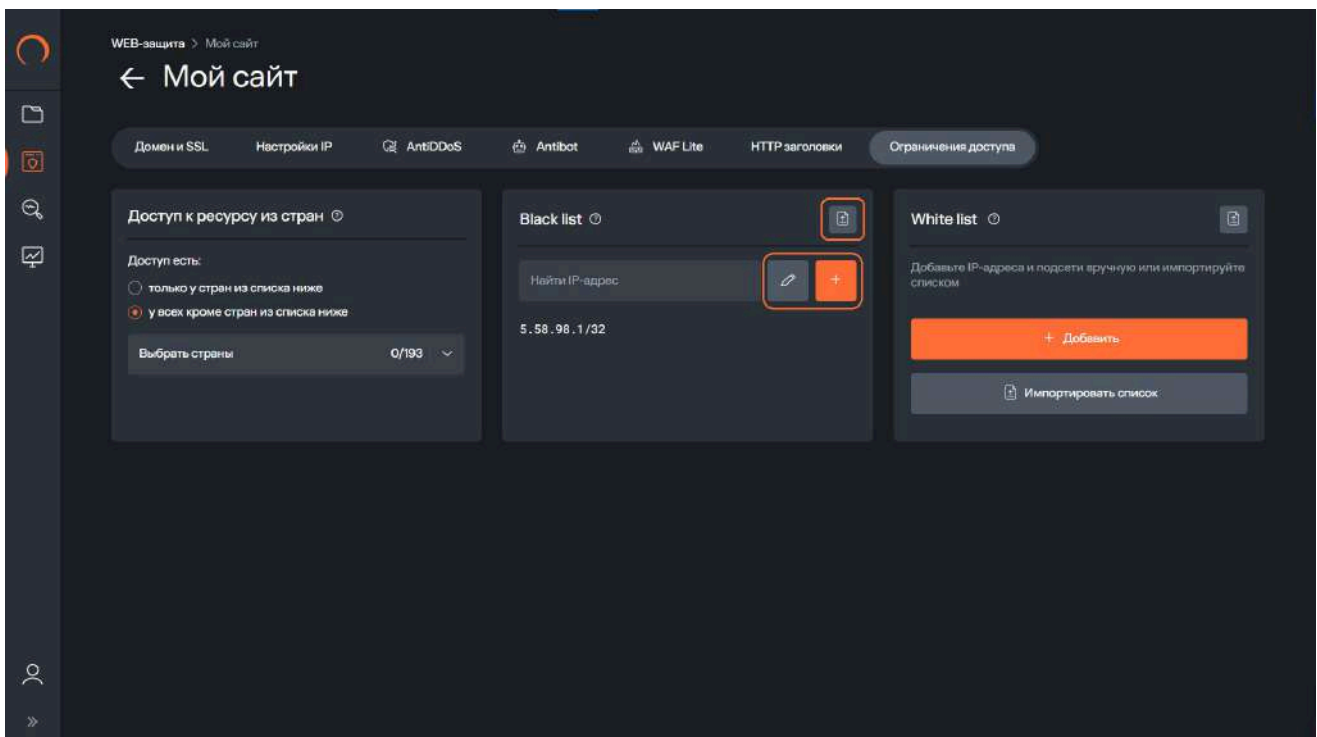
После введения IP-адреса/подсети или загрузки файла со списком нажмите кнопку "Сохранить" в нижней части экрана.



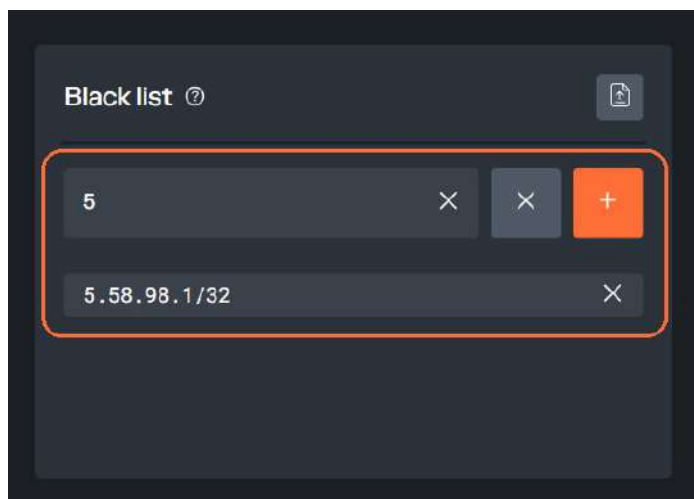
В нижней части экрана вы увидите сообщение "Настройки ресурса успешно сохранены".
Добавленный IP-адрес отражается в списке подлежащих блокировке.



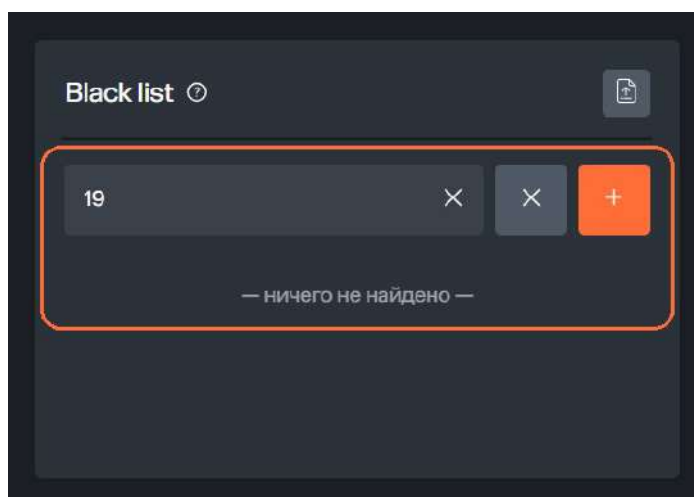
- Если хотите отредактировать введенные данные, нажмите на иконку редактирования рядом с полем поиска
- Если хотите добавить новые IP-адреса/подсети, нажмите на кнопку "+" рядом с полем поиска
- Для загрузки списка нажмите иконку загрузки файла в верхнем правом углу формы



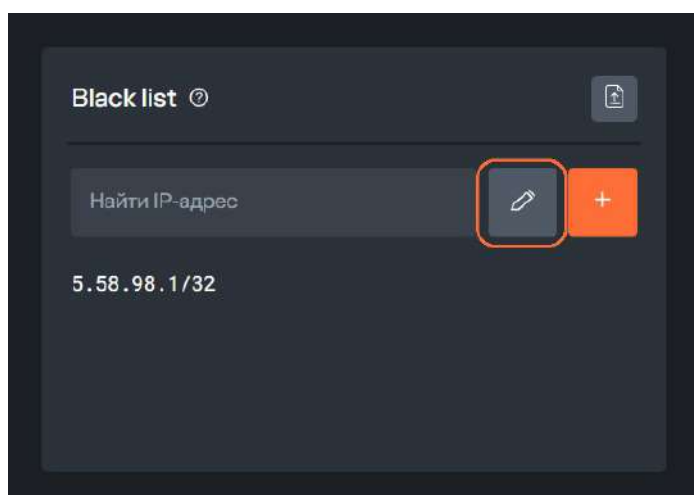
Нужный IP-адрес можно найти через поле поиска. Вы можете задать в нем любой уровень. Если IP-адрес есть в списке, система его найдет.

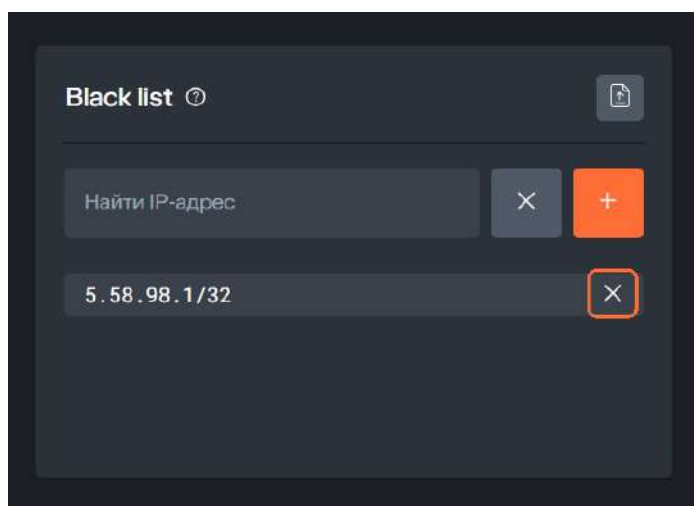


Если IP-адреса нет в списке, вы увидите сообщение "ничего не найдено".

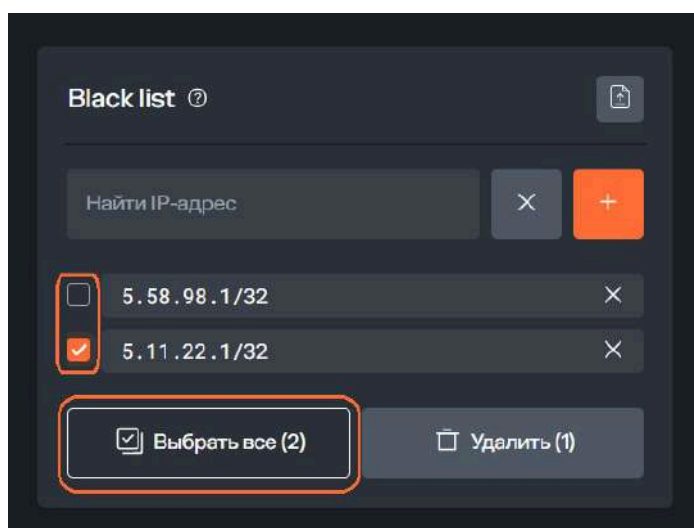


Для удаления IP-адреса из Black list нажмите на иконку редактирования в виде карандаша рядом с полем поиска. После этого найдите нужный IP-адрес в списке и нажмите на крестик справа от него.





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".

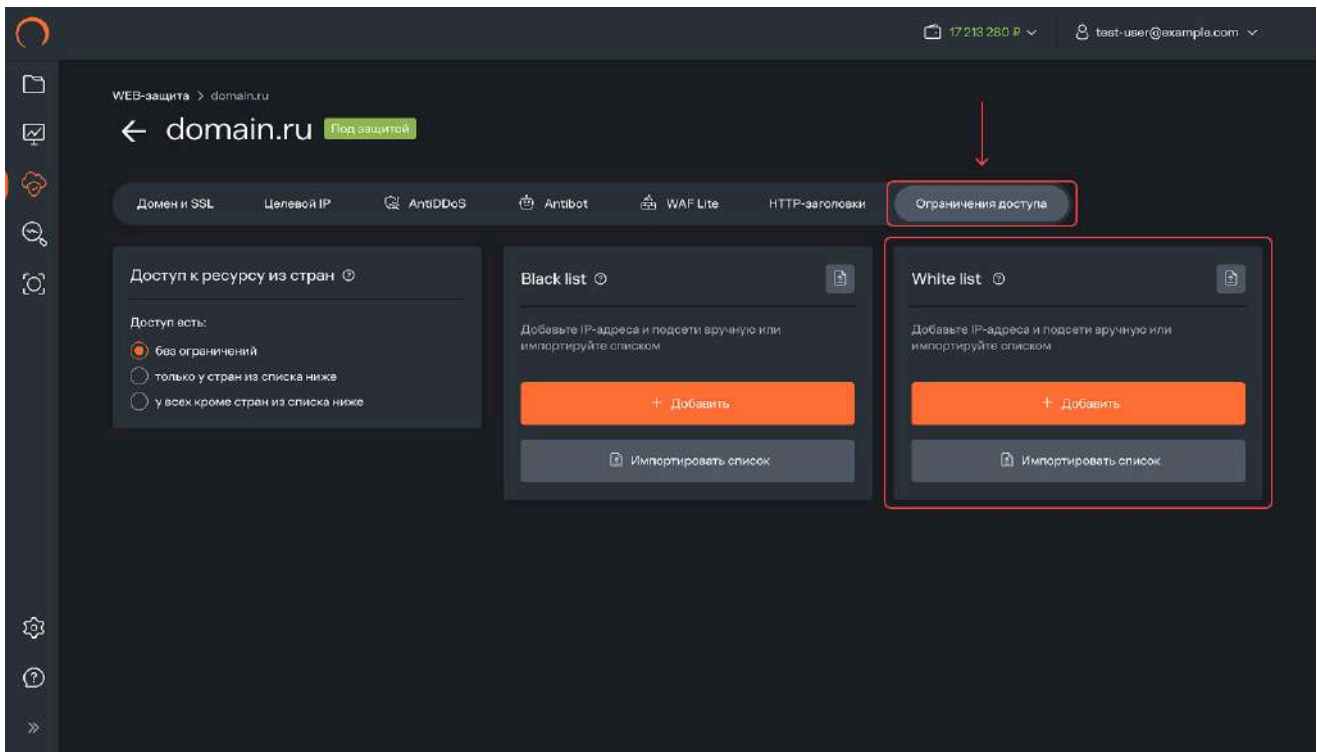


❗ Обратите внимание

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 добавлен в White list, он будет пропущен без дальнейших проверок сервисами защиты.



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

Когда трафик проходит проверку через **Black list** и фильтрацию **по геолокации**, система анализирует, внесён ли в White list IP-адрес, с которого поступает запрос:

- **Если внесён**, пользователь сразу получает доступ к ресурсу.
- **Если не внесён**, запрос направляется на сервисы защиты — AntiDDoS, Antibot или WAF Lite (в зависимости от активных сервисов). После анализа этих запросов система принимает решение о допуске пользователя или блокировке.

Добавление IP-адресов, подсетей и списков в White list выполняется аналогично процедуре в **Black list**. Пользователю доступны те же действия: добавление, редактирование, удаление (выборочное или всех записей).

Добавьте IP-адреса (IPv4) и подсети (группы IP-адресов), запросы от которых система будет пропускать без дополнительных проверок, за исключением фильтров Black list и правил доступа по странам. Адреса можно указать вручную или загрузить списком в формате `.csv`.

ⓘ Обратите внимание

Настройки добавления и импортирования IP-адресов в White list идентичны настройкам Black list.

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:

- **93.185.164.0/25**

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 93.185.164.0/25 -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -s 93.185.164.0/25 -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 93.185.164.0/25 to any port 80 proto tcp comment "Allow HTTP"
sudo ufw allow from 93.185.164.0/25 to any port 443 proto tcp comment "Allow HTTPS"
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 93.185.164.0/25 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 93.185.164.0/25 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=93.185.164.0/25
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:

- **93.185.164.0/25**

Веб-сервер Nginx

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

```
http {  
    ...  
    set_real_ip_from 93.185.164.0/25;  
    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 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 93.185.164.0/25
</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

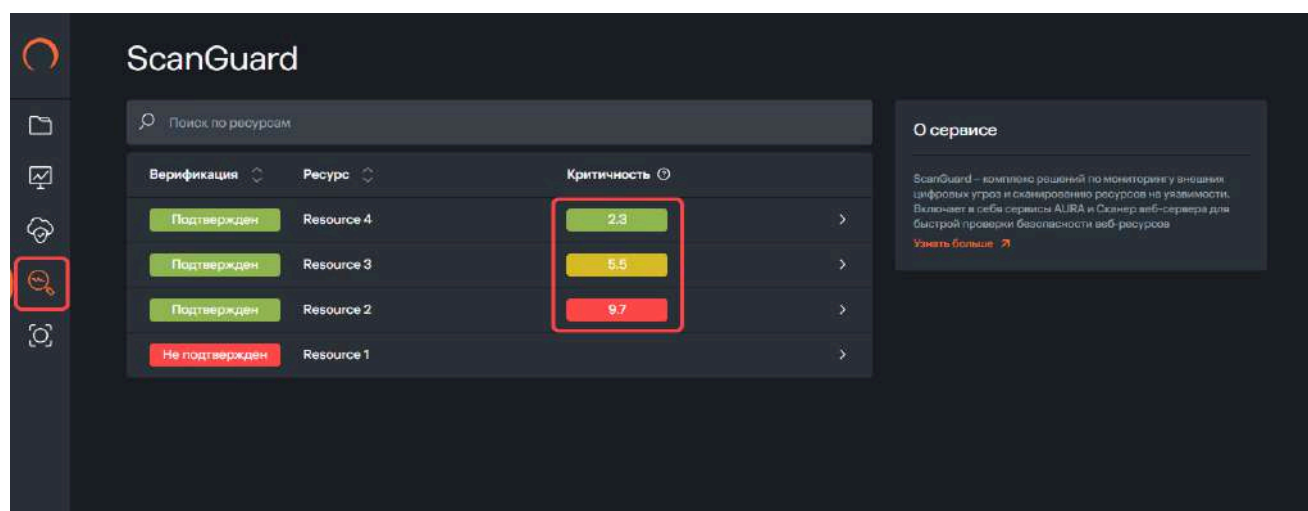
Подробную инструкцию по настройке IIS вы можете прочитать [здесь](#).

Сканирование уязвимостей

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

- [Сканер веб-сервера](#)
- [AURA](#)
- [Zero Day](#)

Перейти на страницу "ScanGuard" вы можете из бокового меню, нажав на иконку "ScanGuard".



На странице ScanGuard в личном кабинете отображается список ваших ресурсов. Для каждого из них показан статус верификации и оценка критичности. Она появляется только после успешной верификации, когда ресурс получает статус "Подтвержден".

При открытии ресурса вам доступны сервисы для сканирования: [Сканер веб-сервера](#) и [AURA](#)

Сканер веб-сервера

Облачный сканер веб-сервера — сервис для контроля защищенности внешнего периметра компании. Он сканирует IP-адреса и выявляет уязвимости, которыми могут воспользоваться злоумышленники для получения доступа к конфиденциальным данным, управлению сайтом и т.д.

Возможности сканера:

- Порт-сканирование — автоматически выявляет открытые порты в сетевой инфраструктуре и идентифицирует работающие на них типы сервисов и ПО
- Проверка уязвимостей по агрегированным базам данных — по собственной базе, БДУ ФСТЭК, NIST NVD (Национальная база уязвимостей США), Exploit-DB, CVE и другие публичные репозитории, узкоспециализированные базы (например, WordFence для анализа уязвимостей WordPress)
- Анализ криптографических уязвимостей — проверяет алгоритмы шифрования на соответствие современным стандартам безопасности, выявляет слабые протоколы (SSL/TLS устаревших версий, некорректные настройки SSH, уязвимые cipher suites)
- Поверхностный анализ веб-содержимого — выявляет риски, связанные с конфигурацией веб-серверов (Apache, Nginx и др.), проверяет HTTP/HTTPS-порты на наличие типовых веб-уязвимостей: небезопасных заголовков, устаревших CMS, публично доступных критических файлов
- Аудит конфигураций по протоколам — анализирует настройки сетевых служб (FTP, SMTP, DNS, SMB и др.) на соответствие стандартам и лучшим практикам, обнаруживает уязвимые конфигурации, например, анонимный доступ, отсутствие шифрования, открытые ресурсы
- Формирование рекомендаций — подробно описывает, как устранить уязвимости

Как работает сканер веб-сервера?

При верификации нового ресурса в личном кабинете Solar Space платформа автоматически сканирует IP-адрес и оценивает его уязвимости без вторжения на ресурс клиента. Эта оценка отражается в строке ресурса.

Оценка выводится по 10-балльной шкале CVSS — Общей системы оценки уязвимостей — и соответствует определенному уровню критичности:

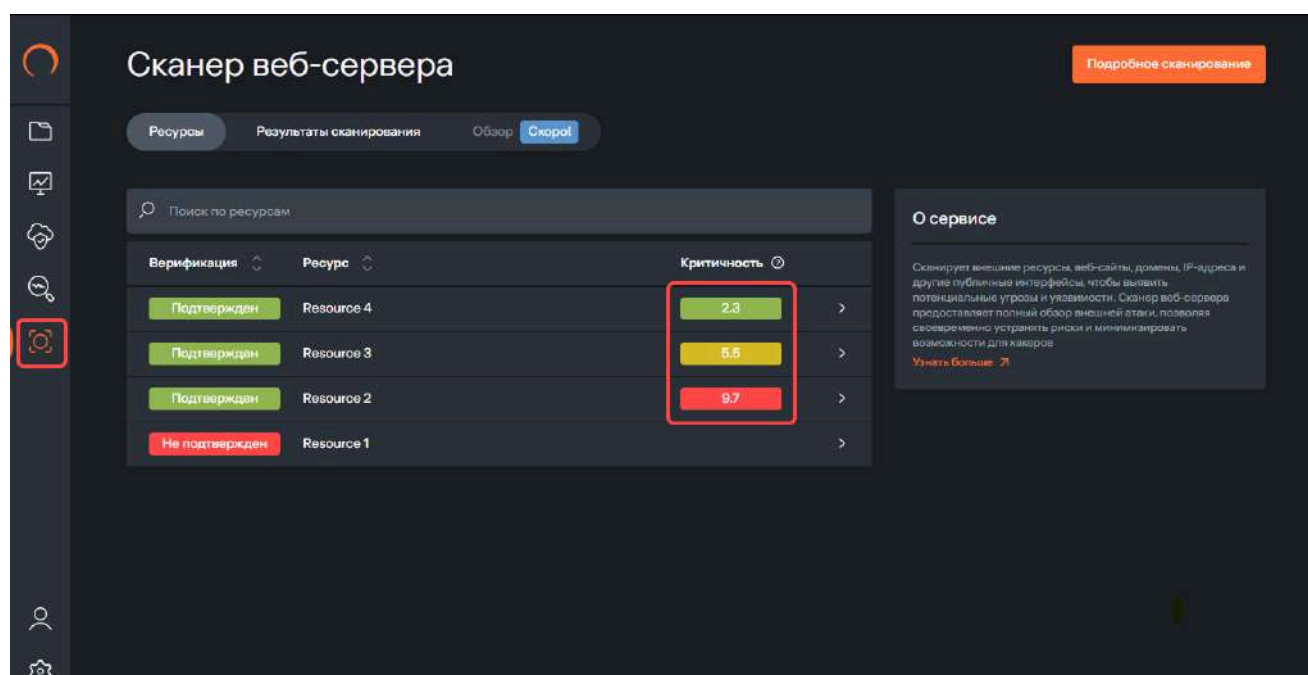
- **0-3** — низкая степень риска
- **4-7** — средняя степень риска
- **8-10** — критическая степень риска

В большинстве случаев по каждому IP-адресу будет выявлено несколько уязвимостей разной степени критичности. В строке ресурса отображается оценка, которая соответствует наиболее критичной из найденных уязвимостей и отражает максимальный уровень опасности.

Оценка уязвимости доступна без оплаты любому пользователю платформы, но она отражает только степень защищенности ресурса. Для того, чтобы увидеть полный отчет всех уязвимостей, на основе которого и сформирована эта оценка, необходимо просканировать ресурс.

Как просканировать?

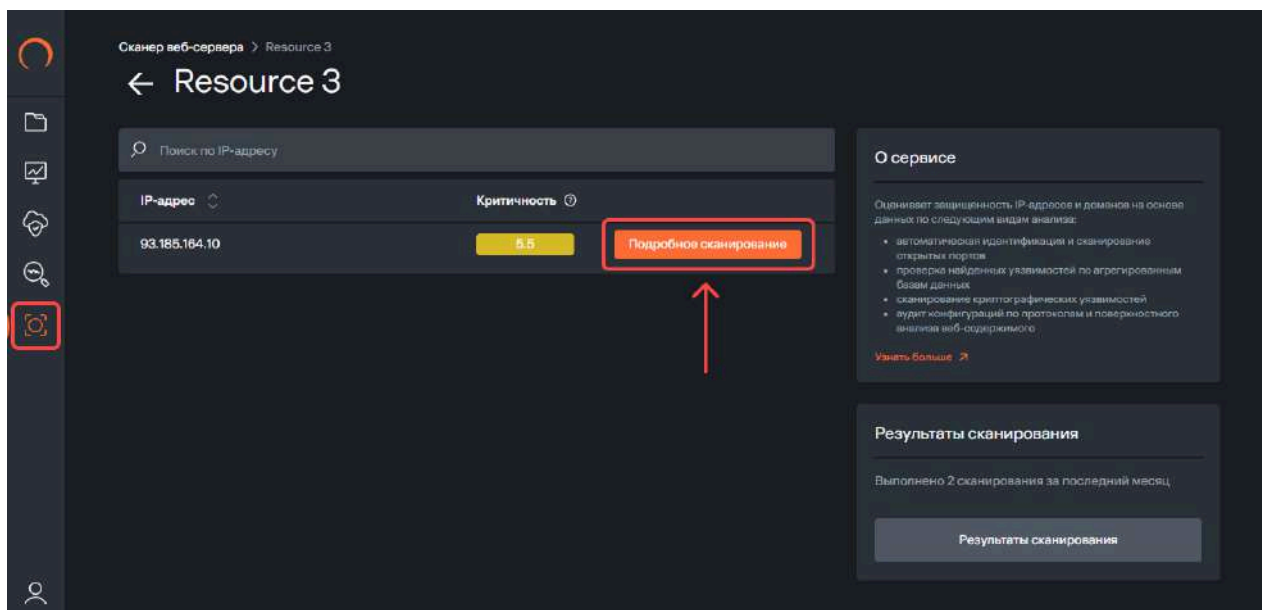
Для сканирования IP-адресов перейдите на вкладку "Сканер веб-сервера".



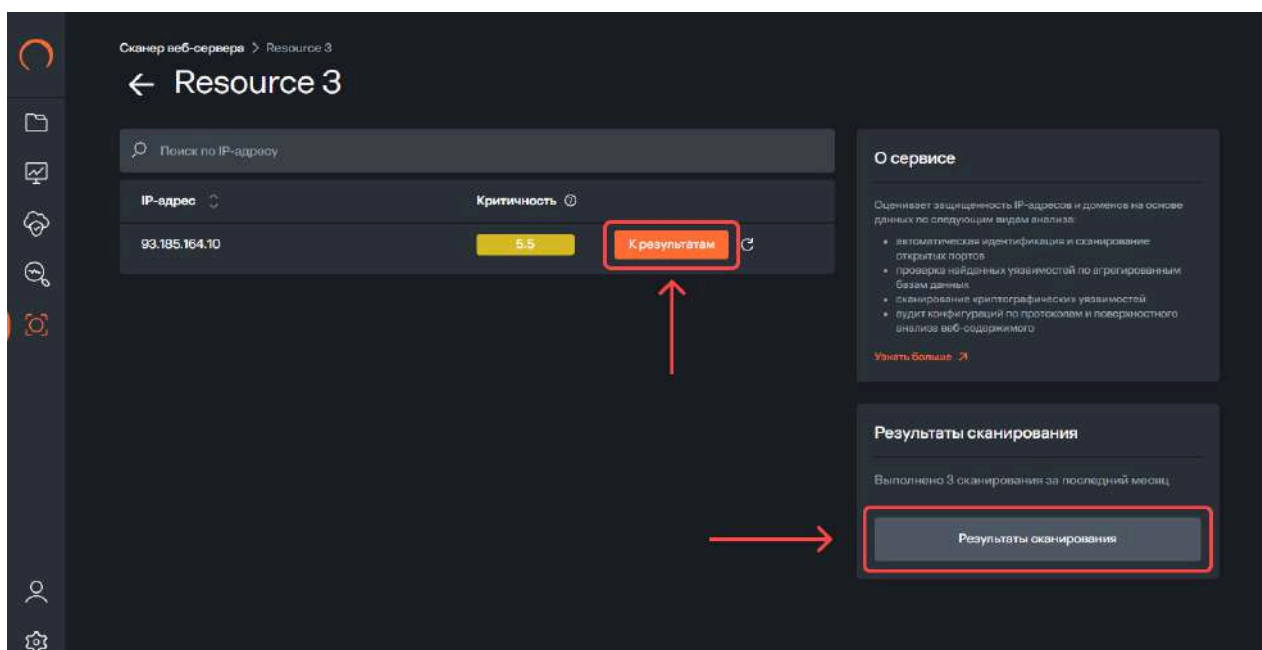
ⓘ Обратите внимание

Сканирование IP-адресов доступно только для верифицированных ресурсов. Для ресурсов со статусом "Подтвержден" отображается оценка критичности по самому уязвимому IP-адресу домена.

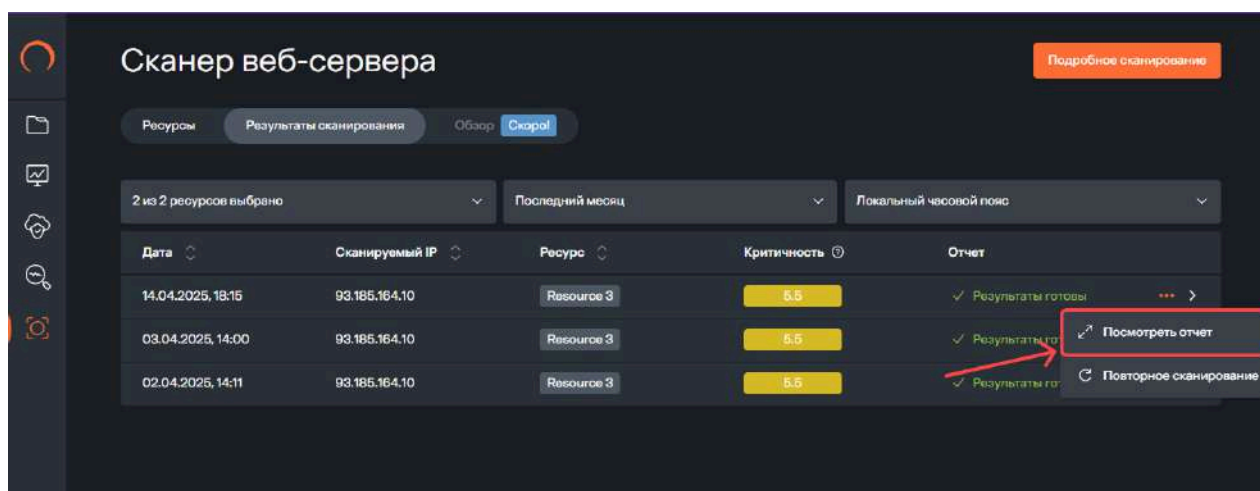
1. Откройте нужный ресурс и нажмите на кнопку "Подробное сканирование" напротив нужного IP-адреса. Обычно процесс занимает не более 1 часа.



2. После успешного сканирования вы можете просмотреть результаты, нажав на кнопку "К результатам" в строке IP-адреса, либо "Результаты сканирования".



3. На странице результатов сканирования для просмотра подробного отчета нажмите на кнопку "Посмотреть отчет" для IP-адреса, который был просканирован.

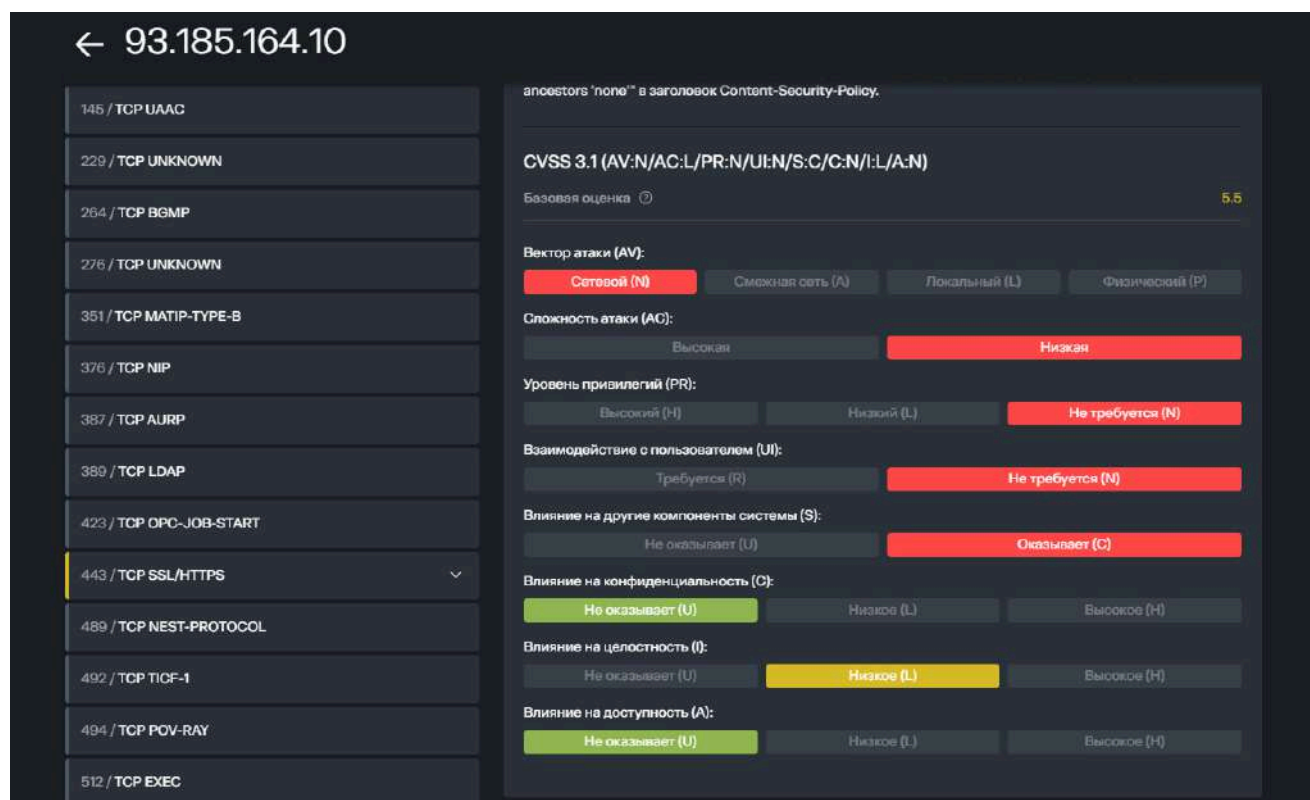


ⓘ Обратите внимание

Просмотр отчета по сканированию доступен только для IP-адресов со статусом отчета "Результаты готовы"

Отчет по сканированию

После открытия отчета на странице вы увидите подробную информацию по каждой найденной уязвимости.



Система формирует общую оценку уязвимости IP-адреса на основе 3 оценок:

- Базовая оценка — основные характеристики уязвимости, которые не изменяются в зависимости от времени и контекста
- Оценка возможности эксплуатации — насколько легко злоумышленникам использовать уязвимость для достижения своих целей
- Оценка последствий воздействия — насколько серьезны для системы последствия эксплуатации уязвимости

Чем ниже оценка по каждому пункту, тем лучше. Самые высокие оценки — от 8 до 10 — соответствуют максимальному уровню опасности.

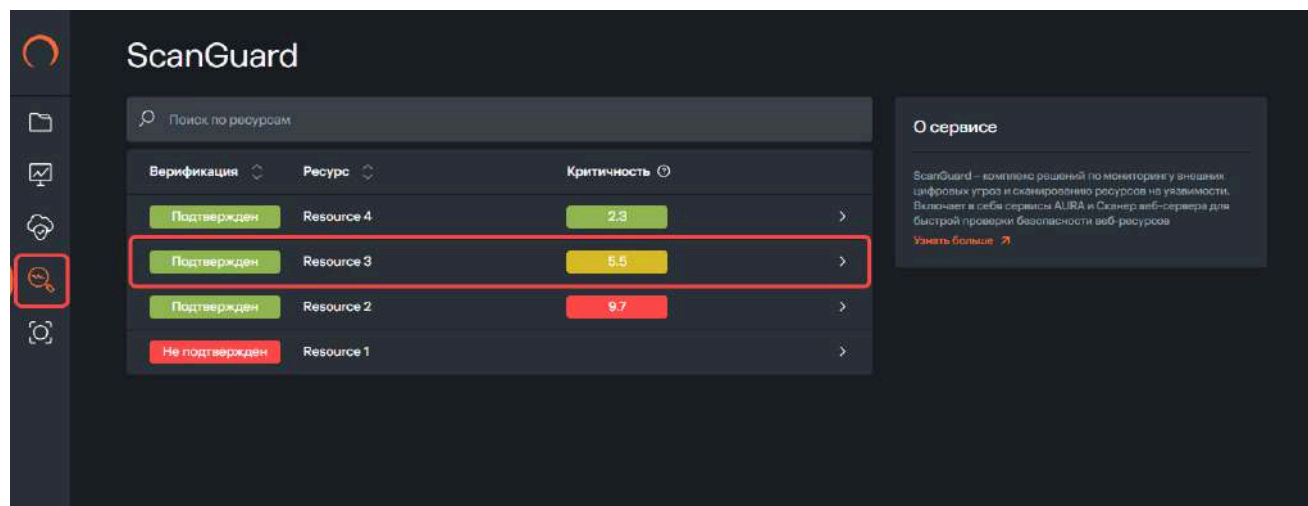
Базовая оценка формируется по нескольким метрикам на основе Общей системы оценки уязвимостей (CVSS):

- Вектор атаки (AV) — отображает, как эксплуатируется уязвимость
- Сложность атаки (AC) — показывает, насколько сложно использовать уязвимость, когда доступ к целевой системе уже получен
- Уровень привилегий (PR) — описывает, какой уровень привилегий и прав нужен злоумышленнику для использования уязвимости
- Взаимодействие с пользователем (UI) — требует ли атака активного участия человека или можно ее автоматизировать
- Влияние на другие компоненты системы (S) — определяет, может ли злоумышленник, эксплуатируя эту уязвимость, повлиять на компонент за пределами его области
- Влияние на конфиденциальность (C) — описывает, насколько уязвимость может повлиять на конфиденциальность данных
- Влияние на целостность (I) — отображает, насколько уязвимость может повлиять на целостность данных
- Влияние на доступность (A) — описывает, насколько уязвимость может повлиять на доступность данных

AURA

AURA — сервис для мониторинга внешних цифровых угроз. Он не требует подключения: доступен без оплаты любому пользователю платформы Solar Space сразу после создания и верификации ресурса. Сервис выявляет фишинговые домены, похожие на ваши, обнаруживает утечки логинов и анализирует открытые порты.

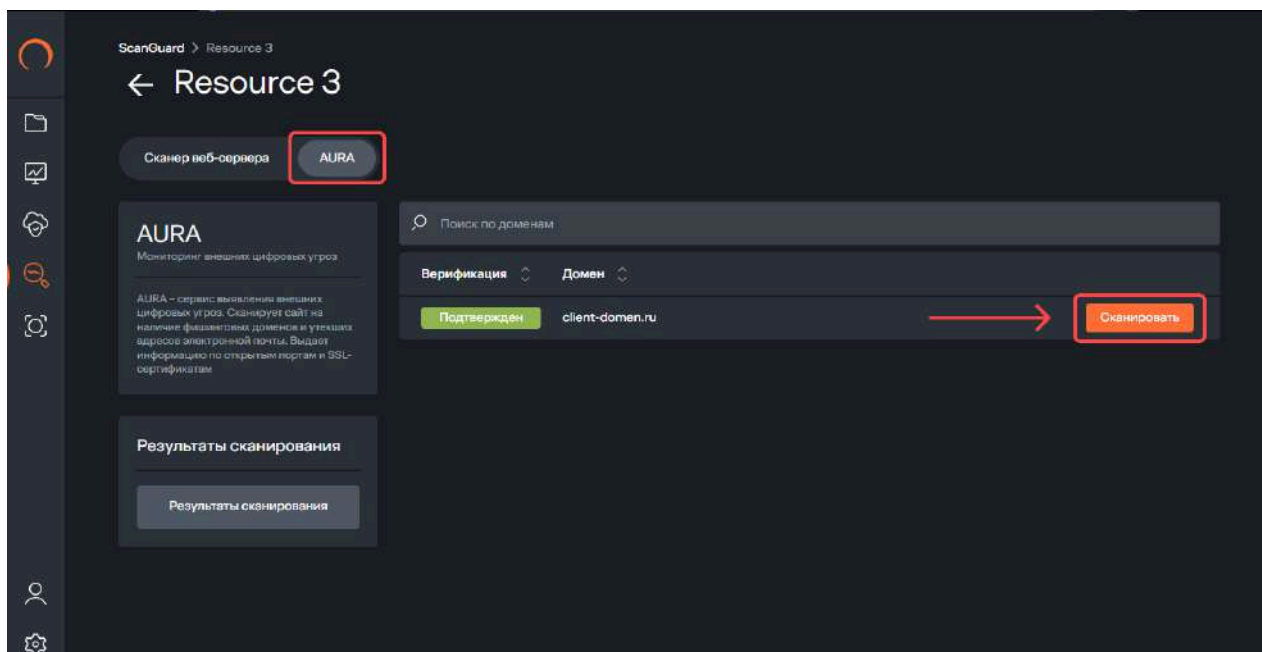
Для сканирования доменов перейдите на вкладку **ScanGuard**, откройте нужный ресурс и перейдите на вкладку AURA.



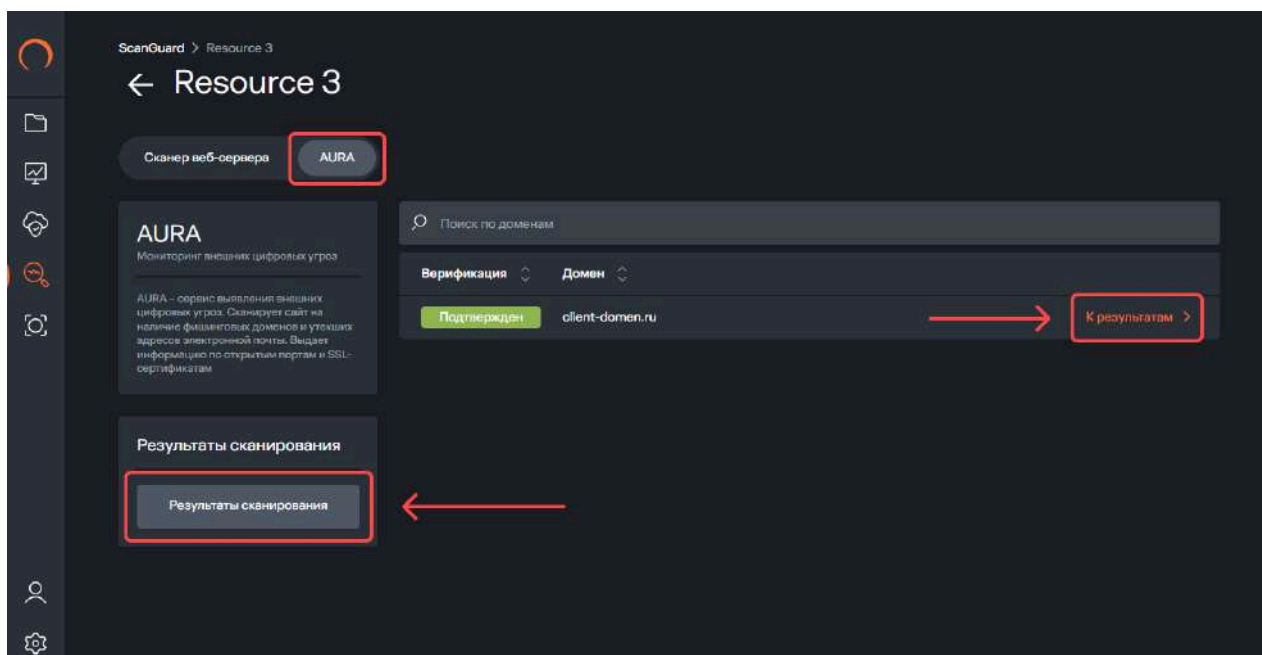
ⓘ Обратите внимание

Сканирование доменов доступно только для верифицированных ресурсов

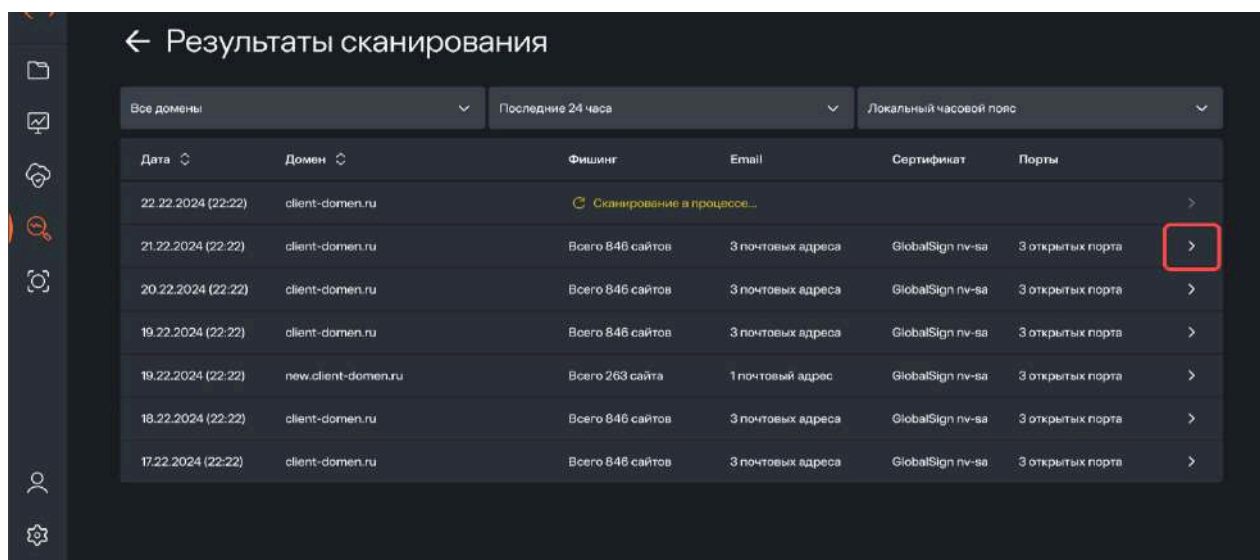
1. Нажмите на кнопку "Сканировать". Обычно процесс сканирования занимает до 30 минут.



2. После успешного завершения сканирования вы можете просмотреть результаты нажав на кнопку "К результатам" в строке домена или "Результаты сканирования".



3. На странице результатов сканирования отображается список всех доменов. Нажмите на стрелочку в строке домена для просмотра информации после сканирования.



← Результаты сканирования

Все домены | Последние 24 часа | Локальный часовой пояс

Дата	Домен	Фишинг	Email	Сертификат	Порты
22.22.2024 (22:22)	client-domen.ru	Сканирование в процессе...			
21.22.2024 (22:22)	client-domen.ru	Всего 846 сайтов	3 почтовых адреса	GlobalSign nv-sa	3 открытых порта
20.22.2024 (22:22)	client-domen.ru	Всего 846 сайтов	3 почтовых адреса	GlobalSign nv-sa	3 открытых порта
19.22.2024 (22:22)	client-domen.ru	Всего 846 сайтов	3 почтовых адреса	GlobalSign nv-sa	3 открытых порта
19.22.2024 (22:22)	new.client-domen.ru	Всего 263 сайта	1 почтовый адрес	GlobalSign nv-sa	3 открытых порта
18.22.2024 (22:22)	client-domen.ru	Всего 846 сайтов	3 почтовых адреса	GlobalSign nv-sa	3 открытых порта
17.22.2024 (22:22)	client-domen.ru	Всего 846 сайтов	3 почтовых адреса	GlobalSign nv-sa	3 открытых порта

4. В открывшемся окне отображается информация о домене после сканирования:

- Фишинговые сайты — 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 — сведения о действующем SSL-сертификате веб-ресурса
- Порты — открытые порты, доступные для внешних соединений

22.22.2024 (22:22)

client-domen.ru

Фишинговые сайты

2021 год:

123 фишинговых сайта

2022 год:

321 фишинговый сайт

2023 год:

456 фишинговых сайта

2024 год:

654 фишинговых сайта

Утекшие email:

mail@mydomain.com, leaked@anotherdomain.ru, bad@thirddomain.info

Сертификат

Регистратор:

GlobalSign nv-sa
GlobalSign GCC R3 DV TLS CA 2020

Домены:

*.mydomain.com, mydomain.com

Зарегистрирован:

24 июня 2024г. в 09:35:44

Истекает:

16 сентября 2024г. в 09:35:43

Шифрование:

TLSv1.2

Серийный номер:

6B:1C:78:03:CE:21:41:BA:50:5C:75:78

Fingerprint (MD5):

B0:4E:DB:E9:0A:19:26:4B:EF:3E:E5:C8:16:A6:E6:8B

Порты (81.1.219.13)

22

Название: SSH

Продукт: OpenSSH

80

Название: HTTP

Продукт: Nginx

443

Название: HTTP

Продукт: Nginx

Назад

Если сервис не обнаружил сведений о фишинговых сайтах, утекших email и сертификатах, для каждого параметра будет отображаться "Не найдено".

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 Awareness

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.

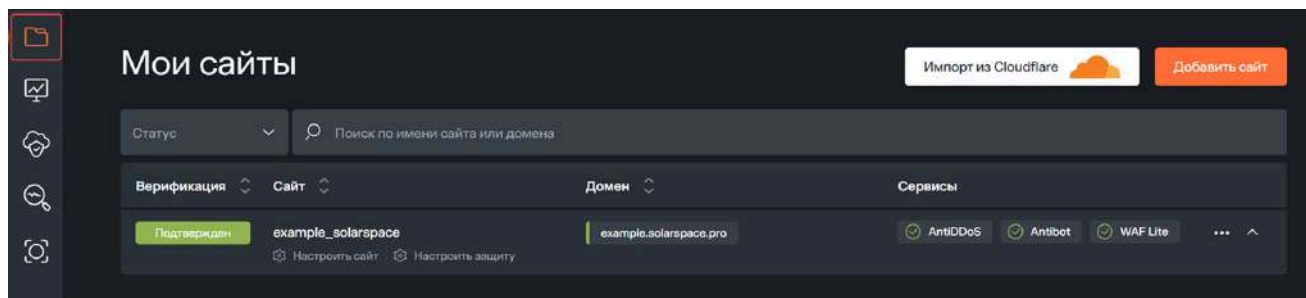
Сервис в разработке. Если хотите протестировать его одним из первых, сообщите об этом письмом на почту solarspace@rt-solar.ru. Мы свяжемся с вами, когда он будет готов к релизу.

Сейчас вы можете подключить сервисы из WEB-защиты: [AntiDDoS](#), [Antibot](#) и [WAF Lite](#).

Мои сайты

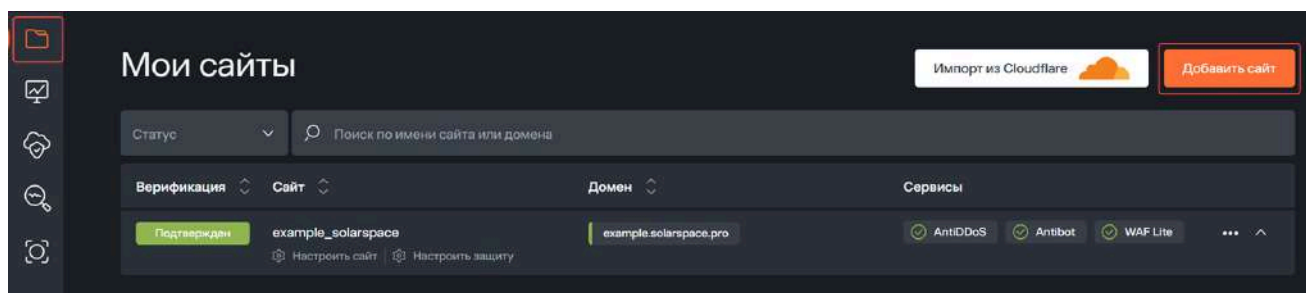
На странице «Мои сайты» отображается список всех созданных вами сайтов.

Для быстрого доступа к странице «Мои сайты» из любого раздела кликните на иконку в виде папки в боковом меню.



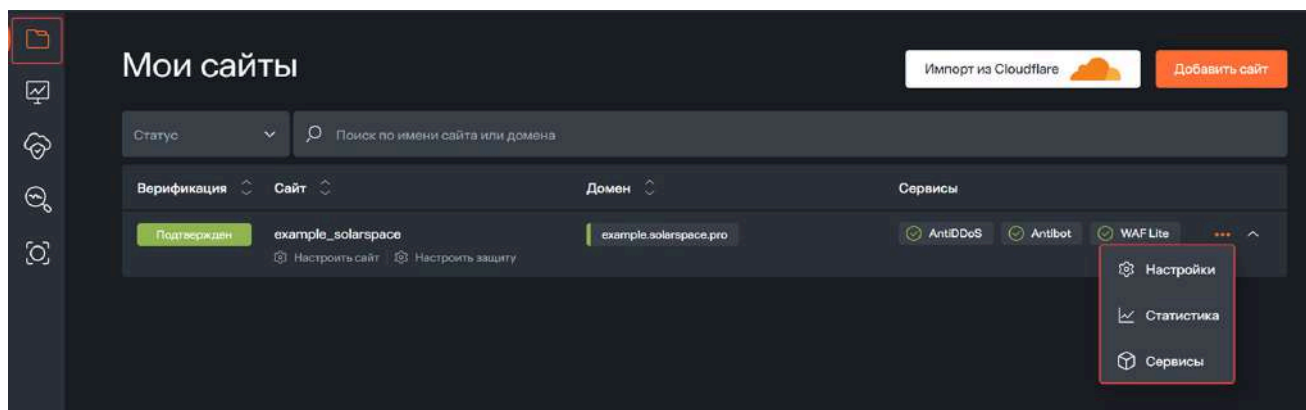
Если у вас ещё нет сайта под защитой Solar Space, выполните шаги из [Быстрого старта](#) — в инструкции подробно описано, как добавить сайт и подключить домен к защите.

В Solar Space один сайт соответствует одному домену. Если нужно подключить к защите ещё один домен, создайте для него отдельный сайт на странице «[Мои сайты](#)».



На странице "Мои сайты" можно:

- Отфильтровать список по статусу через выпадающий список "Статус".
- Найти нужный сайт через строку поиска.
- Посмотреть домен и статусы подключенных сервисов в строке сайта.
- Открыть меню действий по сайту через кнопку с тремя точками.



Из меню действий доступны разделы сайта:

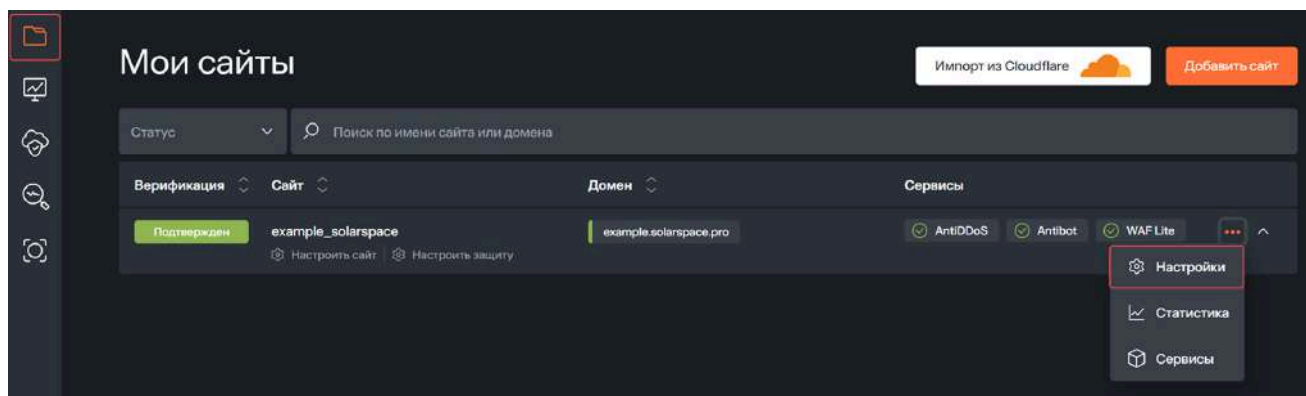
- [Настройки](#)
- [Статистика](#)
- [Сервисы](#)

Чтобы перейти к настройкам, статистике или управлению сервисами конкретного сайта, откройте меню действий «…» в строке сайта и выберите нужный раздел.

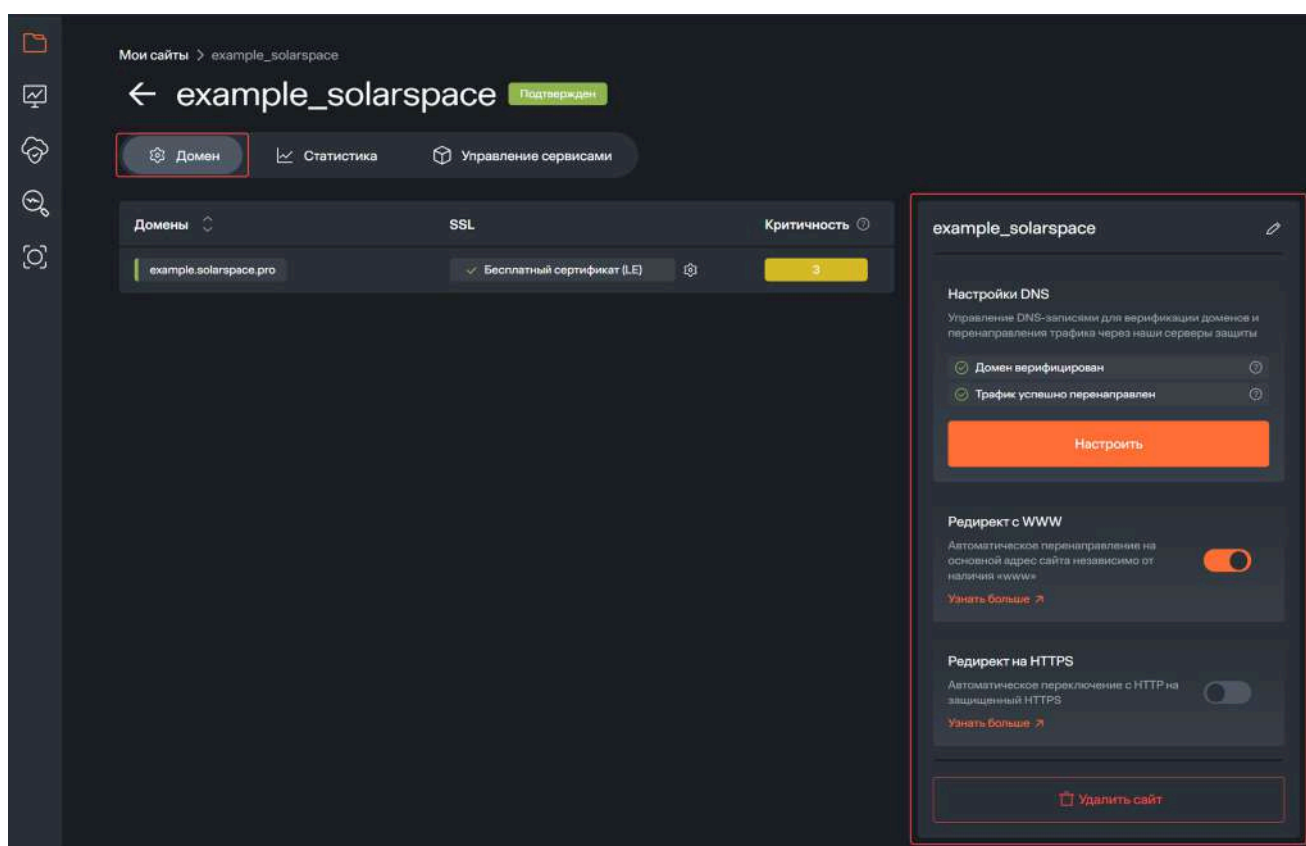
Настройки сайта

Настройки сайта позволяют управлять доменом и параметрами подключения: DNS-записями, SSL-сертификатом и перенаправлениями. Здесь же можно удалить сайт при необходимости.

Чтобы открыть настройки сайта, перейдите на страницу «[Мои сайты](#)». В строке нужного сайта откройте меню действий «…» и выберите пункт «**Настройки**».



На вкладке «Домен» собраны основные настройки, связанные с доменом сайта: DNS-записи, сертификат и поведение перенаправлений. Здесь же можно удалить сайт при необходимости.



На вкладке «Домен» доступны:

- **Настройки DNS** — настройка DNS A-записи для перенаправления трафика на защиту и DNS TXT-записи для подтверждения владения доменом.
 - **SSL-сертификат** — просмотр информации о бесплатном сертификате Let's Encrypt для домена.
 - **Редирект с WWW** — автоматическое перенаправление на основной адрес сайта независимо от наличия `www`.
 - **Редирект на HTTPS** — автоматическое перенаправление с HTTP на защищённый HTTPS.
 - **Удаление сайта** — удаление сайта и отключение подключенных сервисов.
-

Настройки DNS

В блоке «Настройки DNS» настраивается:

- перенаправление трафика на защиту (через DNS A-запись);
- подтверждение владения доменом (через DNS TXT-запись).

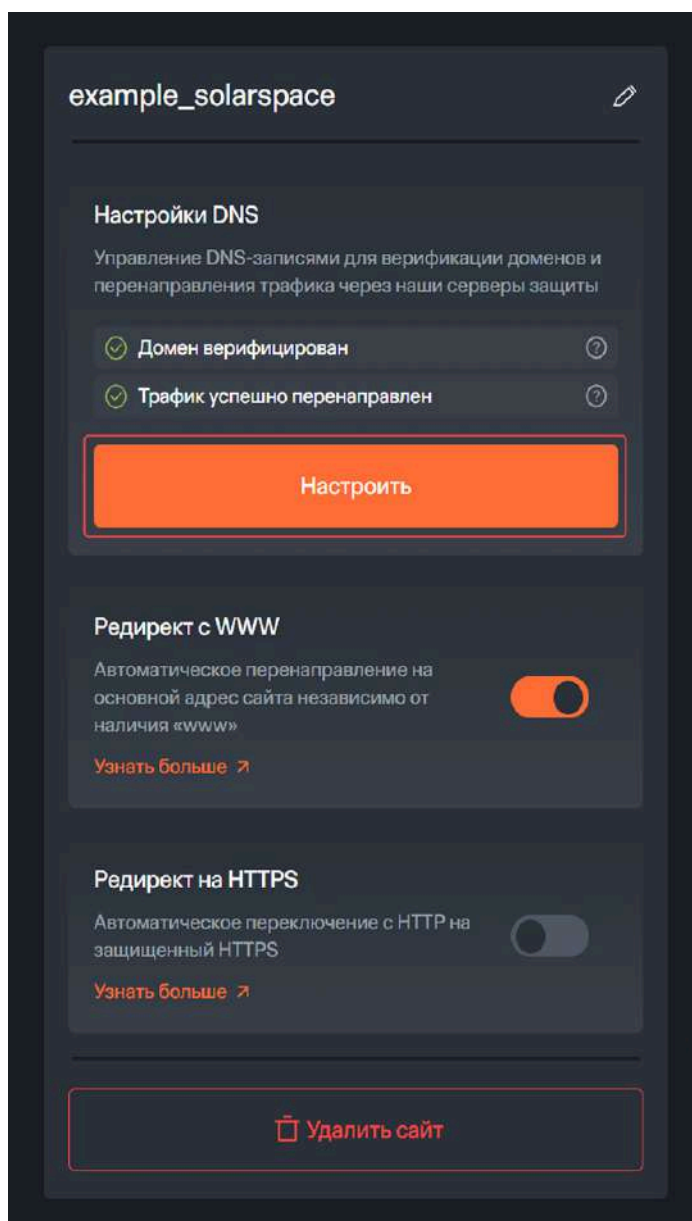
Если вы уже выполняли эти шаги в рамках Быстрого старта, повторно настраивать их не нужно:

- перенаправление трафика: [Постановка домена под защиту](#);
- подтверждение владения доменом: [Верификация домена](#).

ⓘ Важно

В большинстве случаев достаточно настроить DNS A-запись и перевести трафик на защиту — этого хватает для подключения защиты и подтверждения домена. DNS TXT-запись используется, если нужно подтвердить владение доменом без перенаправления трафика (например, чтобы использовать только сервисы сканирования).

Нажмите «Настроить» и следуйте подсказкам в окне «Верификация домена».



Откроется окно «Верификация домена» с двумя вкладками:

- «Перенаправление трафика для подключения защиты» — на этой вкладке отображается значение DNS A-записи, которое нужно добавить у регистратора/хостинг-провайдера.

Верификация домена

Перенаправление трафика
для подключения защиты

Верификация домена
для подтверждения владения доменом

1 Автоматическая верификация

После обновления DNS-A записи и проверки, домен получит статус «Верифицирован». TXT-запись добавлять не нужно

DNS-A

93.185.164.134

Скопируйте запись из поля и добавьте её в настройках DNS у вашего регистратора или хостинг-провайдера

Если возникли сложности с добавлением записи в настройках DNS у регистратора или хостинг-провайдера, воспользуйтесь инструкциями ниже или напишите в поддержку:
support@solarspace.pro

Как добавить DNS-записи в регистраторе nic.ru

Как добавить DNS-записи в регистраторе reg.ru

☐ Я добавил A-запись в настройках DNS у своего регистратора или хостинг-провайдера

Заккрыть

Перенаправить трафик

- «Верификация домена для подтверждения владения доменом» — на этой вкладке отображается значение DNS TXT-записи для подтверждения владения доменом.

Верификация домена

Перенаправление трафика
для подключения защиты

Верификация домена
для подтверждения владения доменом

1 Доступ к сканированию на уязвимости

Верифицируйте домен через DNS-TXT, если подтверждение нужно без перенаправления трафика. После подтверждения система выполнит первичный анализ и определит уровень защищённости. Подключить защиту можно в любой момент — в настройках сайта

DNS-TXT

sc-domain-verification=6ce...

Скопируйте запись из поля и добавьте её в настройках DNS у вашего регистратора или хостинг-провайдера

Если возникли сложности с добавлением записи в настройках DNS у регистратора или хостинг-провайдера, воспользуйтесь инструкциями ниже или напишите в поддержку:
support@solarspace.pro

Как добавить DNS-записи в регистраторе nic.ru

Как добавить DNS-записи в регистраторе reg.ru

☐ Я добавил TXT-запись в настройках DNS у своего регистратора или хостинг-провайдера

Заккрыть

Верифицировать

ⓘ Обратите внимание

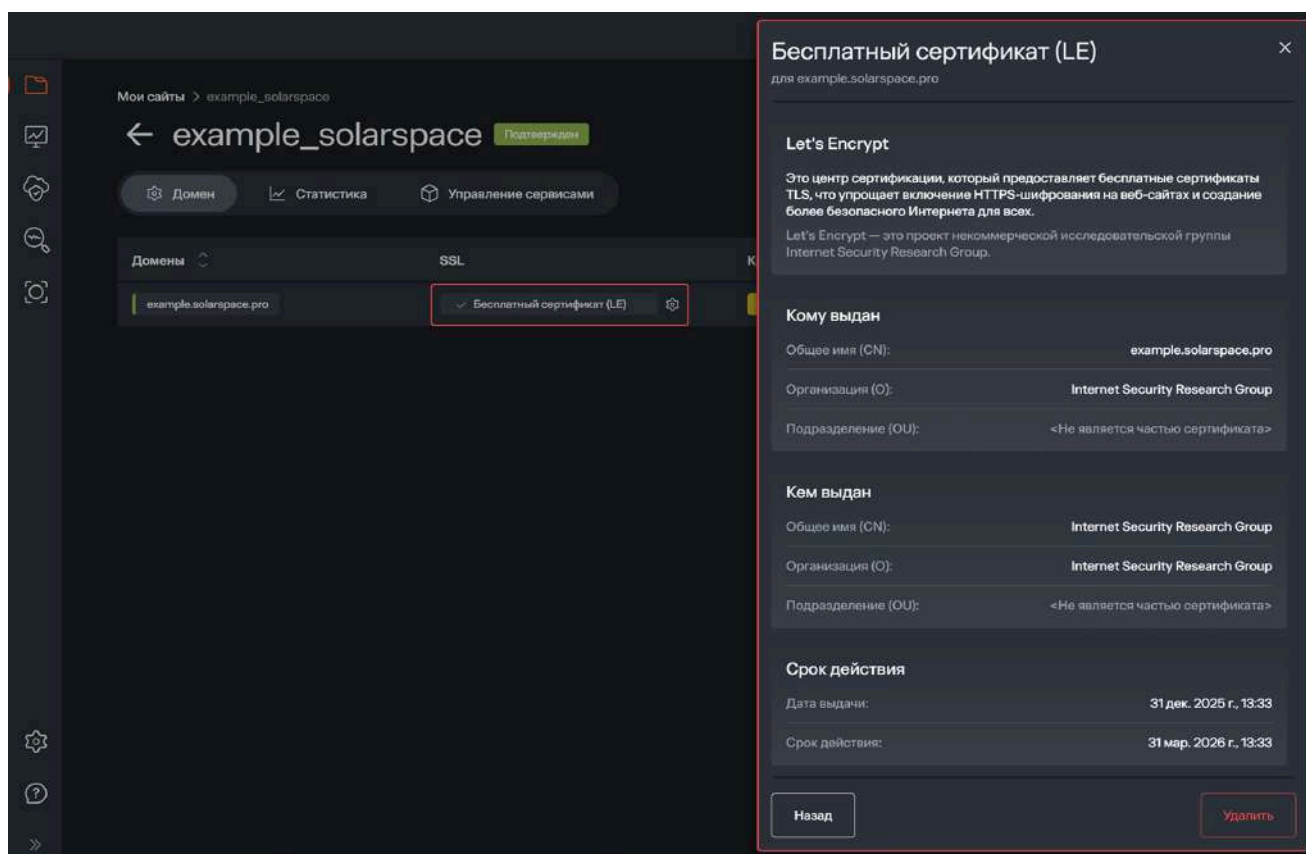
Если после настройки DNS ваш сайт находится в статусе «Не подтвержден», проверьте возможные причины в статье [Ошибки при верификации и перенаправлении трафика](#).

SSL-сертификат

Для домена сайта автоматически выпускается бесплатный SSL-сертификат Let's Encrypt. Сертификат используется для работы сайта по HTTPS и шифрования соединения.

Подробная инструкция по подключению и проверке SSL-сертификата приведена в статье [Домен и SSL](#).

Чтобы посмотреть информацию о сертификате в личном кабинете, откройте вкладку «Домен» и в строке домена нажмите на иконку настроек рядом с полем SSL. В открывшемся окне отображаются основные сведения о сертификате и срок его действия.



Редирект с WWW

Перенаправляет обращения к сайту, введённые с префиксом `www` (например, `www.example.com`), на основной домен без `www` (`example.com`). Функция помогает использовать единый адрес сайта и снижает риск появления дублей страниц в поисковой выдаче. При отключённой настройке обращения с `www` могут завершаться ошибкой «Страница не найдена».

Рекомендуется включать редирект после подключения защиты (после настройки DNS A-записи) в разделе [Постановка домена под защиту](#).

Редирект на HTTPS

Перенаправляет все запросы с небезопасного протокола HTTP на HTTPS.

Редирект работает только при наличии SSL-сертификата. Если SSL-сертификат для домена не добавлен, перенаправление выполняться не будет.

После включения редиректа:

- запросы к `http://` будут автоматически перенаправляться на `https://`;
- сайт будет открываться только по защищённому протоколу.

Рекомендуется включать редирект на HTTPS после [добавления SSL-сертификата](#).

Удаление сайта

Для удаления сайта выполните следующие действия:

1. Нажмите кнопку «Удалить сайт».
2. В появившемся окне нажмите кнопку «Да, удалить сайт».
3. После подтверждения действия появится сообщение об успешном удалении. Сайт будет исключен из списка всех сайтов на странице «[Мои сайты](#)», а все его сервисы будут отключены.

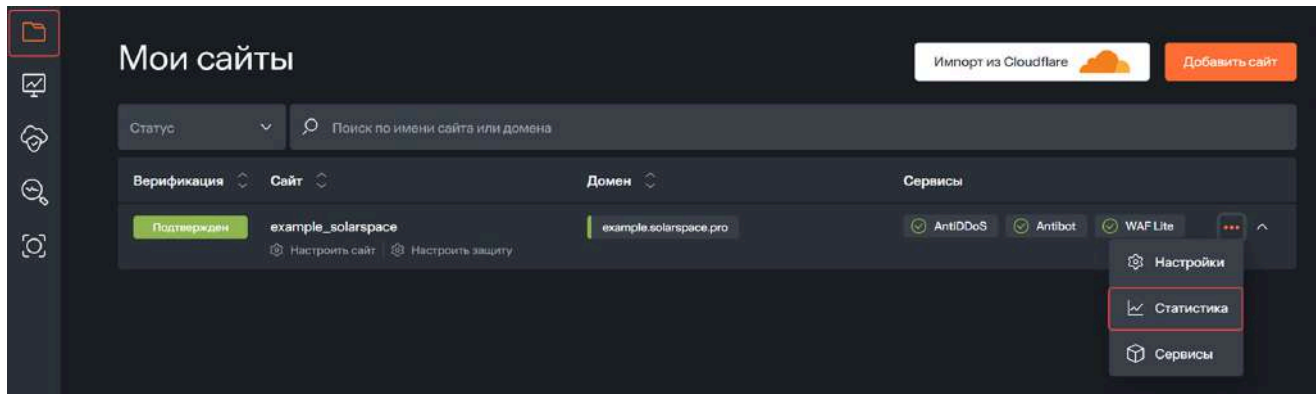
Важно

Удаление сайта приведет к отключению всех его сервисов.

Статистика сайта

Раздел «Статистика» показывает сетевую активность по выбранному сайту: трафик, количество запросов, коды ответов и географию обращений.

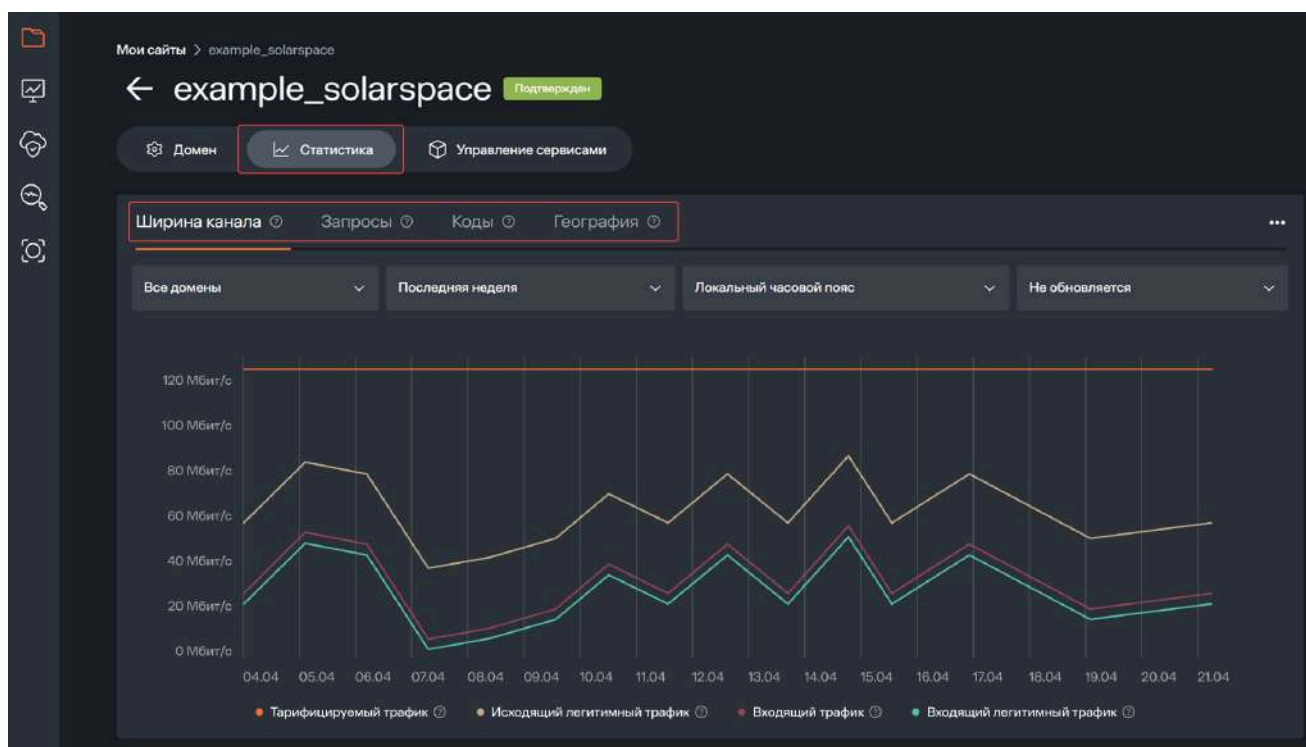
Чтобы открыть статистику сайта, перейдите на страницу «**Мои сайты**». В строке нужного сайта откройте меню действий «⋮» и выберите пункт «**Статистика**».



После перехода откроется страница сайта с вкладкой «**Статистика**». В верхней части доступны четыре отчёта — переключайтесь между ними, чтобы просматривать разные срезы активности.

На вкладке «Статистика» доступны отчёты:

- **Ширина канала** — динамика трафика по сайту.
- **Запросы** — количество входящих запросов и доля легитимных.
- **Коды** — распределение ответов по группам HTTP-кодов (2xx/3xx/4xx/5xx).
- **География** — страны, из которых приходят запросы.

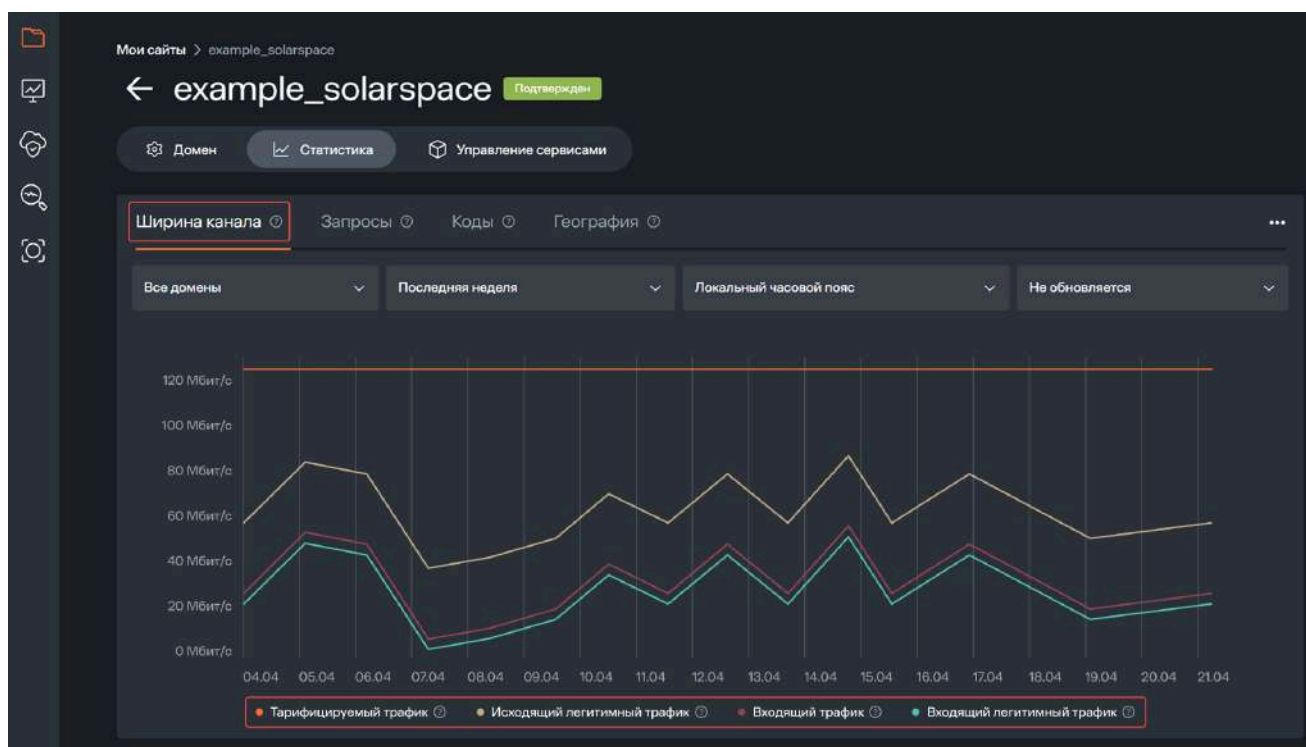


Над графиком расположена панель параметров отображения. В ней можно выбрать домен, период, часовой пояс и режим обновления данных.

Под графиком перечислены показатели — по ним видно, какая линия чему соответствует. Чтобы посмотреть значение в конкретный момент времени, наведите курсор на график. Чтобы оставить на графике только один показатель, отключите лишние показатели в списке под графиком.

Ширина канала

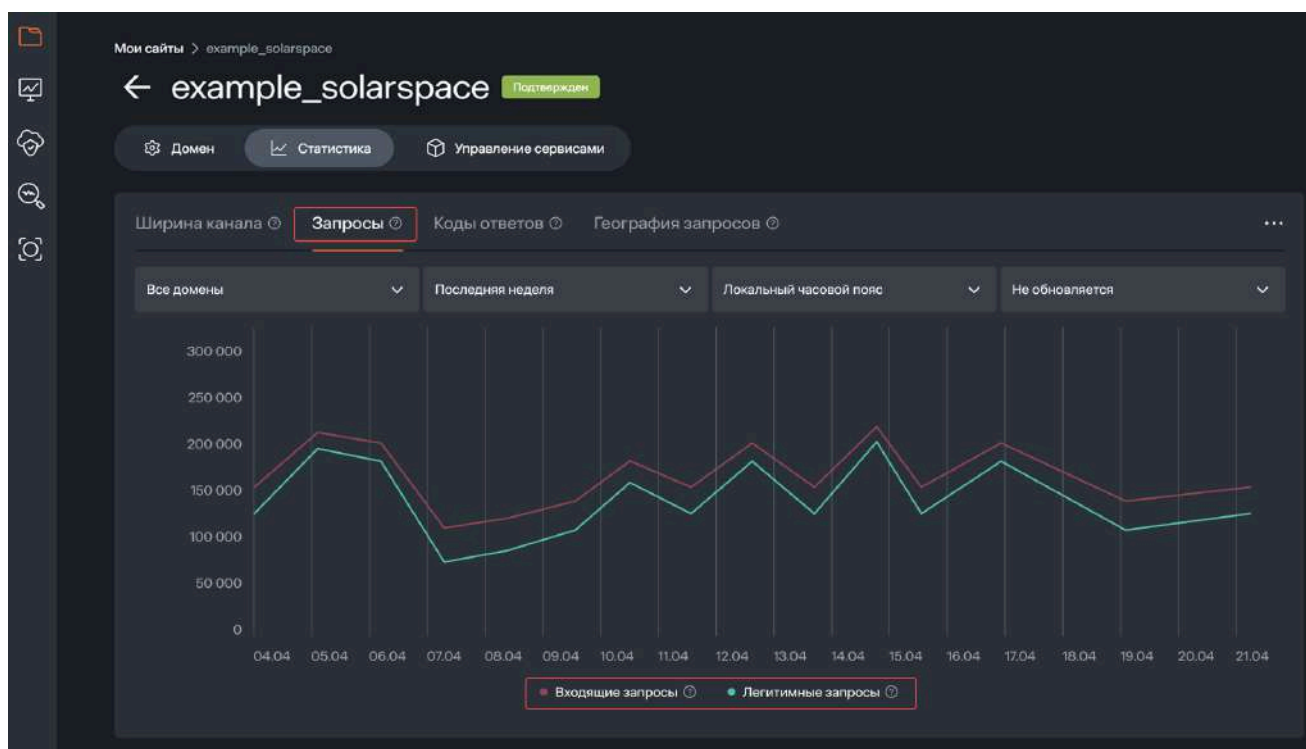
Раздел показывает динамику трафика сайта за выбранный период: входящий и исходящий потоки данных. График помогает оценить общую нагрузку и увидеть периоды повышенной активности.



Резкий рост входящего трафика при относительно стабильном исходящем может указывать на всплеск обращений к сайту, включая нетипичную активность. Синхронный рост входящего и исходящего трафика чаще связан с реальной пользовательской нагрузкой (например, скачиваниями или ростом посещаемости).

Запросы

Раздел показывает динамику количества запросов к сайту и долю легитимных запросов. По графику можно оценить, как меняется общий объем обращений и какая часть трафика распознаётся системой как нормальная активность.

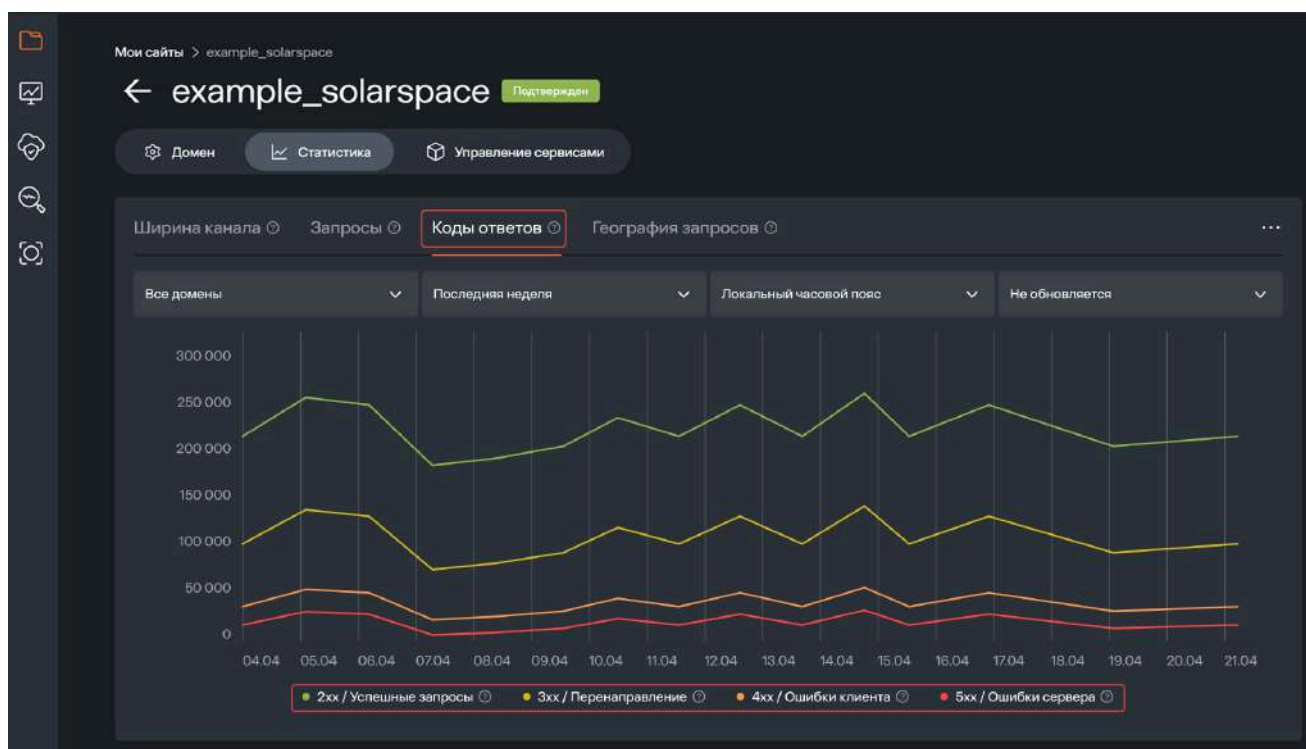


Рост общего числа запросов при одновременном снижении доли легитимных может указывать на увеличение подозрительной активности. Для сопоставления с внутренними событиями (релизы, промо-активность, инциденты) рекомендуется выбирать часовой пояс и период, соответствующие используемому в мониторинге.

Коды

Раздел показывает распределение ответов сайта по группам HTTP-кодов. Отчёт помогает заметить аномалии: рост ошибок (4xx/5xx), увеличение количества редиректов (3xx) или нестабильность backend'a.

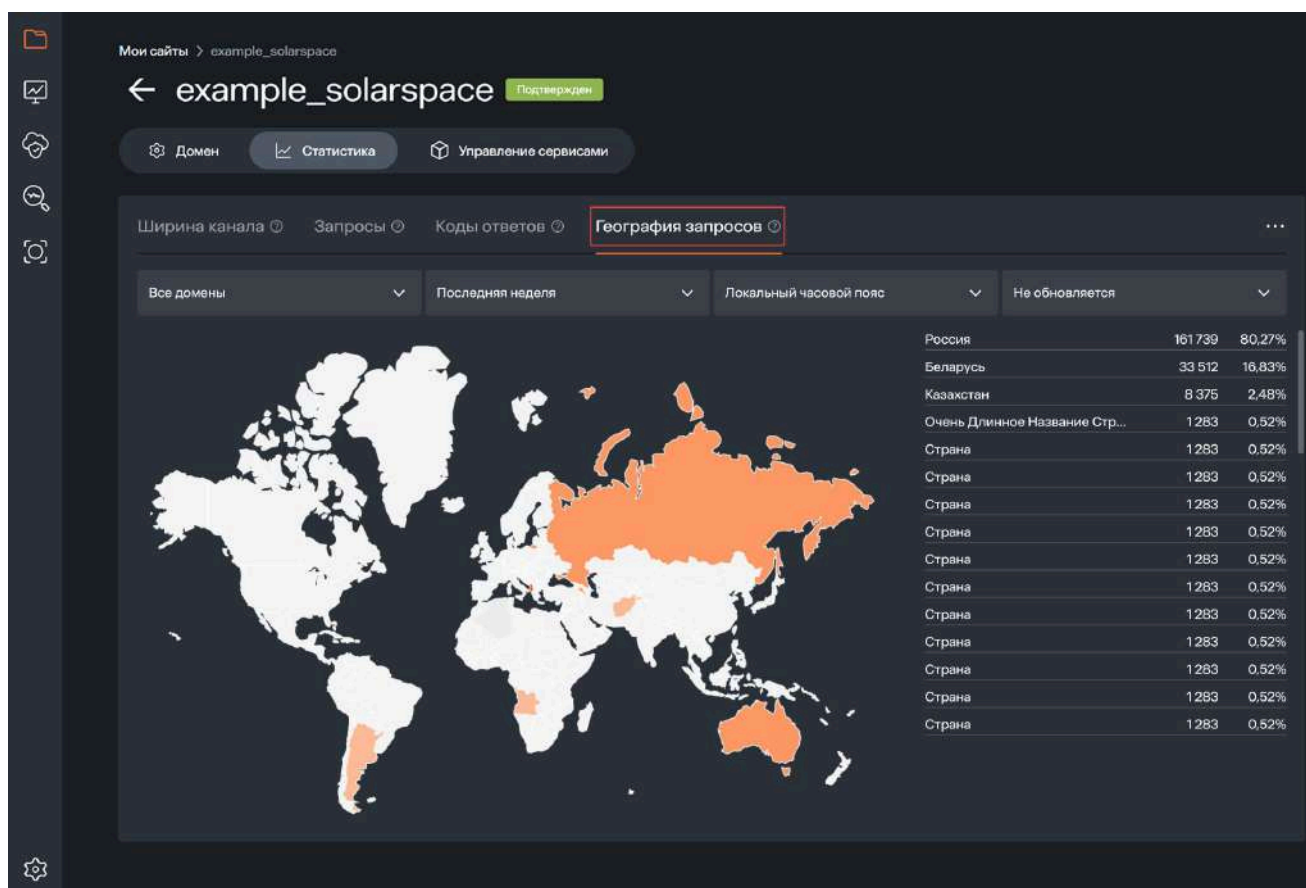
- **2xx** — успешные ответы;
- **3xx** — перенаправления;
- **4xx** — ошибки клиента (например, неверный URL или отсутствующая страница);
- **5xx** — ошибки сервера (проблемы на стороне приложения или инфраструктуры).



Рост доли **4xx** часто связан с неверными URL, бот-сканированием или ошибками навигации. Рост доли **5xx** обычно указывает на проблемы на стороне сайта или инфраструктуры. Для быстрой проверки удобно выбрать короткий период (например, «Последний час») и оценить, носит ли всплеск кратковременный характер.

География

Раздел показывает географию запросов к сайту: карту и список стран. Отчёт помогает определить, из каких стран идёт основная активность, и заметить нетипичные регионы в трафике.



Интенсивность на карте отражает распределение активности, а таблица справа показывает долю запросов по странам в числах. Появление активности из регионов, нехарактерных для сайта, может быть поводом дополнительно проверить источники трафика и настройки защиты.

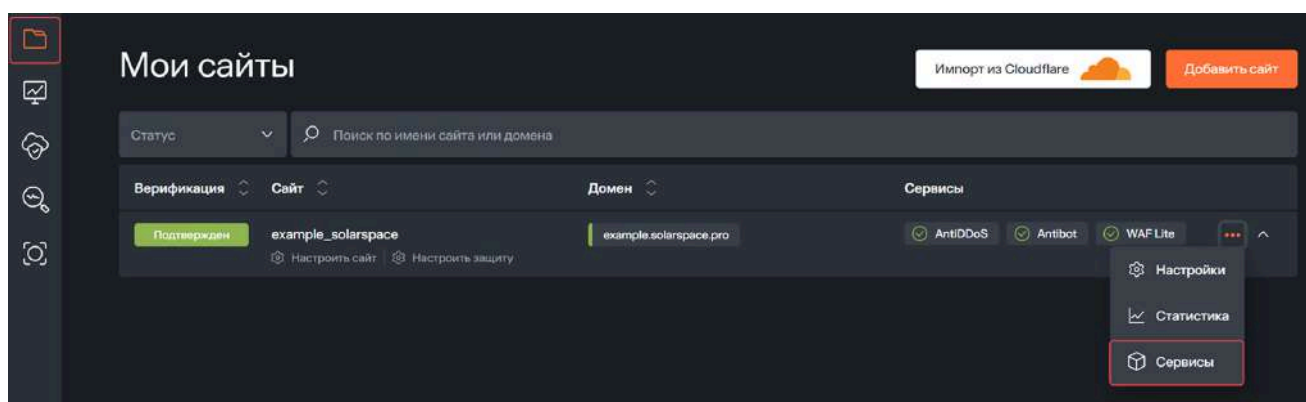
Статистика на странице сайта соответствует данным раздела «Статистика» и отображается для выбранного сайта.

Сервисы сайта

Раздел «**Сервисы**» объединяет основные настройки веб-защиты выбранного сайта в одном месте. Здесь можно:

- перейти к настройкам сервисов **AntiDDoS**, **Antibot** и **WAF Lite**;
- открыть статистику по каждому сервису;
- управлять связанными параметрами веб-защиты: сертификатами, целевым IP, HTTP-заголовками и ограничениями доступа.

Чтобы открыть управление сервисами, перейдите на страницу «**Мои сайты**». В строке нужного сайта откройте меню действий «**⋮**» и выберите пункт «**Сервисы**».



После перехода откроется страница сайта с вкладкой «**Управление сервисами**».

В верхней части доступен переключатель «**Расширенные настройки**» — при включении отображаются дополнительные разделы, например «**HTTP-заголовки**».

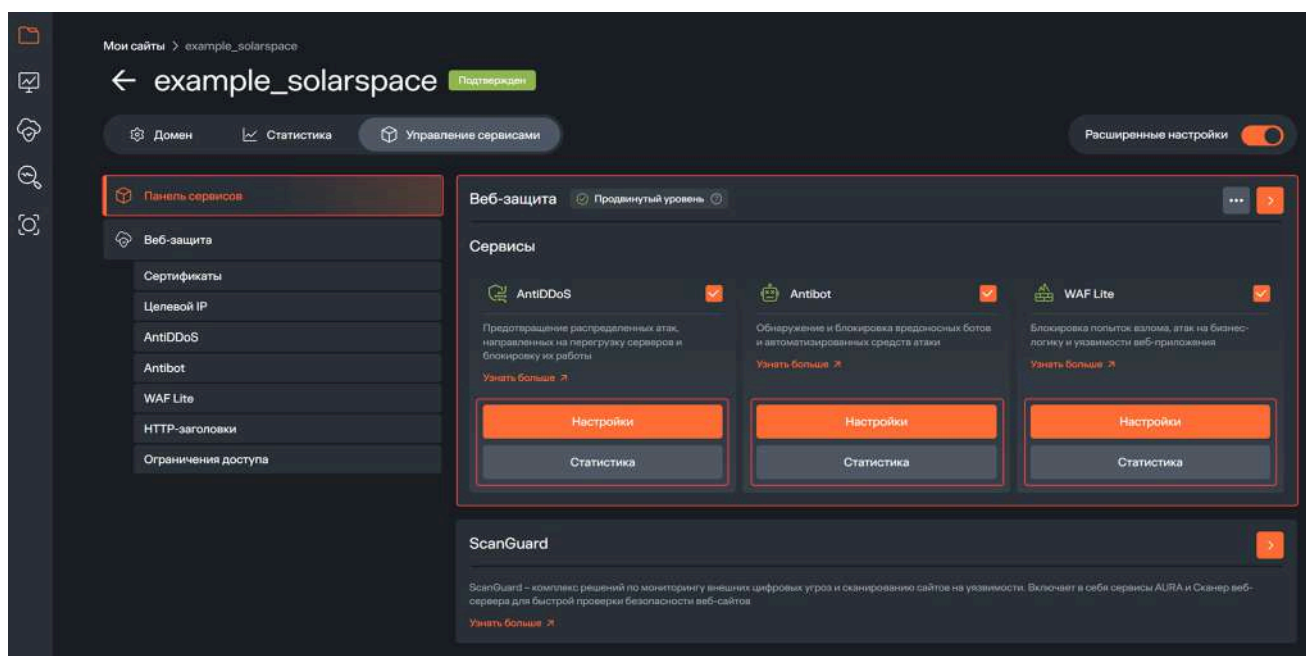
Панель сервисов

Слева расположен список разделов веб-защиты (сертификаты, целевой IP, AntiDDoS, Antibot, WAF Lite и др.).

В центральной части страницы показаны сервисы веб-защиты: **AntiDDoS**, **Antibot** и **WAF Lite**.

Для каждого сервиса доступны:

- **включение и отключение** сервиса (переключатель в правой части плитки);
- переход в **Настройки** сервиса;
- переход в **Статистику** сервиса.

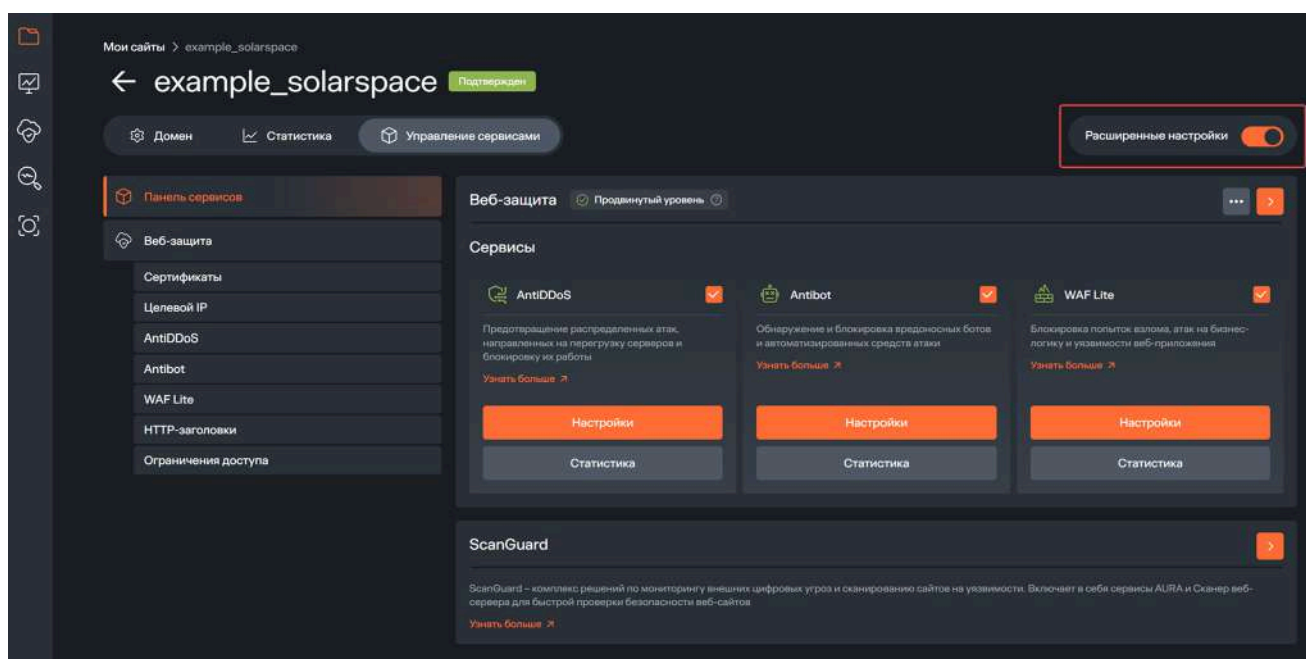


Особенности перехода в статистику:

- **AntiDDoS** открывает **общую статистику сайта**.
- **Antibot** открывает статистику сервиса **Antibot**.
- **WAF Lite** открывает статистику сервиса **WAF Lite**.

Расширенные настройки

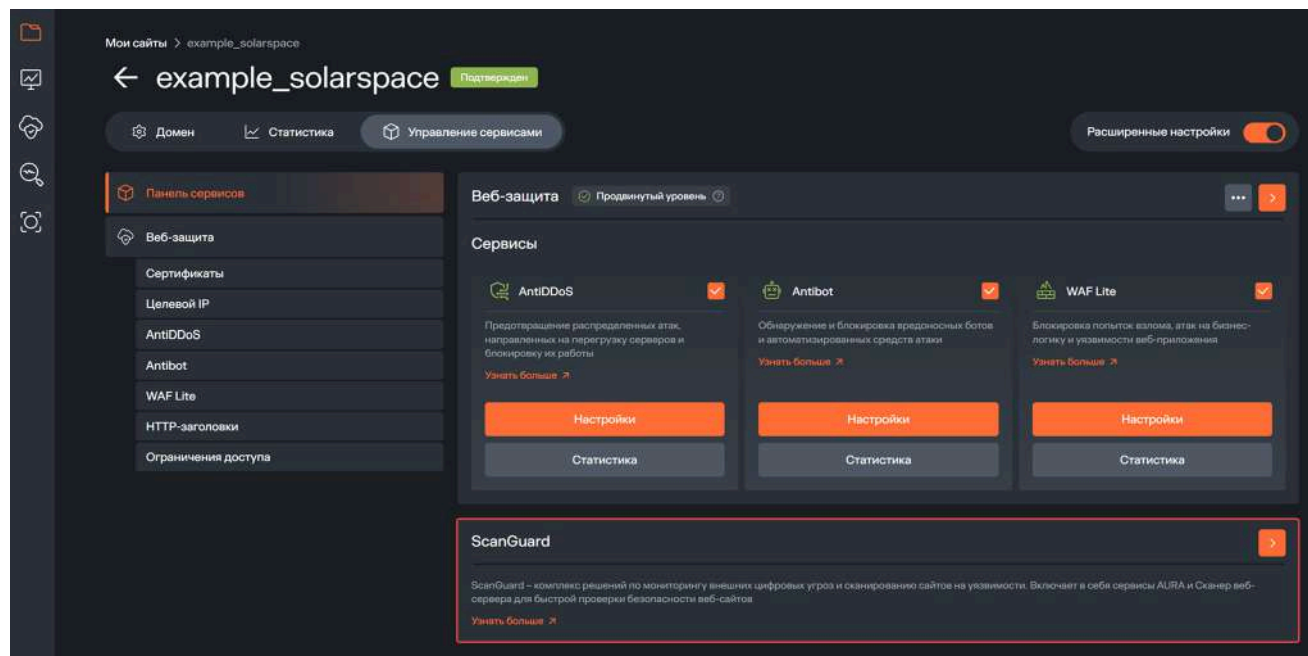
Переключатель «**Расширенные настройки**» включает дополнительные элементы интерфейса в ряде разделов веб-защиты.



Например, при выключенных расширенных настройках **раздел «HTTP-заголовки» не отображается**. Состав расширенных параметров зависит от конкретного сервиса и сценария.

ScanGuard

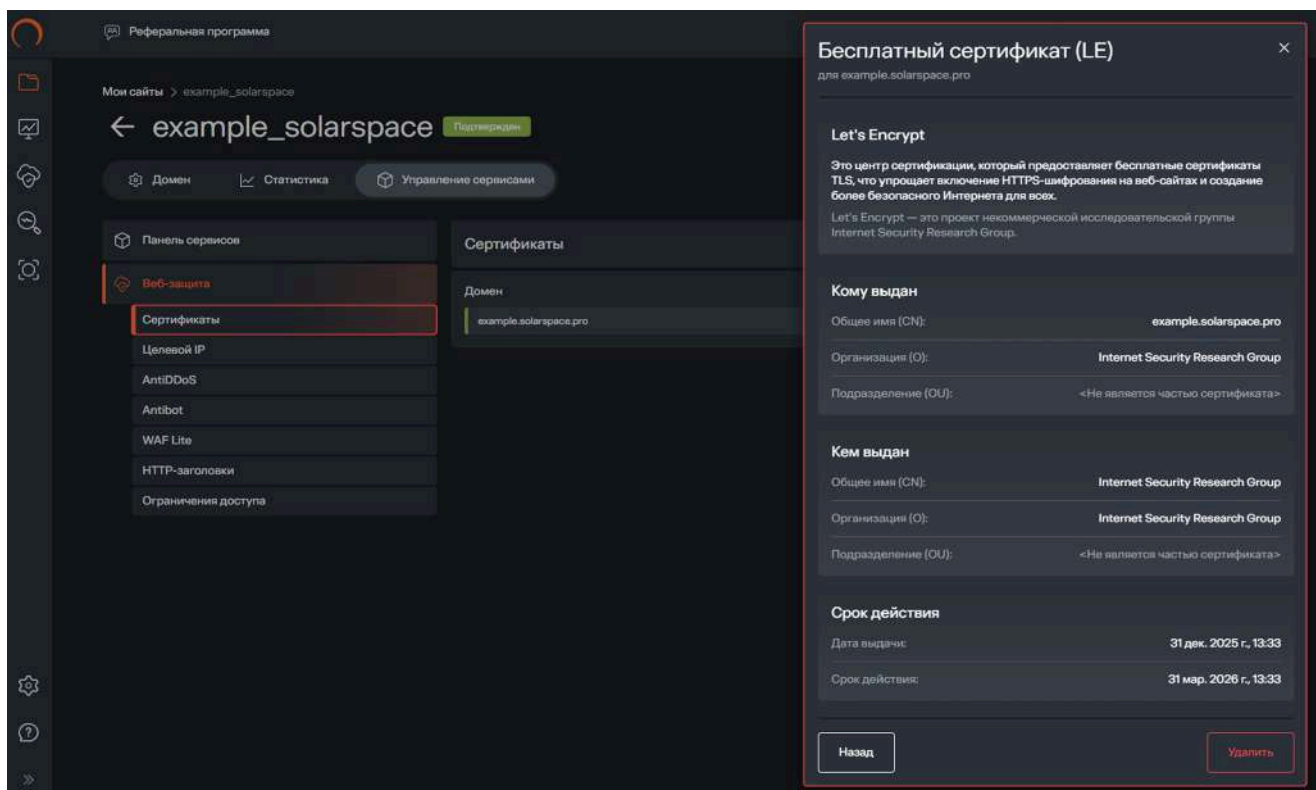
На странице «**Управление сервисами**» также доступен **ScanGuard**.



После перехода по стрелке на плитке ScanGuard по умолчанию открывается вкладка **AURA**. При необходимости можно переключиться на вкладку «**Сканер веб-сервера**».

Сертификаты

Раздел «**Сертификаты**» показывает SSL-сертификат, который используется для домена сайта.

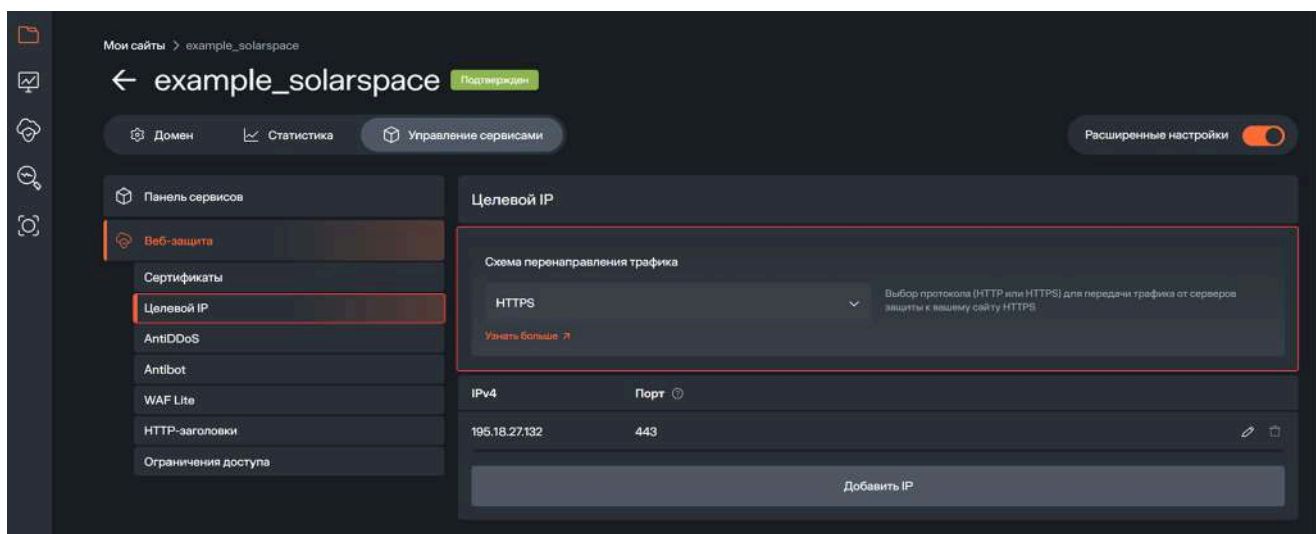


Обычно здесь достаточно проверить, что:

- сертификат выбран для нужного домена;
- сертификат действителен и используется сервисами защиты.

Целевой IP

Раздел «**Целевой IP**» задаёт, **куда передавать трафик после обработки на стороне защиты** — то есть IP-адрес и порт вашего сервера, на который должен попасть запрос после фильтрации.



В этом разделе можно:

- выбрать **схему перенаправления трафика** (HTTP или HTTPS);
- добавить и редактировать **целевые IP-адреса и порты**.

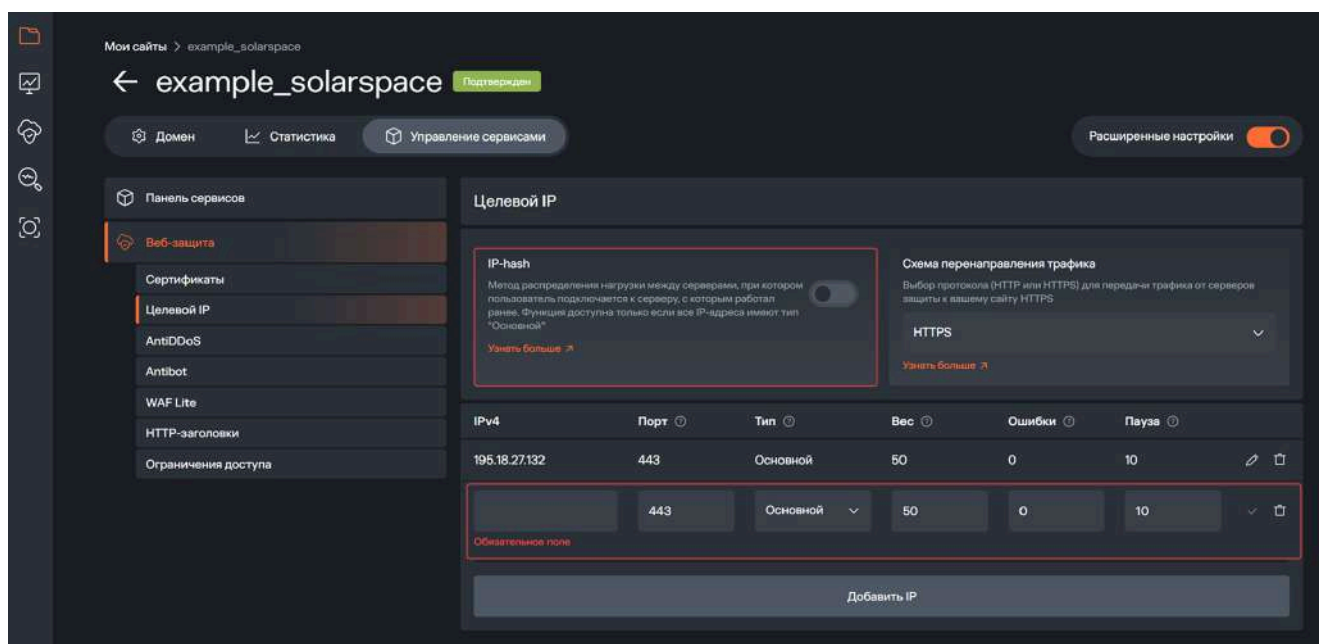
Схема перенаправления трафика

Схема определяет протокол, по которому трафик будет передаваться от серверов защиты к вашему серверу:

- **HTTP** — передача без шифрования. Обычно используется только для тестовых сценариев.
- **HTTPS** — передача в зашифрованном виде. Рекомендуется для рабочих ресурсов.

Добавление целевого IP-адреса

Чтобы добавить IP-адрес сервера, нажмите «**Добавить IP**», укажите **IPv4-адрес** и **порт**, затем сохраните изменения.

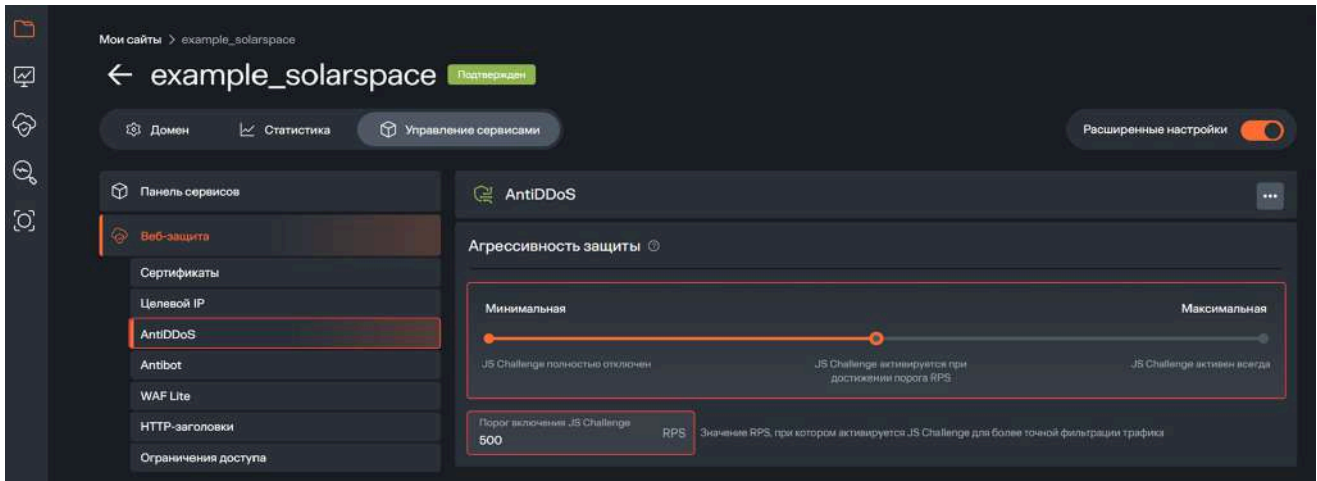


Если для сайта задано несколько IP-адресов, в разделе могут быть доступны дополнительные параметры распределения трафика, включая **IP-hash**.

Опция **IP-hash** закрепляет пользователя за одним и тем же сервером (по IP), что полезно для сайтов с пользовательскими сессиями (например, личные кабинеты и интернет-магазины).

AntiDDoS

Раздел **AntiDDoS** отвечает за защиту от DDoS-атак и массовых запросов и работает как базовый уровень фильтрации в цепочке веб-защиты.



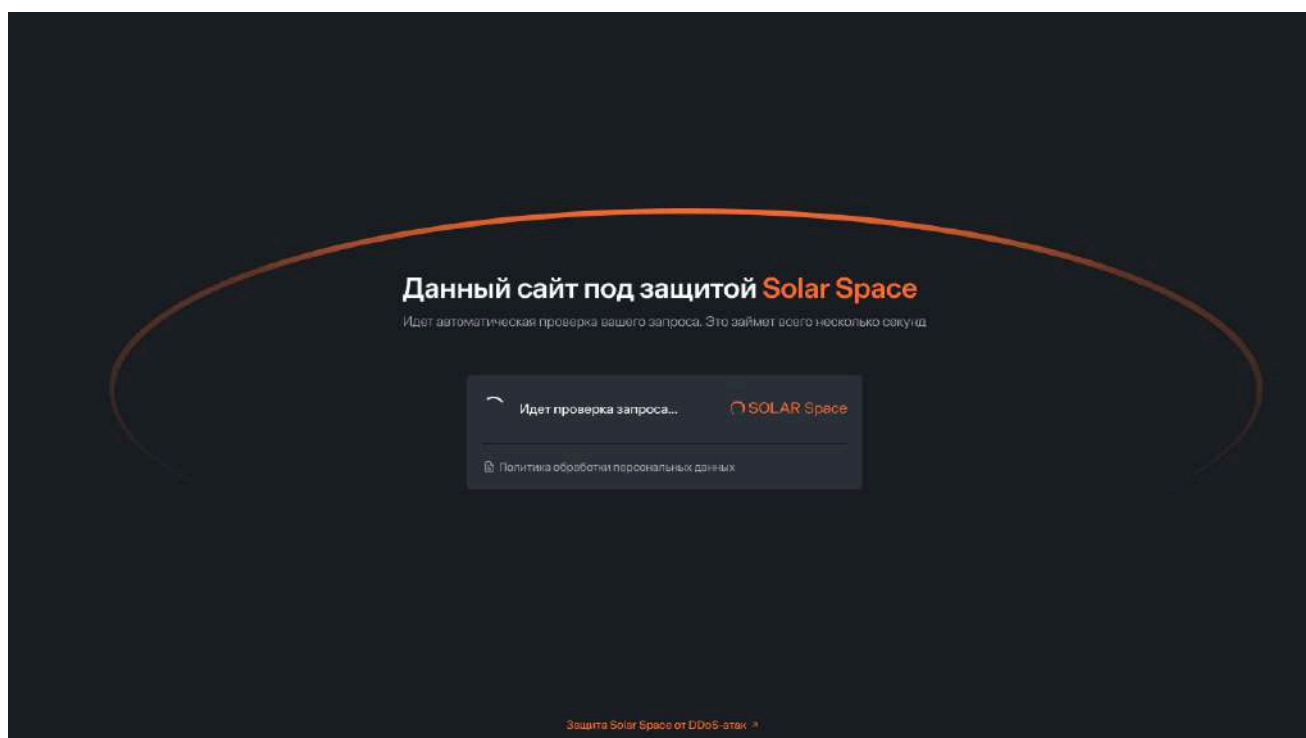
Агрессивность защиты и JS Challenge

Основная логика AntiDDoS строится вокруг ограничения подозрительной нагрузки и интерактивной проверки **JS Challenge**:

- **Минимальная агрессивность** — работает только базовый уровень (лимиты запросов).
- **Средняя агрессивность (по умолчанию)** — JS Challenge включается при превышении порога RPS.
- **Максимальная агрессивность** — JS Challenge применяется ко всем запросам.

Порог включения JS Challenge (RPS)

Порог RPS определяет, **при какой нагрузке** включается интерактивная проверка в режиме средней агрессивности. На изображении приведён пример страницы автоматической проверки.

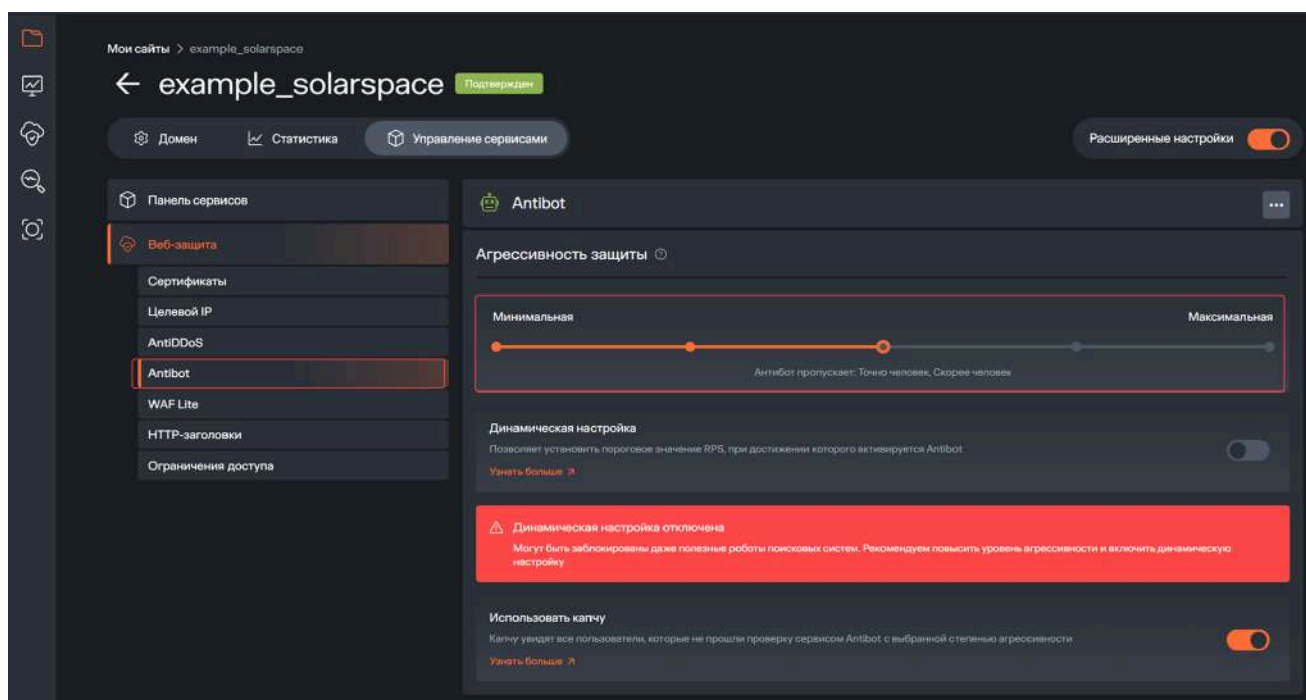


JS Challenge выполняется **кратковременно и автоматически** — как правило, проверка занимает доли секунды и не требует действий и обычно незаметна для пользователя. После завершения проверки пользователь автоматически перенаправляется на запрошенную страницу.

Корректно подобранный порог помогает сохранить баланс между удобством пользователей и эффективностью фильтрации.

Antibot

Раздел **Antibot** предназначен для защиты от вредоносных и автоматизированных запросов уровня L7.



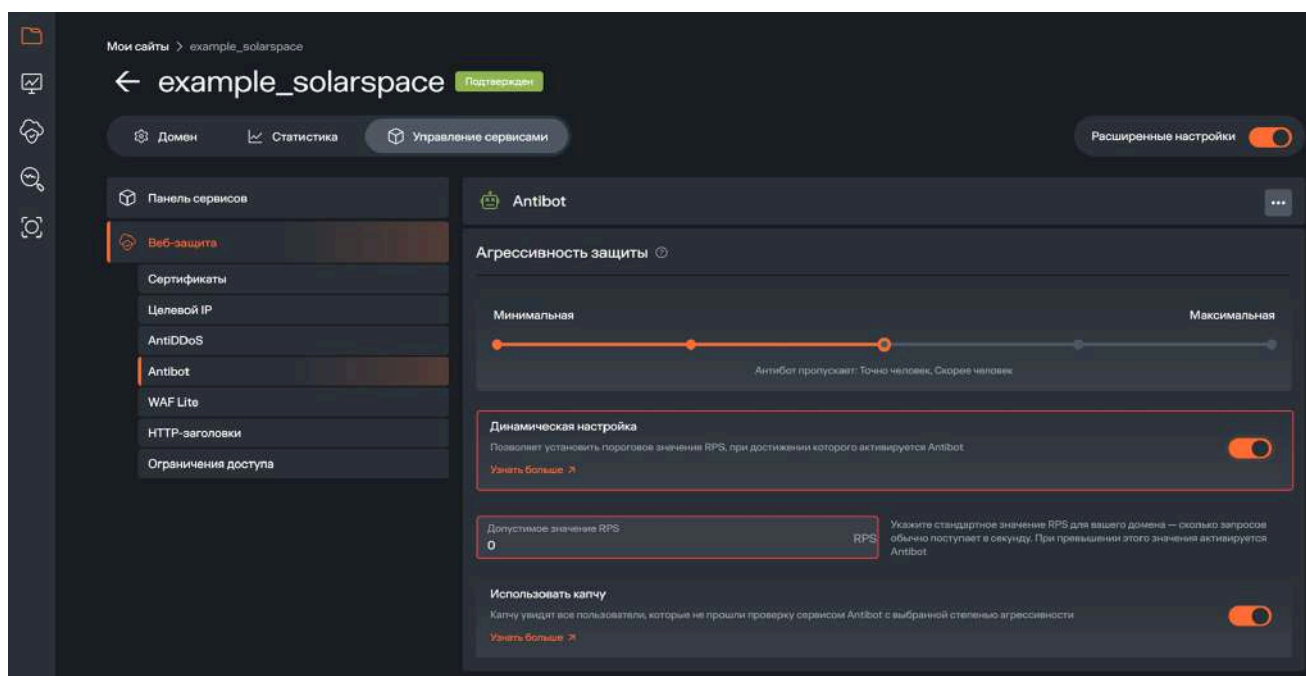
Сервис анализирует поведение и помогает фильтровать ботов, которые:

- сканируют страницы и ищут уязвимости;
- создают нагрузку и замедляют сайт;
- спамят в формах и комментариях;
- ухудшают поведенческие показатели.

Динамическая настройка и порог RPS

Опция «**Динамическая настройка**» позволяет задать порог срабатывания Antibot по количеству запросов в секунду (**RPS**):

- когда реальный RPS превышает установленное значение, система усиливает фильтрацию;
- после включения опции появляется поле «**Допустимое значение RPS**».

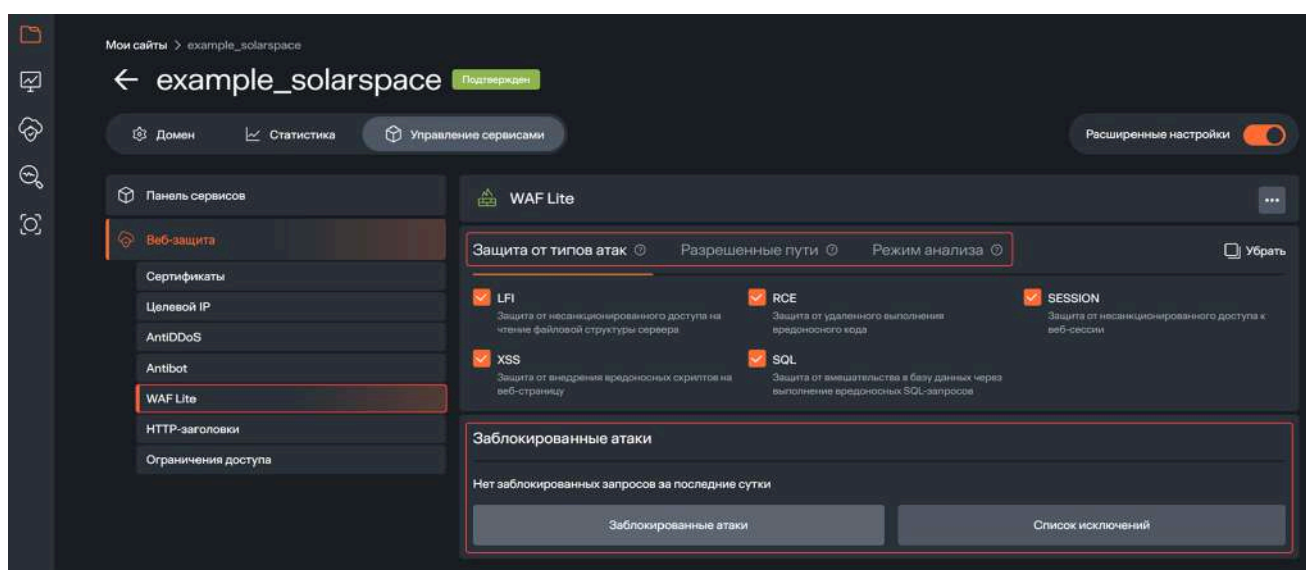


Использовать капчу

Настройка «**Использовать капчу**» задаёт дополнительный уровень проверки при срабатывании антибот-фильтра.

WAF Lite

Раздел **WAF Lite** предназначен для базовой защиты веб-приложения от типовых атак (например, XSS, SQL-инъекций, RCE и др.). WAF Lite анализирует HTTP-запросы к сайту и блокирует запросы, которые соответствуют признакам выбранных типов атак.



В разделе WAF Lite доступны:

- включение защиты от выбранных типов атак;
- просмотр заблокированных запросов;
- настройка исключений;
- настройка разрешённых путей;
- включение или отключение режима анализа.

Защита от типов атак

В блоке «**Защита от типов атак**» выберите типы атак, которые WAF Lite будет отслеживать и блокировать. Включайте только те типы атак, которые актуальны для вашего приложения и инфраструктуры.

Разрешённые пути

Разрешённые пути — это список URI (путей внутри сайта), для которых WAF Lite **не выполняет проверку**.

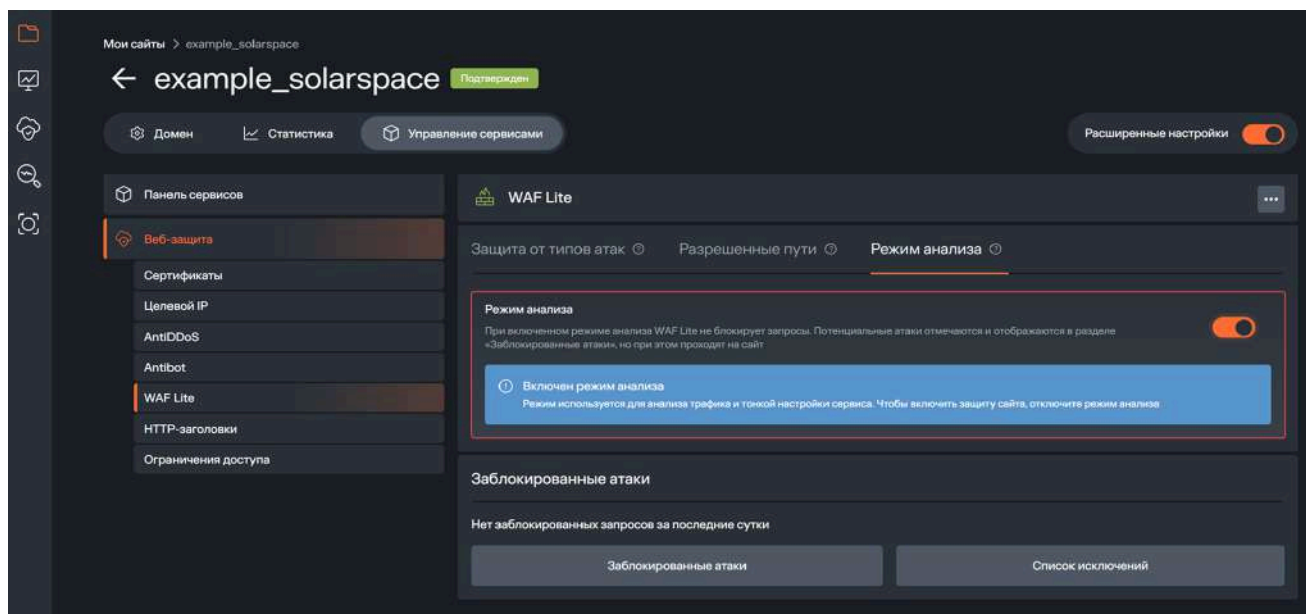
Разрешённые пути используют, чтобы:

- снизить риск ложных срабатываний на легитимные запросы (например, интеграции и нестандартные API-вызовы);
- исключить из проверки служебные или технические страницы, которые не требуют фильтрации.

Добавляйте в список только те пути, в безопасности которых вы уверены.

Режим анализа

В **режиме анализа** WAF Lite **не блокирует** запросы. Потенциально вредоносные запросы фиксируются в событиях, но продолжают проходить на сайт.



Режим анализа используют:

- перед включением защиты, чтобы проверить, какие запросы будут попадать под правила;
- после изменения настроек, чтобы оценить влияние на легитимный трафик.

Чтобы включить полноценную блокировку, отключите режим анализа.

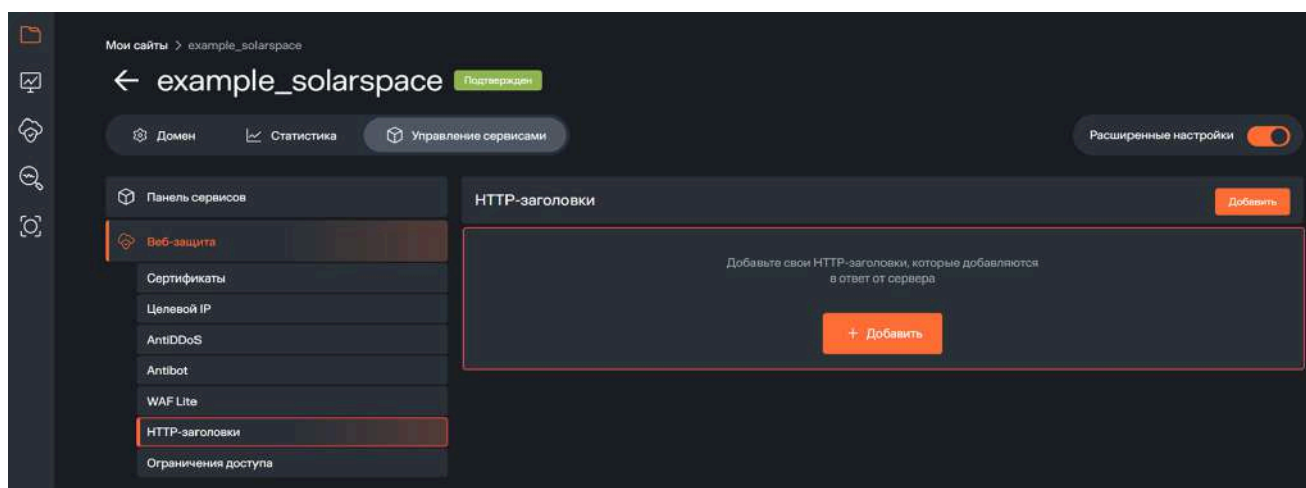
Заблокированные атаки и список исключений

В блоке **«Заблокированные атаки»** отображаются запросы, которые WAF Lite определил как вредоносные и заблокировал.

Если WAF Lite блокирует легитимные запросы, добавьте их в **список исключений**. Исключения применяются точно и позволяют пропускать аналогичные запросы по выбранному пути без блокировки.

HTTP-заголовки

Раздел **«HTTP-заголовки»** предназначен для добавления HTTP-заголовков, которые сервис защиты возвращает в **ответах сервера**.

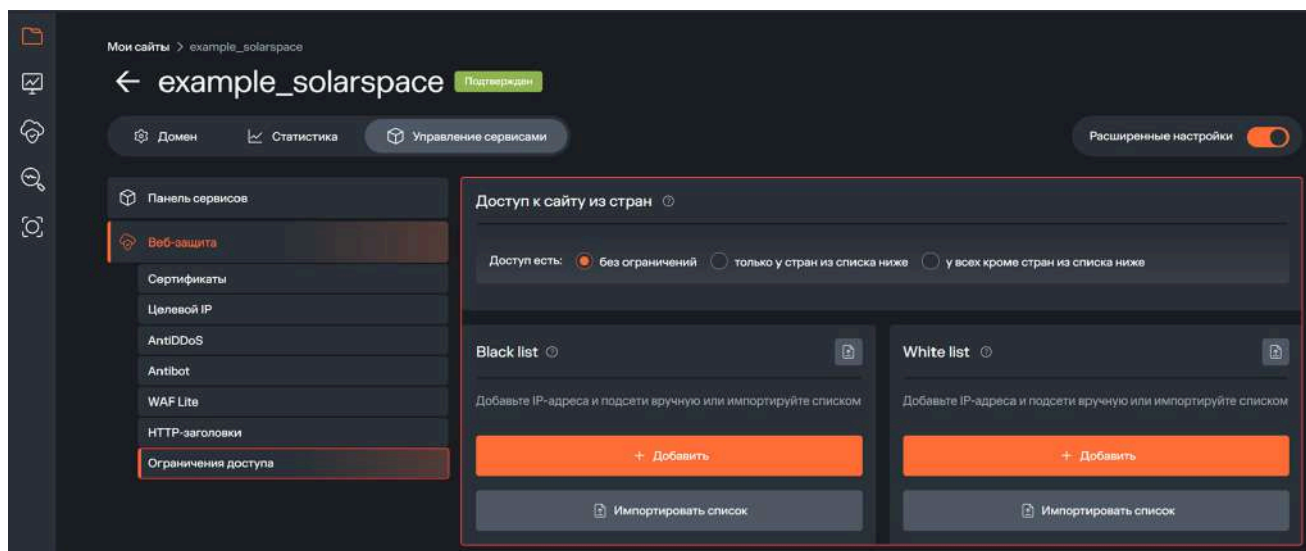


Раздел отображается только при включённом переключателе «**Расширенные настройки**».

Подробное описание сценариев использования и примеры настройки заголовков приведены в статье «**HTTP-заголовки**».

Ограничения доступа

Раздел «**Ограничения доступа**» позволяет управлять входящими запросами к сайту: ограничивать доступ по географии и по спискам IP-адресов.



В разделе доступны ограничения:

- **Доступ к ресурсу из стран** — настройка доступа в зависимости от страны, из которой приходит запрос.
- **Black list** — запрет доступа для конкретных IP-адресов или подсетей.
- **White list** — разрешение доступа для конкретных IP-адресов или подсетей.

Порядок применения ограничений

Каждое входящее обращение к сайту система обрабатывает в следующей последовательности:

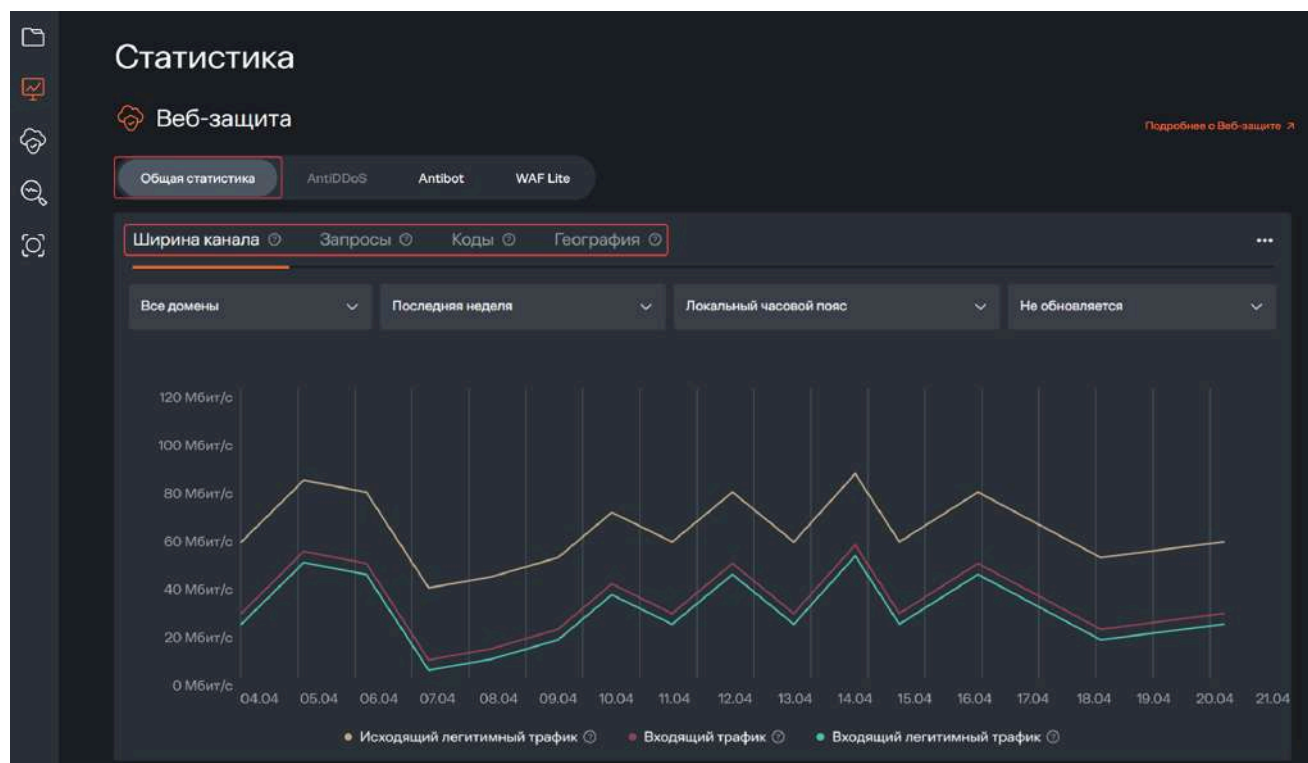
1. **Black list** — если IP-адрес запроса найден в списке, запрос блокируется. Если нет — выполняется проверка по странам.
2. **Доступ к ресурсу из стран** — система сопоставляет страну запроса с заданным режимом (разрешить только выбранные / запретить выбранные / без ограничений). Если страна разрешена — запрос пропускается на сайт. Если страна запрещена — выполняется проверка по White list.
3. **White list** — если IP-адрес присутствует в списке, доступ разрешается даже при запрете по стране. Если IP-адрес отсутствует — запрос обрабатывается сервисами веб-защиты (AntiDDoS, Antibot, WAF Lite) в зависимости от подключённых сервисов.

Подробные сценарии и примеры настройки приведены в статьях:

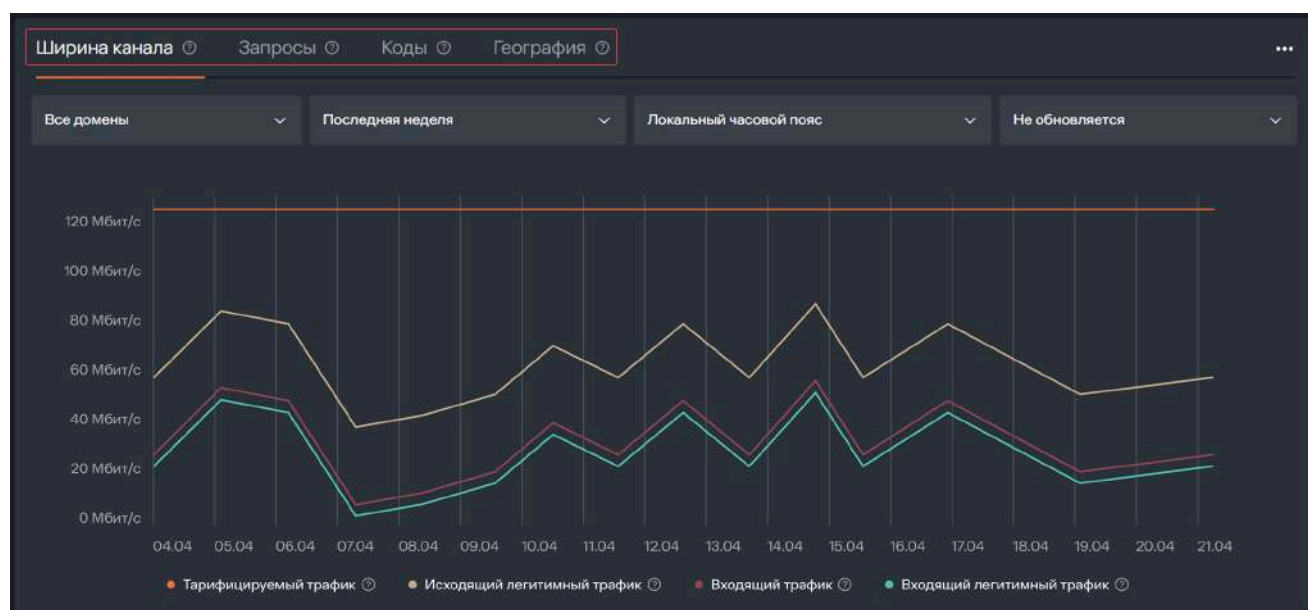
- [«Доступ к ресурсу из стран»](#)
- [«Black list»](#)
- [«White list»](#)

Статистика

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



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



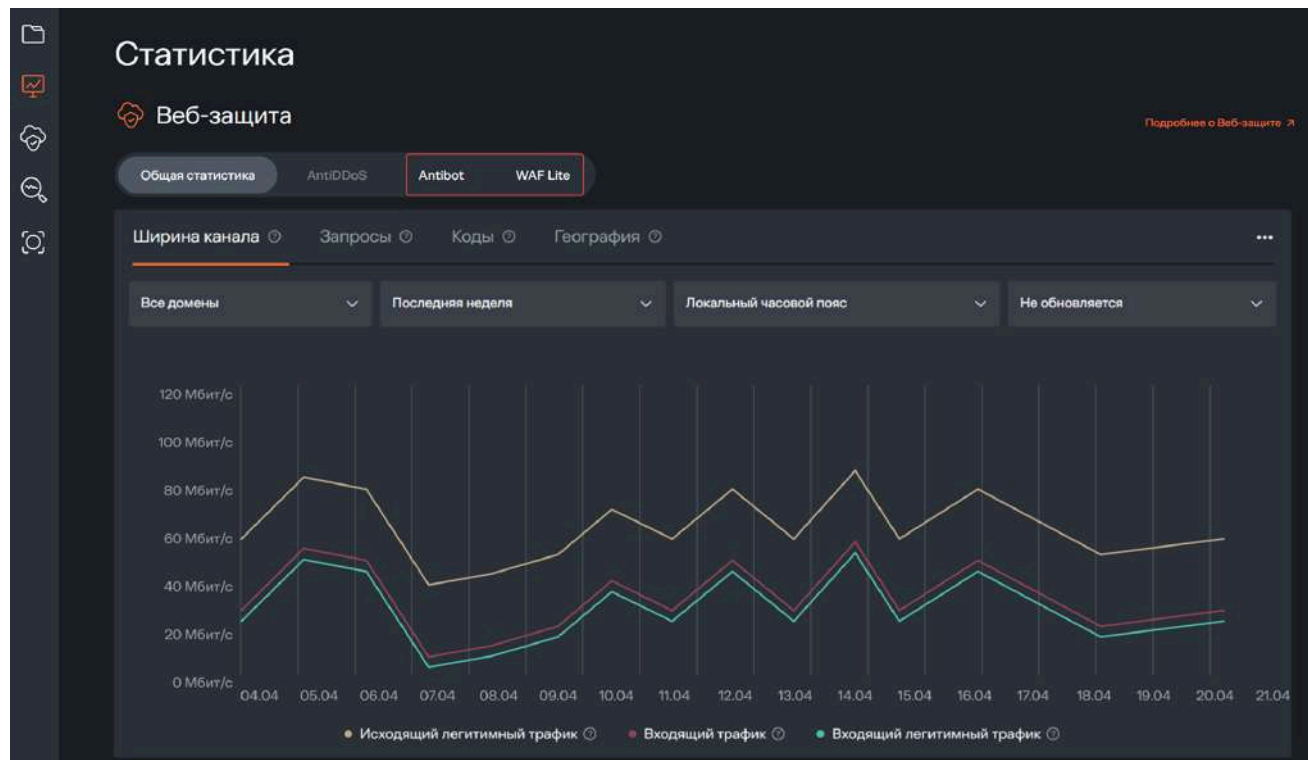
- Ширина канала
- Запросы

- Коды ответов
- География запросов

Система предоставляет детальную аналитику по защитным функциям.

В модулях **WAF Lite** и **Antibot** доступна статистика:

- **Проанализированные запросы** — общее количество запросов, прошедших проверку.
- **Валидные запросы** — запросы, успешно допущенные к обработке.

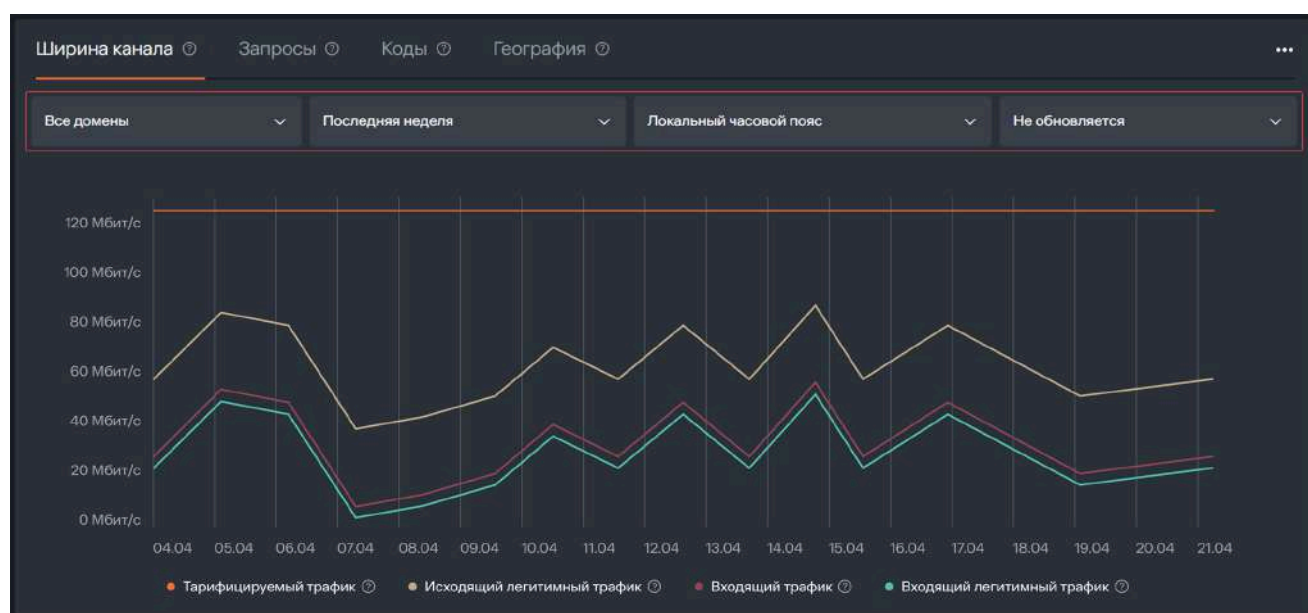


Все виды статистики доступны в едином интерфейсе для удобного мониторинга работы сервиса.

Ширина канала

Чтобы открыть ширину канала, перейдите на страницу "[Статистика](#)", нажав на иконку монитора в левом меню с любой страницы личного кабинета.

Ширина канала отображается первым разделом на странице статистики. Здесь представлена подробная информация о трафике. В верхней части над графиком можно выбрать домены, установить период отображения отчёта, часовой пояс и частоту обновления.



Под графиком обозначены 4 типа трафика:

Тарифицируемый трафик

Определяется объёмом полосы трафика, зафиксированной в вашем тарифе. Для расчёта используется алгоритм 95-го перцентиля по исходящему и входящему легитимному (очищенному) трафику. 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 расчёта оплаты.

Исходящий легитимный трафик

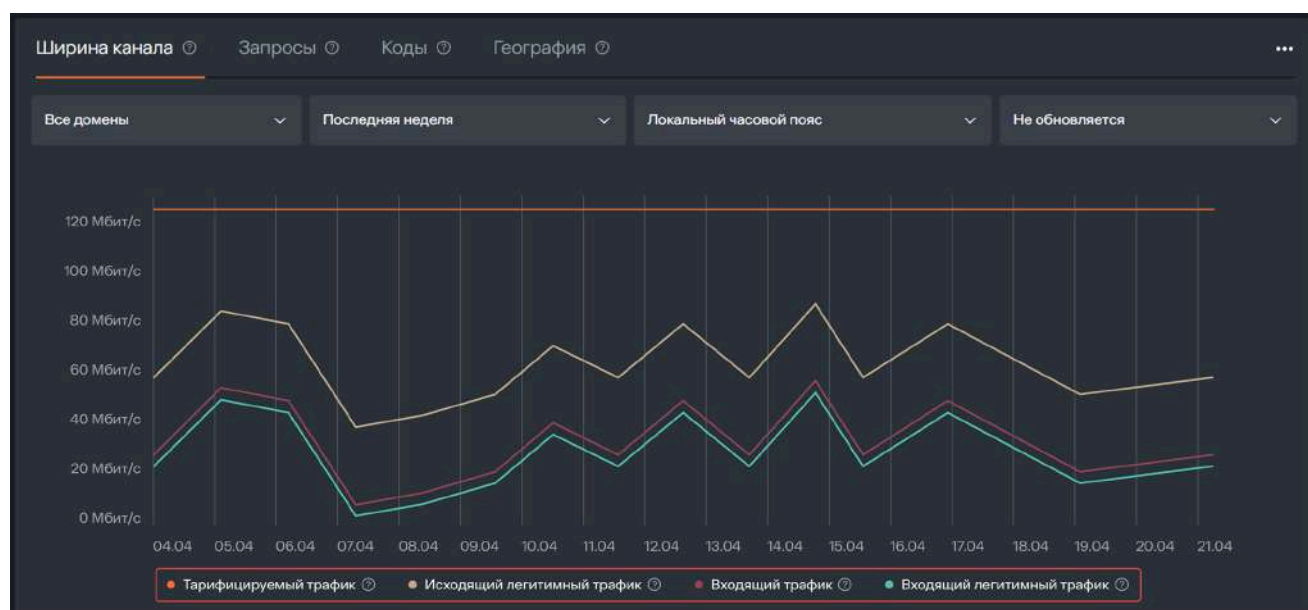
Трафик, который ваш сервер отправил посетителям сайта через платформу фильтрации. Отражает объём очищенных исходящих данных — ответов на запросы, прошедшие через систему защиты. Включает только легитимные (разрешённые) ответы веб-сервера.

Входящий трафик

Общий трафик, который платформа фильтрации принимает и проверяет на предмет подозрительной активности. Включает обращения реальных пользователей и паразитный трафик: DDoS-атаки, фишинг, спам, вредоносные файлы и автоматические программы сканирования.

Входящий легитимный трафик

Трафик, прошедший полную фильтрацию. После удаления вредоносных и подозрительных запросов остаются обращения от реальных пользователей и доверенных сервисов. Участвует в расчёте тарифицируемого объёма трафика наряду с исходящим легитимным трафиком.



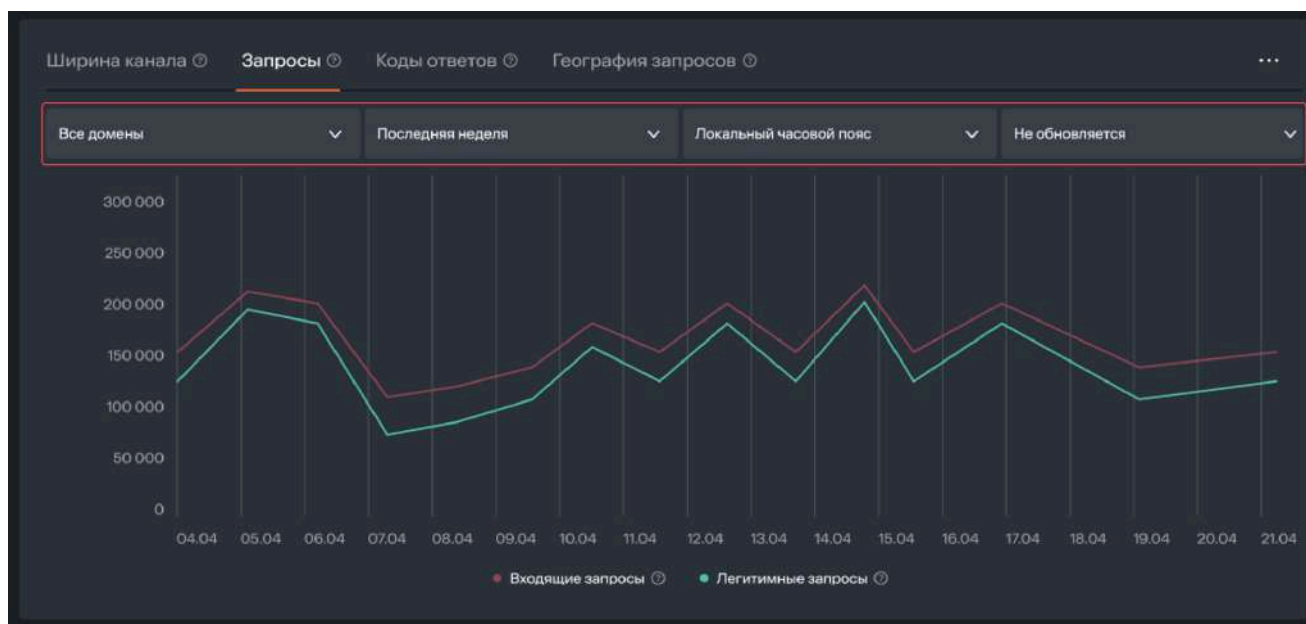
Нажимая на название типа трафика, вы можете исключить его из графика. В этом случае название станет серым. Чтобы вернуть отображение, повторно нажмите на него.

Запросы

Чтобы открыть запросы, перейдите на страницу "[Статистика](#)", нажав на иконку монитора в левом меню с любой страницы личного кабинета.

Нажмите на раздел «Запросы».

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



Под графиком обозначено два типа запросов:

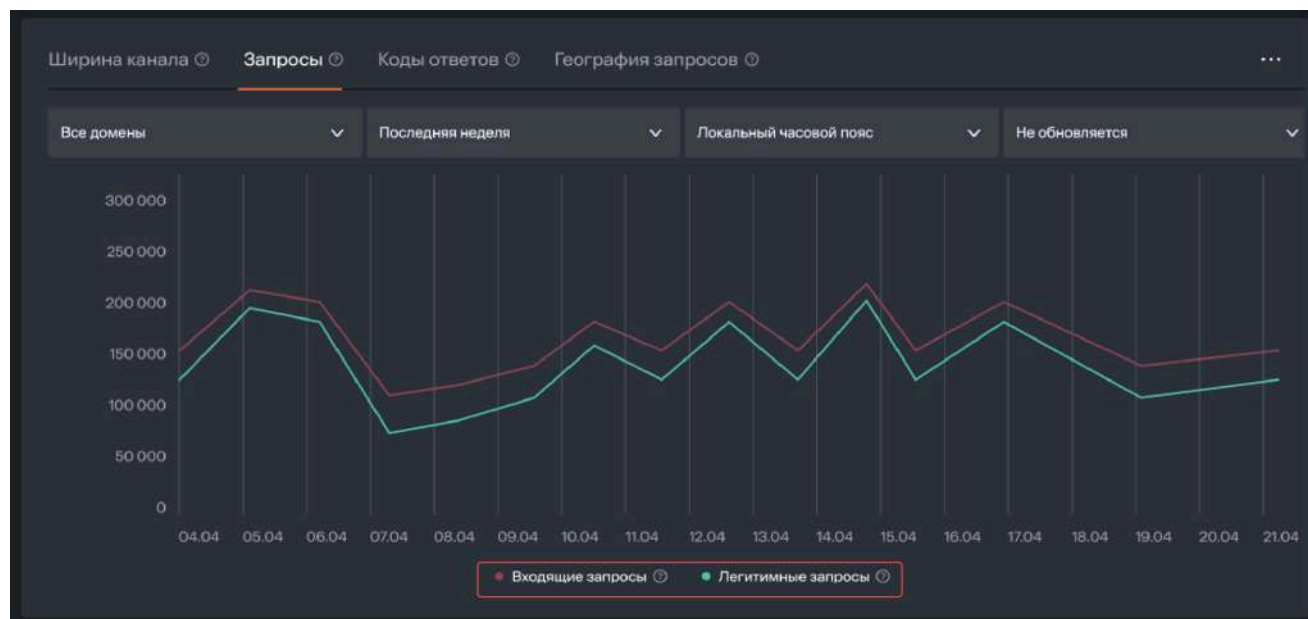
Входящие запросы

Все запросы, поступившие на платформу фильтрации до обработки. Включают обращения от реальных пользователей, поисковых роботов и автоматизированных сканеров (в том числе потенциально вредоносных). Именно этот показатель отражает общий объём трафика, проходящий через систему до этапа фильтрации.

Легитимные запросы

Запросы, прошедшие фильтрацию и признанные безопасными. Включают только обращения, характерные для поведения реальных пользователей и надёжных сервисов (например,

поисковых систем). Легитимные запросы позволяют оценить реальную активность аудитории после очистки трафика от паразитных и вредоносных обращений.



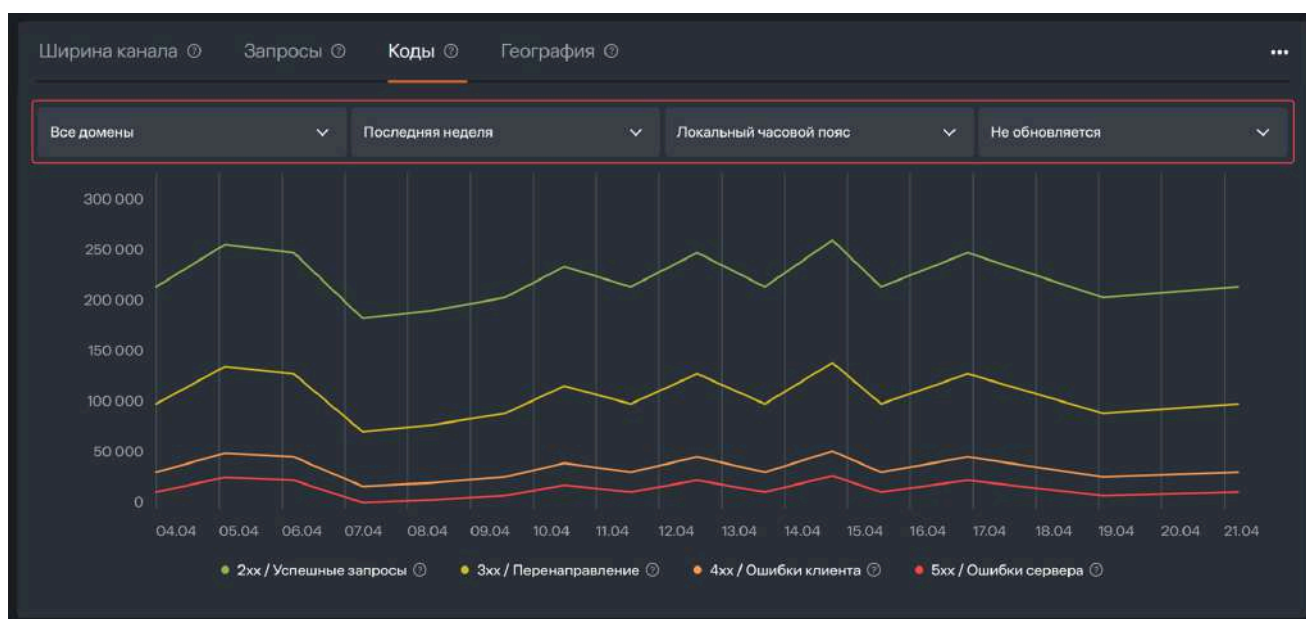
Нажимая на название типа запроса, вы можете исключить его из графика. В этом случае название станет серым. Чтобы вернуть отображение, повторно нажмите на него.

Коды

Чтобы открыть коды, перейдите на страницу "[Статистика](#)", нажав на иконку монитора в левом меню с любой страницы личного кабинета.

Нажмите на раздел «Коды».

Здесь отображается результат взаимодействия пользователей с сервером. Параметры в верхней части можно изменять аналогично вкладкам [Ширина канала](#), [Запросы](#) и [География запросов](#).



Под графиком обозначены четыре типа кодов:

2xx — Успешные ответы

Обозначают, что запрос пользователя был корректно обработан, и он сразу перешёл на ваш сайт. Такие коды указывают на нормальную работу ресурса и успешное взаимодействие клиента с сервером.

3xx — Перенаправления

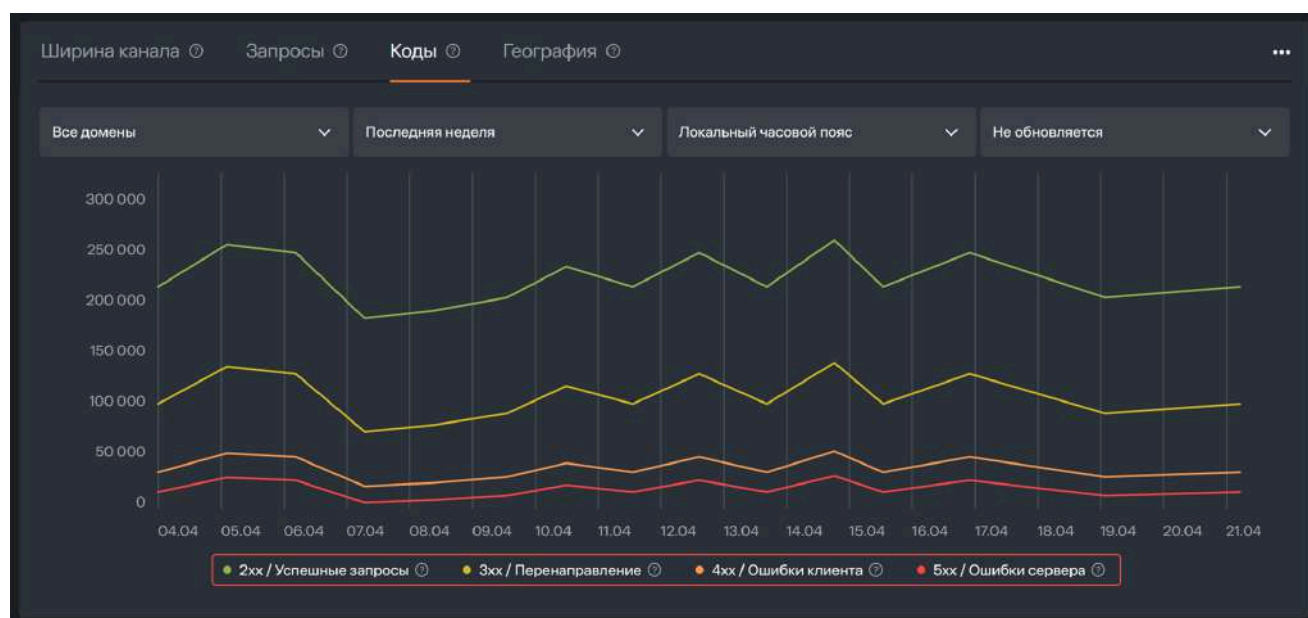
Обозначают, что запрос был успешно принят, но пользователь был перенаправлен на другую страницу. Это нормальное поведение, если вы настроили редиректы (например, при смене структуры сайта или протокола HTTP→HTTPS).

4xx — Ошибки клиента

Обозначают, что проблема возникла на стороне пользователя — например, он перешёл по устаревшей ссылке на удалённую страницу (ошибка 404) или запросил недоступный ресурс. Такие ошибки часто связаны с некорректными действиями клиента, но могут указывать и на неверно настроенные ссылки на сайте.

5xx — Ошибки сервера

Обозначают сбой на стороне вашего сервера. Это может быть результатом перегрузки, кратковременной недоступности, ошибок в работе приложений или веб-сервера. Если количество таких ошибок возрастает, рекомендуется проверить логи и стабильность инфраструктуры.



Нажимая на название кода, вы можете исключить его из графика. В этом случае название станет серым. Чтобы вернуть отображение, повторно нажмите на его название.

География

Чтобы открыть географию, перейдите на страницу "[Статистика](#)", нажав на иконку монитора в левом меню с любой страницы личного кабинета.

Нажмите на раздел «География».

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

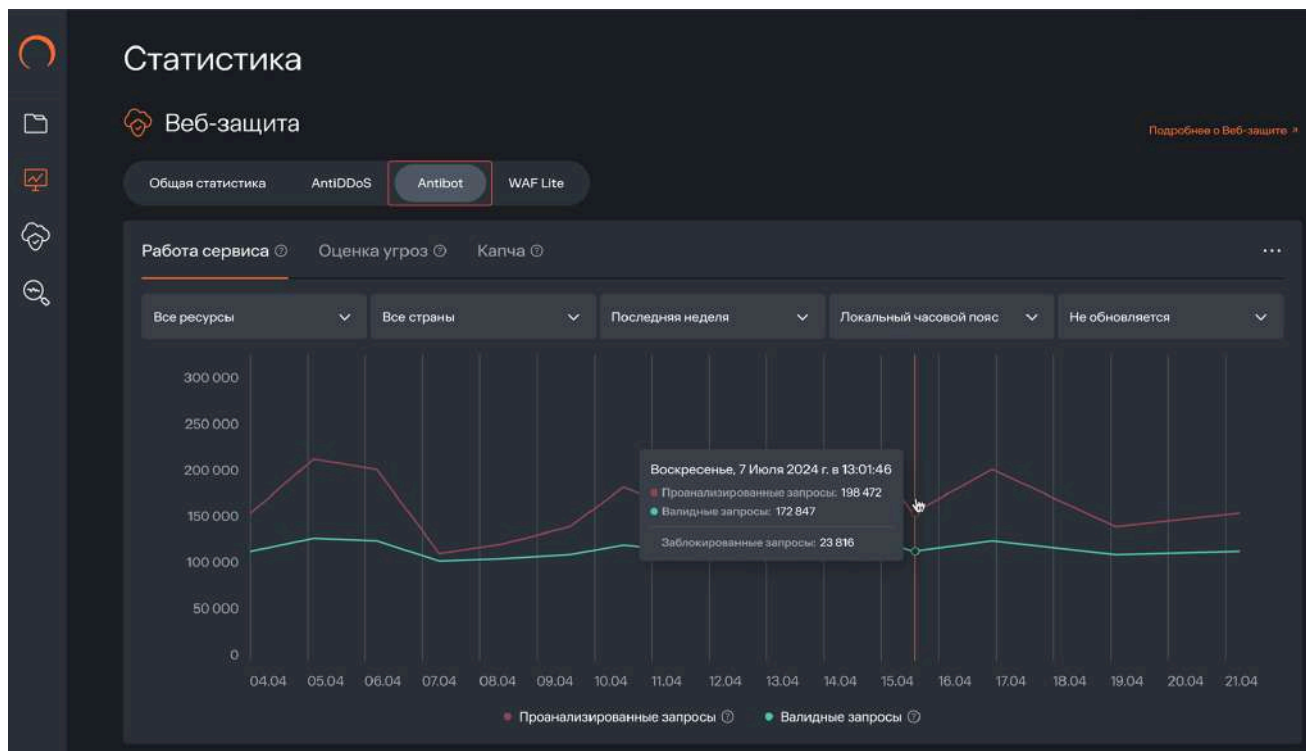


На карте вы можете навести на страну и увидеть количество запросов оттуда. Чем насыщеннее оттенок, тем больше запросов пришло из этой страны. Белым цветом на карте обозначены страны, из которых не было обращений к ресурсу.

Antibot

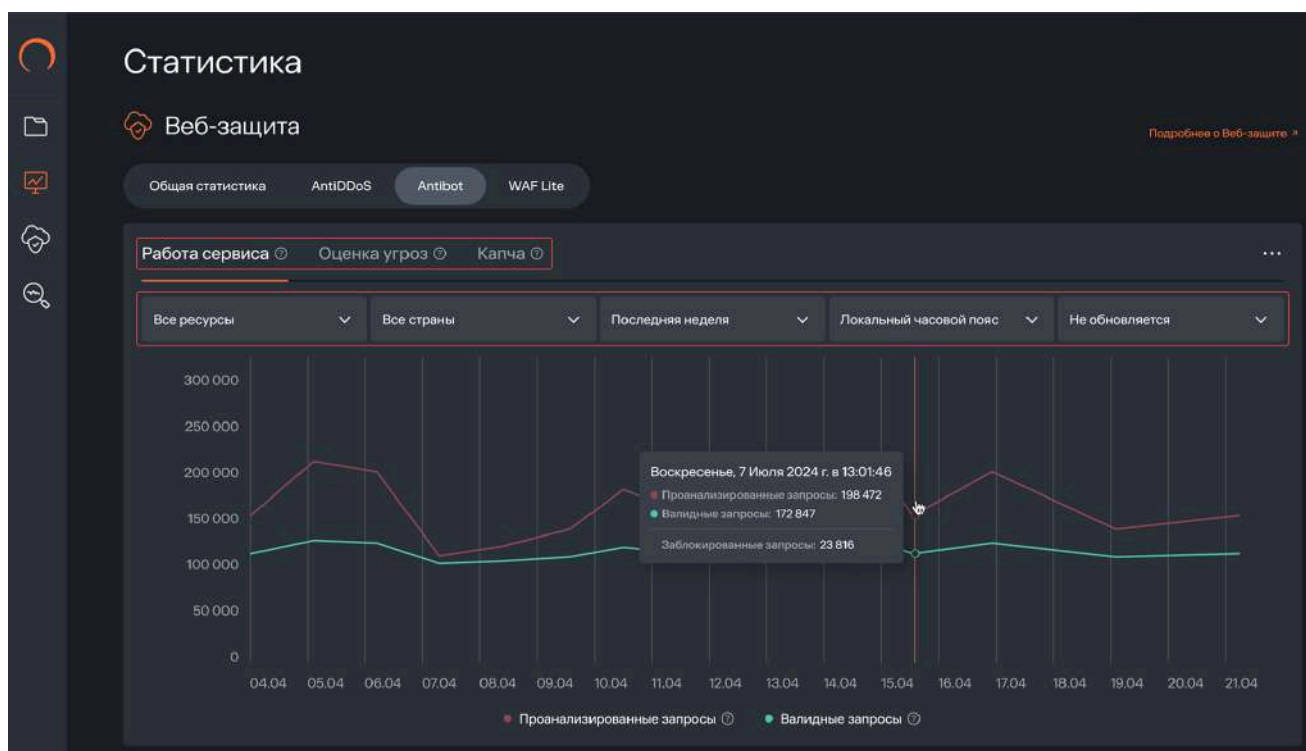
Чтобы открыть статистику Antibot, перейдите на страницу "**Статистика**", нажав на иконку монитора в левом меню с любой страницы личного кабинета.

В блоке «**Веб-защита**» выберите вкладку **Antibot**.



На вкладке **Antibot** доступны три раздела:

- **Работа сервиса**
- **Оценка угроз**
- **Капча**



Над графиками можно задать параметры отображения:

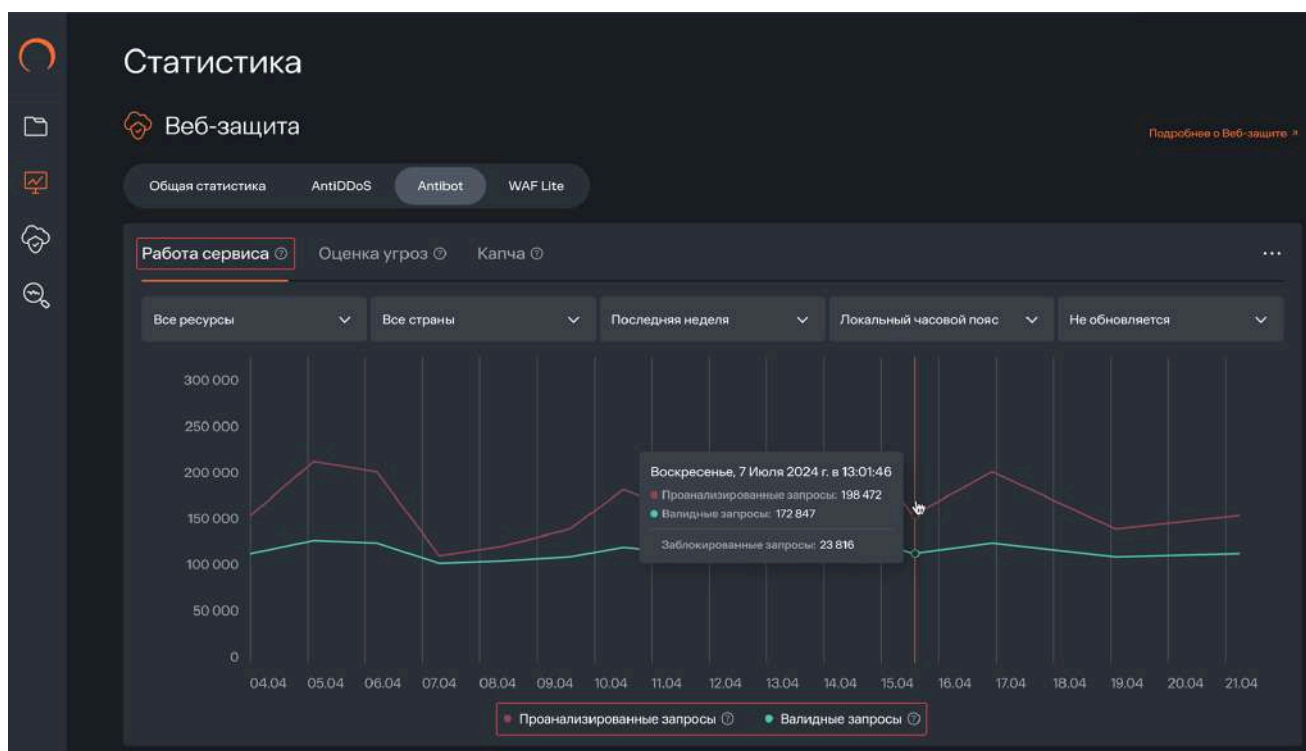
- домены
- страны
- период отчёта
- часовой пояс
- частота обновления

Работа сервиса

Раздел «**Работа сервиса**» показывает динамику запросов, обработанных модулем Antibot за выбранный период. Сопоставляя количество **проанализированных** и **валидных** запросов, можно оценить общий объём проверяемого трафика и долю обращений, допущенных к обработке.

На графике доступны показатели:

- **Проанализированные запросы** — общее количество запросов, прошедших проверку модулем Antibot
- **Валидные запросы** — количество запросов, допущенных к обработке



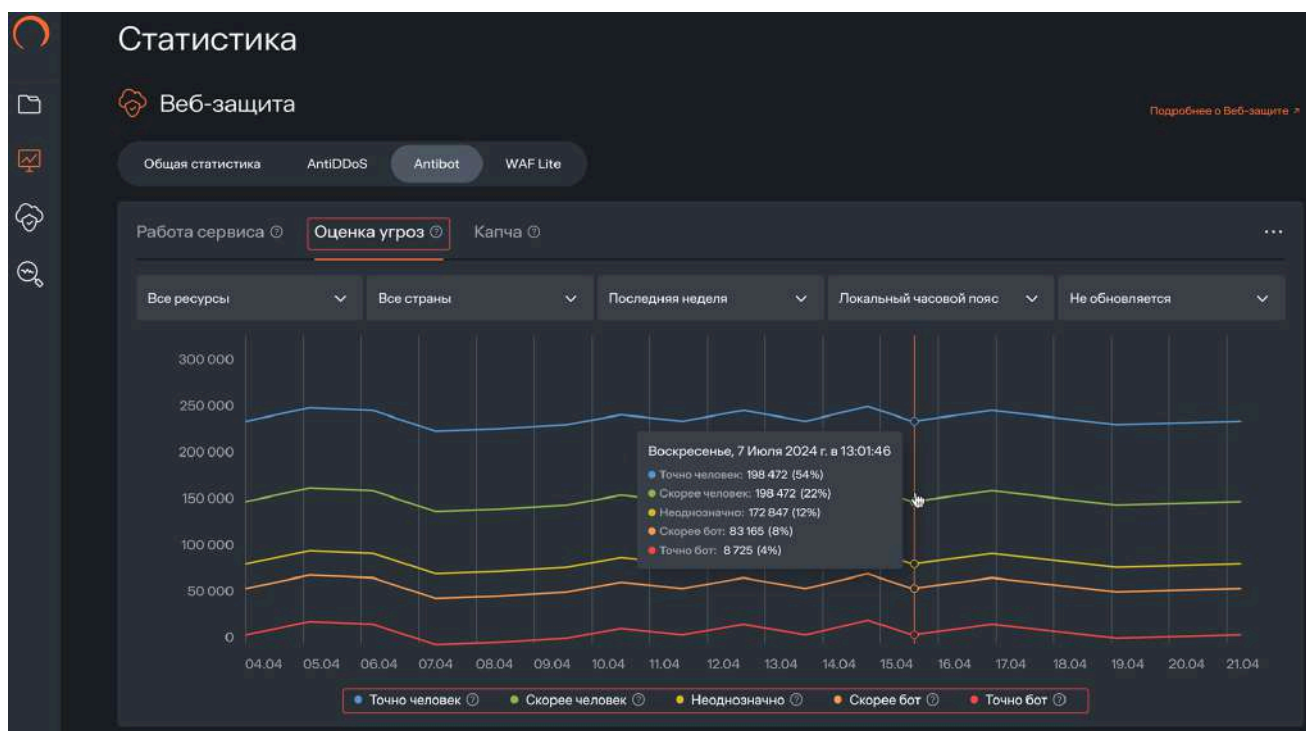
По соотношению этих показателей можно оценить долю запросов, которые успешно проходят проверку и допускаются к обработке.

Оценка угроз

Раздел «**Оценка угроз**» показывает распределение запросов по вероятности автоматизированного поведения. Категории от «**Точно человек**» до «**Точно бот**» позволяют оценить структуру трафика и определить, какая часть обращений может относиться к автоматизированным системам.

На графике доступны категории:

- Точно человек
- Скорее человек
- Неоднозначно
- Скорее бот
- Точно бот



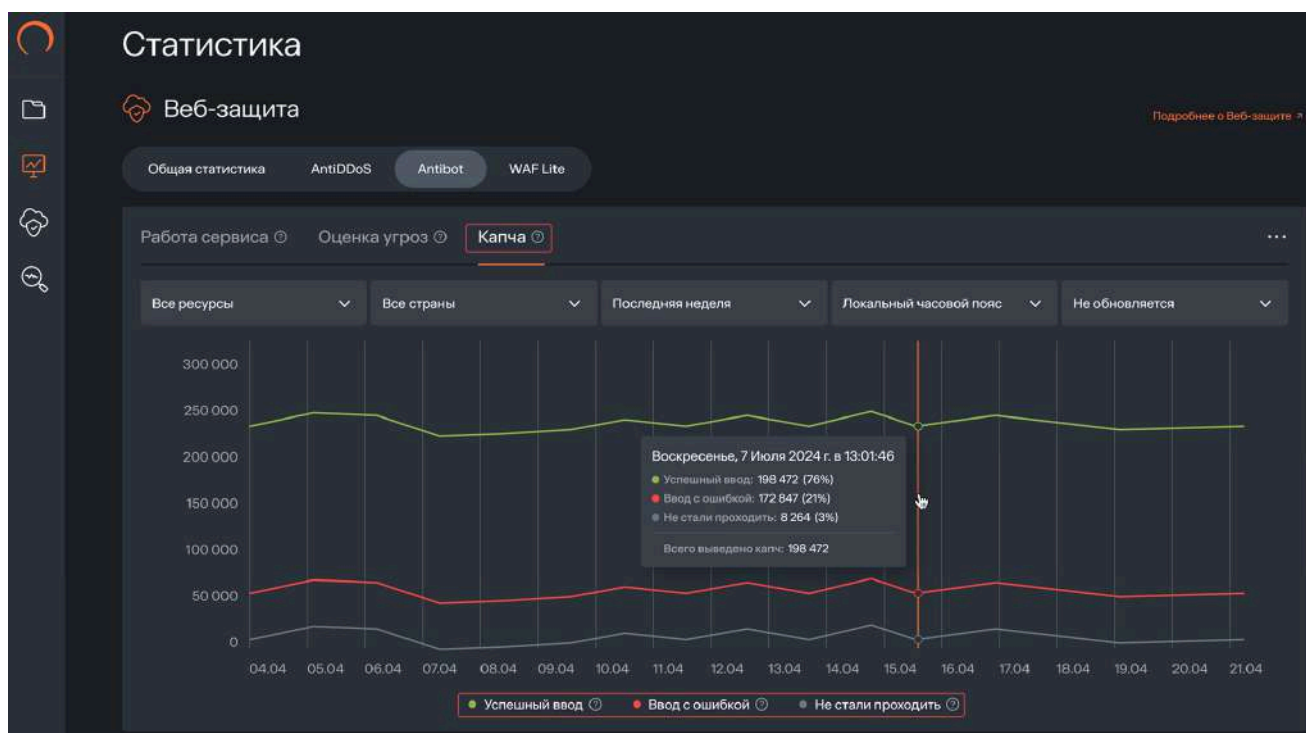
Такое распределение помогает понять характер входящего трафика и выявить возможные всплески автоматизированной активности.

Капча

Раздел «**Капча**» показывает результаты прохождения проверки пользователями. По соотношению успешных и неуспешных попыток можно оценить, как часто пользователи сталкиваются с проверкой и успешно ли проходят её.

На графике доступны показатели:

- **Успешный ввод** — пользователи прошли проверку без ошибок
- **Ввод с ошибкой** — попытки прохождения капчи, завершившиеся ошибкой
- **Не стали проходить** — пользователи, которые не завершили прохождение проверки

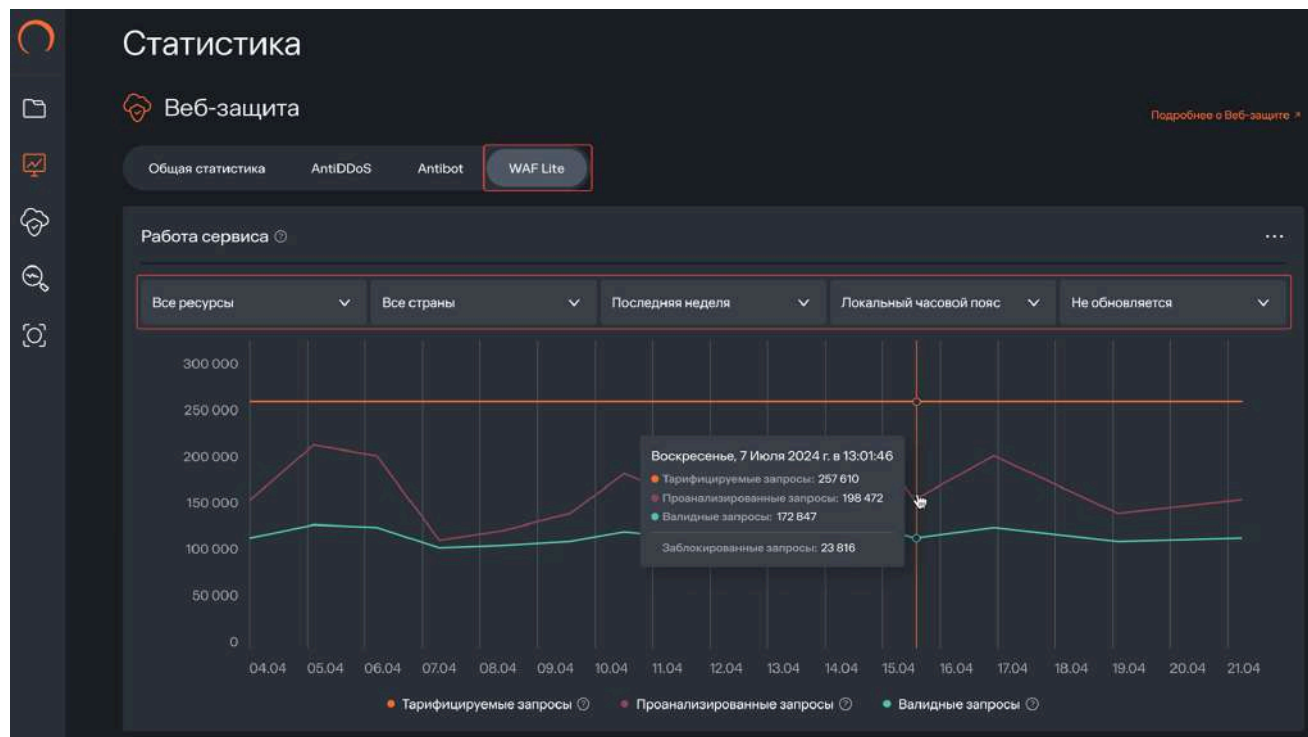


Эти данные позволяют оценить, насколько эффективно проверка отделяет автоматизированные запросы от действий реальных пользователей.

WAF Lite

Чтобы открыть статистику WAF Lite, перейдите на страницу "**Статистика**", нажав на иконку монитора в левом меню с любой страницы личного кабинета.

В блоке «**Веб-защита**» выберите вкладку **WAF Lite**.



На вкладке **WAF Lite** доступен раздел «**Работа сервиса**».

Над графиком можно задать параметры отображения:

- ресурсы
- страны
- период отчёта
- часовой пояс
- частота обновления

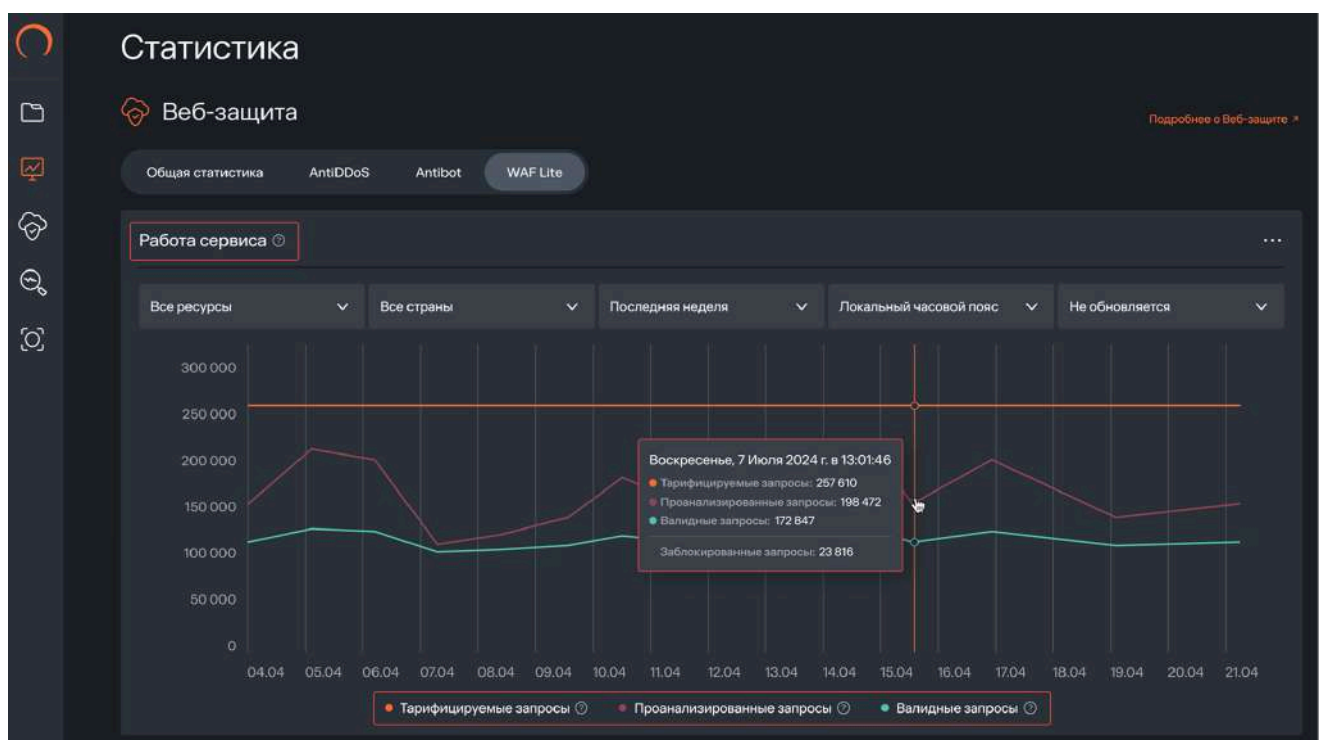
Работа сервиса

Раздел «**Работа сервиса**» показывает динамику запросов, обработанных модулем WAF Lite за выбранный период. Сопоставляя количество **проанализированных**, **валидных** и

заблокированных запросов, можно оценить структуру трафика и интенсивность срабатывания защитных правил.

На графике доступны показатели:

- **Фактические тарифицируемые запросы** — среднее количество запросов в секунду после фильтрации, определённое на основе 95-го перцентиля. Подробнее о расчёте см. в разделе «[Тарификация и оплата](#)»
- **Проанализированные запросы** — общее количество запросов, проверенных модулем WAF Lite
- **Валидные запросы** — количество запросов, допущенных к обработке
- **Заблокированные запросы** — количество запросов, отклонённых в результате срабатывания защитных правил



По этим данным можно определить, насколько активно модуль фильтрует запросы и соответствует ли фактическая нагрузка выбранным параметрам защиты.

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**. Чтобы пользоваться сервисами, нужно пополнить баланс в личном кабинете на сумму, соответствующую выбранному тарифу.

Пополнить баланс можно двумя способами:

- Онлайн с карты — для типов контрагента «Физическое лицо» и «Самозанятый»
- Через поддержку Solar Space по электронной почте solar@rt-solar.ru — для типов контрагента «Юридическое лицо» и «Индивидуальный предприниматель»

Списание средств происходит в формате предоплаты на 30 дней вперед — аналогично оплате интернета или онлайн-кинотеатров.

Отключение за неоплату

За 7 и за 3 дня до начала нового расчетного периода на вашу почту придут уведомления о необходимости пополнить баланс.

Если к этой дате средств на счёте не окажется, защита домена будет приостановлена.

Важно

При подключении сервисов веб-защиты в настройках DNS изменяется А-запись: вместо вашего IP-адреса указывается адрес нашего сервера.

Если баланс не пополнен и защита отключена, сайт станет временно недоступен для посетителей до момента пополнения баланса.

Чтобы этого не произошло, можно заранее скорректировать А-запись: указать свой IP-адрес вместо нашего. После пополнения баланса достаточно снова изменить запись по [инструкции](#), чтобы трафик снова шёл через сервер защиты.

Измерение тарифицируемого трафика

Для расчёта оплаты используется понятие **тарифицируемого трафика**. Выделим основные его виды:

- **Тарифицируемый трафик** — определяется объёмом полосы пропускания, указанным в [тарифах на веб-защиту](#)
- **Исходящий трафик** — данные, которые ваш сервер отправляет посетителям сайта
- **Входящий трафик** — весь поток, поступающий на платформу фильтрации: реальные пользователи и нежелательные запросы (DDoS-атаки, спам, фишинг, вредоносные файлы, автоматизированные сканеры)
- **Входящий легитимный трафик** — поток после очистки системой защиты: только реальные пользователи и полезные поисковые роботы

Для расчета используется **алгоритм 95-го перцентиля по исходящему и входящему легитимному трафику**.

В течение 30-дневного расчетного периода показатели фиксируются каждые 5 минут. Из замеров исключаются 5% наибольших значений, и из оставшихся 95% выбирается максимальное.

Система сравнивает 95-й перцентиль исходящего и входящего легитимного трафика и берёт большее значение для расчёта.

Таким образом, в течение 30-дневного периода трафик может превышать параметры тарифа в сумме до **36 часов** (5% от 30 дней).

У большинства сайтов выше оказывается входящий легитимный трафик. Исключение — ресурсы с трансляциями и стримами, где исходящий поток больше.

Пример расчета тарифицируемого трафика

Дано:

- Количество доменов — 1
- Уровень защиты — оптимальный (AntiDDoS + Antibot)
- Выбранный тариф — 10 Мбит/с
- Трансляции с сайта — нет

Решение:

Система измеряет исходящий и входящий легитимный трафик каждые 5 минут. Исходящий трафик низкий, так как сайт не ведёт трансляций. Входящий легитимный трафик обычно не превышает 10 Мбит/с.

Однако в конце периода зафиксирована атака: почти сутки входящий поток достигал 300 Мбит/с.

После анализа оказалось: превышение длилось 14 часов. По правилам 95-го перцентиля допускается до 36 часов превышений в течение расчётного периода. Значение уложилось в

выбранные 10 Мбит/с.

Ответ: оплачивается только фиксированная стоимость тарифа (10 Мбит/с). Для оптимального уровня защиты это 1500 рублей в месяц (без НДС). Список всех тарифов доступен на странице [Тарифы на веб-защиту](#).

Расчет RPS для продвинутой защиты

RPS — это максимальное количество запросов в секунду, которое может обработать сайт. Показатель используется для тарификации сервиса [WAF Lite](#).

Чтобы рассчитать RPS, разделите пиковое количество посетителей сайта в сутки на число секунд в сутках (86 400).

Например:

$50\,000 / 86\,400 = \mathbf{0,57\ RPS}$.

Это значение соответствует минимальному тарифу (5 RPS) и будет достаточным для такого уровня нагрузки.

Как оплачивается превышение

В тарифах закреплены значения полосы пропускания или количества RPS.

Если по итогам 30-дневного расчётного периода 95-й перцентиль превышает параметры тарифа, на почту, указанную при регистрации, придёт счёт за превышение параметров тарифа.

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

Превышение оплачивается тем же способом, что и основной тариф — через [внесение средств на баланс](#) в личном кабинете.

 Важно

Доплаты за превышение чаще всего возникают, если выбранный тариф не соответствует фактической нагрузке.

Если уведомления приходят несколько месяцев подряд, рекомендуется перейти на более подходящий тариф — это поможет снизить расходы и обеспечить стабильную работу защиты.

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.

Бесплатный тариф

Подходит для одного ресурса.

Ограничение по ширине канала — **1 Мбит/с**.

Включает только сервис **AntiDDoS**.

Это простой способ подключить базовую защиту и познакомиться с платформой без расходов.

Демо-тариф (14 дней)

Доступен пользователям, у которых ранее не было активных тарифов с сервисами веб-защиты.

На 14 дней вы получаете полный доступ ко всем сервисам: **AntiDDoS**, **Antibot** и **WAF Lite** — без ограничений по ширине канала и количеству запросов (RPS).

После завершения периода система проанализирует статистику использования и предложит подходящий платный тариф (Базовый, Оптимальный или Продвинутый) с параметрами, соответствующими нагрузке на ваш сайт.

Базовый уровень веб-защиты — AntiDDoS

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

- фиксированной абонентской платы за выбранную ширину канала (Мбит/с);
- динамической платы в случае **превышения** тарифицируемого трафика.

Подробные правила измерения и подсчета описаны в статье "[Тарификация и оплата](#)".

Оптимальный уровень веб-защиты — AntiDDoS + Antibot

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

- фиксированной абонентской платы за выбранную ширину канала (Мбит/с);
- динамической платы в случае **превышения** тарифицируемого трафика.

Подробные правила измерения и подсчета описаны в статье "[Тарификация и оплата](#)".

Продвинутый уровень веб-защиты — AntiDDoS + Antibot + WAF Lite

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

- фиксированной абонентской платы за выбранную ширину канала (Мбит/с);
- фиксированной платы за количество запросов в секунду (RPS);
- динамической платы в случае **превышения** параметров тарифа.

Рекомендации по расчету RPS и правила тарификации описаны в статье "[Тарификация и оплата](#)".

ⓘ Обратите внимание

При выборе тарифа ориентируйтесь на реальные показатели трафика вашего сайта. Если в течение расчетного периода фактическая нагрузка превысит параметры тарифа, система направит уведомление о превышении. При регулярных превышениях рекомендуется изменить тариф на более подходящий, чтобы снизить дополнительные расходы и обеспечить стабильную работу защиты.

Как подобрать тариф

На что ориентироваться при выборе тарифа в личном кабинете:

- **Бесплатный тариф** — если нужен минимальный старт и защита одного ресурса.
- **Демо-тариф на 14 дней** — если хотите протестировать весь функционал защиты без ограничений.
- **1–5 Мбит/с, 5–10 RPS** — для сайта-визитки с контактами.
- **10–30 Мбит/с, 20–50 RPS** — для каталога товаров и услуг без 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.

Эти рекомендации помогут определиться, если нет данных веб-аналитики.

Для каждого сайта ситуация может быть разной, возможны всплески трафика (например, в период рекламных кампаний).

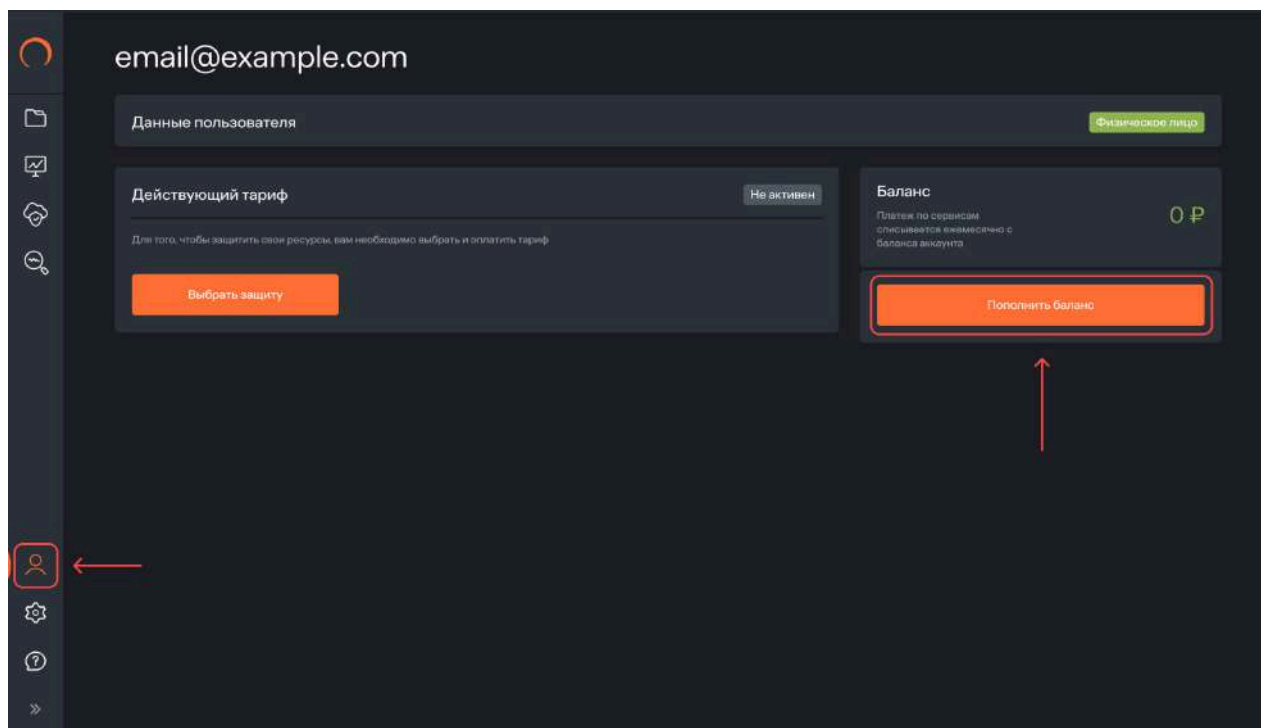
Тариф всегда можно скорректировать позже, основываясь на данных использования за 2–3 месяца.

Как изменить тариф, описано [здесь](#).

Пополнение баланса

Актуальный баланс отображается в верхнем меню страницы. Для пополнения выполните следующие шаги:

1. Перейдите на [страницу профиля](#).
2. Нажмите на кнопку «Пополнить баланс».



ⓘ Обратите внимание

Оплата картой доступна для контрагентов типа «Физическое лицо» и «Самозанятый». Для «Индивидуального предпринимателя» и «Юридического лица» предусмотрена оплата по счёту.

Тип контрагента «Физическое лицо» и «Самозанятый»

1. В разделе оплаты введите сумму пополнения (минимальная сумма — 500 рублей) и нажмите кнопку «Оплатить».

Баланс
Платеж по тарифу списывается ежемесячно с баланса аккаунта **0 Р**

Оплата

Сумма к оплате
1000

Минимальная сумма к оплате — 500 Р

Оплатить

Назад

2. Введите данные карты в форму оплаты и подтвердите платеж.

Баланс
Платеж по тарифу списывается ежемесячно с баланса аккаунта **0 Р**

Оплата

Номер карты
4242 4242 4242 4242 **VISA**

MM / ГГ
04 / 24

CVV
...

☒ Отправить квитанцию на E-mail

E-mail
email@example.com

Оплатить 1 000,00 Р

При оплате данные вашей карты сохраняются (?)

Secure
Verified by **VISA** Mastercard SecureCode

Secured by **CloudPayments**

Тип контрагента «Индивидуальный предприниматель» и
«Юридическое лицо»

Пользователям с этими типами контрагентов доступна оплата по счёту.

Для выставления счёта свяжитесь с поддержкой Solar Space (solar@rt-solar.ru) и укажите в письме название компании, тип контрагента и сумму, которую необходимо внести на баланс.

Баланс

Платеж по тарифу списывается ежемесячно с баланса аккаунта

0 ₽

Оплата

Сумма к оплате

5000

×

Минимальная сумма к оплате — 500 ₽

Оплата по карте пока недоступна для вашего типа контрагента. Пожалуйста, обратитесь в службу поддержки:

support@solarspace.pro

Укажите в письме название компании, тип контрагента и желаемую сумму для пополнения баланса. В ответ вам придет счет для оплаты на эту сумму

Назад

Изменение тарифа

⚠ Обратите внимание

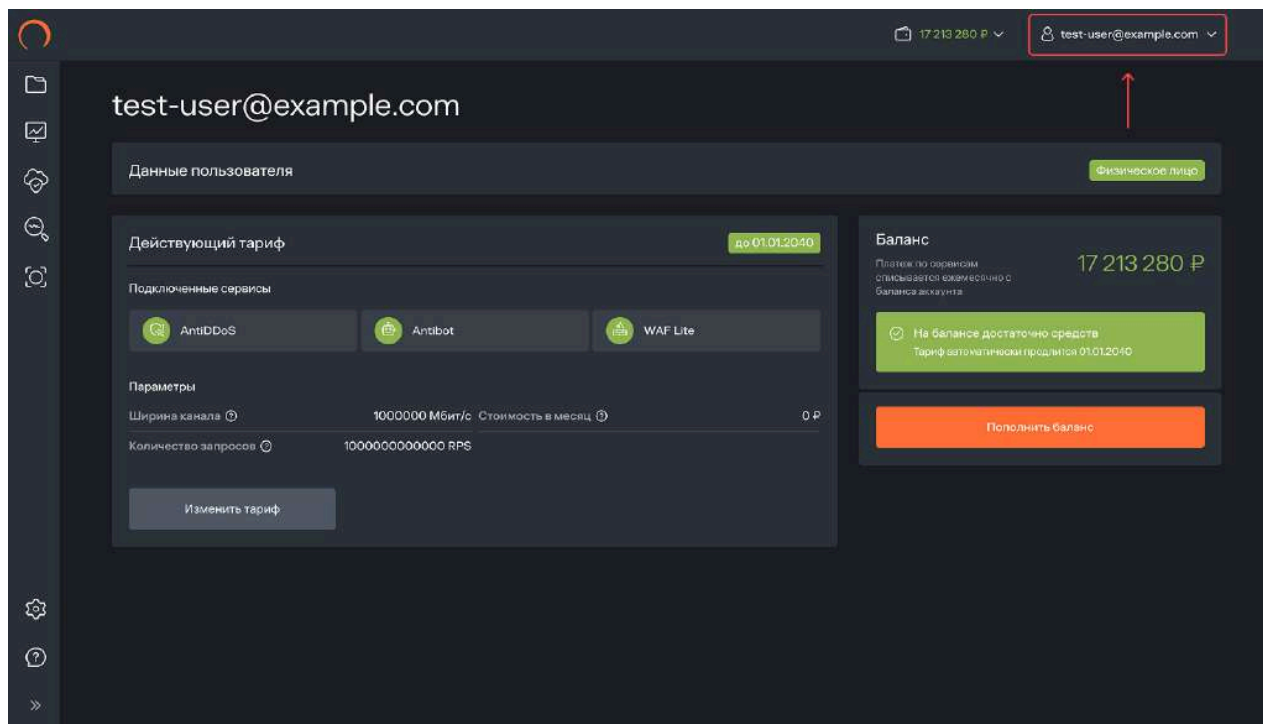
Изменение тарифа доступно только для пользователей с активным оплаченным тарифом

В рамках изменения тарифа вам доступны следующие действия:

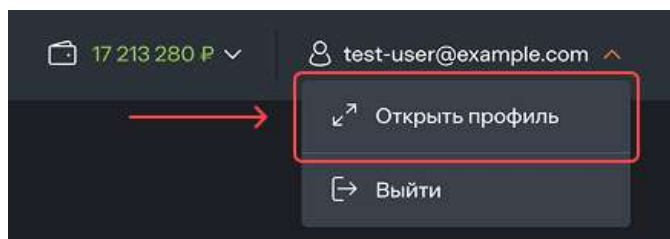
- Добавление нового сервиса
- Отключение сервисов
- Изменение параметров тарифа

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

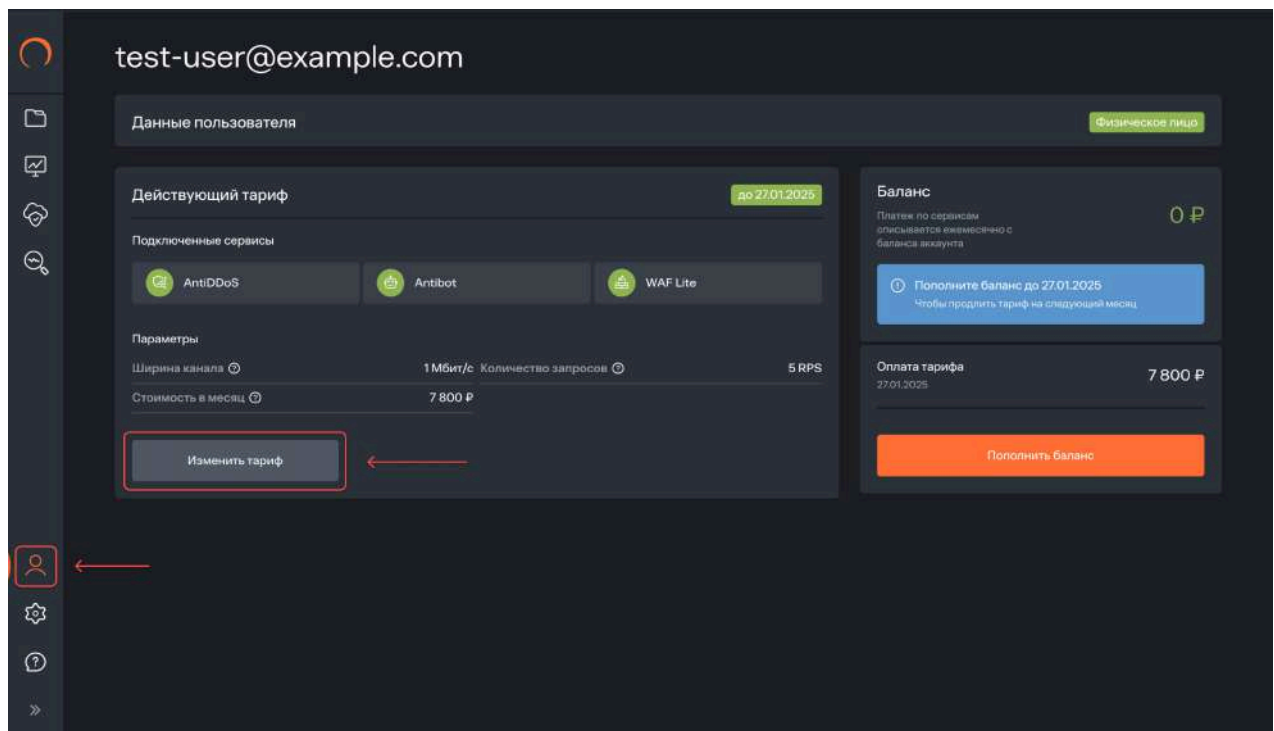
1. Перейдите на страницу профиля в личном кабинете. Для этого нажмите на имя вашего домена в верхнем меню страницы.



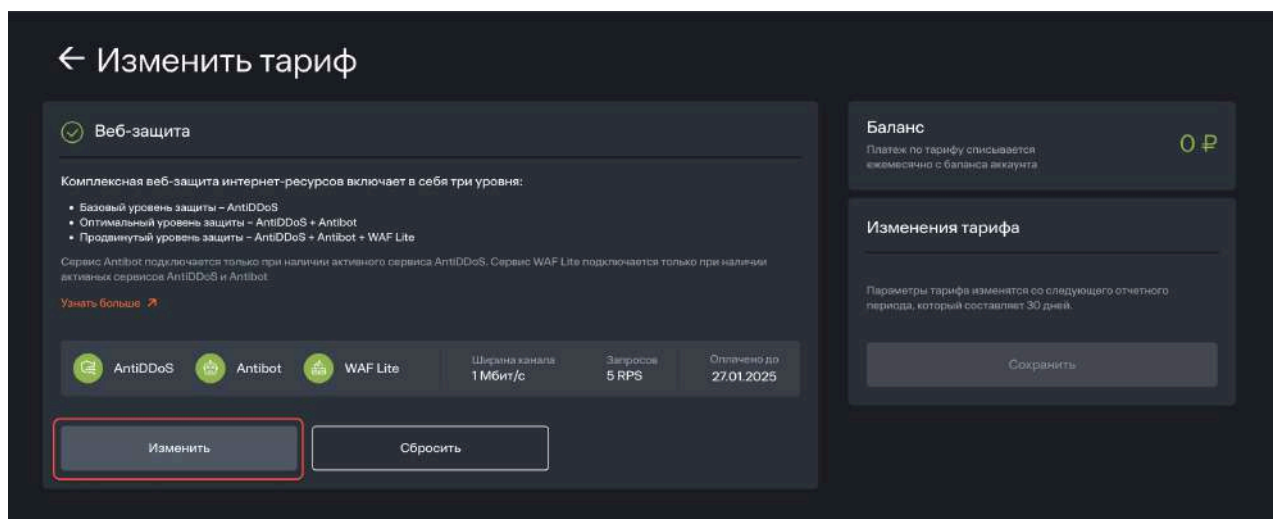
2. Откроется выпадающий список. Нажмите "Открыть профиль".



3. Нажмите на кнопку "Изменить тариф".



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



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

Добавление нового сервиса

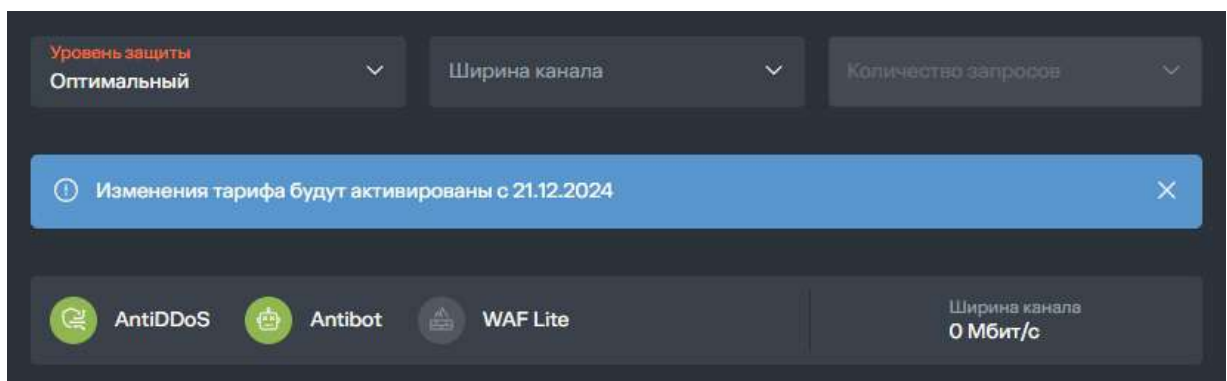
Добавление нового сервиса заключается в изменении уровня защиты:

- 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"

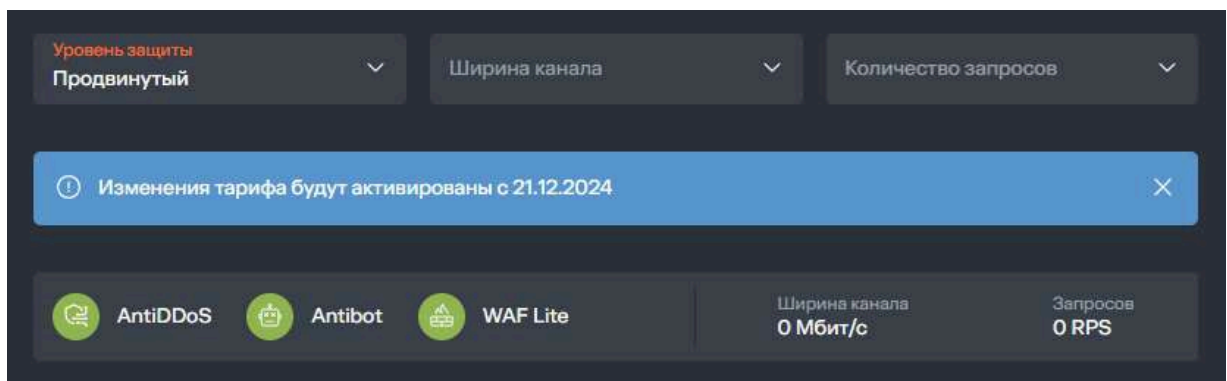
Для того, чтобы добавить новый сервис, выполните следующие действия:

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).

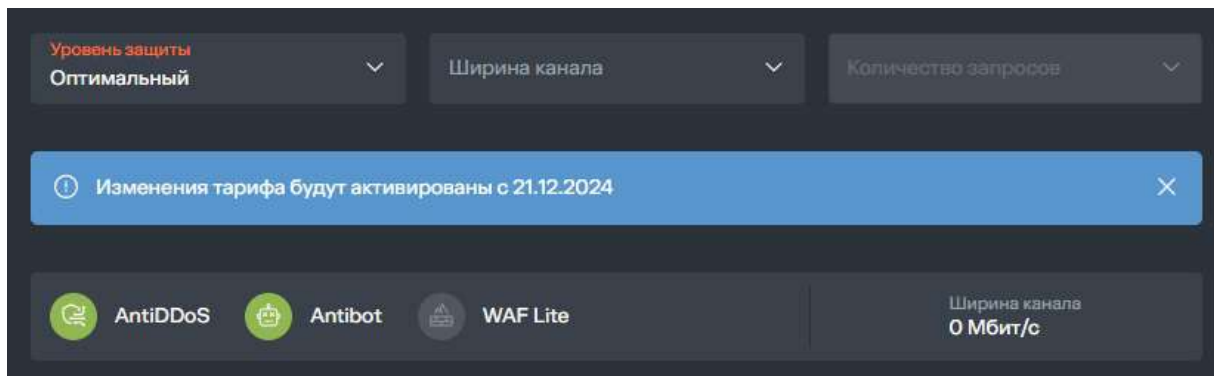
Пример.

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.

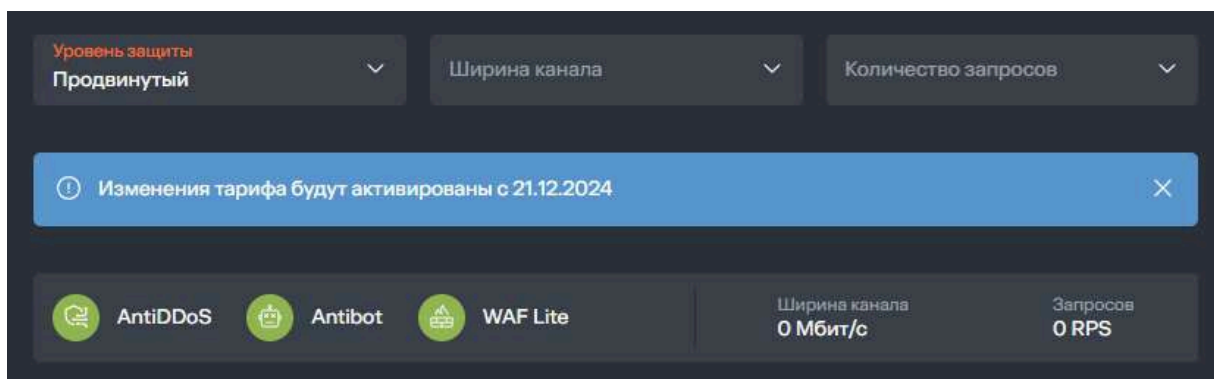
Для активации нового сервиса сразу выполните следующие действия:

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**



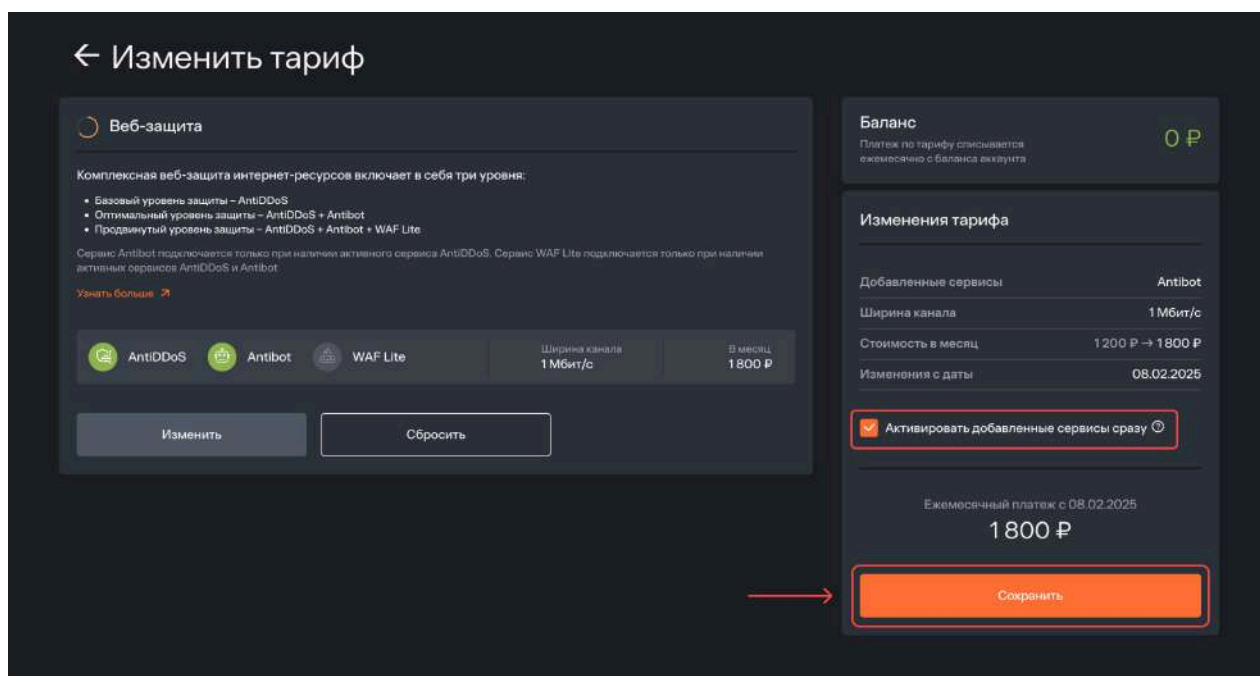
- Если у вас подключен **оптимальный** уровень защиты, то вы можете выбрать **продвинутый**, добавив сервис **WAF Lite**

The screenshot shows a dark-themed interface with three dropdown menus at the top: 'Уровень защиты' (Protection level) set to 'Продвинутый' (Advanced), 'Ширина канала' (Channel width), and 'Количество запросов' (Number of requests). Below these is a blue notification bar with a warning icon and the text 'Изменения тарифа будут активированы с 21.12.2024'. At the bottom, there are three service icons: AntiDDoS, Antibot, and WAF Lite. To the right of these icons, the current settings are displayed: 'Ширина канала' (Channel width) is '0 Мбит/с' and 'Запросов' (Requests) is '0 RPS'.

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".

This screenshot shows the same interface as the previous one, but with updated values. The 'Уровень защиты' (Protection level) remains 'Продвинутый' (Advanced). The 'Ширина канала' (Channel width) dropdown is now set to '1 Мбит/с'. The 'Количество запросов' (Number of requests) dropdown is set to '5 RPS'. The notification bar now says 'Изменения тарифа будут активированы с 08.02.2025'. Below the service icons, the current settings are shown: 'Ширина канала' (Channel width) is '1 Мбит/с', 'Запросов' (Requests) is '5 RPS', and 'В месяц' (Per month) is '7 800 ₽'. A red arrow points to the 'Применить' (Apply) button, which is highlighted with a red border. The 'Отменить' (Cancel) button is also visible.

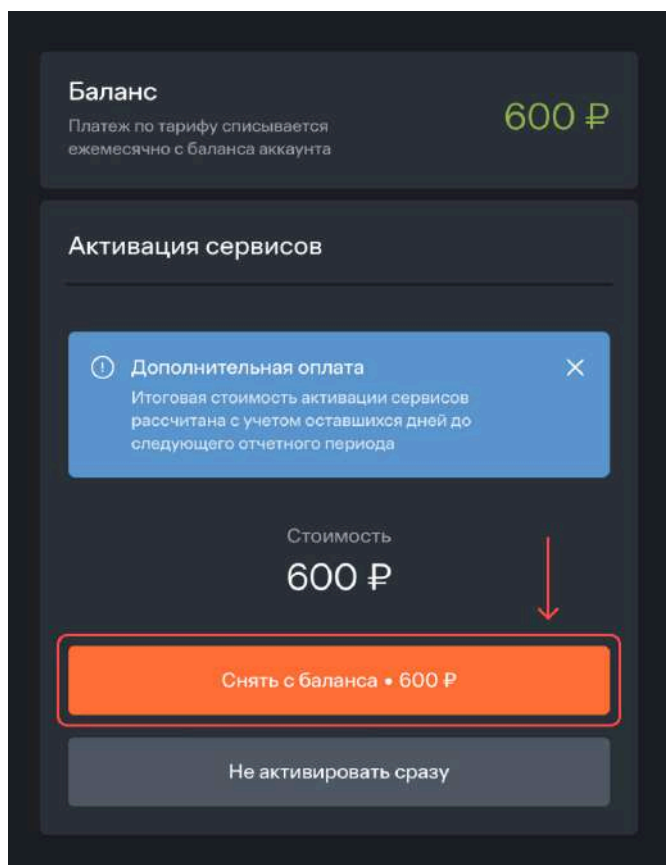
3. Проверьте информацию в блоке "Изменения тарифа", поставьте галочку "Активировать добавленные сервисы сразу" и нажмите на кнопку "Сохранить".



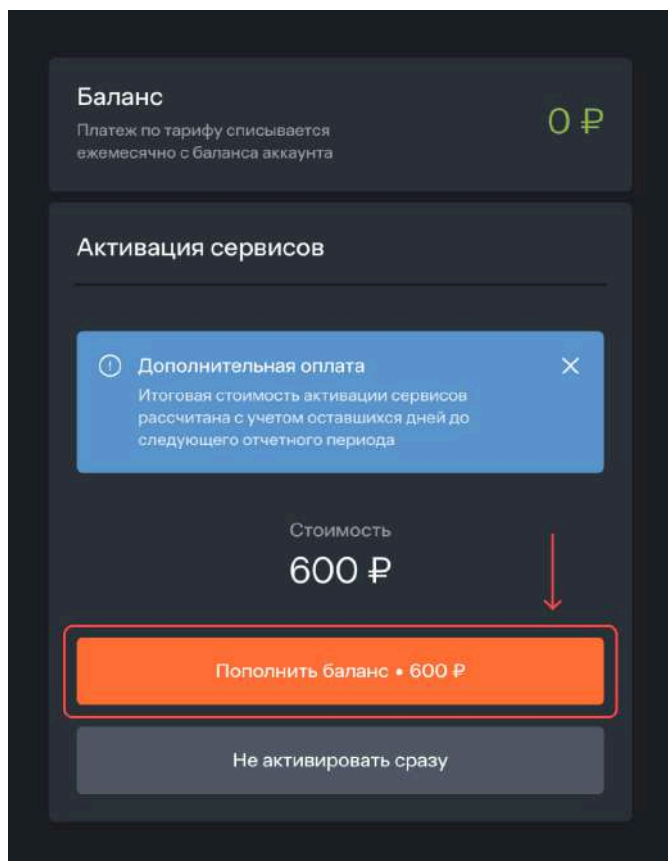
ⓘ Обратите внимание

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.

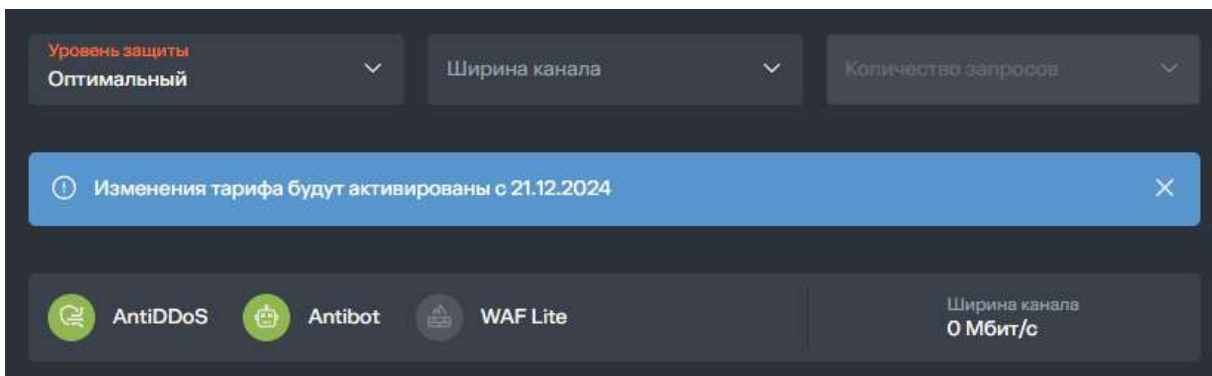
⚠ Важно

При удалении сервиса AntiDDoS защита веб-ресурса полностью отключается

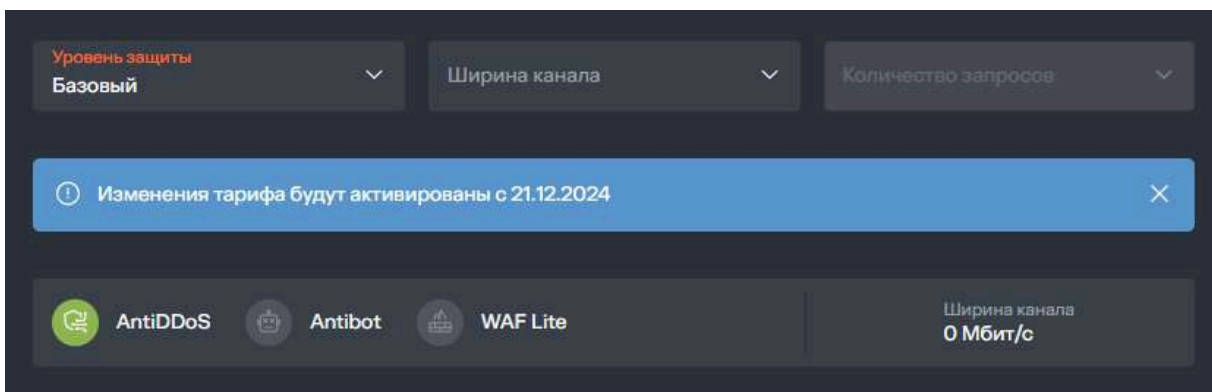
Для отключения сервисов выполните следующие действия:

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**

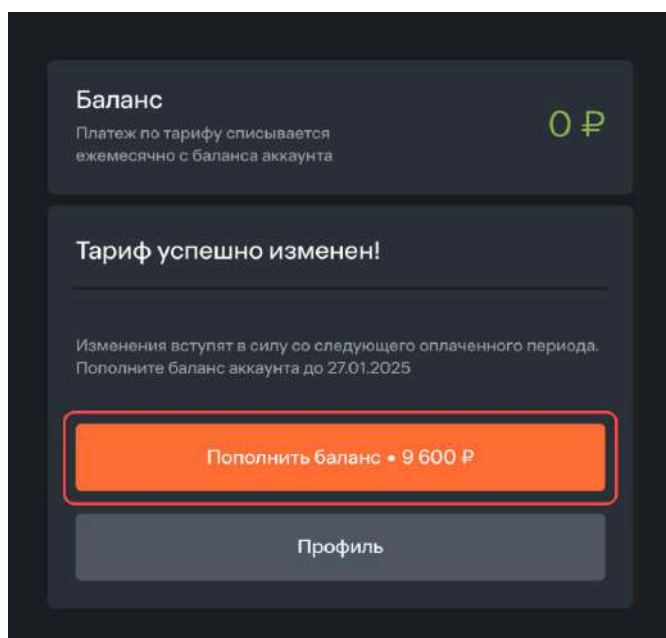


- С **оптимального** на **базовый** — для отключения сервиса Antibot. Активным останется сервис AntiDDoS

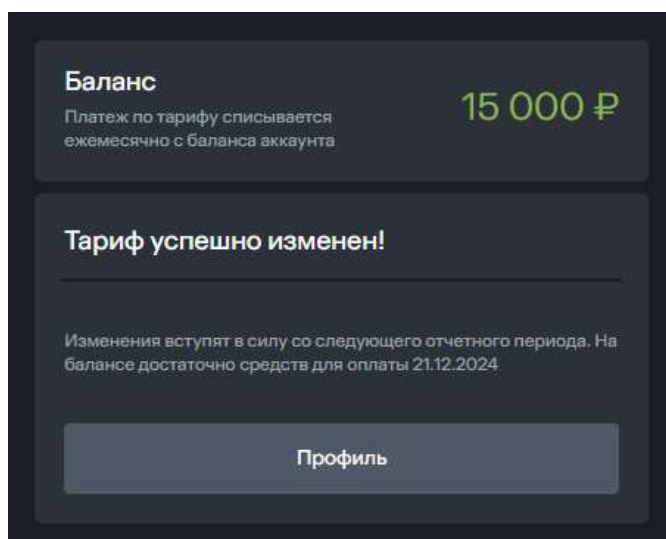
2. Укажите значение для поля "Ширина канала" и нажмите на кнопку "Применить".

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

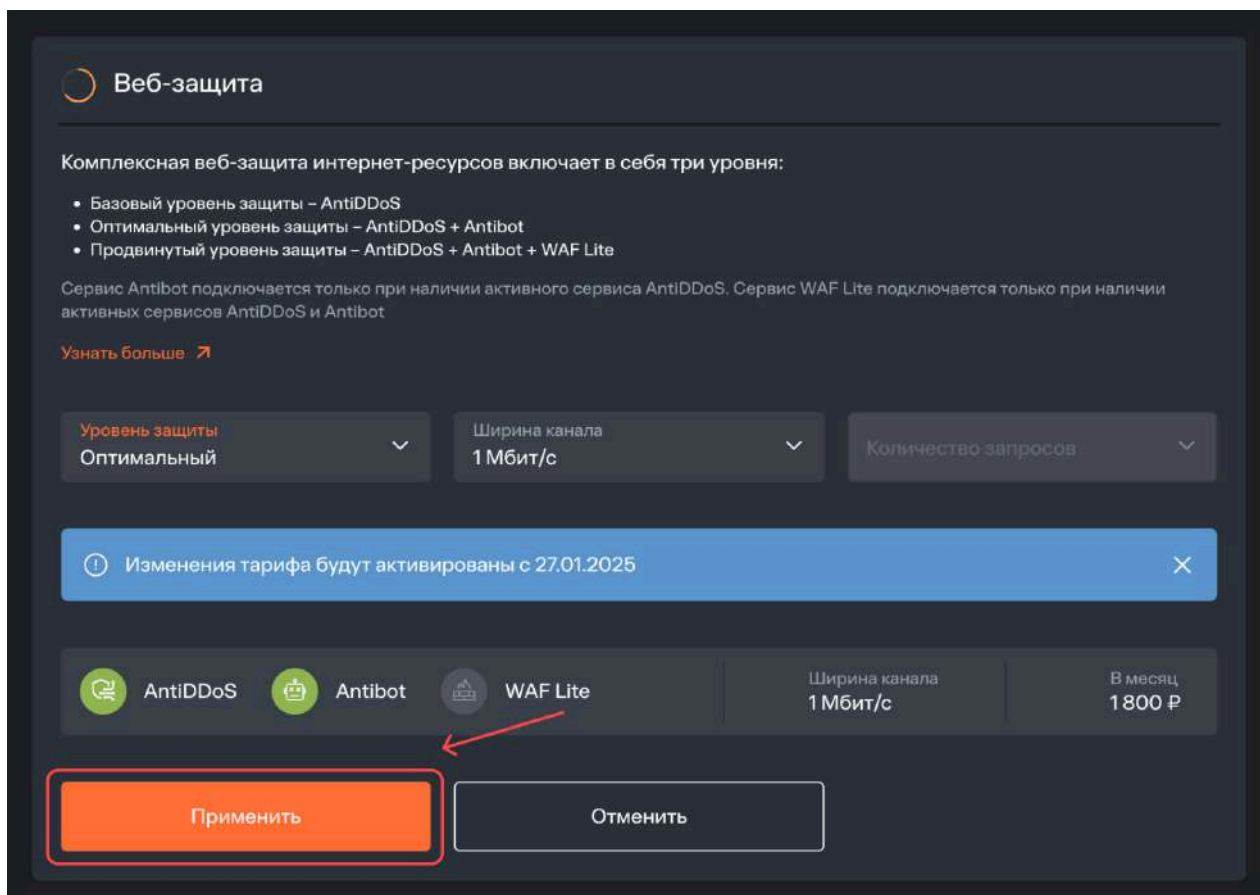
Параметры тарифа — это поля "Ширина канала" и "Количество запросов", которые редактируются вручную.

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

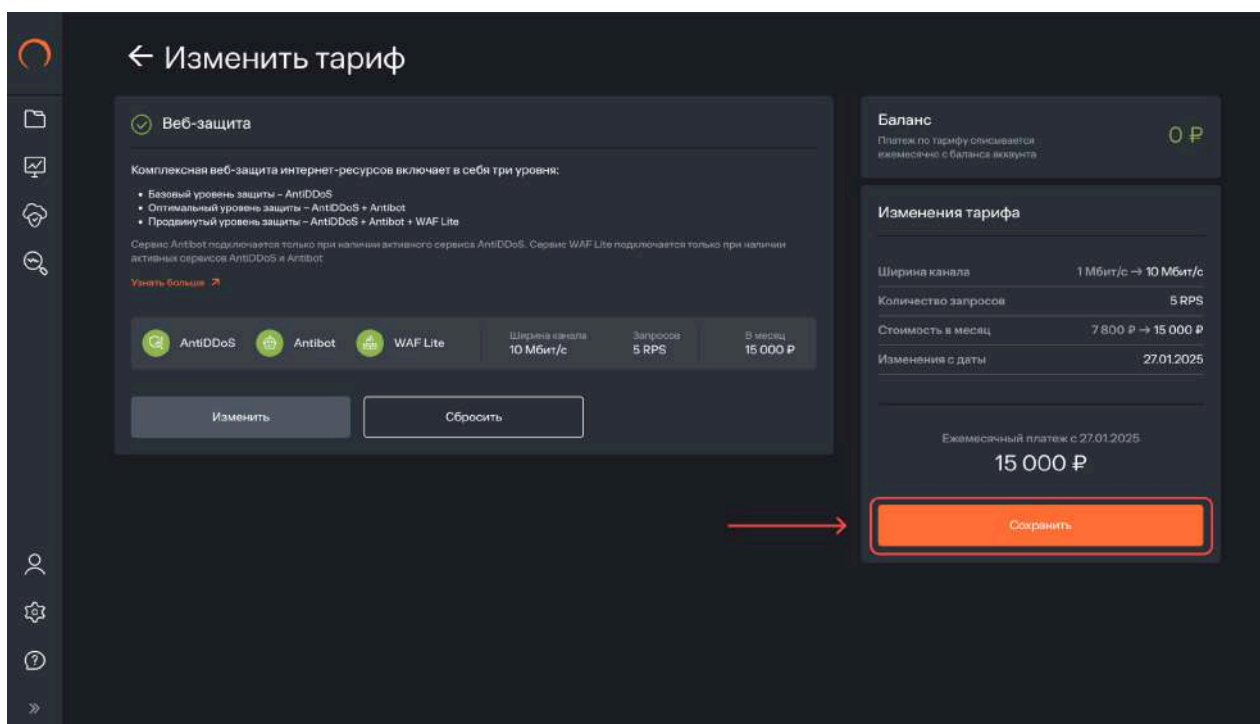
1. Отредактируйте значения нужных полей. В редактирование параметров тарифа входят:
 - Изменение ширины канала для любого уровня защиты (например, с 5 Мбит/с на 20 Мбит/с)
 - Изменение количества запросов для продвинутого уровня защиты (например, с 10 RPS на 20 RPS)

Если вы редактируете параметры тарифа и одновременно добавляете новый сервис, то все эти изменения вступят в силу со следующего отчетного периода.

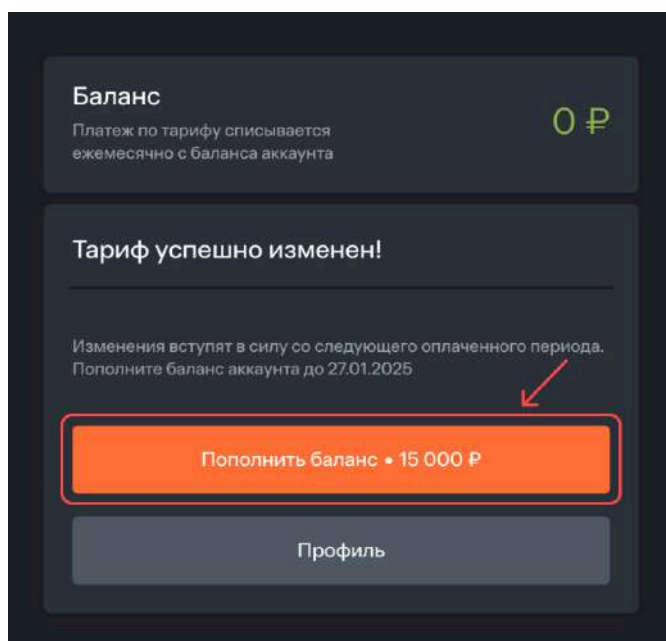
1. После редактирования параметров тарифа нажмите на кнопку "Применить".



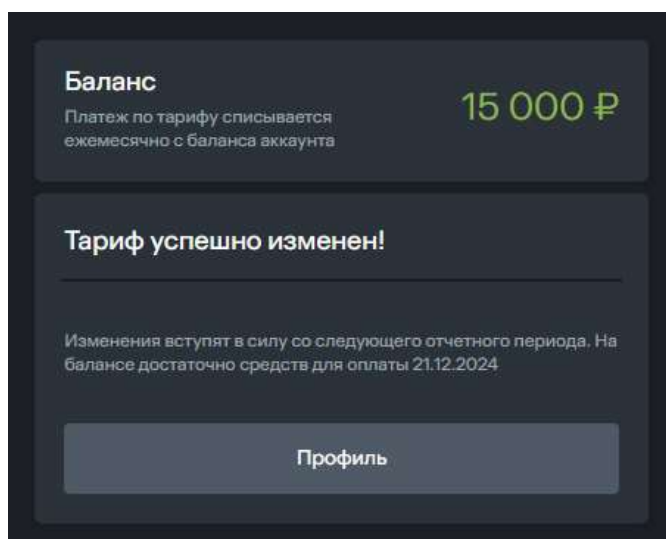
2. Проверьте информацию в блоке "Изменения тарифа" и нажмите на кнопку "Сохранить". Сумма к оплате в следующем месяце будет изменена.



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



4. 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 авторизоваться?](#)
- [Как восстановить пароль?](#)
- [Какие могут возникнуть ошибки при верификации и перенаправлении трафика?](#)
- [Как удалить ресурс?](#)
- [Как добавить DNS-TXT-запись для Timeweb?](#)
- [Как работает TTL?](#)
- [Solar Space — альтернатива Cloudflare?](#)
- [Как добавить свой SSL-сертификат?](#)
- [Как добавить DNS-записи в регистраторе nic.ru?](#)
- [Как добавить DNS-записи в регистраторе reg.ru?](#)
- [Почему может сработать капча или антибот?](#)
- [Как подобрать параметры тарифа веб-защиты?](#)

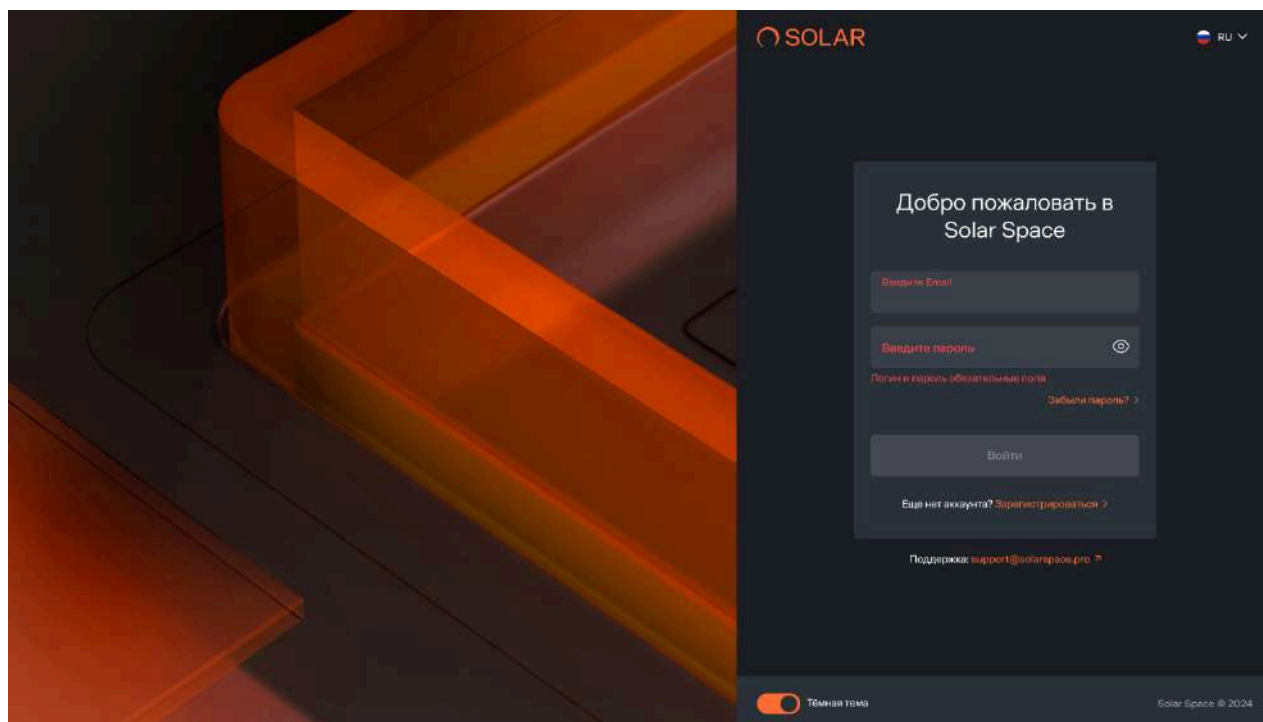
Авторизация

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.rt-solar.ru>. Откроется страница авторизации.



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

Добро пожаловать в
Solar Space

Введите Email
email@example.com

Введите пароль
.....

[Забыли пароль? >](#)

Войти

Еще нет аккаунта? [Зарегистрироваться >](#)

A red arrow points from the password field area down to the 'Войти' button.

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

Добро пожаловать в
Solar Space

Введите Email
email@example.com

Введите пароль
.....

Логин или пароль неверен

[Забыли пароль? >](#)

Войти

Еще нет аккаунта? [Зарегистрироваться >](#)

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

Добро пожаловать в
Solar Space

Введите Email
email@gmail.com

Введите пароль
..... 

[Забыли пароль? >](#)

Введите текст с картинки

Войти

Еще нет аккаунта? [Зарегистрироваться >](#)

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

Добро пожаловать в
Solar Space

Введите Email
email@gmail.com

Введите пароль
..... 

[Забыли пароль? >](#)

Введите текст с картинки
61144 

Неверный текст

Войти

Еще нет аккаунта? [Зарегистрироваться >](#)

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? >](#)



Введите текст с картинки
19130



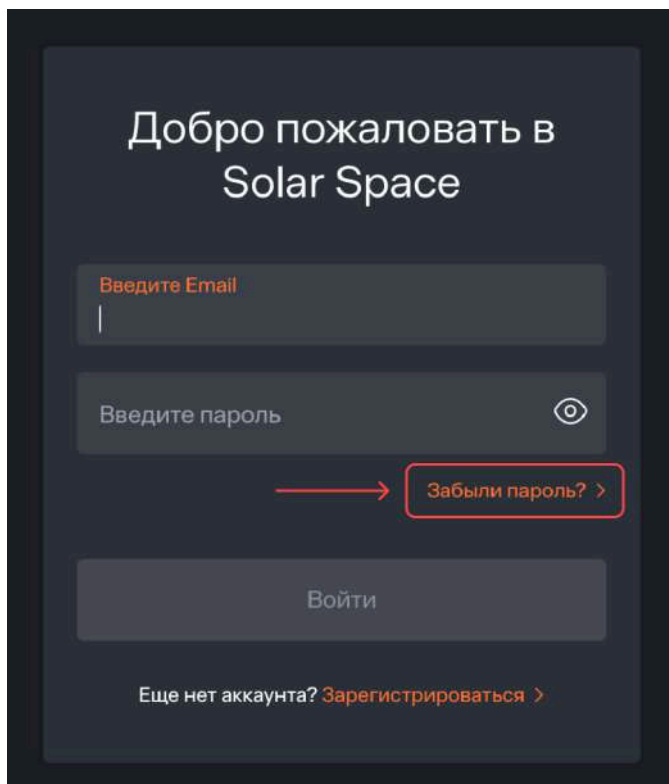
Войти

Еще нет аккаунта? [Зарегистрироваться >](#)

Восстановление пароля

Для восстановления пароля выполните следующие действия:

1. Откройте [страницу авторизации](#)
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".

Восстановление пароля

Введите ваш адрес электронной почты для получения письма с информацией по восстановлению пароля

Введите Email
email@example.com

Отправить

Еще нет аккаунта? [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 "Отправить".

Восстановление пароля

Введите текст с картинки ниже для получения проверочного кода

06535

Введите текст с картинки
06535

Отправить

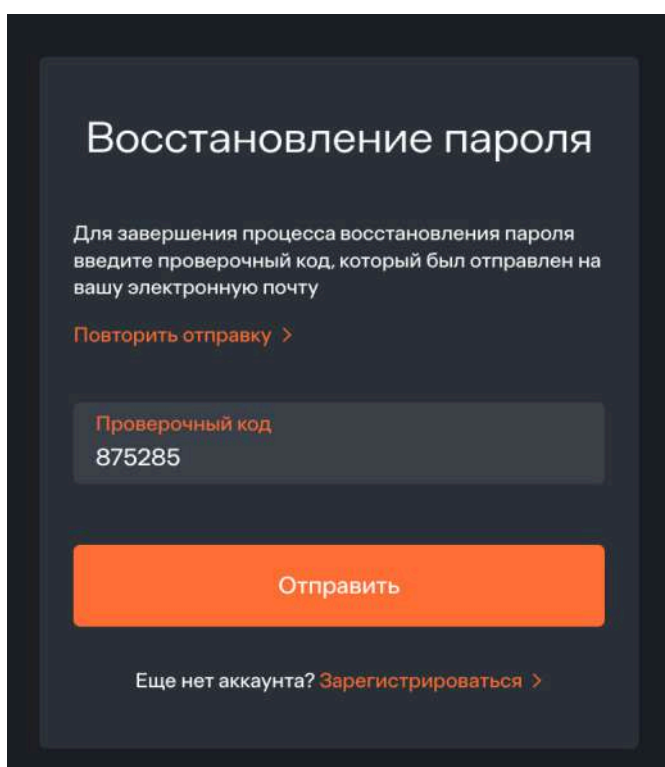
Еще нет аккаунта? [Зарегистрироваться](#) >

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

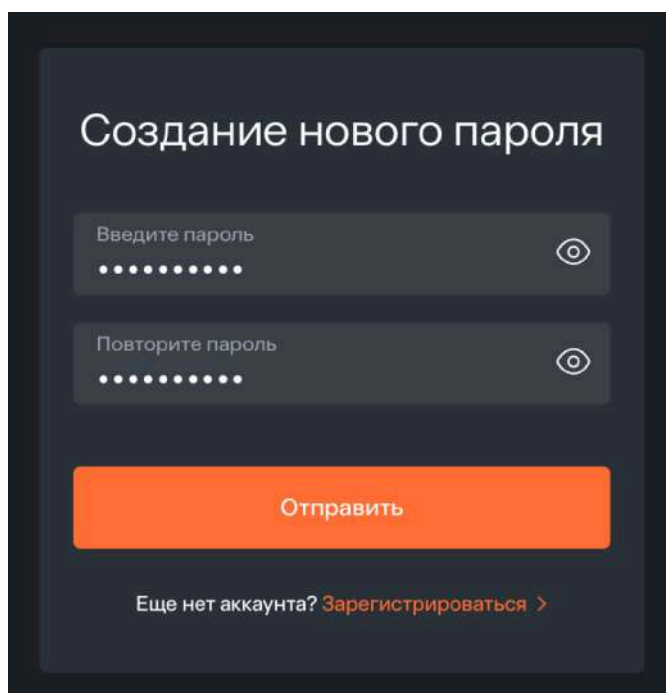


Если данного письма нет в папке "Входящие", проверьте папку "Спам". В случае, если письмо не пришло, перепроверьте введенную электронную почту и отправьте код повторно, нажав на кнопку "Повторить отправку". Запросить повторный код можно 1 раз в 60 секунд. Код действителен в течение 10 минут.

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".



Создание нового пароля

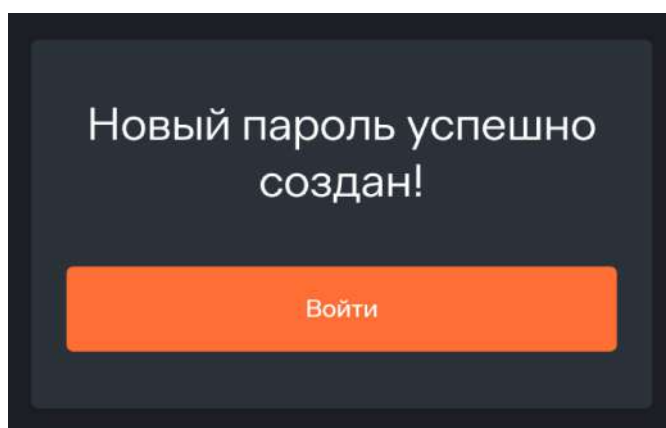
Введите пароль
.....

Повторите пароль
.....

Отправить

Еще нет аккаунта? [Зарегистрироваться >](#)

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.



Новый пароль успешно
создан!

Войти

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 обновления DNS- записей. Чтобы ускорить процесс, попробуйте очистить кэш DNS. Для этого обратитесь в поддержку регистратора или хостинг-провайдера.

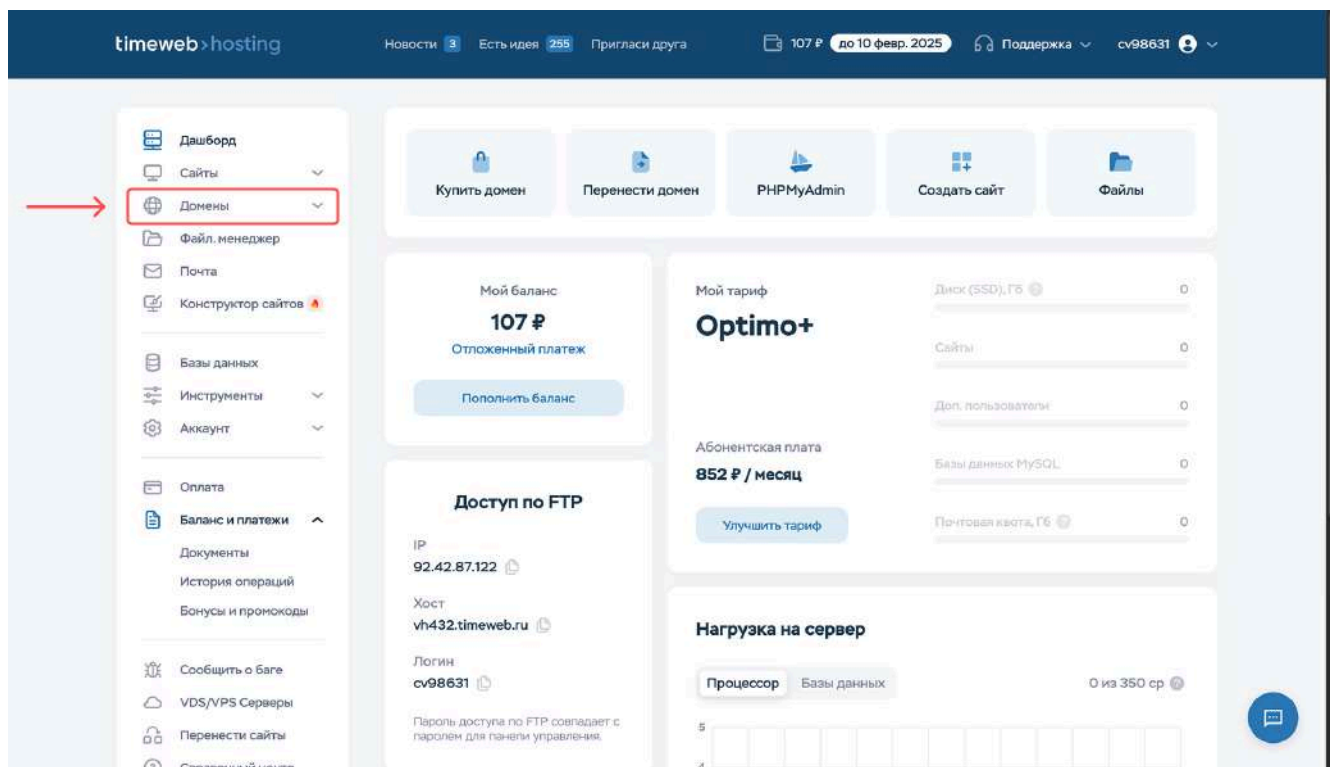
Технические проблемы

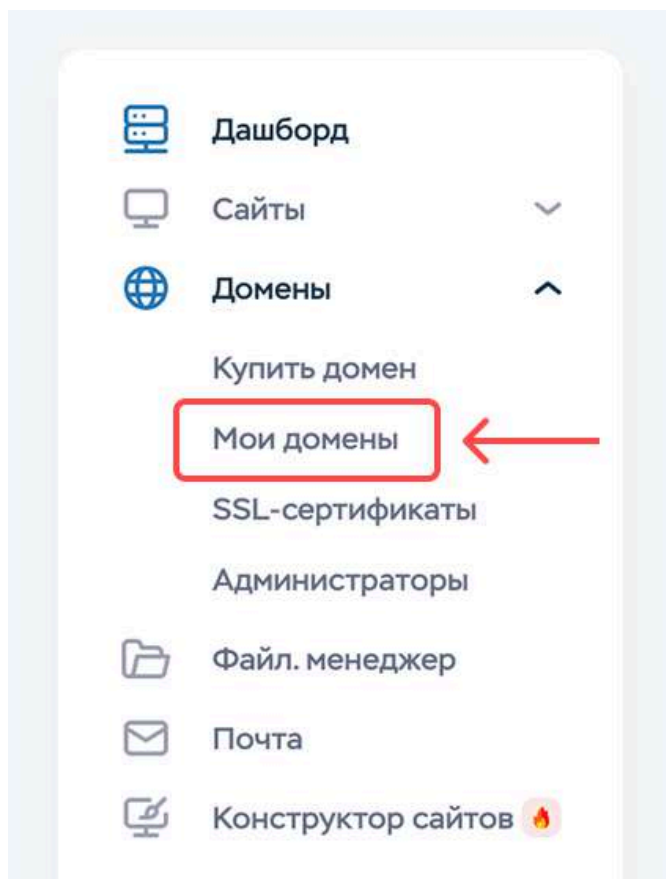
В некоторых случаях долгое обновление записей может быть связано с техническими проблемами на стороне DNS-сервера. Обратитесь в поддержку регистратора или хостинг-провайдера.

Добавление TXT-записи для Timeweb

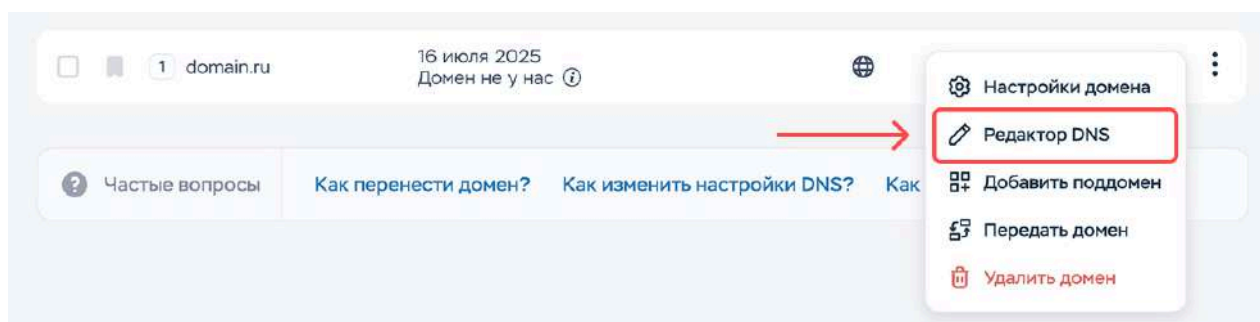
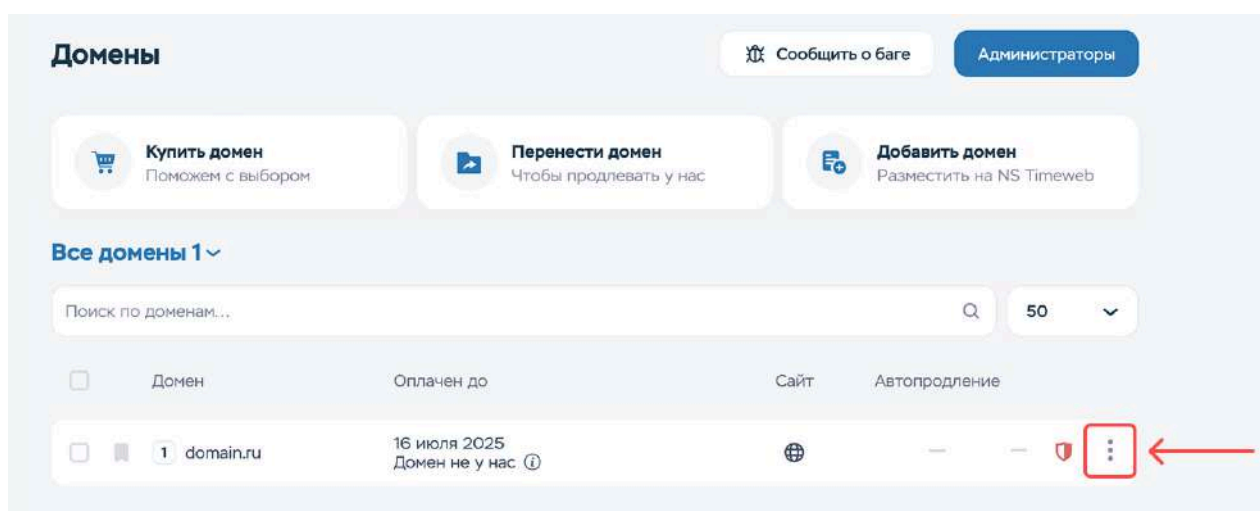
По инструкции ниже вы можете верифицировать ваш домен на примере хостинг-провайдера Timeweb. Добавление TXT-записи у других регистраторов или хостинг-провайдеров аналогично.

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

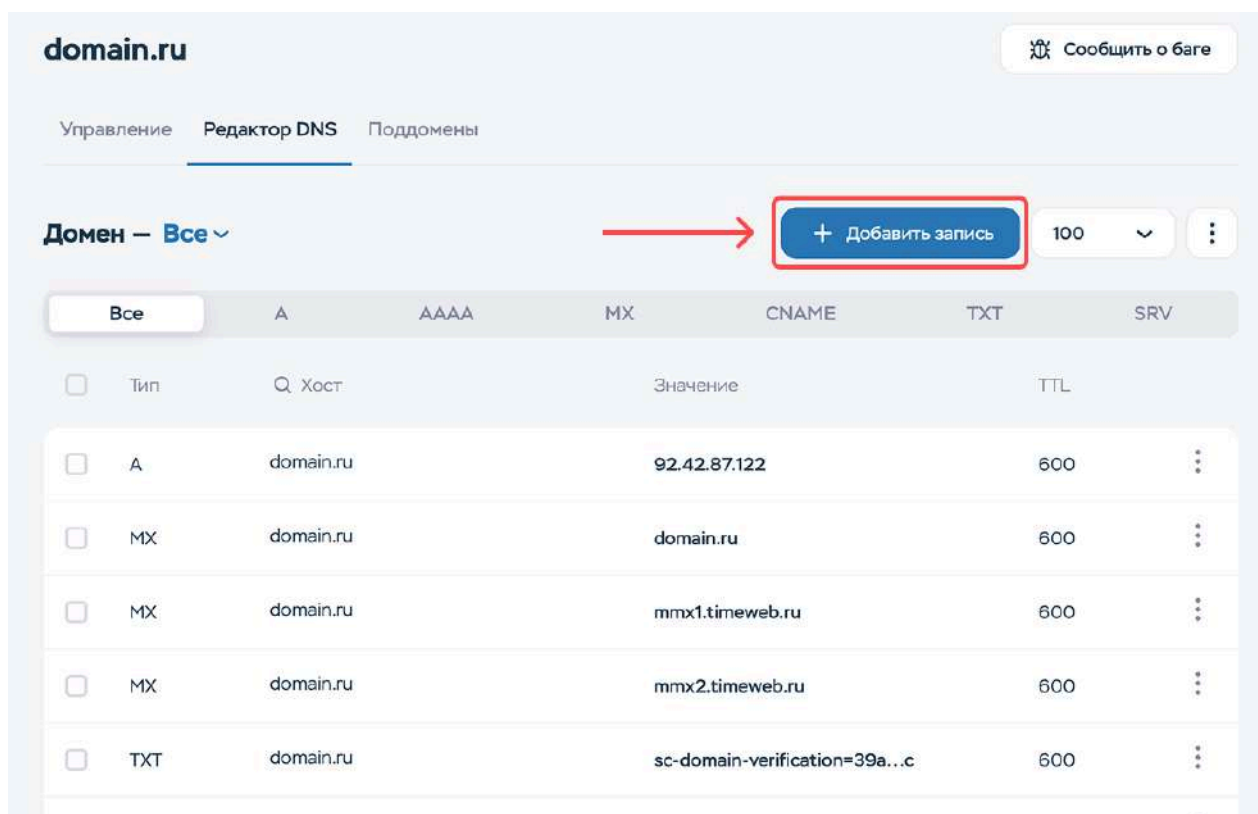




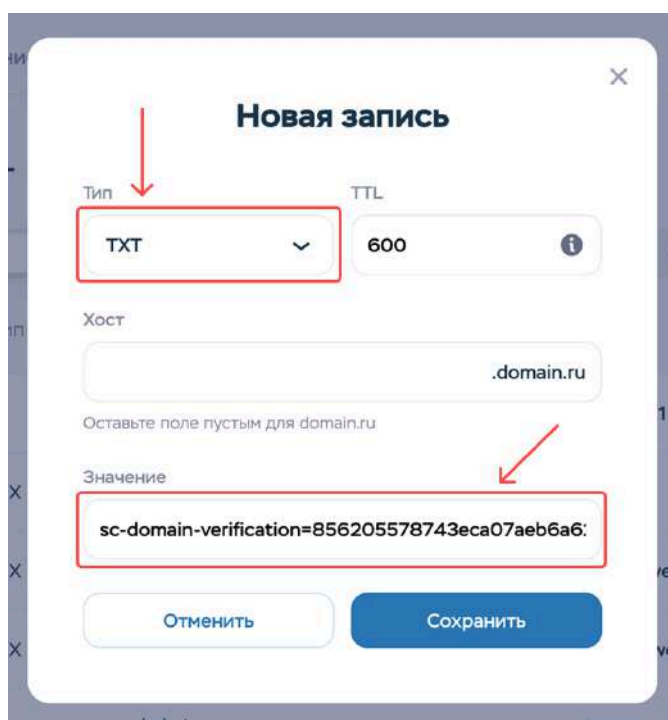
2. Выберите нужный домен и в правой части строки, нажав на три точки, выберите из выпадающего списка пункт "Редактор DNS". Откроется страница с записями.



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 количества 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.

Добавление своего SSL-сертификата

Из этой статьи вы узнаете, как добавить свой SSL-сертификат в личный кабинет Solar Space. Это необходимо для корректной работы системы защиты. Мы приводим инструкцию для регистратора nic.ru. Для других регистраторов шаги будут аналогичны.

Если у вас нет SSL-сертификата, вы можете выпустить бесплатный сертификат Let's Encrypt в личном кабинете Solar Space. Он будет автоматически продлеваться каждые 90 дней.

Компоненты SSL-сертификата

SSL-сертификат состоит из публичного (открытого) и приватного (закрытого) ключей шифрования.

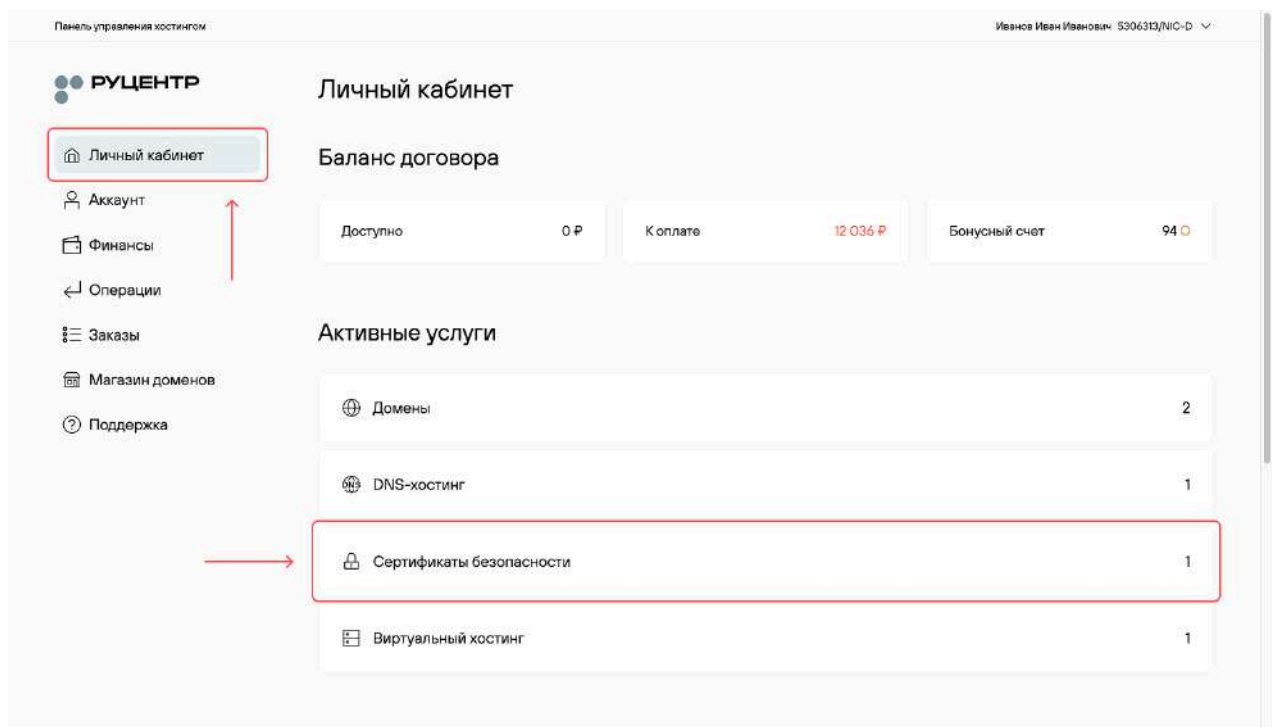
Публичный ключ шифрует данные при обращении пользователя к серверу. Он состоит из следующих элементов:

- сертификат,
- промежуточный сертификат,
- корневой сертификат.

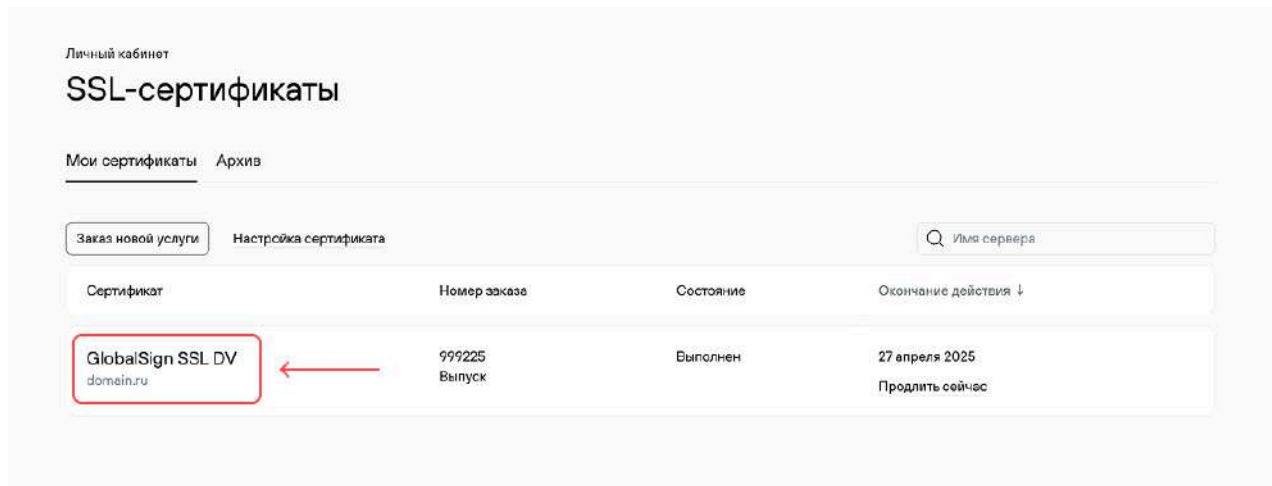
Приватный ключ расшифровывает данные, которые пользователь отправил серверу.

Как скачать SSL-сертификат

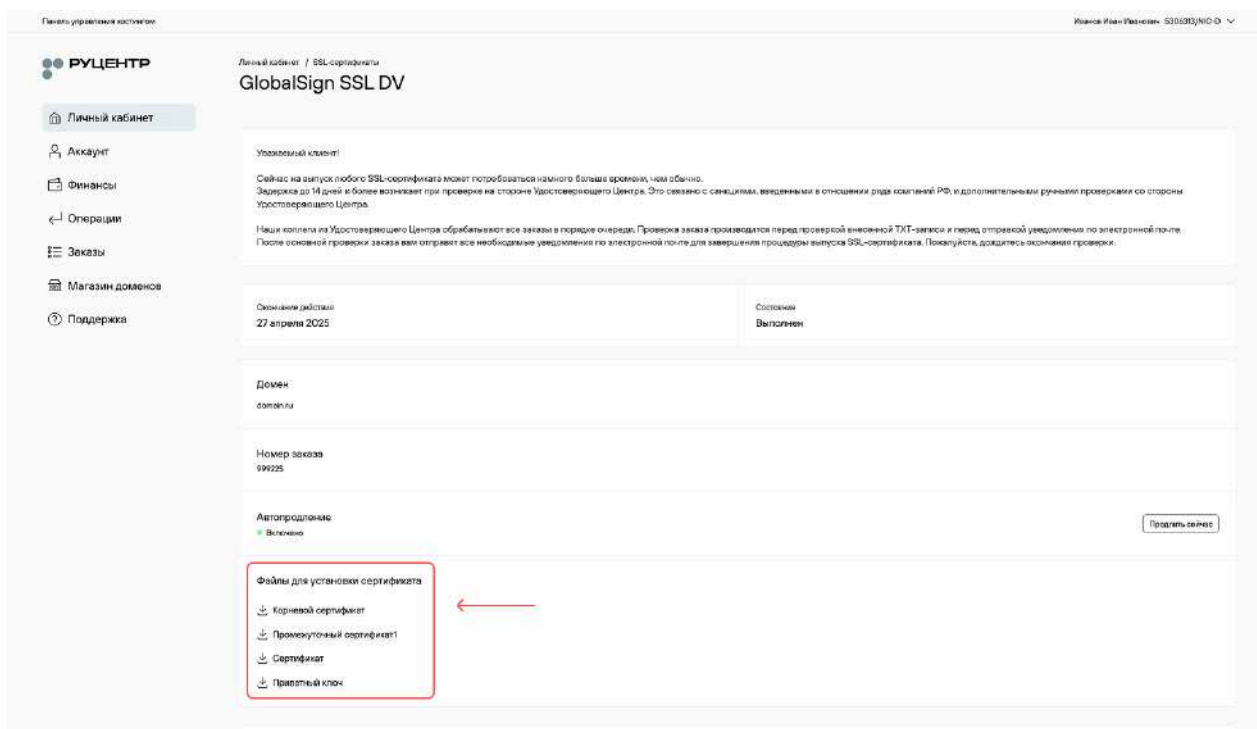
1. Войдите в личный кабинет вашего доменного регистратора, который выдал вам SSL-сертификат, — в нашей инструкции это nic.ru. Откройте блок "Личный кабинет" в меню слева и перейдите в раздел "Сертификаты безопасности".



2. Нажмите на название сертификата "GlobalSign SSL DV".



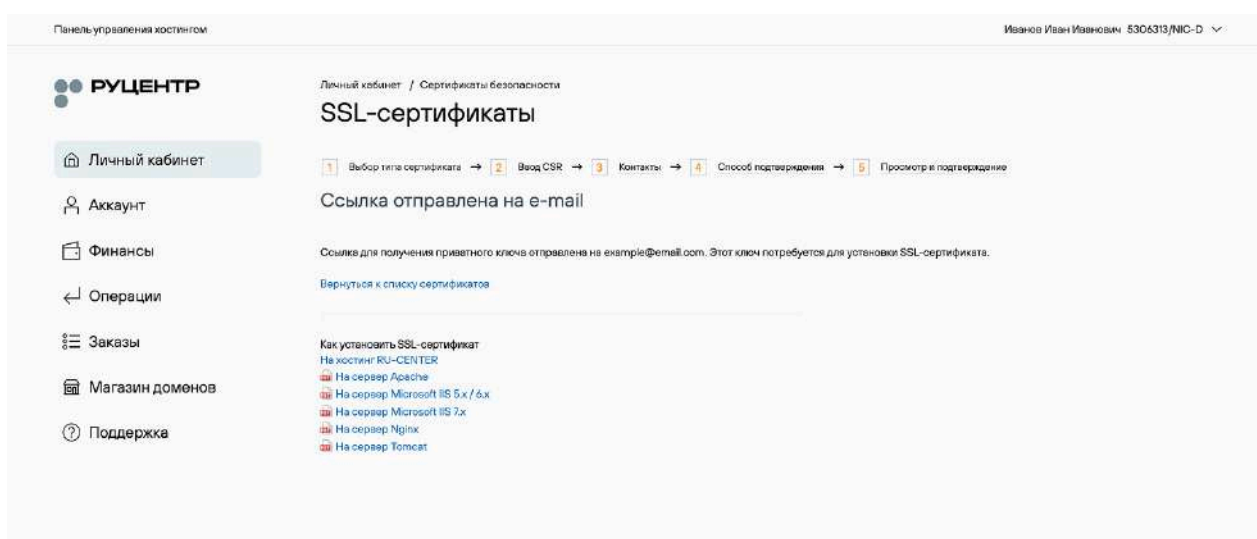
3. Откроются данные вашего SSL-сертификата. В нижней части страницы вы увидите блок "Файлы для установки сертификата", в который входят компоненты публичного ключа (корневой сертификат, промежуточный сертификат, сертификат) и приватный ключ.



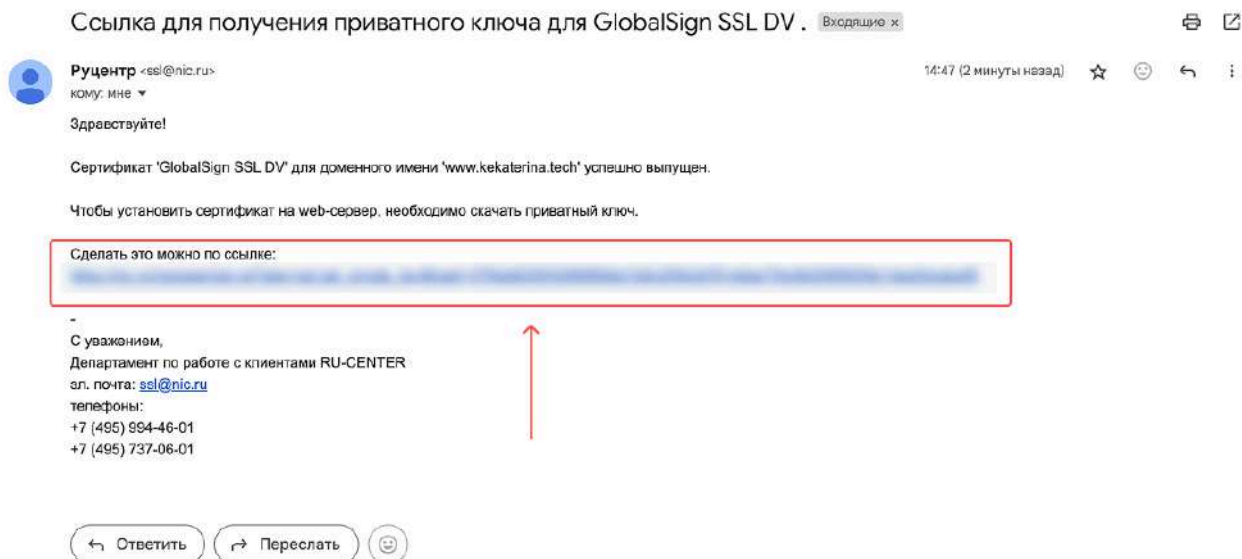
❗ Обратите внимание

Для других типов сертификатов или у других доменных регистраторов перечень компонентов SSL-сертификата иногда отличается. Например, может не быть промежуточного сертификата.

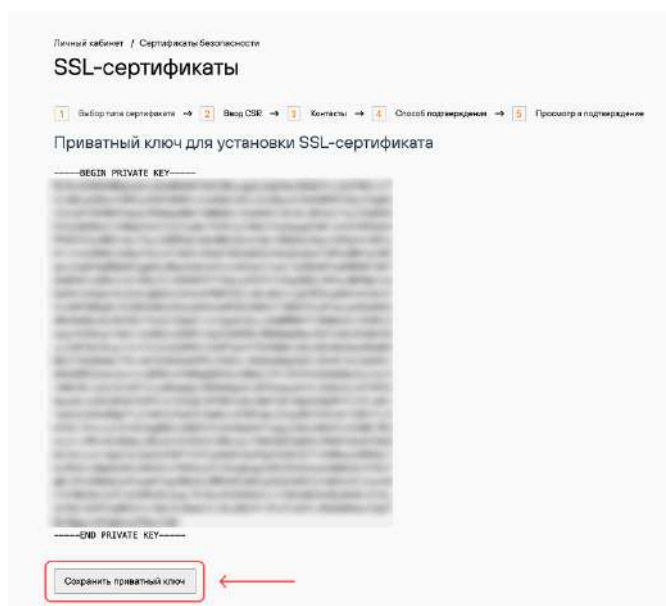
1. Нажмите на значок загрузки напротив каждого сертификата и приватного ключа. У регистратора nic.ru сертификаты скачиваются напрямую на устройство, а ссылка на скачивание приватного ключа приходит на электронную почту, привязанную к личному кабинету. У других регистраторов алгоритм получения сертификатов и приватного ключа может отличаться.



2. Откройте письмо от регистратора в электронной почте и перейдите по ссылке. У некоторых регистраторов сертификаты и приватный ключ приходят сразу в письме.



3. Вас перенаправит на страницу регистратора на вкладку "SSL-сертификаты", где вы можете скачать приватный ключ. Для этого нажмите "Сохранить приватный ключ". Он сохранится на ваше устройство.



4. Вы скачали все части SSL-сертификата. Файлы будут выглядеть следующим образом:

- Файл сертификата с названием вашего домена (сохранен на ваше устройство):



- Промежуточный сертификат (сохранен на ваше устройство):



- Корневой сертификат (сохранен на ваше устройство)



- Приватный ключ (сохранен на ваше устройство):



SSL-сертификат будет состоять из:

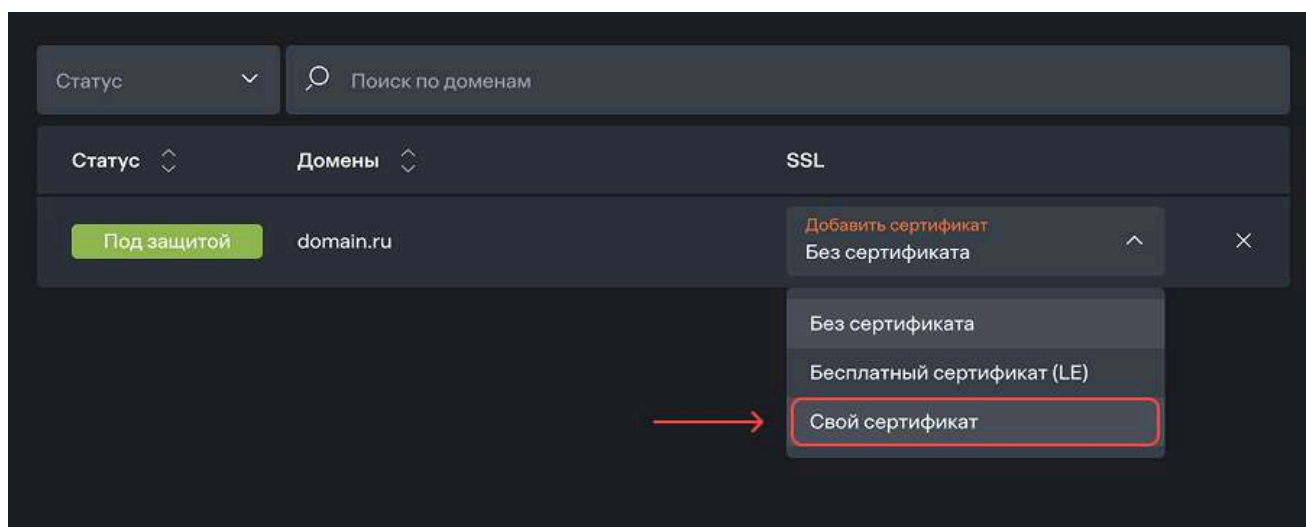
- приватного ключа — это файл key.txt
- публичного ключа — он состоит из сертификата, промежуточного сертификата и корневого сертификата, которые нужно будет расположить в определенной последовательности уже в Личном кабинете Solar Space.

Ниже расскажем, как это сделать.

Загрузка своего SSL-сертификата в личный кабинет Solar Space

Перейдите в раздел **Веб-защита**. Нажмите на строку нужного ресурса, откроется вкладка "Домен и SSL". В столбце "SSL" нажмите на поле "Добавить сертификат", откроется выпадающий список.

Выберите "Свой сертификат".



В открывшемся окне вам нужно вставить приватный и публичный ключи шифрования.

Добавить свой сертификат

domain.ru

Приватный ключ

Загрузите файл

Выбрать файл

или вставьте текстом

Приватный ключ

Публичный ключ

Загрузите файл

Выбрать файл

или вставьте текстом

Сертификат

Отменить Добавить

Приватный ключ и части публичного ключа нужно копировать обязательно вместе с их границами. Они содержатся в начале и в конце каждого ключа:

- границы приватного ключа:

```
-----BEGIN PRIVATE KEY-----  
-----END PRIVATE KEY-----
```

- границы для каждого из трех компонентов публичного ключа:

```
-----BEGIN CERTIFICATE-----  
-----END CERTIFICATE-----
```

Эти границы — часть ключей, без них шифрование не будет работать.

Добавление приватного ключа

1 вариант:

Для приватного ключа загрузите файл key.txt по кнопке "Выбрать файл". Они находятся на вашем устройстве в папке, куда ранее вы его скачивали.

2 вариант:

Откройте приватный ключ в текстовом редакторе Блокнот, скопируйте его полностью и вставьте в поле "Приватный ключ".

Добавление публичного ключа

Для публичного ключа вам нужно составить цепочку из его компонентов (сертификатов) в следующей последовательности:

1. Откройте файл "Сертификат" с названием домена в текстовом редакторе Блокнот, скопируйте его вместе с границами:

```
-----BEGIN CERTIFICATE-----  
(данные сертификата)  
-----END CERTIFICATE-----
```

Вставьте данные в текстовое поле "Сертификат" в личном кабинете Solar Space.

2. Откройте файл "Промежуточного сертификата" (в названии должно быть intermediate) в текстовом редакторе Блокнот, скопируйте его вместе с его границами:

```
-----BEGIN CERTIFICATE-----  
(данные промежуточного сертификата)  
-----END CERTIFICATE-----
```

Вставьте скопированный текст в поле "Сертификат" в личном кабинете Solar Space сразу после первого сертификата. 3. Откройте файл "Корневой сертификат" (в названии должно быть root) в текстовом редакторе Блокнот, скопируйте его вместе с границами:

```
-----BEGIN CERTIFICATE-----  
(данные корневого сертификата)  
-----END CERTIFICATE-----
```

Вставьте скопированный текст в поле "Сертификат" в личном кабинете сразу после данных промежуточного сертификата. Убедитесь, что вы вставили все компоненты публичного ключа вместе с их границами и расположили в правильной последовательности. Она должна быть такой:

1. Сертификат — файл с именем вашего домена.
2. Промежуточный сертификат — файл с названием "intermediate".
3. Корневой сертификат — файл с названием "root".

После того, как вы ввели в личном кабинете данные приватного и публичного ключей, нажмите кнопку "Добавить".

Добавить свой сертификат

domain.ru

Приватный ключ

Загрузите файл

✓ key.txt

или вставьте текстом

```
Приватный ключ
bXIM86v3Nq49jH6+k8kVex17hCVasZCIIAvgeWgsXVp3EGn0skaxb2Neh9rET9wf
qN41PnnS0b0JwFzpmF5ac...R2Dz...MM4V310AECgYEAc50ATjh1WGSvAfe1xwrB
C1h7NEB96v3jPCJehhMk1Ms0cc/7E1RavPV205DeX+1176Kx08LMelEYMail0+FIJSL
1o76j1CBFPvq4M1hfv9SALCU3FwdzY11DvjN2cPz1P3vFvehFc/NQ35QHeardCmpF
RUPppzz4F6pDzUCTKey?x=
-----END PRIVATE KEY-----
```

Публичный ключ

Загрузите файл

Выбрать файл

или вставьте текстом

```
Сертификат
jjM5Kc00SL1X0Kf8Epbst8YT5CRsuZRj+9x1a6dWPo64zzUhw81o/s7awl0qzJCK
6fBdPoyVQXpYK9ovnd7MAd6Bj+1EbddTKjd+82eEHbX1pc669SMJ5RMC3Nz4vQX
mcIfcg7jLQitChws/zyrVQ4PkX426BNK5b7hLi10YIVQVETIG309zJr1A0smeca
Hx86cyXSHK000yy6eM1NlxS67t1V09+57gJJT98a2HL06Z_KZR7ckpDMlhz1cpH
W09t
-----END CERTIFICATE-----
```

Отменить **Добавить**

Нажмите "Сохранить" в нижней части экрана.

← domain.ru Под защитой

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

Статус: Под защитой | Поиск по доменам

Статус	Домены	SSL
Под защитой	domain.ru	Добавить сертификат Свой сертификат

Настройки

Перенаправление трафика

Добавьте DNS-A запись для доменов в вашем хостинг-провайдере, чтобы перенаправить весь трафик через наши серверы защиты

Узнать больше

✓ Трафик успешно перенаправлен

Редирект с WWW

Перенаправление трафика на домен без www

Узнать больше

Редирект на HTTPS

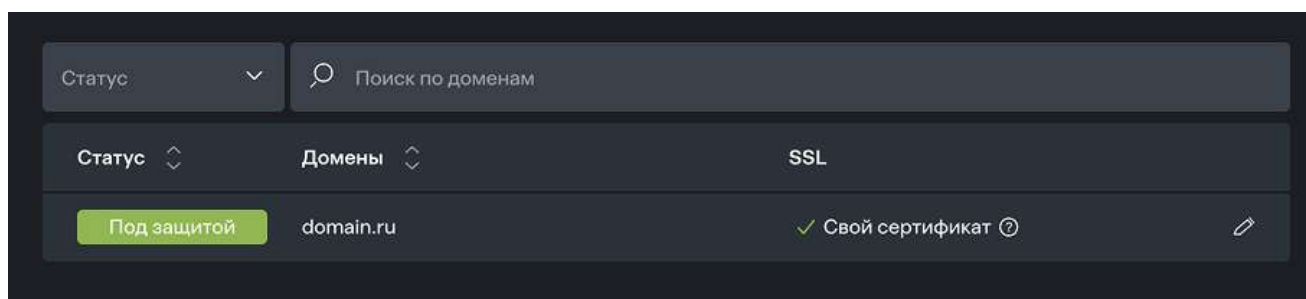
Отключение возможности подключения к доменам без SSL-сертификатов

Узнать больше

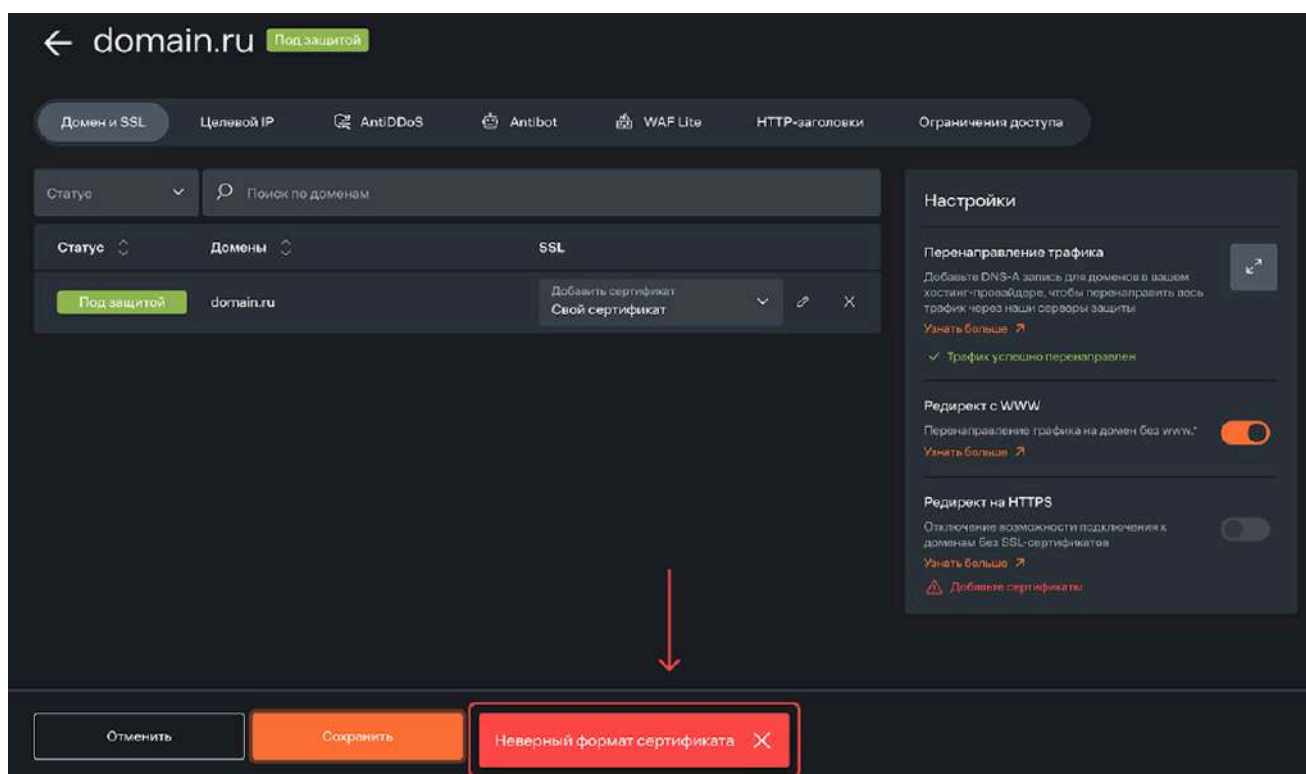
Добавьте сертификаты

Отменить **Сохранить**

Если данные SSL-сертификата были введены правильно, вы увидите зеленую галочку и статус "Свой сертификат" в столбце "SSL".



Если вы ввели данные неверно, при сохранении вы увидите в нижней части экрана оповещение об ошибке “Неверный формат сертификата”.



В этом случае проверьте, что вы скопировали публичный и приватный ключи вместе с границами и добавили компоненты публичного ключа в правильной последовательности. Убедитесь, что вы использовали все необходимые данные для SSL-сертификата.

Как добавить DNS-записи в регистраторе nic.ru

В этой статье описано, как добавить TXT-запись и A-запись в настройках домена, зарегистрированного в nic.ru. TXT-запись необходима для верификации домена в личном кабинете Solar Space, A-запись — для перенаправления трафика через сервер защиты.

Если вы используете reg.ru, инструкция по добавлению DNS-записей [здесь](#). Если вы используете timeweb, инструкция по добавлению DNS-записей [здесь](#). Если вы используете другой хостинг-провайдер, действия будут аналогичны, но названия разделов могут отличаться от приведенных в этой статье. Воспользуйтесь инструкциями ваших провайдеров.

Войдите в личный кабинет nic.ru с вашим паролем и логином — это номер вашего договора NIC-D или NIC-REG.

Вход

NIC-D NIC-REG

Номер договора NIC-D

Пароль

Административный ▾

Войти

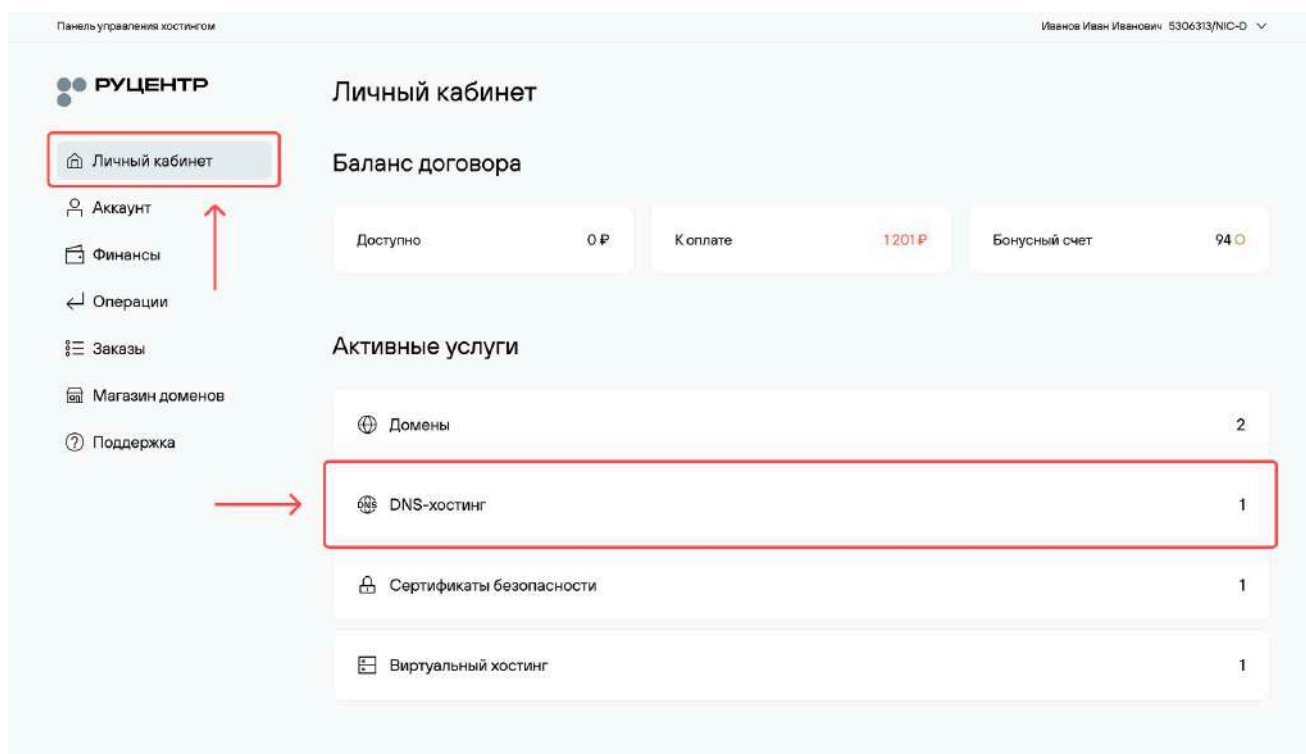
или

госуслуги

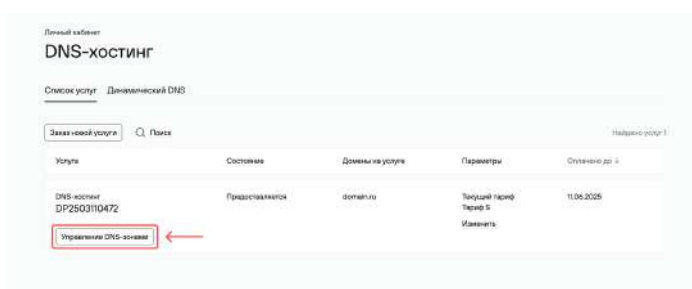
Вход по электронной подписи

Напомнить номер договора и пароль

Перейдите в раздел "DNS-хостинг", где находятся настройки управления вашим хостингом и ресурсными записями.



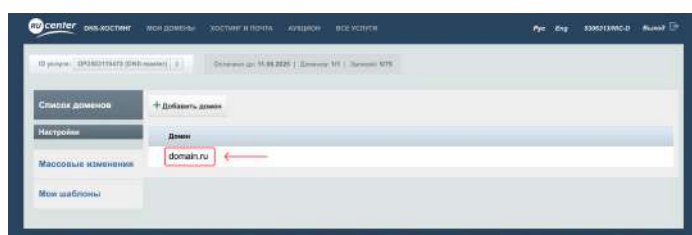
В столбце "Состояние" должен быть статус "Предоставляется". Это значит, что DNS-хостинг успешно подключен к домену, и вы можете добавлять и удалять ресурсные записи для него. Нажмите "Управление DNS-зонами" под названием услуги DNS-хостинга.



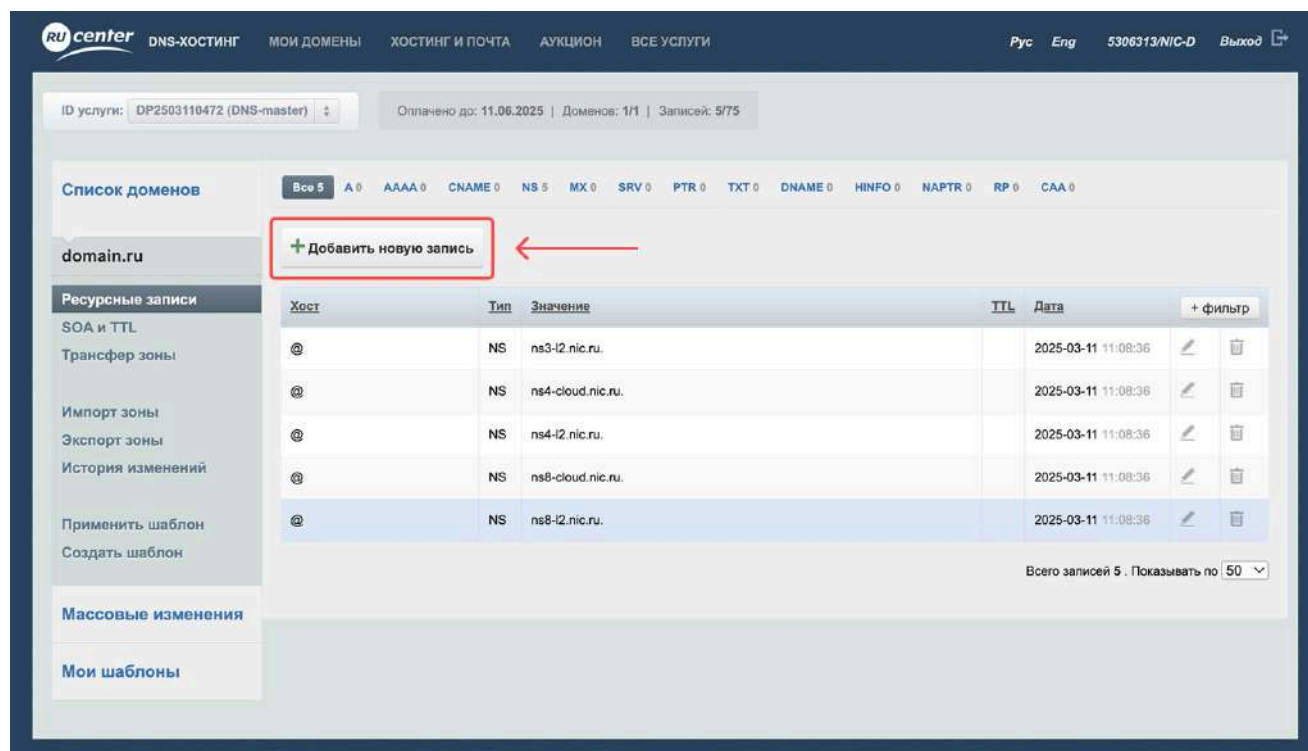
Чтобы убедиться, что вы переходите в управление нужного хостинга, проверьте название домена в столбце "Домены на услуге". Имя домена должно совпадать с DNS-хостингом, который вы собираетесь редактировать.

Вас перенаправит на страницу DNS-хостинга — RU-CENTER, где вы можете добавить DNS-записи.

Нажмите на название домена.

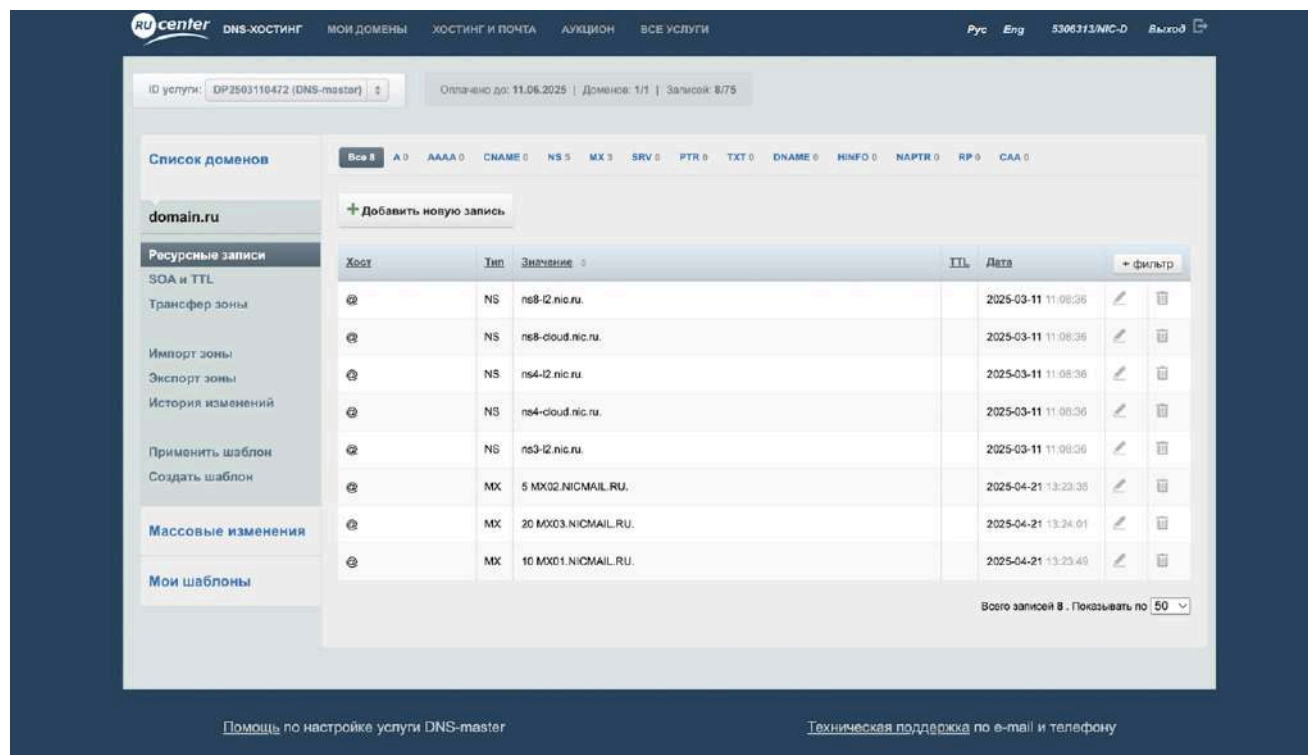


Вас перенаправит на страницу "Ресурсные записи".



Добавление TXT-записи

Нажмите "Добавить новую запись".



Вы увидите поля для заполнения данных о новой DNS-записи.

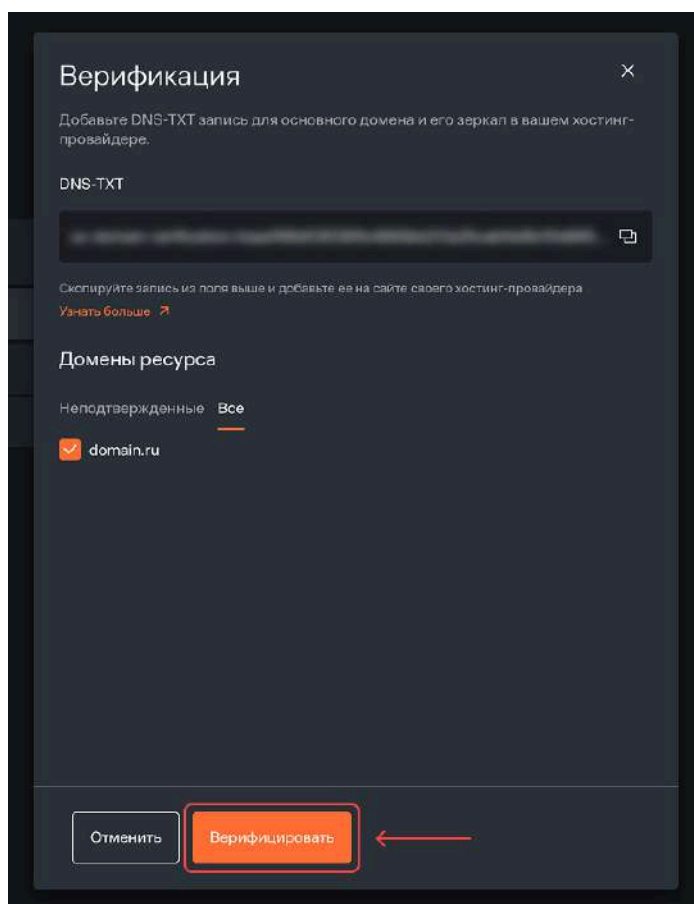
Хост	Тип	Значение	TTL	Дата	Файл
@	NS	ns3-42.nic.ru		2025-03-11 11:08:30	
@	NS	ns4-cloud.nic.ru		2025-03-11 11:08:30	
@	NS	ns4-42.nic.ru		2025-03-11 11:08:30	
@	NS	ns8-cloud.nic.ru		2025-03-11 11:08:30	
@	NS	ns8-42.nic.ru		2025-03-11 11:08:30	

Добавьте DNS-TXT-запись:

- В поле "Name" — введите имя домена, для которого добавляете запись.
- В поле "Type" выберите тип DNS-записи — "TXT".
- В поле "Text" введите скопированную DNS-TXT-запись из личного кабинета Solar Space.
- В поле "TTL" введите время в секундах. Это время, в течение которого DNS-записи хранятся в кэше на серверах и клиентских устройствах. Чтобы TXT-запись при настройке защиты Solar Space обновилась быстрее, рекомендуем установить в этом поле значение "300". Подробнее про TTL и выбор его оптимального значения, читайте здесь.

Нажмите «**Добавить**», затем — «**Выгрузить зону**» в верхней части страницы.

Если вы добавляете одновременно и A-запись, то сразу переходите к следующему пункту статьи "Добавление A-записи". Если вы добавляете только TXT-запись, то вернитесь в личный кабинет и нажмите "Верифицировать".



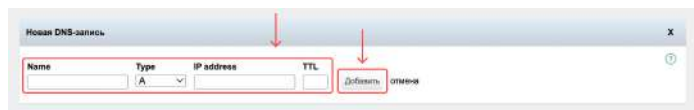
Как только TXT-запись будет подтверждена, вам придет уведомление об этом на электронную почту, указанную при регистрации.

Добавление A-записи

Для добавления DNS-A-записи снова нажмите на кнопку "Добавить новую запись".

- В поле "Name" введите имя вашего домена, для которого добавляете запись.
- В поле "Type" выберите тип DNS-записи — A.
- В поле "IP address" введите скопированную DNS-A-запись из личного кабинета Solar Space.
- В поле "TTL" введите время в секундах. Это время, в течение которого DNS-записи хранятся в кэше на серверах и клиентских устройствах. Чтобы TXT-запись при настройке защиты Solar Space обновилась быстрее, рекомендуем установить в этом поле значение "300". Подробнее про TTL и выбор его оптимального значения, читайте здесь.

— Нажмите "Добавить" и следом, - "Выгрузить зону" в верхней части страницы.



⚠ Зона содержит изменения, не выгруженные на сервер. [Отменить изменения](#). [предпросмотр зоны](#) [Выгрузить зону](#)

Все 6 A 0 AAAA 0 CNAME 0 NS 5 MX 0 SRV 0 PTR 0 TXT 1 DNAME 0 HINFO 0 NAPTR 0 RP 0 CAA 0

+ Добавить новую запись

Новая DNS-запись X

Name Type IP address TTL ?

Добавить отмена

Хост	Тип	Значение	TTL	Дата	+ фильтр
domain.ru	A	93.185.164.139	660	2025-03-12 13:31:26	
@	NS	ns3-l2.nic.ru.		2025-03-11 11:08:36	
@	NS	ns4-cloud.nic.ru.		2025-03-11 11:08:36	
@	NS	ns4-l2.nic.ru.		2025-03-11 11:08:36	
@	NS	ns8-cloud.nic.ru.		2025-03-11 11:08:36	
@	NS	ns8-l2.nic.ru.		2025-03-11 11:08:36	
domain.ru	TXT	sc-domain-verification=601f519357f16d039e80ec65cdaa2931ac67287a3e24058e8374974e8b80bd15	660	2025-03-12 13:24:14	

Сразу после выгрузки зоны DNS-записи станут активными.

Все 7 A 1 AAAA 0 CNAME 0 NS 5 MX 0 SRV 0 PTR 0 TXT 1 DNAME 0 HINFO 0 NAPTR 0 RP 0 CAA 0

+ Добавить новую запись

Хост	Тип	Значение	TTL	Дата	+ фильтр
@	NS	ns3-l2.nic.ru.		2025-03-11 11:08:36	
@	NS	ns4-cloud.nic.ru.		2025-03-11 11:08:36	
@	NS	ns4-l2.nic.ru.		2025-03-11 11:08:36	
@	NS	ns8-cloud.nic.ru.		2025-03-11 11:08:36	
@	NS	ns8-l2.nic.ru.		2025-03-11 11:08:36	
domain.ru	A	93.185.164.139	660	2025-03-12 13:31:26	
domain.ru	TXT	sc-domain-verification=601f519357f16d039e80ec65cdaa2931ac67287a3e24058e8374974e8b80bd15	660	2025-03-12 13:24:14	

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

Все 10

A 1AAAA 0CNAME 0NS 5MX 3SRV 0PTR 0TXT 1DNAME 0HINFO 0NAPTR 0RP 0CAA 0

+ Добавить новую запись

Хост	Тип	Значение	TTL	Дата	+ фильтр	
domain.com	TXT	sc-domain-verification=abe8509d04565c3f731482c142fcd00955b59f7bdade768125f03388b6cd0833	600	2025-04-21 16:22:56		
@	NS	ns8-l2.nic.ru.		2025-03-11 11:08:36		
@	NS	ns8-cloud.nic.ru.		2025-03-11 11:08:36		
@	NS	ns4-l2.nic.ru.		2025-03-11 11:08:36		
@	NS	ns4-cloud.nic.ru.		2025-03-11 11:08:36		
@	NS	ns3-l2.nic.ru.		2025-03-11 11:08:36		
domain.com	A	93.185.164.10		2025-04-21 16:22:50		
@	MX	5 MX02.NICMAIL.RU.		2025-04-21 13:23:35		
@	MX	20 MX03.NICMAIL.RU.		2025-04-21 13:24:01		
@	MX	10 MX01.NICMAIL.RU.		2025-04-21 13:23:49		

Как только DNS-записи будут подтверждены, вам придет уведомление об этом на электронную почту, указанную при регистрации.

Как добавить DNS-записи в регистраторе reg.ru

В этой статье описано, как добавить TXT-запись и A-запись в настройках домена, зарегистрированного в reg.ru. TXT-запись необходима для верификации домена в личном кабинете Solar Space, A-запись — для перенаправления трафика через сервер защиты.

Если вы используете nic.ru, инструкция по добавлению DNS-записей [здесь](#). Если вы используете timeweb, инструкция по добавлению DNS-записей [здесь](#). Если вы используете другой хостинг-провайдер, действия будут аналогичны, но названия разделов могут отличаться от приведенных в этой статье. Воспользуйтесь инструкциями ваших провайдеров.

Войдите в личный кабинет reg.ru с вашим паролем и логином.

Войдите в аккаунт

Если у вас еще нет аккаунта,
перейдите на вкладку Регистрация
и зарегистрируйтесь в один клик

Регистрация

Вход

Электронная почта или логин

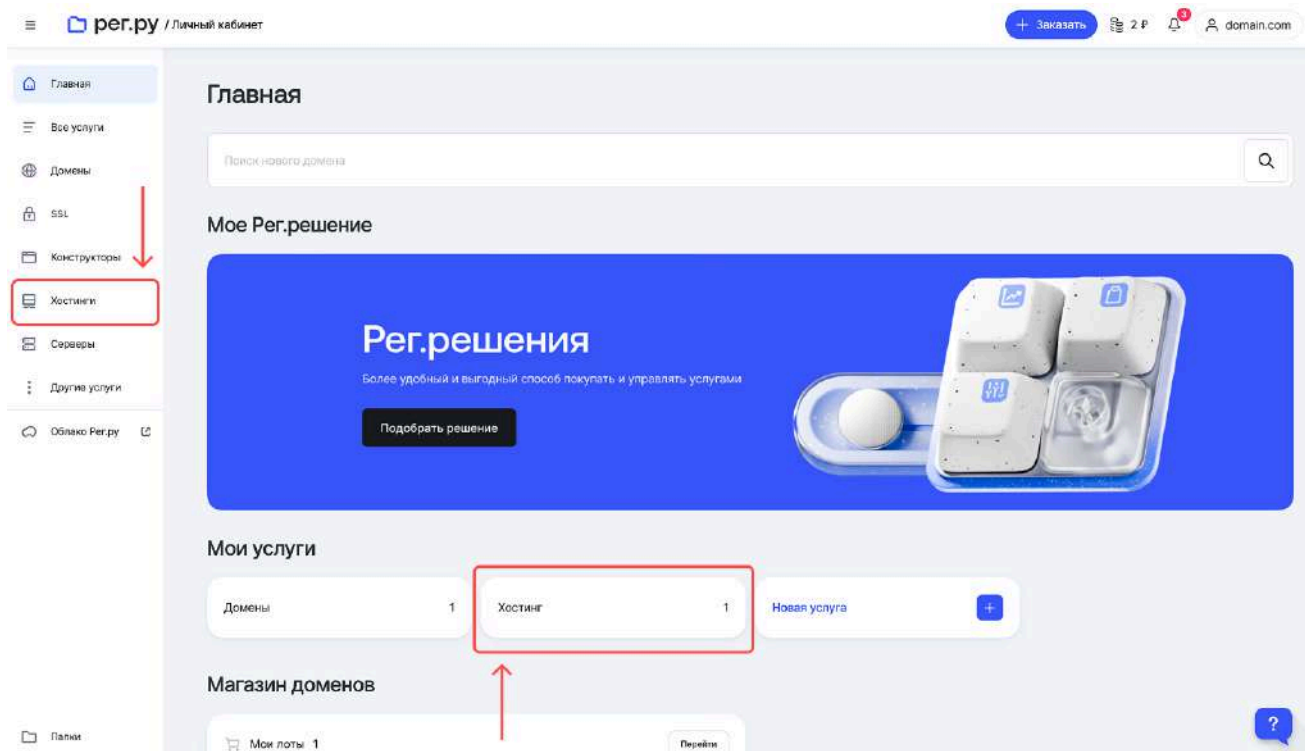
Пароль

👁

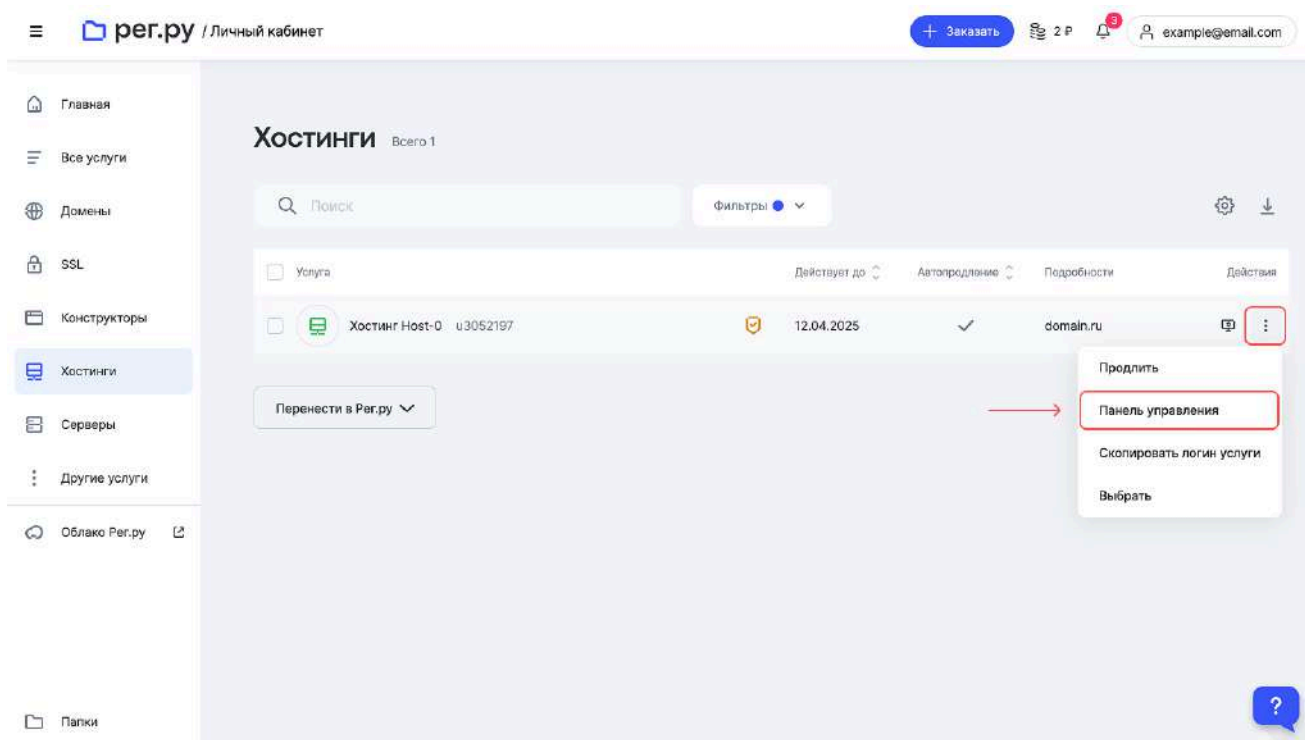
[Забыли пароль?](#)

Войти

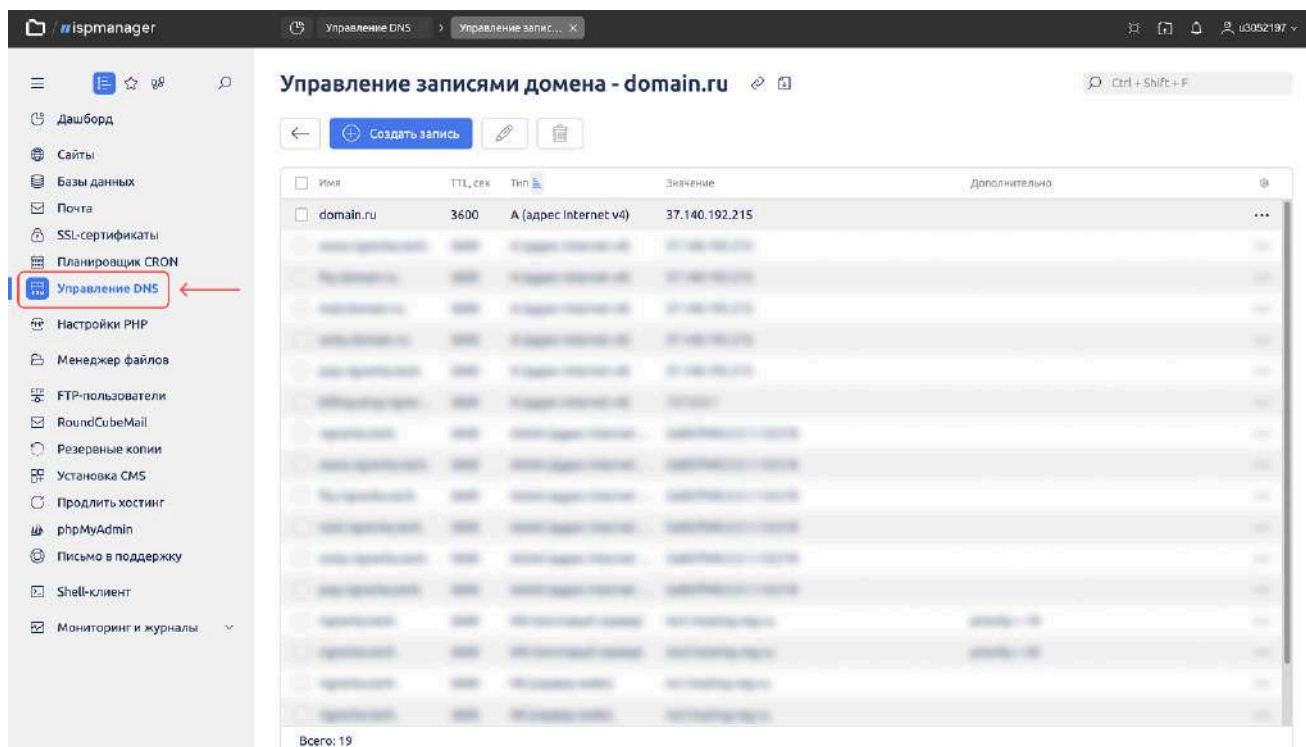
Нажмите на "Хостинг" в левом меню или на "Хостинг" в "Мои услуги" на главной странице.



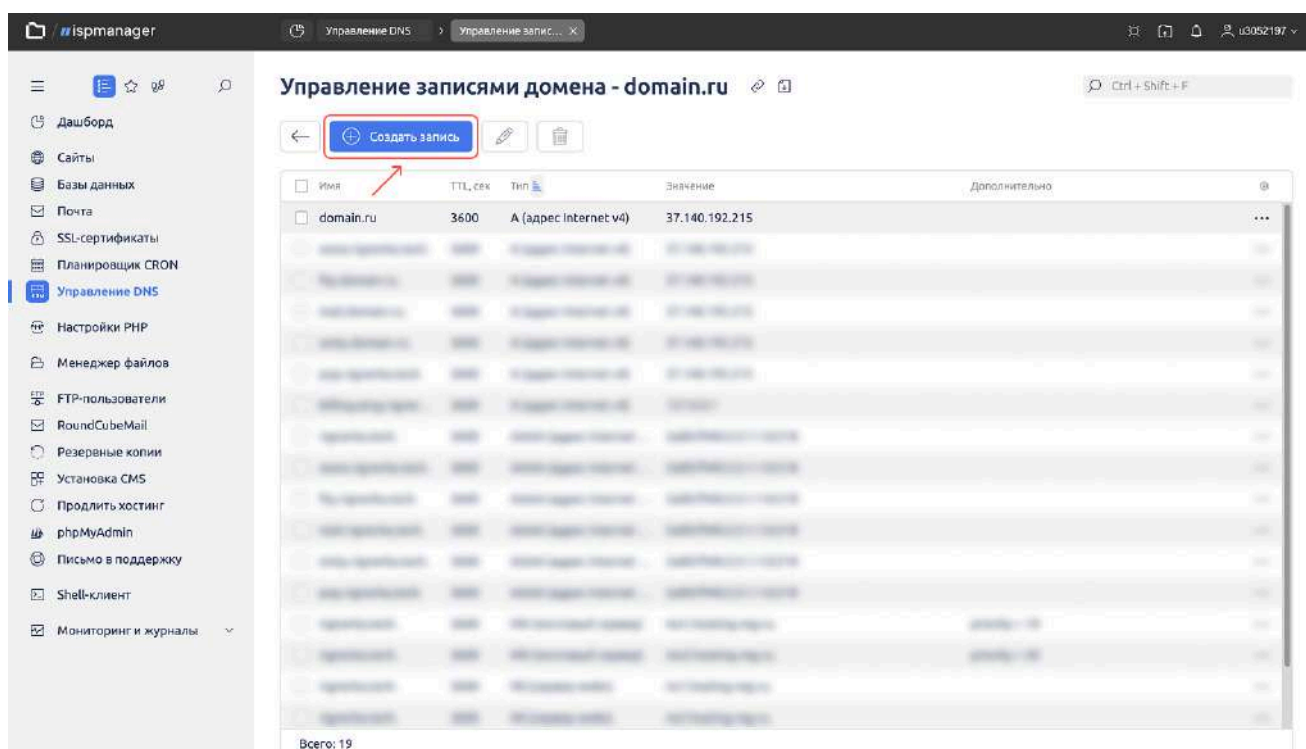
Оба пути переведут вас на страницу "Хостинги". Нажмите на три точки справа в строке вашего хостинга. Выберите "Панель управления".



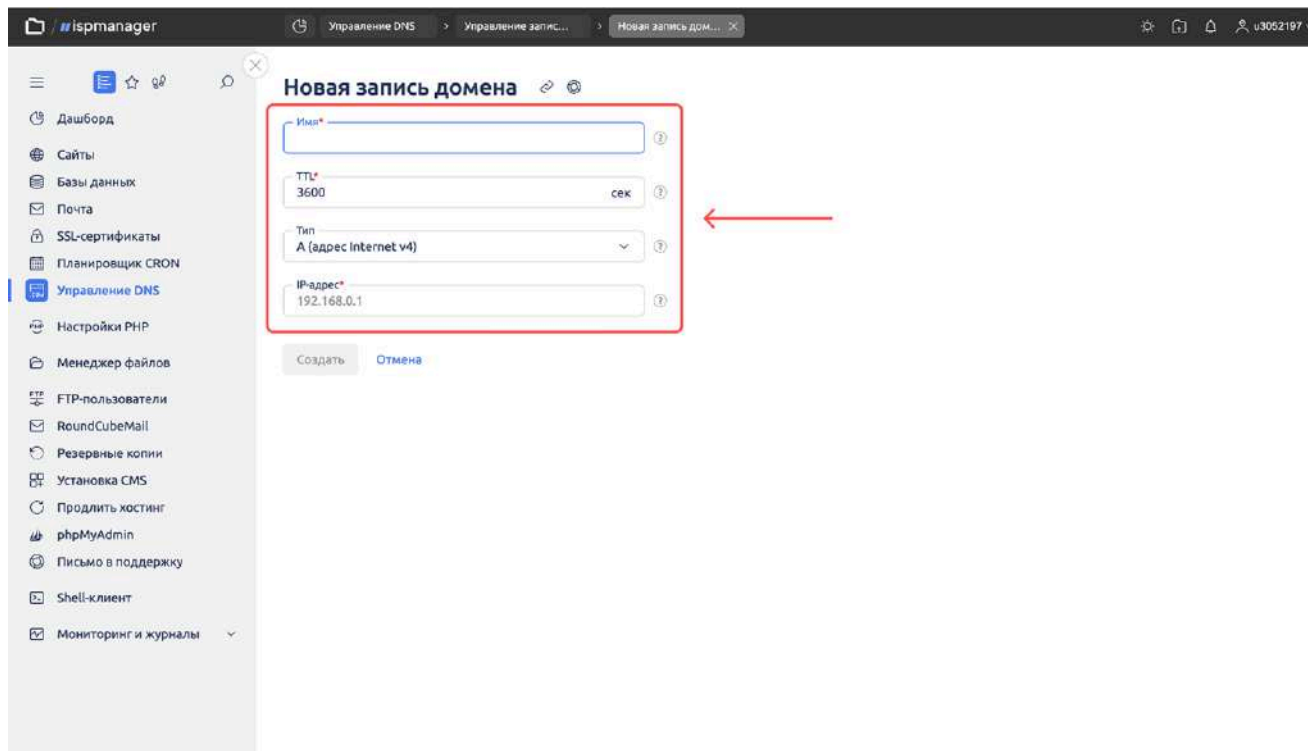
Откроется новая вкладка в браузере. В меню слева выберите "Управление DNS". Откроется страница со списком существующих доменов.



Кликните на название нужного домена, чтобы открыть страницу со списком существующих DNS-записей. Нажмите "Создать запись".



Вы увидите поля, которые нужно заполнить для создания новой записи.



Добавление TXT-записи

Введите следующие значения в поля:

- В поле "Имя" введите название вашего домена
- В поле "TTL" введите время в секундах. Это время, в течение которого DNS-записи хранятся в кэше на серверах и клиентских устройствах. Чтобы TXT-запись при настройке защиты Solar Space обновилась быстрее, рекомендуем установить в этом поле значение "300". Подробнее про TTL и выбор его оптимального значения, читайте [здесь](#).
- В поле "Тип" выберите тип DNS-TXT-записи "TXT (текстовая запись)"
- В поле "Значение" вставьте скопированную DNS-TXT-запись из личного кабинета Solar Space

Нажмите "Создать"

Новая запись домена

Имя*
domain.ru

TTL*
300 сек

Тип
TXT (текстовая запись)

Значение*

Создать Отмена

Если вы добавляете только TXT-запись, вернитесь в личный кабинет и нажмите "Верифицировать".

Верификация

Добавьте DNS-TXT запись для основного домена и его зеркал в вашем хостинг-провайдере.

DNS-TXT

Скопируйте запись из поля выше и добавьте ее на сайте своего хостинг-провайдера

Узнать больше

Домены ресурса

Неподтвержденные **Все**

☒ domain.ru

Верифицировать Отменить

Если вы добавляете сразу A-запись, следуйте следующему пункту.

Добавление А-записи

- В поле "Имя" — введите имя вашего домена
- В поле "TTL" — введите время в секундах. Это время, в течение которого DNS-записи хранятся в кэше на серверах и клиентских устройствах. Чтобы TXT-запись при настройке защиты Solar Space обновилась быстрее, рекомендуем установить в этом поле значение "300". Подробнее про TTL и выбор его оптимального значения, читайте [здесь](#).
- В поле "Тип" — выберите тип DNS-А-записи "A (адрес Internet v4)"
- В поле "IP-адрес" — вставьте скопированный IP-адрес из личного кабинета Solar Space

Нажмите "Создать".

Новая запись домена

Имя*
domain.ru

TTL*
300 сек

Тип
A (адрес Internet v4)

IP-адрес*
192.168.0.1

Создать Отмена

Все остальные А-записи и AAAA-записи из этой таблицы необходимо удалить. Это нужно для того, чтобы весь входящий трафик перенаправлялся на сервер защиты для анализа и фильтрации.

Далее перейдите в личный кабинет Solar Space и нажмите "Подтвердить".

Все 10 A 1 AAAA 0 CNAME 0 NS 5 MX 3 SRV 0 PTR 0 TXT 1 DNAME 0 HINFO 0 NAPTR 0 RP 0 CAA 0

+ Добавить новую запись

Хост	Тип	Значение	TTL	Дата	+ фильтр	
domain.com	TXT	sc-domain-verification=abe8509d04565c3f731482c142fcd00955b59f7bdade768125f03388b6cd0833	600	2025-04-21 16:22:56		
@	NS	ns8-l2.nic.ru.		2025-03-11 11:08:36		
@	NS	ns8-cloud.nic.ru.		2025-03-11 11:08:36		
@	NS	ns4-l2.nic.ru.		2025-03-11 11:08:36		
@	NS	ns4-cloud.nic.ru.		2025-03-11 11:08:36		
@	NS	ns3-l2.nic.ru.		2025-03-11 11:08:36		
domain.com	A	93.185.164.10		2025-04-21 16:22:50		
@	MX	5 MX02.NICMAIL.RU.		2025-04-21 13:23:35		
@	MX	20 MX03.NICMAIL.RU.		2025-04-21 13:24:01		
@	MX	10 MX01.NICMAIL.RU.		2025-04-21 13:23:49		

Почему может сработать капча или антибот

В этой статье разберем причины, из-за которых может сработать антибот:

- некоторые антивирусы
- использование некоторых видов VPN и прокси
- специфические или устаревшие браузеры
- отсутствие fingerprint'a
- подозрительное поведение
- сомнительная сетевая активность
- технические признаки автоматизации

Некоторые антивирусы

Это одна из самых частых причин ложного срабатывания антибота. При HTTPS-соединении браузер пользователя отправляет серверу сайта список поддерживаемых алгоритмов шифрования, и тот выбирает один для обмена данными.

Антивирус «встает» между браузером и сайтом, разрывая соединение. Когда браузер отправляет серверу зашифрованные данные, антивирус перехватывает их, шифрует по-своему и направляет дальше в сторону сайта.

Если сайт использует антибот-систему, она ожидает запрос с определенным алгоритмом. Получая другой, антибот показывает капчу. Реальный пользователь проходит ее и попадает на сайт.

Если сотрудники вашей компании не могут получить доступ к вашему сайту из-за установленных на корпоративных устройствах антивирусов, системные администраторы могут внести сайт в список доверенных веб-ресурсов, то есть в список исключений. Антивирус не будет перехватывать и заново шифровать такие запросы.

Инструкции обычно есть на сайте поставщиков антивирусов, например:

- [Инструкция Kaspersky](#)
- [Инструкция Dr.Web](#)

Использование некоторых видов VPN и прокси

Причина — та же, что описана выше для антивируса. Некоторые сервисы VPN и прокси-серверы аналогичным образом переупаковывают трафик, из-за чего антибот-система может показать капчу даже если запрос идет от реального пользователя.

Специфические или устаревшие браузеры

Если пользователь пытается зайти на сайт с анонимных браузеров, он тоже увидит капчу. Эти браузеры используют прокси и собственное шифрование.

Капчу придется пройти и пользователям, которые заходят на защищаемый сайт со специфических, редко встречающихся или устаревших браузеров. Часто они используются операционной системой по умолчанию.

Отсутствие или несовпадение fingerprint'a

Fingerprint — это уникальный набор данных об устройстве или браузере пользователя, который позволяет сайтам и сервисам однозначно идентифицировать его среди других.

Антибот срабатывает, если фиксирует отсутствие fingerprint'a или видит несостыковки: например, IP-адрес пользователя соответствует одной стране, а настройки языка или часового пояса в его браузере — другой.

Подозрительное поведение

Антибот выявляет поведенческие паттерны и реагирует на те, которые характерны для ботов:

- множество быстрых запросов за короткое время (rate limit exceeded)
- отсутствие движений мыши, скrolла и кликов
- слишком быстрое перемещение по страницам и короткое время просмотра
- попытки обхода JavaScript-проверки (браузер не проходит ее или в нем отключена возможность такой проверки)

Сомнительная сетевая активность

Антибот анализирует IP-адреса и блокирует при следующих признаках:

- IP-адрес из “грязных” диапазонов, которые попали в черные списки (blacklists) из-за подозрительной или вредоносной активности
- IP-адрес уже был “замечен” за атакой или сканированием сайтов на уязвимости

- IP-адрес ранее не попадал в поле зрения системы, но сразу начинает агрессивную активность

Технические признаки автоматизации

Есть ряд параметров, которые с большой долей вероятности характеризуют ботовый трафик:

- запросы без HTTP-заголовков, характерных для реальных пользователей (Referer, Accept-Language, Origin и другие)
- отсутствие cookies или ошибки в них — боты в отличие от человека не получают и не хранят cookies
- нетипичный порядок загрузки элементов страницы — пользователи сначала загружают HTML, потом JS и CSS, а бот может напрямую скачивать API

Как подобрать параметры тарифа веб-защиты

Ежемесячный платеж за веб-защиту одного домена второго уровня определяется двумя факторами:

1. Уровнем защиты:

- базовый — WEB AntiDDoS,
- оптимальный — WEB AntiDDoS + WEB Antibot,
- продвинутый — WEB AntiDDoS + WEB Antibot + WAF Lite.

2. Параметрами тарифа:

- для базового или оптимального уровней защиты — шириной канала,
- для продвинутого уровня защиты — шириной канала и запросами в секунду (RPS).

Уровень защиты вы определяете исходя из нужного вам набора сервисов, а как выбрать ширину канала и запросы в секунду, расскажем в этой статье.

Как выбрать ширину канала

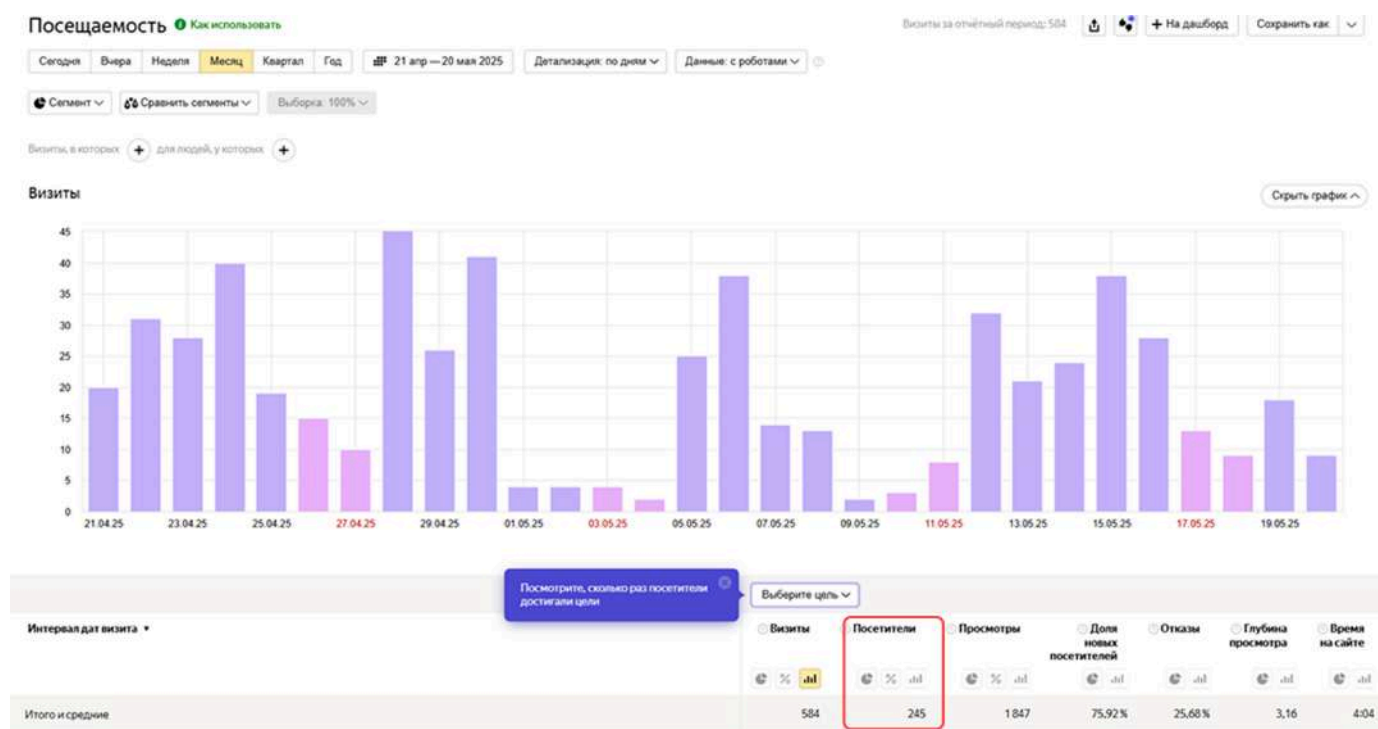
Ширина канала — это объем очищенного трафика без учета трафика атак. Вы платите только за трафик, который попадает на ваш сайт после того, как наш сервер защиты отбросил паразитные и подозрительные запросы. Ширина канала соотносится с количеством посетителей сайта.

Ширина канала (Мбит/с)	Посетителей в месяц (примерно)
1	до 5000
5	до 25 000
10	до 50 000
30	до 150 000
50	до 250 000
100	до 500 000

❗ Это ориентировочные данные, так как ширина канала зависит также от типа сайта: визитка, интернет-магазин, сайт с видеотрансляциями и т. д. Небольшим сайтам-визиткам обычно хватает минимальных тарифов (1 или 5 Мбит/с). Интернет-магазинам, особенно в период распродаж или других повышенных нагрузок, стоит выбирать более емкие тарифы.

Где посмотреть количество посетителей на вашем сайте

Среднее ежемесячное количество посетителей на вашем сайте можно посмотреть в Яндекс.Метрике в разделе Отчеты → Аудитория → Посещаемость.



Как выбрать RPS — запросы к сайту в секунду

RPS — количество запросов к вашему сайту за 1 секунду. Этот параметр используется для расчета тарифа только при продвинутом уровне защиты. Один пользователь может отправить несколько обращений в секунду: например, загрузка страницы предполагает запросы HTML, API, изображений и других.

Где посмотреть RPS вашего сайта

Определить примерное количество запросов на ваш сайт можно несколькими способами:

1. Обратиться к администратору ресурса.

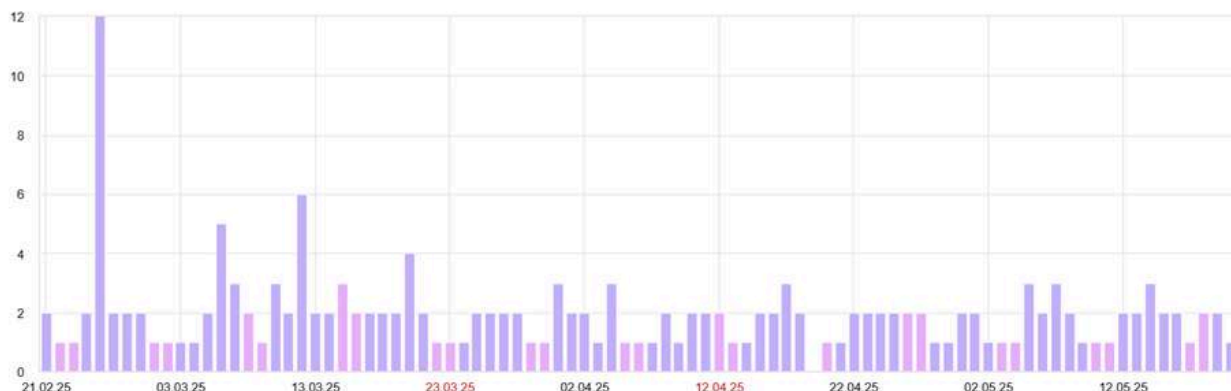
2. Посмотреть в Яндекс.Метрике: раздел Отчеты → Мониторинг → Нагрузка на сайт.

Нагрузка на сайт Как использовать

Сегодня Вчера Неделя Месяц **Квартал** Год 21 фев — 20 мая 2025 Детализация: по дням

Запросы в секунду (максимум)

Скрыть график ^



ⓘ Запросы в секунду — это динамический показатель, и данные в Яндекс.Метрике за разный период будут различаться. Рекомендуем формировать отчет за квартал и смотреть среднее значение.

3. Рассчитать самостоятельно: взять 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 — Яндекс.Метрике и других.

Например, 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 в поле 5 RPS.

Что такое превышение по тарифу и почему оно может произойти

Когда вы только начинаете пользоваться веб-защитой, может быть сложно определить ширину канала или RPS. Это похоже на подключение тарифа мобильной связи: вы сначала не знаете, сколько гигабайт интернета в месяц расходуете, и выбираете ориентировочно. Спустя несколько месяцев понимаете, хватает ли вам гигабайтов, заложенных в тариф, или нужно его сменить.

С выбором шириной канала или RPS может быть аналогичная ситуация. Допустим, вы подключили оптимальный уровень защиты с шириной канала 5 RPS. Через 30 дней после окончания расчетного периода вам на почту приходит уведомление о том, что выявлено

превышение параметров, которое нужно оплатить сверх фиксированной ежемесячной суммы. Как мы рассчитываем оплату за тарифицируемый трафик и превышение, описано [здесь](#).

Такие ситуации происходят крайне редко, но они возможны. Советуем понаблюдать за трафиком в течение 2-3 месяцев: если вам ежемесячно приходит счет за превышение, стоит сменить тариф. Если превышение было зафиксировано разово, проанализируйте причины: возможно, вы запускали рекламную кампанию для привлечения новых пользователей на сайт, из-за чего и был превышен лимит.

Куда обратиться за помощью в подборе тарифа

Если при подключении веб-защиты вам сложно выбрать параметры тарифа самостоятельно, воспользуйтесь демотарифом:

- Отправьте запрос на подключение демотарифа письмом на почту solar@rt-solar.ru. Укажите в нем, какие сервисы вас интересуют.
- Пользуйтесь сервисами 14 дней бесплатно.
- По итогам тестового периода специалисты подберут для вашего сайта тариф с оптимальными параметрами ширины канала и RPS.