

# DNSSEC. Подключение

## DNSSEC в DNSmanager

### DNSSEC

DNSSEC — расширение DNS, которое проверяет подлинность ответа от DNS-сервера, то есть защищает от подмены IP-адресов. Это позволяет защитить ваш сайт от кибератак (загрязнения кеша DNS-серверов, перенаправления или подмены DNS-запросов).

DNSSEC не может обеспечить тотальную защиту вашего сайта. Он:

НЕ защищает от DDoS-атак;

НЕ гарантирует конфиденциальность обмена данными;

НЕ шифрует информацию веб-сайтов.

Чтобы никто не смог взломать ваш сайт, используйте DNSSEC в комплекте с SSL-шифрованием, защитой от DDoS-атак и двухступенчатой аутентификацией.

## DNSSEC

DNSSEC — расширение DNS, которое проверяет подлинность ответа от DNS-сервера, то есть защищает от подмены IP-адресов. Это позволяет защитить ваш сайт от кибератак (загрязнения кеша DNS-серверов, перенаправления или подмены DNS-запросов).

DNSSEC не может обеспечить тотальную защиту вашего сайта. Он:

- НЕ защищает от DDoS-атак;
- НЕ гарантирует конфиденциальность обмена данными;
- НЕ шифрует информацию веб-сайтов.

Чтобы никто не смог взломать ваш сайт, используйте DNSSEC в комплекте с SSL-шифрованием, защитой от DDoS-атак и двухступенчатой аутентификацией.

### Как работает DNSSEC

В системе DNS долгое время не было механизмов защиты от подмены информации. Это значит, что операция обмена данными между клиентом (резолвером) и сервером провайдера не была застрахована от вторжения «третьей стороны» (злоумышленника). Он перехватывает запрос резолвера, возвращает ему произвольный IP-адрес вместо запрашиваемого. Также атака переходит и на серверы провайдера: их кеш заполняется ложными данными.

Протокол DNSSEC исключает из цепи возможного злоумышленника. Если ответ на запрос резолвера проходит проверку на авторитетность, то «кража» и «подмена» будут обнаружены и предотвращены сразу.

DNSSEC работает по тому же принципу, что и цифровая подпись. С помощью ключей асимметричного шифрования обеспечивается сохранность, аутентичность и безопасность передачи ресурсных записей доменных зон по DNS-запросам.

Ключ состоит из 2 частей:

- **Секретная часть** известна только владельцу ключа и хранится в безопасном месте. Используется для генерирования электронной подписи.
- **Публичная часть** может быть опубликована и доступна для проверки подписей, осуществленных секретной частью ключа. Открытая часть ключа подписи вычисляется, как значение некоторой функции от закрытой части ключа, но знание открытой части ключа не даёт возможности определить закрытый ключ.

В работе DNSSEC используется 2 типа ключей:

1. **ZSK** — ключ подписывания **зон**. Используется для подписывания наборов ресурсных записей доменной зоны. Обычно есть один ключ, которым подписываются данные зоны, но допускается и несколько ключей. Например, могут быть ключи для каждого из разных алгоритмов цифровой подписи. Важной концепцией DNSSEC является то, что ключ, которым подписаны данные зоны, ассоциирован с самой зоной, а не с ответственным сервером имён зоны.
2. **KSK** — ключ подписывания **ключей**. Используется для подписывания ключей ZSK. Он также связывает цепочкой доверия вашу и родительскую доменные зоны.

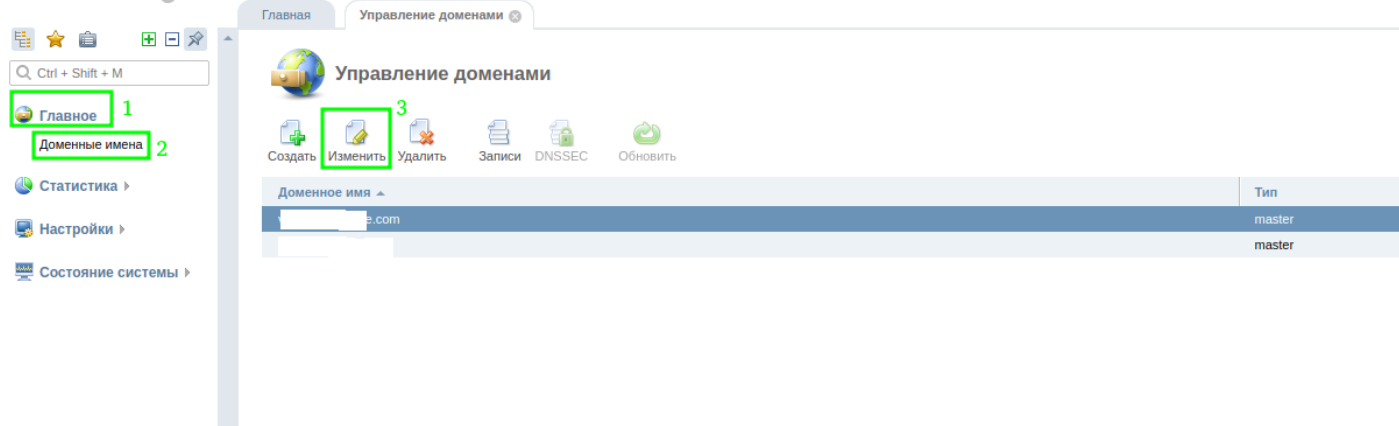
Для безопасности рекомендуется обновлять ключи со следующей периодичностью:

- **ZSK** — каждые 2-3 месяца;
- **KSK** — раз в 6 месяцев.

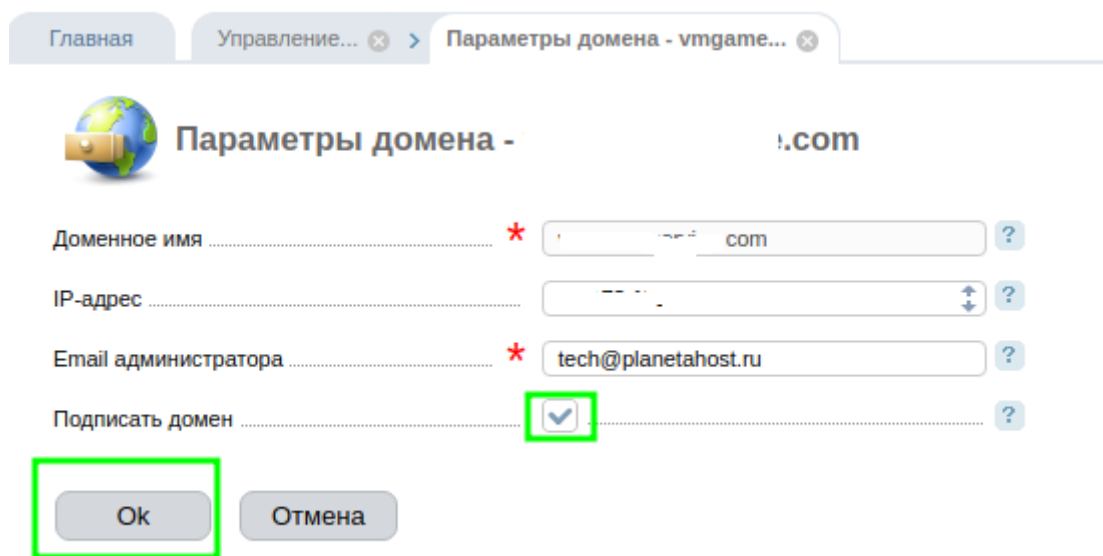
## Как подключить DNSSEC в DNSmanager

Для начала зайдите в DNSmanager.

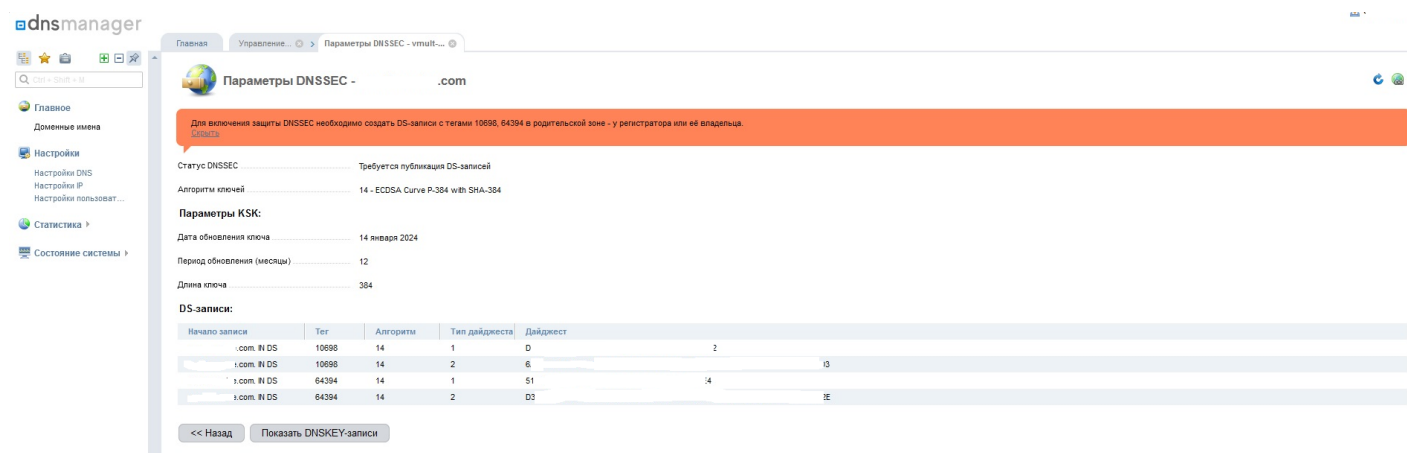
Слева в меню выберите "Главное" - "Доменные имена". Затем выберите доменное имя и нажмите на кнопку "Изменить"



Затем поставьте галочку напротив "подписать домен" и нажмите "OK"



После этого Вам нужно будет добавить DS-записи. Скорее всего у Вас появится уведомление, как в этом случае:



Для включения защиты DNSSEC Вам необходимо добавить DS-записи. Сделать это нужно у регистратора доменного имени.

[Подключение DNSSEC в reg.ru](#)

[Подключение DNSSEC в ru-center](#)

После того, как записи будут добавлены, после обновления DNS защита DNSSEC будет подключена.

Если у Вас возникли вопросы/трудности, напишите нам в поддержку. Мы поможем решить вопрос.

[Как написать запрос в поддержку](#)

---

Версия #1

Кирилл создал 11 октября 2023 09:15:57

Кирилл обновил 12 октября 2023 10:43:16