Переход с HTTP на HTTPS

С недавнего времени поисковые системы стали отдавать предпочтения сайтам, использующим защищенный протокол https. Поэтому, оценивая большие возможности появления нового фактора ранжирования по протоколу, необходимо перевести сайт на защищенную версию.

Справка Google относительно использования https версии:
https://support.google.com/webmasters/answer/6073543?hl=ru

Оглавление

Далее пошагово описан процесс перехода.

1. Смена ссылок внутренней перелинковки с абсолютных на относительные

Для того чтобы начать переход на HTTPS, еще перед сменой протокола рекомендуем абсолютные внутренние ссылки на сайте заменить на относительные.
Например, http://domain.com/landing/ заменить на //domain.com/landing/ или на формат URI /landing/

1.1. Исправление вложений медиа-контента

Изображения, видео, презентации, и др. необходимо тоже все перевести в относительные адреса, и тогда при переходе на HTTPS медиа-контент также должен подгружаться с защищенных сайтов:

- Если используемые картинки хранятся на нашем сайте, то просто используйте относительные адреса.
- Если подгружаются картинки с внешних ресурсов (CDN или других сайтов), то они также должны поддерживать HTTPS, иначе стоит отказаться от этих вложений.

Популярные сервисы, которые позволяют внедрять свой контент, типа YouTube, SlideShare, виджеты VK или Facebook, и другие, уже давно поддерживают HTTPS, поэтому с ними проблем не возникнет.

Но если есть медиа-контент с непопулярных сервисов, то уточните, будет ли этот контент работать/отображаться, если вы смените протокол.

1.2. Исправление подключений внешних скриптов

Необходимо во внешних скриптах также нужно использовать относительные URL. Например, для библиотеки jQuery, вместо кода:

```
<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"></script>
```

Нужно использовать:

```
<script src="//ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"></script>
```

Также и с другими скриптами: Яндекс.Метрика, LiveInternet, Google Analytics, Яндекс.Директ, различные javascript библиотеки и др. Здесь принцип тот же: популярные сервисы и библиотеки поддержкивают HTTPS, а вот с непопулярными могут возникнуть проблемы.

Важно: Также следует изменить URL в атрибутах

- rel=”canonical”;
- link rel="alternate" hreflang (при наличии нескольких языковых версий);
- rel="next" и rel="prev" (на страницах пагинации).

2. Выбор и приобретение подходящего SSL-сертификата

Существует несколько видов SSL-сертификатов по степени защиты:

- **Organization Validation**. Подтверждает домен и организацию. Могут проверить информацию в прессе, наличие компании в Whois, свидетельство о государственной регистрации. Средняя цена колеблется от $40 до $200 в год.
- **Extended Validation**. Сертификат с расширенной проверкой — для его получения проверяется наличие компании по адресу, свидетельство о регистрации, операционная деятельность, торговая марка. Все для того, чтобы получить зеленую строку в адресной строке браузера. Стоимость в среднем от $120 до $300 в год.

Существует и классификация сертификатов по функциональности:

- обычные SSL-сертификаты;
- Wildcard сертификаты — используйте, если хотите установить HTTPS на поддоменах;
- SAN сертификаты — используется для нескольких доменов.

Нам нужен обычный SSL-сертификат, Domain Validation. После установки сайт должен стать доступен как по http, так и по https.

Важно: после получения сертификата и переходе на https необходимо сообщить SEO

специалисту, чтобы он в “инструменте для вебмастеров” указал нужный домен.

3. **Установка сертификата на сервере**

После выбора сертификата необходимо установить его на сервере:

✓ Сервер должен поддерживать SSL-протокол.

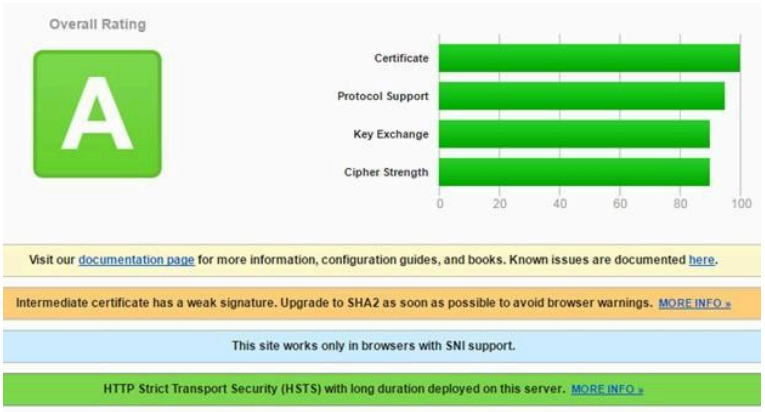
✓ Установка выполняется через панель управления хостингом

4. **Проверка корректности работы сертификата**

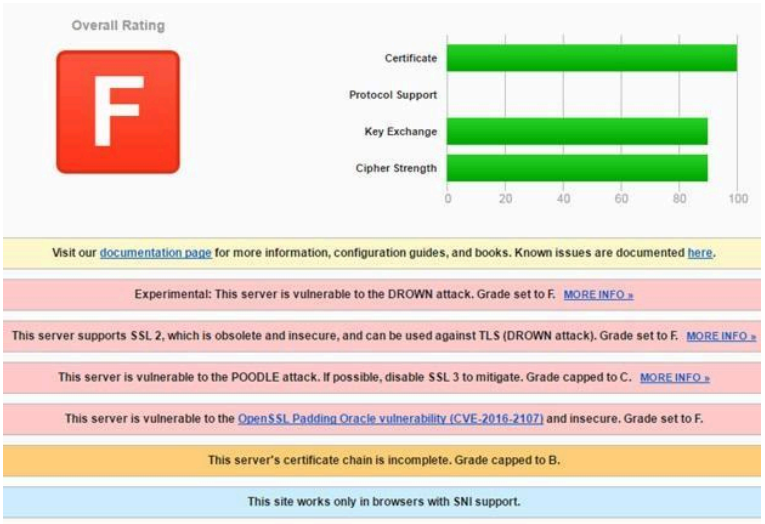
- Убедитесь, что SSL-сертификат настроен корректно. Сделать подробный анализ конфигурации SSL можно с помощью сервиса

https://www.ssllabs.com/ssltest/analyze.html

Вот так будет выглядеть результат, если все хорошо:



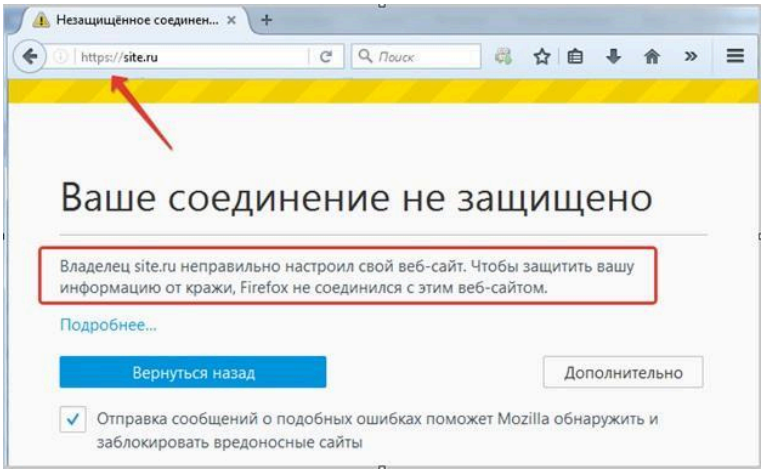
и так, если есть проблема:



В данном случае есть проблемы с настройкой сертификата и сайт не открывается в браузере Firefox.

Обязательно протестируйте настройку SSL и проверьте как отображается сайт в разных браузерах, в том числе на мобильных устройствах: отдельно проверьте сайт с iPhone и

Android.



Если есть критичные проблемы, необходимо провести настройки по их решению.

5. **Настройка robots.txt и XML-карты сайта**

Необходимо создать карту сайта со ссылками на https-версии страниц сайта, и обеспечить ее доступность по ссылке https://domain.com/sitemap.xml
Т.е. ресурс должен содержать 2 файла sitemap.xml со ссылками двух протоколов.

Также нужно обеспечить доступность файла robots.txt по двум протоколам и привести к следующему виду:

Для версии http:	**и для версии https:**
User-Agent: * Disallow: … Sitemap: http://domain.com/sitemap.xml User-Agent: Yandex Disallow: … Sitemap: http://domain.com/sitemap.xml Host: https://domain.com/	User-Agent: * Disallow: … Sitemap: https://domain.com/sitemap.xml User-Agent: Yandex Disallow: … Sitemap: https://domain.com/sitemap.xml Host: https://domain.com/

6. **Настройка редиректов**

После выполнения всех выше указанных пунктов необходимо настроить постраничный 301 редирект с HTTP версии сайта на HTTPS.

При этом файлы robots.txt и sitemap.xml сайта должны быть доступны и по http, и по https протоколу. Для этого необходимо указать исключение в файле htacess при настройке редиректов.