ИПМ им.М.В.Келдыша РАН

Абрау-2017 • Труды конференции

Ф.О. Каспаринский

Адаптация интернет-сайтов к работе в безопасном режиме информационного обмена (HTTPS)

Рекомендуемая форма библиографической ссылки

Каспаринский Ф.О. Адаптация интернет-сайтов к работе в безопасном режиме информационного обмена (HTTPS) // Научный сервис в сети Интернет: труды XIX Всероссийской научной конференции (18-23 сентября 2017 г., г. Новороссийск). — М.: ИПМ им. М.В.Келдыша, 2017. — С. 235-242. — URL: http://keldysh.ru/abrau/2017/30.pdf doi:10.20948/abrau-2017-30

Размещена также презентация к докладу

Адаптация интернет-сайтов к работе в безопасном режиме информационного обмена (HTTPS)

Ф.О. Каспаринский[1,2]

[1] *Биологический факультет Московского государственного университета имени М.В.Ломоносова*
[2] *ООО «МАСТЕР-МУЛЬТИМЕДИА»*

Аннотация. В 2017 году по инициативе Google в практику использования сети Интернет введены новые правила селекции поисковой выдачи и репутационной маркировки сайтов, дискредитирующие сайты без SSL-сертификатов, которые позволяют передавать данные по безопасному протоколу HTTPS. Переход сайта к работе по HTTPS требует не только подключения квалифицированного SSL-сертификата, но и адаптации компонентов, связанных с распределёнными небезопасными медиаресурсами, поскольку подозрительный функционал блокируется, а репутации сайта наносится ущерб в результате получения метки «Ненадёжный».

Ключевые слова: Интернет, сайт, HTTPS, SSL, TLS, безопасность, репутация, адаптация, ранжирование, маркировка

Завершающий квартал 2016 года ознаменовался началом массированной агитационной деятельности со стороны компании *Google*, целью которой было убеждение интернет-сообщества в необходимости тотального перевода интернет-сайтов с обычного *HTTP*-режима в защищенный *HTTPS*-режим с начала 2017 года. В качестве главных идеологически привлекательных аргументов приводились: необходимость противодействия кибертерроризму, радение о защите персональных данных, обеспечение безопасности финансовых операций, а также забота о репутации интернет-представительств физических и юридических лиц. Для стимуляции заблаговременного приобретения владельцами сайтов *SSL*-сертификатов, необходимых для функционирования в *HTTPS*-режиме, был анонсирован список санкций в отношении сайтов, продолжающих работу в *HTTP*-режиме: отвращение пользователей от просмотра небезопасных сайтов посредством демонстрации устрашающих репутационных меток адресной строки браузера («Не защищено», «Опасно» и др.) и умышленное понижение в ранжировании поисковой выдачи.

В течение первых двух месяцев массового перевода сайтов в режим безопасного инфообмена обнаружилось, что подключение *SSL*-сертификата нарушает работу неадаптированных динамических сайтов. Это привело к

закономерному появлению коммерческих предложений с вариантами помощи при переходе к *HTTPS*-режиму. Идеологи массовой интродукции *SSL*-сертификатов и услуг по их подключению через полгода установили, что большинство пользователей игнорирует репутационные метки, а наличие безопасного режима передачи данных не оказывает заметного влияния на ранжирование поисковой выдачи.

1. Особенности и назначение *HTTPS*-протокола передачи данных

Прикладной протокол передачи гипертекста *HTTP* (*HyperText Transfer Protocol*) между клиентами (пользователями) и поставщиками (интернет-серверами) был создан в 1992 году [1] и до настоящего времени широко используется в глобальной сети Интернет наряду с протоколами иного назначения (*FTP, SMTP*). Особенностью протокола *HTTP* является возможность указать в запросе и ответе альтернативные способы представления в браузере пользователя одного и того же веб-ресурса (хранящегося на сервере файла) по различным параметрам: формату, кодировке, языку и т. д. Протокол *HTTP* может использоваться также в качестве «транспорта» для других протоколов прикладного уровня, таких как *SOAP, XML-RPC, WebDAV*.

В 2000 году в связи с возникновением потребности обеспечения безопасной передачи информации для электронной коммерции появился расширенный вариант протокола *HTTP* с модифицированным названием *HTTPS* (*HyperText Transfer Protocol Secure* [2]), который поддерживает шифрование данных посредством их шифрованной передачи поверх криптографических протоколов *SSL* [3] или *TLS* [4].

2. Криптографические протоколы *SSL* и *TLS*

В 1995 году компания *Netscape Communications* разработала криптографический протокол *SSL* (*Secure Sockets Layer*) для использования в своём передовом браузере *Netscape Navigator* который использовался с 1994 по 2007 год. К настоящему времени протокол *SSL* широко применяется для обмена мгновенными сообщениями, передачи аудиовизуальных и платежных данных, пересылки электронной почты и интернет-факсов благодаря своей возможности создавать между пользователем и сервером безопасный частный канал обмена данными, который использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности и коды аутентификации сообщений для проверки их целостности [3]. Более безопасным протоколом обмена данными является *TLS* (*Transport Layer Security*), предотвращающий прослушивание пакетов данных и осуществление несанкционированного доступа к ним [4].

В 2014 году вследствие обнаруженной неустранимой уязвимости протокола *SSL* [3] началась постепенная адаптация интернет-среды к тотальному переходу на применение *TLS*-протокола при обеспечении

HTTPS-режима обмена данными. Внедрение более безопасного и прогрессивного протокола *TLS* в широкую практику затрудняется наличием дополнительных требований к программному и аппаратному обеспечению.

Для использования *SSL* и *TLS* протоколов требуется наличие цифрового сертификата на стороне сервера (см. раздел 3), что предоставляет Удостоверяющим центрам и их реселлерам возможность заработка от продажи сертификатов, не требующего значительных капиталовложений. Тактически объяснимое, но стратегически контрпродуктивное желание коммерческих структур получить максимальную прибыль от реализации морально устаревшего продукта привело к началу пропагандистской кампании популяризации использования *SSL*-протокола наряду с замалчиванием необходимости его замены на *TLS*-протокол для обеспечения реальной безопасности. Подобная история произошла в 2003 году, когда морально устаревший стандарт представления аудиовизуальных данных *MPEG2* был навязан пользовательскому рынку в форме *DVD*, что на десятилетие затормозило развитие интерактивного сетевого потокового видео, основанного на прогрессивном стандарте *MPEG4* 1998 года выпуска [5].

3. *SSL* и *TLS*-сертификаты

Для подготовки веб-сервера к обработке *HTTPS*-соединений администратор должен получить и установить в систему сертификат открытого ключа для этого веб-сервера [2]. В протоколе *TLS* используется как асимметричная схема шифрования (для выработки общего секретного ключа), так и симметричная (для обмена данными, зашифрованными общим ключом). Сертификат открытого ключа подтверждает принадлежность данного открытого ключа владельцу сайта. Сертификат открытого ключа и сам открытый ключ посылаются клиенту при установлении соединения, а закрытый ключ используется для расшифровки сообщений от клиента.

Цифровой сертификат представляет собой файл небольшого размера (1.5-2 Кб) с расширением **.crt*, содержащий непрерывную буквенно-знаково-цифровую текстовую последовательность между условными обозначениями «-----BEGIN CERTIFICATE-----» и «-----END CERTIFICATE-----». Существует возможность создать сертификат открытого ключа, не обращаясь в Удостоверяющий центр сертификации посредством самоподписывания сертификата (*self-signed*) и использовать его для формального применения *HTTPS*режима обмена данными между пользователями, подтвердившими в браузере своё согласие на осуществление потенциально небезопасного соединения [6]. Самоподписанные сертификаты отвергаются при подключении к платежным системам. Для получения доверенного сертификата требуется обращение в удостоверяющий центр, имеющий официальные права на выпуск и юридическое сопровождение *SSL*-сертификатов. Цена сертификатов ($10-$200 в год) зависит от распространения защиты на один домен или поддомен,

на все поддомены определённого домена, на несколько доменов и отображения названия компании-владельца сайта в адресной строке браузера посетителя [7].

4. Выпуск и подключение *SSL*-сертификата к домену

Трехлетний опыт использования различных *SSL*-сертификатов на доменах проекта МАСТЕР-МУЛЬТИМЕДИА позволяет сделать вывод, что штатная процедура получения доверенного сертификата в отсутствие культивируемого ажиотажного спроса состоит из 5 частей: 1) проверки данных владельца домена; 2) генерации запроса на получение сертификата и формирования приватного ключа; 3) подключения закрытого ключа, основного и промежуточного сертификатов к домену на веб-сервере; 4) переключения режима доступа к домену по умолчанию; 5) проверки работоспособности компонентов сайта. Солидные Удостоверяющие центры предоставляют для размещения на сайте кода «Печати доверия» (*Trusted Seal*), необходимую для убеждения пользователей в безопасности совершаемых на сайте действий.

Для выпуска сертификатов, удостоверяющих домен и его владельца (сертификаты категории *OV*), а также для сертификатов с расширенной проверкой и отображением названия компании в адресной строке браузера (сертификаты категории *EV*), требуется предоставить Удостоверяющему центру цифровую копию Свидетельства о регистрации юридического лица в форматах *jpg*, *png*, *gif* или *pdf*. Удостоверяющий центр вправе затребовать дополнительные данные (сведения о программном обеспечении сервера), если предоставленной информации не будет достаточно для проведения полноценной проверки. Одним из этапов проверки данных об организации-заказчике сертификата является поиск ее контактных данных (адреса местонахождения, корпоративного телефонного номера, адреса электронной почты) в открытых источниках (*WhoIs.com* и др.).

Запрос на получение сертификата (*CSR, Certificate Signing Request*) представляет собой файл небольшого размера (1.5-2 Кб) с расширением **.csr*, содержащий непрерывную буквенно-знаково-цифровую текстовую последовательность между условными обозначениями «-----BEGIN CERTIFICATE REQUEST-----» и «-----END CERTIFICATE REQUEST-----» содержащий в закодированном виде информацию об администраторе домена и открытый ключ. *CSR* генерируется с использованием закрытого ключа на стороне сервера, где будет устанавливаться сертификат. Закрытый ключ обычно создается непосредственно перед генерацией *CSR* и представляет собой файл длиной не менее 2048 *bit* с расширением **.key*, содержащий непрерывную буквенно-знаково-цифровую текстовую последовательность между условными обозначениями «-----BEGIN RSA PRIVATE KEY-----» и «-----END RSA PRIVATE KEY-----». Для генерации *CSR* в соответствии с данными, указанным в *WhoIs*-сервисе по домену, необходимо заполнить латинскими символами следующие поля: Имя сервера (*Common Name*) — полностью определенное доменное имя, например, «*www.master-multimedia.ru*»; Название страны

(*Country Name*) — двухбуквенный код страны, для РФ — «*RU*»; Область (*State or Province Name*) — регион, например, «*Moscow*»; Город или населенный пункт (*Locality Name*); Название организации или ФИО физического лица (*Organization Name*). При заказе сертификата категории *DV* (с проверкой владения доменом) в поле «*Organisation Name*» должны быть указаны данные, аналогичные тем, которые указаны в поле «Администратор домена» в сервисе *Whois*. При заказе сертификатов категорий *OV* и *EV*: в поле «*Organisation name*» необходимо указать название организации, на имя которой выпускается сертификат, так же как оно указано в Свидетельстве о регистрации юридического лица. При этом нельзя писать название организации в *CSR* в кавычках. По мере развития ажиотажного спроса на *SSL*-сертификаты при хостингах и у реселлеров сертификатов появились сервисы автоматической генерации *CSR*.

В зависимости от типа сертификата основной сертификат может быть дополнен цепочной нескольких промежуточных сертификатов, при подключении которых к домену вместе с закрытым ключом важно соблюдать определенную Удостоверяющим центром последовательность. Для определения корректности подключения цепочки сертификатов к домену Удостоверяющие центры предоставляют специальные сервисы, тестирующие безопасность передачи данных домена в *HTTPS*-режиме. До начала ажиотажа с подключением *SSL*-сертификатов к доменам большинство хостингов предоставляло возможность использования *SSL*-сертификата только на одном из доменов каждого аккаунта. С ноября 2016 года это ограничение было снято на отечественном хостинге «Джино» [8]. В конце апреля 2017 года хостинг «Джино» анонсировал автоматическое создание, подключение и продление бесплатных *SSL*-сертификатов от удостоверяющего центра *Let's Encrypt* для любого количества доменов одного аккаунта [9].

После подключения сертификатов безопасности в файле *robots.txt* следует установить директиву *Host* на протокол *HTTPS* и соответствующим образом изменить ссылки в файле *sitemap.xml*. Для настройки автоматического перенаправления запросов к сайту с *HTTP* на *HTTPS* (301 редирект) следует добавить в файл *.htaccess* в папке нужного домена следующие строки:

RewriteEngine On # Если этой строки нет
RewriteCond %{HTTP:X-Forwarded-Protocol} !=https
RewriteRule . https://%{SERVER_NAME}%{REQUEST_URI} [R=301,L]*

Без настройки вышеуказанного перенаправления сайт может использовать любой протокол передачи данных по явному выбору пользователя или посредством целенаправленной модификации гиперссылок на страницы сайта. Эта возможность позволяет использовать *HTTPS*-протокол только в определенных случаях (при платежных операциях и работе с персональными данными), а при обращении к сторонним ресурсам применять незащищённую передачу данных в *HTTP* режиме.

5. Последствия перевода сайта в *HTTPS*-режим передачи данных

После успешного подключения *SSL*-сертификата к домену оказывается возможным использование на сайте модулей платежных систем и обработка персональных данных без нарушения 152-ФЗ. Распространение скриптов и медиаресурсов в многосайтовой системе посредством географически распределённой сети через защищённый *SSL*-сертификатом домен в 10 раз снижает количество *DDoS*-атак [10]. На этом преимущества *HTTPS*-режима заканчиваются.

Оказалось, что компоненты динамических сайтов, подключающие с незащищенных сайтов скрипты, изображения, видеофайлы и пр. понижают определяемый браузером уровень безопасности сайта. Адресная строка с именем сайта в *HTTPS*-режиме обмена меняет нейтральную серую репутационную метку «Не защищено» на предупреждающ**ую** красную метку «Не защищено» с перечеркнутым «*https*» вместо ожидаемой зеленой репутационной метки «Надежный» с закрытым замком. Присваиваемые сайту репутационные метки зависят от браузера. Опыт показывает, что *Google Chrome* сильнее понижает репутационный уровень безопасности сайта в сравнении с браузерами *FireFox, Safari, Internet Explorer* и *Edge*. Нажатие на репутационную метку предоставляет возможность просмотреть сведения о сертификатах безопасности, подозрительных *cookies* и сомнительных *JavaScript*, после чего принять решение об их блокировании или разрешении. Как правило, пользователи не обращают внимания на возможность активации заблокированного содержимого, что вызывает снижение качества информационного наполнения не адаптированных к безопасному режиму сайтов.

Переход в безопасный режим может вызвать отключение лент социальных сетей и виджетов медиахостингов. Исправление этих проблем требует кардинальной ревизии шаблонов и стилей сайта с переводом всех гиперссылок на внутренние и внешние ресурсы с абсолютных на относительные. Для всех подключаемых сторонних медиаресурсов (видео, аудио, анимации и пр.) требуется переподключение разрешений медиахостингов для отображения на страницах защищённых доменов, иначе выводится сообщение о запрете передачи медиафайла в соответствии с политикой безопасности. Дисфункции неадаптированных сайтов негативно влияют на посещаемость. К примеру, количество хитов, хостов, сессий с событий сайта *master-multimedia.ru* снизилось втрое после подключения *HTTPS*-режима и сохранялось на низком уровне в течение месяца до момента перевода сайта на новый микрофреймворк, специально адаптированный к работе в безопасном режиме. О начале работы сайта в безопасном режиме необходимо оповестить поисковики: следует добавить *HTTPS*-версию сайта в панель для вебмастеров *Google Search Console*, а также изменить адрес в панели Яндекс Вебмастера и *Google Search Console*.

Практический опыт показывает, что для полноценной работы сайта в *HTTPS*-режиме требуется не только приобретение и подключение *SSL*-сертификата к домену, но и выполнение большого объема коррекционных работ. Не удивительно, что уже в феврале 2017 года появились многочисленные коммерческие предложения по оказанию помощи при переводе сайта в безопасный режим.

Угрозы понижения в поисковой выдаче позиций сайтов с небезопасным протоколом обмена данными не реализовались. В Периодической таблице факторов ранжирования наличие *HTTPS*-режима находится на второй строчке с конца [11]. В июне 2017 года только 20% из 1000000 лучших сайтов мира [12] и 4% из общего числа зарегистрированных российских доменов [13] использовали *HTTPS*-протокол по умолчанию. Можно ожидать, что новой коммерческой кампанией 2018 года будет дискредитация использования *SSL*-сертификатов и пропаганда приобретения более надежных и дорогих *TLS*-сертификатов.

Таким образом, если обработка платежей и персональных данных не входит в функционал сайтов, их адаптация к *HTTPS*-режиму обмена данными с использованием *SSL*-сертификатов в настоящее время нецелесообразна в связи с неадекватными результату сопутствующими финансовыми и трудовыми затратами.

Литература

1. The Original HTTP as defined in 1991 — URL: https://www.w3.org/Protocols/HTTP/AsImplemented.html
2. Walls, C.. Embedded software — Newnes, 2005. — P. 344. — ISBN 0-7506-7954-9.
3. SSL 3.0 Protocol Vulnerability and POODLE Attack — URL: https://www.us-cert.gov/ncas/alerts/TA14-290A
4. The Transport Layer Security (TLS) Protocol Version 1.3 — URL: https://tools.ietf.org/html/draft-ietf-tls-tls13-21
5. Каспаринский Ф.О., Маланьина Т.В. Видео-лекции: от CD к DVD и Сети // Научный сервис в сети Интернет: труды IV Всероссийской научной конференции (20-25 сентября 2004 г., г. Новороссийск). — М.: Изд-во Московского университета. — С. 181 – 183.
6. Самоподписанный SSL сертификат — преимущества и недостатки. — URL: https://www.emaro-ssl.ru/blog/self-signed-certificate/
7. Сравнение SSL сертификатов с верификацией домена. — URL: https://habrahabr.ru/company/hosting-cafe/blog/278255/
8. SSL-сертификаты для каждого домена. — URL: https://www.jino.ru/about/news/articles/sslcerts-domains/
9. Бесплатные SSL-сертификаты от Let's Encrypt. — URL: https://www.jino.ru/about/news/articles/letsencrypt/

10. Каспаринский Ф.О. Инфоконтинуум как сервис для междисциплинарной системной интеграции профессиональных интернет-представительств // Научный сервис в сети Интернет: труды XVIII Всероссийской научной конференции (19-24 сентября 2016 г., г. Новороссийск). — М.: ИПМ им. М.В.Келдыша, 2016. — С. 162-169. — doi:10.20948/abrau-2016-12
11 The Periodic Table of SEO Success Factors. SEO - Search Engine Optimization News & Trends | Search Engine Land. — URL: http://searchengineland.com/library/channel/seo
12. HTTPS usage statistics on top websites. — URL: https://statoperator.com
13. Статистика российского интернета. — URL: https://www.runfo.ru