

Internet Engineering Task Force (IETF)

Request for Comments: 8996

BCP: 195

Obsoletes: 5469, 7507

Updates: 3261, 3329, 3436, 3470, 3501, 3552,  
3568, 3656, 3749, 3767, 3856, 3871,  
3887, 3903, 3943, 3983, 4097, 4111,  
4162, 4168, 4217, 4235, 4261, 4279,  
4497, 4513, 4531, 4540, 4582, 4616,  
4642, 4680, 4681, 4712, 4732, 4743,  
4744, 4785, 4791, 4823, 4851, 4964,  
4975, 4976, 4992, 5018, 5019, 5023,  
5024, 5049, 5054, 5091, 5158, 5216,  
5238, 5263, 5281, 5364, 5415, 5422,  
5456, 5734, 5878, 5953, 6012, 6042,  
6083, 6084, 6176, 6347, 6353, 6367,  
6460, 6614, 6739, 6749, 6750, 7030,  
7465, 7525, 7562, 7568, 8261, 8422

Category: Best Current Practice

ISSN: 2070-1721

K. Moriarty

CIS

S. Farrell

Trinity College Dublin

March 2021

## Deprecating TLS 1.0 and TLS 1.1

Прекращение поддержки TLS 1.0 и TLS 1.1

### Аннотация

Этот документ формально отменяет протокол TLS<sup>1</sup> версии 1.0 (RFC 2246) и 1.1 (RFC 4346) с переводом упомянутых документов в статус Historic. В этих версиях отсутствует поддержка современных и рекомендуемых криптографических алгоритмов и механизмов, а различные правительственные и отраслевые профили приложений, использующих TLS, рекомендуют отказ от этих устаревших версий TLS. TLS версии 1.2 рекомендован для протоколов IETF с 2008 г., а в 2018 г. заменён TLS версии 1.3, что обеспечило достаточное для перехода к новым версиям время. Прекращение поддержки старых версий сокращает фронт атак, снижает вероятность неверной настройки и упрощает поддержку программ и библиотек.

Этот документ также отменяет DTLS<sup>2</sup> версии 1.0 (RFC 4347), не отменяя DTLS версии 1.2 (DTLS версии 1.1 не существует).

Документ обновляет многие RFC, которые нормативно задавали применение TLS версии 1.0 или TLS версии 1.1, а также рекомендации по использованию TLS в RFC 7525 (следовательно, является частью BCP 195).

### Статус документа

Документ относится к категории Internet Best Current Practice.

Документ является результатом работы IETF<sup>3</sup> и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG<sup>4</sup>. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <https://www.rfc-editor.org/info/rfc8996>.

### Авторские права

Авторские права (Copyright (c) 2021) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

<sup>1</sup>Transport Layer Security - защита транспортного уровня.

<sup>2</sup>Datagram TLS - TLS для дейтаграмм.

<sup>3</sup>Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

<sup>4</sup>Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

## Оглавление

1. Введение.....	2
1.1. Обновлённые RFC.....	2
1.2. Уровни требований.....	3
2. Поддержка отмены.....	3
3. SHA-1 как проблема TLS 1.0 и TLS 1.1.....	3
4. Отказ от TLS 1.0.....	3
5. Отказ от TLS 1.1.....	4
6. Обновление RFC 7525.....	4
7. Вопросы эксплуатации.....	4
8. Вопросы безопасности.....	4
9. Взаимодействие с IANA.....	4
10. Литература.....	4
10.1. Нормативные документы.....	4
10.2. Дополнительная литература.....	7
Благодарности.....	9
Адреса авторов.....	9

## 1. Введение

Протоколы TLS версии 1.0 [RFC2246] и 1.1 [RFC4346] переопределены TLS 1.2 [RFC5246] в 2008 г., а этот протокол был переопределен TLS 1.3 [RFC8446]. Протокол DTLS версии 1.0 [RFC4347] переопределен DTLS 1.2 [RFC6347] в 2012 г. Пришло время отказаться от TLS 1.0, TLS 1.1 и DTLS 1.0 с переводом упомянутых документов в статус Historic.

Технические причины отказа от поддержки старых версий указаны ниже.

- Протоколы требуют поддержки устаревших протоколов, которая нежелательна с точки зрения криптографии. Например, TLS 1.0 требует реализации TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA.
- Отсутствует поддержка рекомендуемых в настоящее время шифров, особенно аутентифицированного шифрования со связанными данными (AEAD<sup>1</sup>), которое не поддерживается до TLS 1.2. Отметим, что записи для устаревших шифров сохраняются в реестрах, но многие реестры TLS были обновлены [RFC8447], где указано, что эти записи не рекомендуются IETF.
- Целостность согласования зависит от хэша SHA-1.
- Проверка подлинности партнера зависит от подписей SHA-1.
- Поддержка 4 версий протокола TLS повышает вероятность некорректной настройки.
- По крайней мере одна из распространённых библиотек планирует отказ от поддержки TLS 1.1 и TLS 1.0 в будущих выпусках, поэтому программам, использующим библиотеки придётся сохранять старую версию для поддержки TLS 1.0 и TLS 1.1, что явно нежелательно.

Прекращение поддержки этих версий предназначено для оказания помощи разработчикам с целью перехода на новые версии (D)TLS, начиная с (D)TLS 1.2. Отмена также позволяет разработчикам прекратить поддержку устаревших версий для сужения фронта атак и объёма поддержки протоколов в своей продукции.

### 1.1. Обновлённые RFC

Этот документ обновляет перечисленные ниже RFC, в которых содержатся нормативные ссылки на TLS 1.0, TLS 1.1, DTLS 1.0. Обновление предназначено для отмены использования этих устаревших версий. Конкретные ссылки на обязательную для реализации минимальную версию протокола TLS 1.0 или TLS 1.1 заменены ссылками на TLS 1.2, а ссылки на DTLS 1.0 - ссылками на DTLS 1.2. Утверждения вида: «TLS 1.0 является наиболее широко распространённой версией» удалены без замены.

[RFC3261] [RFC3329] [RFC3436] [RFC3470] [RFC3501] [RFC3552] [RFC3568] [RFC3656] [RFC3749] [RFC3767] [RFC3856] [RFC3871] [RFC3887] [RFC3903] [RFC3943] [RFC3983] [RFC4097] [RFC4111] [RFC4162] [RFC4168] [RFC4217] [RFC4235] [RFC4261] [RFC4279] [RFC4497] [RFC4513] [RFC4531] [RFC4540] [RFC4582] [RFC4616] [RFC4642] [RFC4680] [RFC4681] [RFC4712] [RFC4732] [RFC4785] [RFC4791] [RFC4823] [RFC4851] [RFC4964] [RFC4975] [RFC4976] [RFC4992] [RFC5018] [RFC5019] [RFC5023] [RFC5024] [RFC5049] [RFC5054] [RFC5091] [RFC5158] [RFC5216] [RFC5238] [RFC5263] [RFC5281] [RFC5364] [RFC5415] [RFC5422] [RFC5456] [RFC5734] [RFC5878] [RFC6012] [RFC6042] [RFC6083] [RFC6084] [RFC6176] [RFC6353] [RFC6367] [RFC6739] [RFC6749] [RFC6750] [RFC7030] [RFC7465] [RFC7525] [RFC7562] [RFC7568] [RFC8261] [RFC8422]

Статус [RFC7562], [RFC6042], [RFC5456], [RFC5024], [RFC4540], [RFC3656] обновлён с разрешения Independent Submissions Editor.

RFC с нормативными ссылками на TLS 1.0 или TLS 1.1, которые устарели и указаны здесь как обновлённые данным документом, чтобы подчеркнуть, что взамен устаревшего протокола следует использовать современную версию TLS включают [RFC3316], [RFC3489], [RFC3546], [RFC3588], [RFC3734], [RFC3920], [RFC4132], [RFC4244], [RFC4347], [RFC4366], [RFC4492], [RFC4507], [RFC4572], [RFC4582], [RFC4934], [RFC5077], [RFC5081], [RFC5101], [RFC5953].

Документ [RFC4642] уже обновлён [RFC8143], но это обновление не идентично вносимому данным документом.

В [RFC6614] указано требование использовать TLS 1.1 и выше, но содержится лишь информационная ссылка на [RFC4346]. Это требование обновлено указанием TLS 1.2 или последующих версий.

[RFC6460], [RFC4744], [RFC4743] уже имеют статус Historic, но указаны здесь как обновлённые данным документом, чтобы подчеркнуть необходимость замены устаревших протоколов современными версиями TLS.

Этот документ обновляет DTLS [RFC6347], где разрешено согласование использования DTLS 1.0, отменённого здесь.

<sup>1</sup>Authenticated encryption with associated data.

Шифры DES и IDEA<sup>1</sup>, заданные в [RFC5469], были удалены из TLS 1.2 документом [RFC5246], поскольку указанные для этих шифров версии TLS, переведены в статус Historic, как и [RFC5469].

Заданное для отката версии шифра Signaling Cipher Suite Value [RFC7507] было определено с целью обнаружения ситуаций, когда клиент и сервер согласуют версию (D)TLS ниже максимальной, поддерживаемой обоими. В TLS 1.3 ([RFC8446]) для этого применяется другой механизм на основе сторожевых значений в поле ServerHello.Random. Версии (D)TLS до 1.2 полностью отменены и единственным вариантом, которым реализации (D)TLS могут согласовать использование версии ниже максимальной для обоих, является согласование (D)TLS 1.2 при поддержке обоими (D)TLS 1.3, а использование (D)TLS 1.3 предполагает поддержку механизма ServerHello.Random. Это переопределяет функциональность [RFC7507] и документ получает статус Obsolete.

## 1.2. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

## 2. Поддержка отмены

Детали атак на TLS 1.0 и TLS 1.1, а также способы их предотвращения рассмотрены в [NIST800-52r2], [RFC7457] и упомянутых там RFC. Несмотря на разработку мер устранения известных уязвимостей, вновь обнаруживаемые проблемы старых версий протоколов не могут быть устранены в старых версиях библиотек, если новые библиотеки не поддерживают эти устаревшие протоколы.

Например, NIST предлагает приведённые ниже рекомендации (раздел 1.1 History of TLS в [NIST800-52r2]).

Протокол TLS 1.1, заданный в RFC 4346 [24], был разработан для устранения слабостей TLS 1.0, прежде всего в части выбора вектора инициализации и обработки ошибок заполнения. Векторы инициализации были сделаны явными для предотвращения определённого класса атак против режима CBC<sup>2</sup>, используемого TLS. Обработка ошибок заполнения была изменена так, чтобы ошибка считалась неверным кодом аутентификации сообщения, а не отказом при расшифровке. Кроме того, в TLS 1.1 RFC подтверждены атаки на режим CBC, основанные на времени расчёта кода MAC<sup>3</sup>. В спецификации TLS 1.1 указано, что для защиты от таких атак реализация должна обрабатывать записи независимо от наличия ошибок заполнения. Дополнительные проблемы реализации режимов CBC (не включённые в RFC 4346 [24]), рассмотрены в параграфе 3.3.2.

Протокол TLS 1.2, заданный в RFC 5246 [25], внёс несколько криптографических улучшений, особенно в сфере функций хэширования, с возможностью использовать или задавать семейство алгоритмов SHA-2 для хэширования и расчётов MAC и PRF<sup>4</sup>. В TLS 1.2 также добавлены шифры AEAD.

Протокол TLS 1.3, заданный в RFC 8446 [57], существенно меняет TLS с целью устранения угроз, обнаруженных в последние годы. Изменения включают новый протокол согласования, новый процесс вывода ключей с использованием функции HKDF<sup>5</sup> [37], а также исключение шифров, использующих транспорт ключей RSA или статический обмен DH (Diffie-Hellman), режимов работы CBC и SHA-1. Многие расширения, заданные для TLS 1.2 и предшествующих версий, не могут применяться с TLS 1.3.

## 3. SHA-1 как проблема TLS 1.0 и TLS 1.1

Целостность TLS 1.0 и TLS 1.1 зависит от хэширования SHA-1 при обмене сообщениями. Это позволяет организовать «атаку с понижением» на процесс согласования злоумышленнику, способному выполнить 2<sup>77</sup> операций, что гораздо ниже доступных в настоящее время возможностей.

Точно так же аутентификация при согласовании зависит от подписей с использованием хэширования SHA-1 или конкатенации хэш-значений MD5 и SHA-1, которая не намного сильнее SHA-1, что позволяет атакующему представиться сервером при успешном взломе слабого хэша SHA-1.

Протоколы TLS 1.0 и TLS 1.1 не позволяют партнёрам выбрать более строгое хэширование подписей в сообщениях ServerKeyExchange и CertificateVerify, доступное лишь при переходе на новые версии протокола.

Дополнительная информация представлена в [Bhargavan2016].

## 4. Отказ от TLS 1.0

Использование TLS 1.0 **недопустимо**. Согласование TLS 1.0 из любой версии TLS **недопустимо**.

Все версии TLS более защищены, нежели TLS 1.0. Хотя в TLS 1.0 можно настроить предотвращение некоторых типов перехвата, предпочтительней использовать старшую из доступных версий.

На практике клиентам **недопустимо** передавать ClientHello с ClientHello.client\_version {03,01}, а серверам **недопустимо** передавать ServerHello с ServerHello.server\_version {03,01}. Любая сторона, получившая сообщение Hello с версией протокола {03,01}, **должна** ответить сообщением protocol\_version и разорвать соединение.

Исторически в спецификациях TLS не было чёткого указания номера версии уровня записи (TLSPplaintext.version) в сообщении ClientHello. Приложение E в [RFC5246] указывает, что TLSPplaintext.version можно выбирать для максимальной совместимости, хотя не было определено «идеального» значения. Эта рекомендация сохраняется, поэтому серверы TLS **должны** воспринимать любое значение {03,XX} (включая {03,00}) как номер версии для уровня записи в ClientHello, но согласование TLS 1.0 **недопустимо**.

<sup>1</sup>International Data Encryption Algorithm - международный алгоритм шифрования данных.

<sup>2</sup>Cipher Block Chaining - цепочка шифрованных блоков.

<sup>3</sup>Message authentication code - код проверки подлинности сообщения.

<sup>4</sup>Pseudorandom Function - псевдослучайная функция.

<sup>5</sup>HMAC-based Extract-and-Expand Key Derivation Function - функция вывода ключей на основе HMAC.

## 5. Отказ от TLS 1.1

Использование TLS 1.1 **недопустимо**. Согласование TLS 1.1 из любой версии TLS **недопустимо**.

На практике клиентам **недопустимо** передавать ClientHello с ClientHello.client\_version {03,02}, а серверам **недопустимо** передавать ServerHello с ServerHello.server\_version {03,02}. Любая сторона, получившая сообщение Hello с версией протокола {03,02}, **должна** ответить сообщением protocol\_version и разорвать соединение.

Все версии более новые версии TLS более защищены, нежели TLS 1.1. Хотя в TLS 1.1 можно настроить предотвращение некоторых типов перехвата, предпочтительней использовать старшую из доступных версий. Поддержка TLS 1.1 в библиотеках сокращается и это будет влиять на безопасность в будущем, если меры противодействия атакам не будут реализованы в старых библиотеках.

Исторически в спецификациях TLS не было четкого указания номера версии уровня записи (TLSPlaintext.version) в сообщении ClientHello. Приложение E в [RFC5246] указывает, что TLSPlaintext.version можно выбирать для максимальной совместимости, хотя не было определено «идеального» значения. Эта рекомендация сохраняется, поэтому серверы TLS **должны** воспринимать любое значение {03,XX} (включая {03,00}) как номер версии для уровня записи в ClientHello, но согласование TLS 1.1 **недопустимо**.

## 6. Обновление RFC 7525

Документ Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) [RFC7525] является BCP 195 - самым свежим в категории Best Current Practice для реализации TLS - и основан на TLS 1.2. В момент публикации документа TLS 1.0 и TLS 1.1 ещё не считались устаревшими. Поэтому здесь BCP 195 упоминается специально для обновления текста рекомендациями этого документа по прекращению поддержки.

Этот документ обновляет параграф 3.1.1 [RFC7525] заменой **не следует на недопустимо**, как указано ниже.

- Реализациям **недопустимо** согласовывать TLS версии 1.0 [RFC2246].

Обоснование. Протокол TLS 1.0 (1999 г.) не поддерживает многие современные строгие шифры. Кроме того, в TLS 1.0 отсутствует вектор инициализации (Initialization Vector или IV) для шифров CBC и не выдаются предупреждения при ошибках заполнения.

- Реализациям **недопустимо** согласовывать TLS версии 1.1 [RFC4346].

Обоснование. Протокол TLS 1.1 (2006 г.) улучшает защиту по сравнению с TLS 1.0, но не поддерживает некоторые современные и более строгие шифры.

Этот документ обновляет параграф 3.1.2 [RFC7525] заменой **не следует на недопустимо** и добавлением ссылки на RFC 6347, как указано ниже.

- Реализациям **недопустимо** согласовывать DTLS версии 1.0 [RFC4347] [RFC6347].

Версия 1.0 протокола DTLS соответствует версии 1.1 протокола TLS (см. выше).

## 7. Вопросы эксплуатации

Этот документ является частью BCP 195 и в этом качестве отражает представление IETF (на момент публикации этого документа) в части опыта применения TLS и DTLS.

Хотя протокол TLS 1.1 устарел с момента публикации [RFC5246] в 2008 г., а DTLS 1.0 устарел с момента публикации [RFC6347] в 2012 г., ещё могут оставаться системы, не поддерживающие (D)TLS 1.2 и выше. Принятие рекомендаций этого документа для всех систем, которым нужно взаимодействовать с вышеупомянутыми системами, будет приводить к отказам. Однако игнорирование рекомендаций для сохранения взаимодействия сопряжено с риском. Характер возникающих рисков рассмотрен в разделах 2 и 3, а сведения о рисках следует учитывать вместе с информацией об их смягчении при решении вопроса об обновлении систем в свете рекомендаций этого документа.

## 8. Вопросы безопасности

Этот документ отменяет поддержку двух устаревших версий протокола TLS и одной устаревшей версии DTLS по описанным выше соображениям безопасности. Фронт возможных атак сужается за счет уменьшения числа поддерживаемых протоколов и возможностей отката к старым версиям.

## 9. Взаимодействие с IANA

Этот документ не требует действий со стороны IANA.

## 10. Литература

### 10.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", [RFC 2246](#), DOI 10.17487/RFC2246, January 1999, <<https://www.rfc-editor.org/info/rfc2246>>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <<https://www.rfc-editor.org/info/rfc3261>>.

[RFC3329] Arkko, J., Torvinen, V., Camarillo, G., Niemi, A., and T. Haukka, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)", RFC 3329, DOI 10.17487/RFC3329, January 2003, <<https://www.rfc-editor.org/info/rfc3329>>.

- [RFC3436] Jungmaier, A., Rescorla, E., and M. Tuexen, "Transport Layer Security over Stream Control Transmission Protocol", RFC 3436, DOI 10.17487/RFC3436, December 2002, <<https://www.rfc-editor.org/info/rfc3436>>.
- [RFC3470] Hollenbeck, S., Rose, M., and L. Masinter, "Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols", BCP 70, RFC 3470, DOI 10.17487/RFC3470, January 2003, <<https://www.rfc-editor.org/info/rfc3470>>.
- [RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL — VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <<https://www.rfc-editor.org/info/rfc3501>>.
- [RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <<https://www.rfc-editor.org/info/rfc3552>>.
- [RFC3568] Barbir, A., Cain, B., Nair, R., and O. Spatscheck, "Known Content Network (CN) Request-Routing Mechanisms", RFC 3568, DOI 10.17487/RFC3568, July 2003, <<https://www.rfc-editor.org/info/rfc3568>>.
- [RFC3656] Siemborski, R., "The Mailbox Update (MUPDATE) Distributed Mailbox Database Protocol", RFC 3656, DOI 10.17487/RFC3656, December 2003, <<https://www.rfc-editor.org/info/rfc3656>>.
- [RFC3749] Hollenbeck, S., "Transport Layer Security Protocol Compression Methods", RFC 3749, DOI 10.17487/RFC3749, May 2004, <<https://www.rfc-editor.org/info/rfc3749>>.
- [RFC3767] Farrell, S., Ed., "Securely Available Credentials Protocol", RFC 3767, DOI 10.17487/RFC3767, June 2004, <<https://www.rfc-editor.org/info/rfc3767>>.
- [RFC3856] Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)", RFC 3856, DOI 10.17487/RFC3856, August 2004, <<https://www.rfc-editor.org/info/rfc3856>>.
- [RFC3871] Jones, G., Ed., "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure", RFC 3871, DOI 10.17487/RFC3871, September 2004, <<https://www.rfc-editor.org/info/rfc3871>>.
- [RFC3887] Hansen, T., "Message Tracking Query Protocol", RFC 3887, DOI 10.17487/RFC3887, September 2004, <<https://www.rfc-editor.org/info/rfc3887>>.
- [RFC3903] Niemi, A., Ed., "Session Initiation Protocol (SIP) Extension for Event State Publication", RFC 3903, DOI 10.17487/RFC3903, October 2004, <<https://www.rfc-editor.org/info/rfc3903>>.
- [RFC3943] Friend, R., "Transport Layer Security (TLS) Protocol Compression Using Lempel-Ziv-Stac (LZS)", RFC 3943, DOI 10.17487/RFC3943, November 2004, <<https://www.rfc-editor.org/info/rfc3943>>.
- [RFC3983] Newton, A. and M. Sanz, "Using the Internet Registry Information Service (IRIS) over the Blocks Extensible Exchange Protocol (BEEP)", RFC 3983, DOI 10.17487/RFC3983, January 2005, <<https://www.rfc-editor.org/info/rfc3983>>.
- [RFC4097] Barnes, M., Ed., "Middlebox Communications (MIDCOM) Protocol Evaluation", RFC 4097, DOI 10.17487/RFC4097, June 2005, <<https://www.rfc-editor.org/info/rfc4097>>.
- [RFC4111] Fang, L., Ed., "Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)", RFC 4111, DOI 10.17487/RFC4111, July 2005, <<https://www.rfc-editor.org/info/rfc4111>>.
- [RFC4162] Lee, H.J., Yoon, J.H., and J.I. Lee, "Addition of SEED Cipher Suites to Transport Layer Security (TLS)", RFC 4162, DOI 10.17487/RFC4162, August 2005, <<https://www.rfc-editor.org/info/rfc4162>>.
- [RFC4168] Rosenberg, J., Schulzrinne, H., and G. Camarillo, "The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)", RFC 4168, DOI 10.17487/RFC4168, October 2005, <<https://www.rfc-editor.org/info/rfc4168>>.
- [RFC4217] Ford-Hutchinson, P., "Securing FTP with TLS", RFC 4217, DOI 10.17487/RFC4217, October 2005, <<https://www.rfc-editor.org/info/rfc4217>>.
- [RFC4235] Rosenberg, J., Schulzrinne, H., and R. Mahy, Ed., "An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)", RFC 4235, DOI 10.17487/RFC4235, November 2005, <<https://www.rfc-editor.org/info/rfc4235>>.
- [RFC4261] Walker, J. and A. Kulkarni, Ed., "Common Open Policy Service (COPS) Over Transport Layer Security (TLS)", RFC 4261, DOI 10.17487/RFC4261, December 2005, <<https://www.rfc-editor.org/info/rfc4261>>.
- [RFC4279] Eronen, P., Ed. and H. Tschofenig, Ed., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, DOI 10.17487/RFC4279, December 2005, <<https://www.rfc-editor.org/info/rfc4279>>.
- [RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, DOI 10.17487/RFC4346, April 2006, <<https://www.rfc-editor.org/info/rfc4346>>.
- [RFC4497] Elwell, J., Derks, F., Mourot, P., and O. Rousseau, "Interworking between the Session Initiation Protocol (SIP) and QSIG", BCP 117, RFC 4497, DOI 10.17487/RFC4497, May 2006, <<https://www.rfc-editor.org/info/rfc4497>>.
- [RFC4513] Harrison, R., Ed., "Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms", RFC 4513, DOI 10.17487/RFC4513, June 2006, <<https://www.rfc-editor.org/info/rfc4513>>.
- [RFC4531] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP) Turn Operation", RFC 4531, DOI 10.17487/RFC4531, June 2006, <<https://www.rfc-editor.org/info/rfc4531>>.
- [RFC4540] Stiemerling, M., Quittek, J., and C. Cadar, "NEC's Simple Middlebox Configuration (SIMCO) Protocol Version 3.0", RFC 4540, DOI 10.17487/RFC4540, May 2006, <<https://www.rfc-editor.org/info/rfc4540>>.
- [RFC4582] Camarillo, G., Ott, J., and K. Drage, "The Binary Floor Control Protocol (BFCP)", RFC 4582, DOI 10.17487/RFC4582, November 2006, <<https://www.rfc-editor.org/info/rfc4582>>.

- [RFC4616] Zeilenga, K., Ed., "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism", RFC 4616, DOI 10.17487/RFC4616, August 2006, <<https://www.rfc-editor.org/info/rfc4616>>.
- [RFC4642] Murchison, K., Vinocur, J., and C. Newman, "Using Transport Layer Security (TLS) with Network News Transfer Protocol (NNTP)", RFC 4642, DOI 10.17487/RFC4642, October 2006, <<https://www.rfc-editor.org/info/rfc4642>>.
- [RFC4680] Santesson, S., "TLS Handshake Message for Supplemental Data", RFC 4680, DOI 10.17487/RFC4680, October 2006, <<https://www.rfc-editor.org/info/rfc4680>>.
- [RFC4681] Santesson, S., Medvinsky, A., and J. Ball, "TLS User Mapping Extension", RFC 4681, DOI 10.17487/RFC4681, October 2006, <<https://www.rfc-editor.org/info/rfc4681>>.
- [RFC4712] Siddiqui, A., Romascanu, D., Golovinsky, E., Rahman, M., and Y. Kim, "Transport Mappings for Real-time Application Quality-of-Service Monitoring (RAQMON) Protocol Data Unit (PDU)", RFC 4712, DOI 10.17487/RFC4712, October 2006, <<https://www.rfc-editor.org/info/rfc4712>>.
- [RFC4732] Handley, M., Ed., Rescorla, E., Ed., and IAB, "Internet Denial-of-Service Considerations", RFC 4732, DOI 10.17487/RFC4732, December 2006, <<https://www.rfc-editor.org/info/rfc4732>>.
- [RFC4743] Goddard, T., "Using NETCONF over the Simple Object Access Protocol (SOAP)", RFC 4743, DOI 10.17487/RFC4743, December 2006, <<https://www.rfc-editor.org/info/rfc4743>>.
- [RFC4744] Lear, E. and K. Crozier, "Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP)", RFC 4744, DOI 10.17487/RFC4744, December 2006, <<https://www.rfc-editor.org/info/rfc4744>>.
- [RFC4785] Blumenthal, U. and P. Goel, "Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)", RFC 4785, DOI 10.17487/RFC4785, January 2007, <<https://www.rfc-editor.org/info/rfc4785>>.
- [RFC4791] Daboo, C., Desruisseaux, B., and L. Dusseault, "Calendaring Extensions to WebDAV (CalDAV)", RFC 4791, DOI 10.17487/RFC4791, March 2007, <<https://www.rfc-editor.org/info/rfc4791>>.
- [RFC4823] Harding, T. and R. Scott, "FTP Transport for Secure Peer-to-Peer Business Data Interchange over the Internet", RFC 4823, DOI 10.17487/RFC4823, April 2007, <<https://www.rfc-editor.org/info/rfc4823>>.
- [RFC4851] Cam-Winget, N., McGrew, D., Salowey, J., and H. Zhou, "The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)", RFC 4851, DOI 10.17487/RFC4851, May 2007, <<https://www.rfc-editor.org/info/rfc4851>>.
- [RFC4964] Allen, A., Ed., Holm, J., and T. Hallin, "The P-Answer-State Header Extension to the Session Initiation Protocol for the Open Mobile Alliance Push to Talk over Cellular", RFC 4964, DOI 10.17487/RFC4964, September 2007, <<https://www.rfc-editor.org/info/rfc4964>>.
- [RFC4975] Campbell, B., Ed., Mahy, R., Ed., and C. Jennings, Ed., "The Message Session Relay Protocol (MSRP)", RFC 4975, DOI 10.17487/RFC4975, September 2007, <<https://www.rfc-editor.org/info/rfc4975>>.
- [RFC4976] Jennings, C., Mahy, R., and A. B. Roach, "Relay Extensions for the Message Sessions Relay Protocol (MSRP)", RFC 4976, DOI 10.17487/RFC4976, September 2007, <<https://www.rfc-editor.org/info/rfc4976>>.
- [RFC4992] Newton, A., "XML Pipelining with Chunks for the Internet Registry Information Service", RFC 4992, DOI 10.17487/RFC4992, August 2007, <<https://www.rfc-editor.org/info/rfc4992>>.
- [RFC5018] Camarillo, G., "Connection Establishment in the Binary Floor Control Protocol (BFCP)", RFC 5018, DOI 10.17487/RFC5018, September 2007, <<https://www.rfc-editor.org/info/rfc5018>>.
- [RFC5019] Deacon, A. and R. Hurst, "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments", RFC 5019, DOI 10.17487/RFC5019, September 2007, <<https://www.rfc-editor.org/info/rfc5019>>.
- [RFC5023] Gregorio, J., Ed. and B. de hOra, Ed., "The Atom Publishing Protocol", RFC 5023, DOI 10.17487/RFC5023, October 2007, <<https://www.rfc-editor.org/info/rfc5023>>.
- [RFC5024] Friend, I., "ODETTE File Transfer Protocol 2.0", RFC 5024, DOI 10.17487/RFC5024, November 2007, <<https://www.rfc-editor.org/info/rfc5024>>.
- [RFC5049] Bormann, C., Liu, Z., Price, R., and G. Camarillo, Ed., "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)", RFC 5049, DOI 10.17487/RFC5049, December 2007, <<https://www.rfc-editor.org/info/rfc5049>>.
- [RFC5054] Taylor, D., Wu, T., Mavrogiannopoulos, N., and T. Perrin, "Using the Secure Remote Password (SRP) Protocol for TLS Authentication", RFC 5054, DOI 10.17487/RFC5054, November 2007, <<https://www.rfc-editor.org/info/rfc5054>>.
- [RFC5091] Boyen, X. and L. Martin, "Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems", RFC 5091, DOI 10.17487/RFC5091, December 2007, <<https://www.rfc-editor.org/info/rfc5091>>.
- [RFC5158] Huston, G., "6to4 Reverse DNS Delegation Specification", RFC 5158, DOI 10.17487/RFC5158, March 2008, <<https://www.rfc-editor.org/info/rfc5158>>.
- [RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, DOI 10.17487/RFC5216, March 2008, <<https://www.rfc-editor.org/info/rfc5216>>.
- [RFC5238] Phelan, T., "Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP)", RFC 5238, DOI 10.17487/RFC5238, May 2008, <<https://www.rfc-editor.org/info/rfc5238>>.
- [RFC5263] Lonnfors, M., Costa-Requena, J., Leppanen, E., and H. Khartabil, "Session Initiation Protocol (SIP) Extension for Partial Notification of Presence Information", RFC 5263, DOI 10.17487/RFC5263, September 2008, <<https://www.rfc-editor.org/info/rfc5263>>.

- [RFC5281] Funk, P. and S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TLSv0)", RFC 5281, DOI 10.17487/RFC5281, August 2008, <<https://www.rfc-editor.org/info/rfc5281>>.
- [RFC5364] Garcia-Martin, M. and G. Camarillo, "Extensible Markup Language (XML) Format Extension for Representing Copy Control Attributes in Resource Lists", RFC 5364, DOI 10.17487/RFC5364, October 2008, <<https://www.rfc-editor.org/info/rfc5364>>.
- [RFC5422] Cam-Winget, N., McGrew, D., Salowey, J., and H. Zhou, "Dynamic Provisioning Using Flexible Authentication via Secure Tunneling Extensible Authentication Protocol (EAP-FAST)", RFC 5422, DOI 10.17487/RFC5422, March 2009, <<https://www.rfc-editor.org/info/rfc5422>>.
- [RFC5469] Eronen, P., Ed., "DES and IDEA Cipher Suites for Transport Layer Security (TLS)", RFC 5469, DOI 10.17487/RFC5469, February 2009, <<https://www.rfc-editor.org/info/rfc5469>>.
- [RFC5734] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Transport over TCP", STD 69, RFC 5734, DOI 10.17487/RFC5734, August 2009, <<https://www.rfc-editor.org/info/rfc5734>>.
- [RFC5878] Brown, M. and R. Housley, "Transport Layer Security (TLS) Authorization Extensions", RFC 5878, DOI 10.17487/RFC5878, May 2010, <<https://www.rfc-editor.org/info/rfc5878>>.
- [RFC5953] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)", RFC 5953, DOI 10.17487/RFC5953, August 2010, <<https://www.rfc-editor.org/info/rfc5953>>.
- [RFC6042] Keromytis, A., "Transport Layer Security (TLS) Authorization Using KeyNote", RFC 6042, DOI 10.17487/RFC6042, October 2010, <<https://www.rfc-editor.org/info/rfc6042>>.
- [RFC6176] Turner, S. and T. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0", RFC 6176, DOI 10.17487/RFC6176, March 2011, <<https://www.rfc-editor.org/info/rfc6176>>.
- [RFC6353] Hardaker, W., "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)", STD 78, RFC 6353, DOI 10.17487/RFC6353, July 2011, <<https://www.rfc-editor.org/info/rfc6353>>.
- [RFC6367] Kanno, S. and M. Kanda, "Addition of the Camellia Cipher Suites to Transport Layer Security (TLS)", RFC 6367, DOI 10.17487/RFC6367, September 2011, <<https://www.rfc-editor.org/info/rfc6367>>.
- [RFC6739] Schulzrinne, H. and H. Tschofenig, "Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol", RFC 6739, DOI 10.17487/RFC6739, October 2012, <<https://www.rfc-editor.org/info/rfc6739>>.
- [RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <<https://www.rfc-editor.org/info/rfc6749>>.
- [RFC6750] Jones, M. and D. Hardt, "The OAuth 2.0 Authorization Framework: Bearer Token Usage", RFC 6750, DOI 10.17487/RFC6750, October 2012, <<https://www.rfc-editor.org/info/rfc6750>>.
- [RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <<https://www.rfc-editor.org/info/rfc7030>>.
- [RFC7465] Popov, A., "Prohibiting RC4 Cipher Suites", RFC 7465, DOI 10.17487/RFC7465, February 2015, <<https://www.rfc-editor.org/info/rfc7465>>.
- [RFC7507] Moeller, B. and A. Langley, "TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks", RFC 7507, DOI 10.17487/RFC7507, April 2015, <<https://www.rfc-editor.org/info/rfc7507>>.
- [RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <<https://www.rfc-editor.org/info/rfc7525>>.
- [RFC7562] Thakore, D., "Transport Layer Security (TLS) Authorization Using Digital Transmission Content Protection (DTCP) Certificates", RFC 7562, DOI 10.17487/RFC7562, July 2015, <<https://www.rfc-editor.org/info/rfc7562>>.
- [RFC7568] Barnes, R., Thomson, M., Pironti, A., and A. Langley, "Deprecating Secure Sockets Layer Version 3.0", RFC 7568, DOI 10.17487/RFC7568, June 2015, <<https://www.rfc-editor.org/info/rfc7568>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8422] Nir, Y., Josefsson, S., and M. Pegourie-Gonnard, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier", RFC 8422, DOI 10.17487/RFC8422, August 2018, <<https://www.rfc-editor.org/info/rfc8422>>.

## 10.2. Дополнительная литература

- [Bhargavan2016] Bhargavan, K. and G. Leuren, "Transcript Collision Attacks: Breaking Authentication in TLS, IKE, and SSH", DOI 10.14722/ndss.2016.23418, February 2016, <<https://www.mitsl.org/downloads/transcript-collisions.pdf>>.
- [NIST800-52r2] National Institute of Standards and Technology, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations NIST SP800-52r2", DOI 10.6028/NIST.SP.800-52r2, August 2019, <<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf>>.
- [RFC3316] Arkko, J., Kuijpers, G., Soliman, H., Loughney, J., and J. Wiljakka, "Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts", RFC 3316, DOI 10.17487/RFC3316, April 2003, <<https://www.rfc-editor.org/info/rfc3316>>.

- [RFC3489] Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, DOI 10.17487/RFC3489, March 2003, <<https://www.rfc-editor.org/info/rfc3489>>.
- [RFC3546] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 3546, DOI 10.17487/RFC3546, June 2003, <<https://www.rfc-editor.org/info/rfc3546>>.
- [RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, DOI 10.17487/RFC3588, September 2003, <<https://www.rfc-editor.org/info/rfc3588>>.
- [RFC3734] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Transport Over TCP", RFC 3734, DOI 10.17487/RFC3734, March 2004, <<https://www.rfc-editor.org/info/rfc3734>>.
- [RFC3920] Saint-Andre, P., Ed., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, DOI 10.17487/RFC3920, October 2004, <<https://www.rfc-editor.org/info/rfc3920>>.
- [RFC4132] Moriai, S., Kato, A., and M. Kanda, "Addition of Camellia Cipher Suites to Transport Layer Security (TLS)", RFC 4132, DOI 10.17487/RFC4132, July 2005, <<https://www.rfc-editor.org/info/rfc4132>>.
- [RFC4244] Barnes, M., Ed., "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 4244, DOI 10.17487/RFC4244, November 2005, <<https://www.rfc-editor.org/info/rfc4244>>.
- [RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, DOI 10.17487/RFC4347, April 2006, <<https://www.rfc-editor.org/info/rfc4347>>.
- [RFC4366] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, DOI 10.17487/RFC4366, April 2006, <<https://www.rfc-editor.org/info/rfc4366>>.
- [RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, DOI 10.17487/RFC4492, May 2006, <<https://www.rfc-editor.org/info/rfc4492>>.
- [RFC4507] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 4507, DOI 10.17487/RFC4507, May 2006, <<https://www.rfc-editor.org/info/rfc4507>>.
- [RFC4572] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, DOI 10.17487/RFC4572, July 2006, <<https://www.rfc-editor.org/info/rfc4572>>.
- [RFC4934] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Transport Over TCP", RFC 4934, DOI 10.17487/RFC4934, May 2007, <<https://www.rfc-editor.org/info/rfc4934>>.
- [RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, DOI 10.17487/RFC5077, January 2008, <<https://www.rfc-editor.org/info/rfc5077>>.
- [RFC5081] Mavrogiannopoulos, N., "Using OpenPGP Keys for Transport Layer Security (TLS) Authentication", RFC 5081, DOI 10.17487/RFC5081, November 2007, <<https://www.rfc-editor.org/info/rfc5081>>.
- [RFC5101] Claise, B., Ed., "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information", RFC 5101, DOI 10.17487/RFC5101, January 2008, <<https://www.rfc-editor.org/info/rfc5101>>.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <<https://www.rfc-editor.org/info/rfc5246>>.
- [RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <<https://www.rfc-editor.org/info/rfc5415>>.
- [RFC5456] Spencer, M., Capouch, B., Guy, E., Ed., Miller, F., and K. Shumard, "IAX: Inter-Asterisk eXchange Version 2", RFC 5456, DOI 10.17487/RFC5456, February 2010, <<https://www.rfc-editor.org/info/rfc5456>>.
- [RFC6012] Salowey, J., Petch, T., Gerhards, R., and H. Feng, "Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog", RFC 6012, DOI 10.17487/RFC6012, October 2010, <<https://www.rfc-editor.org/info/rfc6012>>.
- [RFC6083] Tuexen, M., Seggelmann, R., and E. Rescorla, "Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)", RFC 6083, DOI 10.17487/RFC6083, January 2011, <<https://www.rfc-editor.org/info/rfc6083>>.
- [RFC6084] Fu, X., Dickmann, C., and J. Crowcroft, "General Internet Signaling Transport (GIST) over Stream Control Transmission Protocol (SCTP) and Datagram Transport Layer Security (DTLS)", RFC 6084, DOI 10.17487/RFC6084, January 2011, <<https://www.rfc-editor.org/info/rfc6084>>.
- [RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <<https://www.rfc-editor.org/info/rfc6347>>.
- [RFC6460] Salter, M. and R. Housley, "Suite B Profile for Transport Layer Security (TLS)", RFC 6460, DOI 10.17487/RFC6460, January 2012, <<https://www.rfc-editor.org/info/rfc6460>>.
- [RFC6614] Winter, S., McCauley, M., Venaas, S., and K. Wierenga, "Transport Layer Security (TLS) Encryption for RADIUS", RFC 6614, DOI 10.17487/RFC6614, May 2012, <<https://www.rfc-editor.org/info/rfc6614>>.

- [RFC7457] Sheffer, Y., Holz, R., and P. Saint-Andre, "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)", RFC 7457, DOI 10.17487/RFC7457, February 2015, <<https://www.rfc-editor.org/info/rfc7457>>.
- [RFC8143] Elie, J., "Using Transport Layer Security (TLS) with Network News Transfer Protocol (NNTP)", RFC 8143, DOI 10.17487/RFC8143, April 2017, <<https://www.rfc-editor.org/info/rfc8143>>.
- [RFC8261] Tuexen, M., Stewart, R., Jesup, R., and S. Loreto, "Datagram Transport Layer Security (DTLS) Encapsulation of SCTP Packets", RFC 8261, DOI 10.17487/RFC8261, November 2017, <<https://www.rfc-editor.org/info/rfc8261>>.
- [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/info/rfc8446>>.
- [RFC8447] Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", RFC 8447, DOI 10.17487/RFC8447, August 2018, <<https://www.rfc-editor.org/info/rfc8447>>.

## Благодарности

Спасибо всем, кто представил данные об использовании протоколов, а также рецензентам и тем, кто помог внести улучшения в документ, включая Michael Ackermann, David Benjamin, David Black, Deborah Brungard, Alan DeKok, Viktor Dukhovni, Julien Elie, Adrian Farrell, Gary Gapinski, Alessandro Ghedini, Peter Gutmann, Jeremy Harris, Nick Hilliard, James Hodgkinson, Russ Housley, Hubert Kario, Benjamin Kaduk, John Klensin, Watson Ladd, Eliot Lear, Ted Lemon, John Mattsson, Keith Moore, Tom Petch, Eric Mill, Yoav Nir, Andrei Popov, Michael Richardson, Eric Rescorla, Rich Salz, Mohit Sethi, Yaron Sheffer, Rob Sayre, Robert Sparks, Barbara Stark, Martin Thomson, Sean Turner, Loganaden Velvindron, Jakub Wilk, Christopher Wood.

## Адреса авторов

### Kathleen Moriarty

Center for Internet Security (CIS)

East Greenbush, NY

United States of America

Email: [Kathleen.Moriarty.ietf@gmail.com](mailto:Kathleen.Moriarty.ietf@gmail.com)

### Stephen Farrell

Trinity College Dublin

Dublin

2

Ireland

Phone: +353-1-896-2354

Email: [stephen.farrell@cs.tcd.ie](mailto:stephen.farrell@cs.tcd.ie)

## Перевод на русский язык

Николай Малых

[nmalykh@protokols.ru](mailto:nmalykh@protokols.ru)