Internet Research Task Force (IRTF)
Request for Comments: 9620
Updates: 8280
Category: Informational
ISSN: 2070-1721

G. Grover

N. ten Oever
University of Amsterdam

September 2024

Guidelines for Human Rights Protocol and Architecture Considerations

Рекомендации по правам человека при разработке протоколов и архитектур

Аннотация

В этом документе приведены рекомендации по учёту прав человека при разработке сетевых протоколов и архитектуры, аналогично рекомендациям по учёту приватности (конфиденциальности) в RFC 6973. Документ является обновлением рекомендаций по правам человека, приведённых в RFC 8280.

Документ создан исследовательской группой IRTF Human Right Protocol Considerations (HRPC).

Статус документа

Документ не относится к категории Internet Standards Track и публикуется для информации.

Документ является результатом работы IRTF[1]. IRTF публикует результаты относящихся к Internet исследований и разработок. Эти результаты могут оказаться не пригодными для реализации. Данный RFC представляет согласованное мнение исследовательской группы QIRG в рамках IRTF. Документы, одобренные для публикации IRSG, не претендуют на статус Internet Standard (см. раздел 2 в RFC 7841).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9620.

Оглавление

[1]Internet Research Task Force - комиссия по исследовательским задачам Internet.

1. Введение

В этом документе приведены соображения для разработчиков протоколов, связанные с правами человека. Указаны вопросы, на которые инженерам следует ответить при создании или совершенствовании протоколов, если они хотят понять, как их решения могут повлиять на права человека в Internet. Следует отметить, что влияние протоколов невозможно оценить лишь по их устройству и следует изучить также их реализацию и применение, чтобы полностью оценить влияние на права человека.

Вопросы основаны на исследованиях, выполненных группой Human Rights Protocol Considerations (HRPC) Research Group, которые были документированы до выхода этого документа. Исследования установили, что права человека связаны со стандартами и протоколами, и предоставляют базовый словарь технических понятий, влияющий на права человека, а также способы объединения этих технических понятий для сохранения в Internet благоприятной среды в части прав человека. Это формирует контуры для решения вопросов прав человека в протоколах.

Документ представляет собой итерацию руководств, представленных в [RFC8280]. Методы анализ прав человека (параграф 3.2) и рекомендации по учёту этих прав (параграф 3.3) в данном документе протестированы на предмет актуальности, точности и обоснованности [HR-RT]. Толкование прав человека основано на «Всеобщей декларации прав человека» (Universal Declaration of Human Rights) [UDHR] и последующих соглашениях, которые совместно формируют свод международных законов о правах человека [UNHR].

Документ не содержит подробной классификации характера (возможных) нарушений прав человека (прямых или косвенных, долгосрочных или краткосрочных, которые могут возникать при выборе того или иного протокола. Отчасти это объясняется сильной зависимостью от контекста а также тем, что целью документа является предоставление рекомендаций. Дальнейшие исследования в этой области принесут пользу разработчикам и исполнителям.

Этот информационный документ одобрен для публикации исследовательской группой HRPC в составе IRTF. Документ был рассмотрен, опробован и протестирован исследовательской группой, а также внешними исследователями и практиками. Исследовательская группа признает, что понимание воздействия протоколов и архитектуры Internet на общество ещё не завершено и включает совокупность продолжающихся исследований. Документ не является результатом работы IETF и не задаёт стандартов.

2. Угрозы правам человека

Угрозы реализации прав человека в Internet имеют много форм. Протоколы и стандарты могут наносить ущерб правам на свободу выражения и информации, отсутствие дискриминации, равную защиту, участие в культурной жизни, искусстве и науке, свободу собраний и ассоциаций, безопасность. Конечный пользователь, которому отказано в доступе к неким услугам или содержимому, может оказаться не в состоянии раскрыть важные сведения о недобросовестных действиях правительства или иных органов. Человеку, чьи коммуникации отслеживаются, могут препятствовать в осуществлении его прав на свободу ассоциаций или участие в политических процессах [Penney]. В худшем варианте утечка информации может вызывать физическую опасность. Реалистичным примером являются случаи, когда лица, сочтённые угрозой государству, подвергаются мучениям, внесудебным казням или заключению по стражу на основе сведений, собранных государственными органами путём отслеживания сетевого трафика.

В этом документе приведено несколько примеров реализации угроз правам человека в Internet. Моделирование угроз вдохновлено документом Privacy Considerations for Internet Protocols [RFC6973], основанным на анализе угроз безопасности. Этот метод ещё разрабатывается и не является идеальным для оценки рисков для прав человека в протоколах и системах Internet. Некоторые конкретные угрозы правам человека опосредованно учитываются в протоколах Internet как часть вопросов безопасности [RFC3552], однако соображения приватности [RFC6973], не говоря уже о влиянии протоколов на права человека не стандартизованы и не реализованы.

Многие угрозы, способствующие их возникновению факторы и риски связаны с различными правами. Это неудивительно с учётом взаимосвязанности, взаимозависимости и неделимости прав человека. Однако здесь рассматриваются лишь права человека, связанные с информационными и коммуникационными технологиями (Information and Communication Technologies или ICT) в целом, а также протоколами и стандартами, в частности [Orwat]:

> Основным источником значимости прав человека является «Международный билль о правах человека», состоящий из «Всеобщей декларации прав человека» (UDHR) [UDHR], а также «Международного пакта о гражданских и политических правах (International Covenant on Civil and Political Rights или ICCPR) [ICCPR] и «Международного пакта об экономических, социальных и культурных правах» (International Covenant on Economic, Social and Cultural Rights или ICESCR) [ICESCR]. В свете некоторых фактов цензуры в Internet в 2012 г. была принята резолюция комитета по правам человека ООН (UN Human Rights Council Resolution) 20/8, в которой сказано: « … те же права, которые люди имеют вне сети (offline), должны быть защищены и в сети (online) ...» [UNHRC2016]. В 2015 г. была разработана и опубликована «Хартия прав человека и принципов для Internet (Charter of Human Rights and Principles for the Internet) [IRP] [Jorgensen]. Согласно этим документам, примерами прав человека, связанных с системами ICT, являются человеческое достоинство (ст. 1 UDHR), отсутствие дискриминации (ст. 2), право на жизнь, свободу и безопасность (ст. 3), свобода мнений и их выражения (ст. 19), свобода собраний и ассоциаций (ст. 20), право на равную защиту, правовую защиту, справедливый суд, надлежащее судопроизводство, презумпция невиновности (ст. 7-11), подобающий социальный и международный порядок (ст. 28), участие в общественных делах (ст. 21), участие в культурной жизни, защита интеллектуальной собственности (ст. 27), приватность (ст. 12).

Часть каталога прав человека, связанных с ICT, включая экономически права, приведена в [Hill].

Здесь не предпринимается попыток исключить конкретные права или отдать предпочтение отдельным правам.

3. Обзоры по правам человека

В идеале создателям протоколов и их соавторам следует рассматривать вопросы прав человека в процессе разработки (см. параграф 3.1). В этом разделе приведены рекомендации по выполнению анализа прав человека, т. е. оценке на них протокола или стандарта. Анализ прав человека может выполнять любой участник на разных этапах создания Internet-Draft. Как правило, легче повлиять на разработку технологии на ранних этапах процесса, нежели на более поздних. Это не означает, что рецензии Last Call не имеют значения, но вероятность существенных изменений на их основе будет ниже.

Обзоры прав человека могут выполняться авторами документов, кураторами разработки, членами групп рецензирования, адвокатами и заинтересованными сообществами с целью влияния на процесс разработки стандартов. Документы IETF могут получить пользу от людей с разными знаниями, взглядами и опытом, тем более, что реализация документов может оказывать влияние на множество разных сообществ.

Методы анализа технологий на предмет влияния на права человека ещё только зарождаются. К настоящему моменту группа по анализу прав человека изучила 5 методов, часто применяемых в сочетании друг с другом.

3.1. Анализ Internet-Draft на основе рекомендаций модели

При таком анализе применяется модель, описанная в разделе 4. Описанные категории и вопросы можно применять для рецензирования Internet-Draft. Преимущество этого состоит в предоставлении понятного обзора и авторы документов могут обратиться к этому документу и [RFC8280] для понимания предыстории и контекста.

3.2. Анализ Internet-Draft на основе воздействия

При рассмотрении Internet-Draft конкретное влияние на права человека может стать очевидным при внимательном прочтении документов и попытке понять их воздействие на сети или сообщества. Хотя этот анализ менее структурирован по сравнению с прямым использованием модели рассмотрения прав человека, он может приводить к новому умозрительному пониманию связей между правами человека и протоколами.

3.3. Общение с экспертами

Общение с авторами документов, активными членами рабочей группы или экспертами в предметной области может помочь при изучении характеристик протокола и его влияния. Такой подход обеспечивает два основных преимущества.

1. Возможность рецензента глубже понять (предусмотренную) работу протокола.
2. Возможность рецензента начать обсуждение с экспертами или даже авторами документа, что может помочь в понимании рецензии после её публикации.

3.4. Собеседование с затрагиваемыми лицами и сообществами

Протоколы влияют на пользователей Internet. Собеседования могут помочь рецензентам понять влияние протоколов на использующих их людей. Поскольку права человека лучше всего рассматривать с точки зрения правообладателей, такой подход позволит лучше понять реальные последствия использования технологии. В то же время бывает трудно связать конкретные изменения с определенным протоколом, особенно, если тот не получил широкого распространения.

3.5. Отслеживание влияния реализаций

Реалии развёрнутых протоколов могут отличаться от ожиданий на этапах проектирования и разработки протокола [RFC8980]. Когда для спецификации уже имеется работающий код, его можно проанализировать в среде эксперимента или в Internet, наблюдая влияние протокола. В отличие от рассмотрения текста черновиков, этот подход позволяет рецензенту понять, как спецификации работают на практике и, возможно, обнаружить неизвестные и неожиданные влияния технологии.

4. Рекомендации по вопросам прав человека

В этом разделе приведены рекомендации для авторов документов в форме опросника о протоколах и возможном влиянии технических решений на соблюдение прав человека. Опросник может быть полезен на любом этапе процесса разработки, особенно после того, как авторы создали высокоуровневую модель протокола, как описано в [RFC4101]. Это руководство не стремится заменить какие-либо имеющиеся опорные спецификации, а скорее способствует их развитию и рассматривает процесс разработки с точки зрения прав человека.

Протоколы и стандарты Internet могут выиграть от документированного обсуждения возможных рисков для прав человека, возникающих из-за неправильного применения протокола или технологии, описанных в RFC. Это может быть дополнено заявлением о применимости (Applicability Statement) данного RFC.

Отметим, что представленные в этом разделе рекомендации не задают конкретной практики. Спектр разрабатываемых IETF протоколов слишком широк, чтобы давать рекомендации о конкретном использовании данных или балансе прав человека и других аспектов разработки. Однако тщательное продумывание ответов на приведённые ниже вопросы поможет авторам выполнить всесторонний анализ, который может стать основой для обсуждения адекватности учёта в протоколе конкретных угроз правам человека. Это руководство призвано помочь в процессе анализа прав человека и не содержит конкретных указаний для написания раздела о правах человека (как в примере из [RFC6973]).

При рассмотрении этих вопросов авторы должны учитывать влияние технического прогресса и изменений с течением времени на уровень защиты. В общем случае рассмотрение прав будет, скорей всего, более эффективным при наличии цели и конкретных вариантов применения (в отличие от абстрактных, абсолютных целей).

Хотя в разделе применяется слово «протокол», указанные в вопросах принципы могут применяться и к другим типам решений (расширение имеющихся протоколов, архитектура для решения конкретных задач и т. п.).

4.1. Посредники

Вопросы

Зависит ли протокол от конкретных функций на узлах-посредниках и разрешает ли такие функции?

Пояснения

Принцип сквозной (end-to-end) работы [Saltzer] гласит, что некоторые функции могут выполняться и их следует выполнять на концах сети. В [RFC1958] сказано «в более общем виде сообщество считает, что целью является связность ..., а информация является сквозной, а не спрятанной где-то в сети». При включении в протокол конечных точек и посредников, особенно не находящихся под контролем какой-либо из конечных точек или даже практически невидимых для конечных точек (например, перехватывающие прокси HTTPS [HTTPS-interception]) появляются новые возможности отказов. Это также ведёт к консервативности, поскольку посредники могут задавать ограничения для протоколов (иногда в нарушение спецификации), которые помешают конечным точкам применять более современные протоколы, как описано в параграфе 9.3 [RFC8446].

Отметим, что посредники отличаются от служб. В первом случае сторонний элемент является частью протокольного обмена, а во втором конечные точки явно взаимодействуют со службой. Модель клиент-сервер обеспечивает более чёткое разделение ответственности между элементами, нежели наличие посредников. Однако даже в системах клиент-сервер зачастую полезно обеспечивать сквозное шифрование между конечными точками для элементов протокола, не входящих в сферу действия службы, как это сделано в Messaging Layer Security (MLS) [RFC9420].

Пример

Шифрование между конечными точками можно применять для защиты протокола от воздействия посредников. Примерами являются шифрование информации транспортного уровня в QUIC [RFC9000] и поле индикации имени сервера TLS (Server Name Indication или SNI) [TLS-ESNI]. Одним из следствий этого является ограничение возможности инспектирования трафика операторами сети, в случае шифрования оператору для отслеживания поведения потребуется контроль над ними.

Влияние

- Право на свободу выражения.
- Право на свободу собраний и ассоциаций

4.2. Связность

Вопросы

Оптимизирован ли протокол для соединений с малой пропускной способностью и высокой задержкой? Может ли протокол работать без поддержки состояний (stateless)?

С учётом изменения качества и условий в сети в зависимости от места и времени важно разрабатывать протоколы так, чтобы они были надёжными даже для соединений с малой пропускной способностью и высокой задержкой.

Влияние

- Право на свободу выражения
- Право на свободу собраний и ассоциаций

4.3. Надёжность

Вопросы

Устойчив ли протокол к отказам? Имеются ли механизмы аккуратного «отката» (downgrade) и/или уведомления? Может ли протокол противостоять злонамеренным попыткам сокращения возможностей (degradation)? Имеется ли документированный способ информирования о сокращении возможностей? Имеются ли средства (меры) восстановления или частичного исправления при отказе? Может ли протокол обеспечивать надёжность и производительность при непредвиденных изменениях или обстоятельствах?

Пояснения

Надёжность и отказоустойчивость гарантируют, что протокол будет выполнять свои функции согласованно и устойчиво к ошибкам (как описано), не приводя к неожиданным результатам. Меры обеспечения надёжности в протоколах гарантируют пользователям успешное выполнение желаемых коммуникаций.

Надёжная система сокращает свои возможности (деградирует) аккуратно и имеет документированные средства информирования об этом. Она также будет обеспечивать механизмы аккуратного восстановления после отказов и, по возможности, поддерживать частичное восстановление. Важно отличать случайное сокращение возможностей от злонамеренного. Например, некоторые атаки на прежние версии TLS использовали способность TLS аккуратно переходить к менее стойким шифрам [FREAK] [Logjam], что полезно с точки зрения функциональности, но может быть катастрофическим в плане безопасности.

Для надёжности требуется, чтобы службы уведомляли пользователей об отказах при доставке. В системах, работающих в реальном масштабе времени, протокол также должен обеспечивать своевременную доставку.

Пример

В структуре современного стека IP надёжный транспортный уровень требует индикации успешного завершения транспортной обработки, такой как сообщения TCP ACK [RFC9293]. Протокол прикладного уровня может требовать зависящий от приложения подтверждений, содержащих код состояния, указывающий статус обработки запроса (см. [RFC3724]).

Влияние

- Право на свободу выражения
- Право на безопасность (защиту)

4.4. Распознавание содержимого

Вопросы

Включает ли протокол явные или неявные открытые (plaintext) элементы, которые можно использовать для дифференцированной трактовки? Имеется ли возможность минимизировать утечку таких данных сетевым посредникам? При отсутствии такой возможности имеется ли при внедрении протокола возможность сделать дифференцированную обработку (включая приоритизацию определённого трафика), если таковая имеется, проверяемой на предмет негативного влияния не сетевой нейтралитет?

Пример

Когда сетевые посредники могут определить тип содержимого передаваемых пакетов, они могут воспользоваться этими сведениями для дискриминации одного типа содержимого в пользу другого. Это влияет на возможности пользователей передавать и принимать желаемое содержимое.

Как рекомендовано в [RFC8558], разработчикам протоколов следует избегать конструкций в неявной индикацией содержимого. В общем случае разработчикам следует избегать явных индикаторов содержимого для посредников. Иногда может возникать необходимость в добавлении таких явных индикаторов, но применять их следует лишь в случае уверенности разработчиков в их явной пользе для конечных пользователей (приоритеты пользователей более подробно рассмотрены в [RFC8890]). В таких случаях следует документировать влияние таких сигналов на права человека.

Отметим, что многие протоколы предоставляют предназначенные для конечных точек сигналы, которые посредники могут использовать как неявные индикаторы для разделения трафика по содержимому (например, номер порта TCP) или отправителям/получателям (адреса IP). По возможности следует использовать шифрование для защиты от посредников. Во многих случаях трудно скрыть сигналы (например, адреса IP), но в таких случаях, как TLS Application Layer Protocol Negotiation [RFC7301], предпринимаются усилия по защите данных [TLS-ESNI].

Влияние

- Право на свободу выражения
- Право на недискриминацию
- Право на равную защиту

4.5. Поддержка разных языков

Вопросы

Поддерживает ли протокол или спецификация задание в содержимом или заголовках строковых элементов, которые должны быть поняты или введены человеком? Поддерживает ли спецификация кодировку Unicode? Если эта кодировка поддерживается, принимается ли только UTF-8 или также другие кодировки (может быть опасно в плане совместимости)? Если разрешены кодировки, отличные от UTF-8, требует ли спецификация корректного указания набора символов? Знакомы ли вы с [RFC6365]?

Пояснения

Поддержка разных языков (internationalization) позволяет создавать протоколы, стандарты и реализации, пригодные для использования с различными языками и шрифтами (см. параграф 4.6). В IETF это означает добавление или улучшение обработки в протоколе текстов, отличных от ASCII [RFC6365]. Другая точка зрения, более подходящая для протоколов, изначально предназначенных для глобального применения, используется в определении World Wide Web Consortium (W3C) [W3Ci18nDef]:

> Интернационализация - это проектирование и разработка продукции, приложений и документов, позволяющая легко приспособить (localization) их для целевой аудитории, религии или языка.

Многие протоколы, работающие с текстом, используют лишь одну кодировку (US-ASCII) или оставляют выбор применяемой кодировки и набора символов пользователю (что, безусловно, ведёт к проблемам совместимости). Если поддерживается несколько кодировок, требуется явное указание применяемой [RFC2277]. Добавление в протокол отличного от ASCII текста позволяет обрабатывать большее число текстов, которые, как можно надеяться, представляют пользователей по всему миру. Сегодня это лучше всего обеспечивать за счёт поддержки кодировки Unicode UTF-8.

В современной практике IETF [RFC2277] поддержка разных языков нацелена на обращённые к пользователю строки, а не на элементы протокола, такие как используются в некоторых текстовых протоколах (следует отметить, что некоторые строки, например, идентификаторы, являются одновременно содержимым и элементами протокола). Хотя это разумно для элементов, не видимых пользователю, разработчикам следует обеспечивать полную и равную поддержку всех текстов и кодировок в ориентированных на пользователя функциях протокола, а также любом содержимом, которое передаётся.

Пример

См. параграф 4.6.

Влияние

- Право на свободу выражения
- Право на участие в политической жизни
- Право на участие в культурной жизни, искусстве и науке

4.6. Локализация

Вопросы

Поддерживает ли протокол стандарты интернационализации? Сделаны ли какие-либо шаги в направлении локализации протокола для соответствующей аудитории?

Пояснения

«Локализация - это адаптация продукции, приложения или содержимого документов в соответствии с требованиями языка, культуры и т. д. конкретного целевого рынка (locale)» [W3Ci18nDef]. Для целей документа локализацию можно описать как перевод реализации для обеспечения функциональности на конкретном языке или для пользователей с определёнными локальными настройками (см. параграф 4.5). Интернационализация связана с локализацией, но не совпадает с ней. Поддержка разных языков является необходимым условием локализации.

Пример

Internet является глобальной средой, но многие протоколы и продукция разработаны с учётом интересов некой аудитории, которая часто обладает определёнными свойствами, например, умеет читать и писать в кодировке стандартного американского кода обмена информацией (American Standard Code for Information Interchange или ASCII) и знает английский язык. Это ограничивает возможности значительной части мирового сетевого сообщества использовать Internet так, чтобы сеть была доступна с точки зрения языка и культуры. Пример стандарта, учитывающего мнение о том, что люди хотят иметь доступ к данным, на предпочтительном для них языке, содержится в [RFC5646], где описан способ маркировки информации с помощью языковых тегов. Это позволяет представлять информацию и получать доступ к ней на нескольких языках.

Влияние

- Право на недискриминацию
- Право на участие в культурной жизни, искусстве и науке
- Право на свободу выражения

4.7. Открытые стандарты

Вопросы

Документирован ли протокол полностью так, чтобы его можно было легко реализовать, улучшить, развить или продолжить его разработку? Требуется ли фирменный (proprietary) код для реализации, работы или дальнейшего развития протокола? Отдаёт ли протокол предпочтение своей спецификации перед технически эквивалентами конкурирующих спецификаций, например, делая встроенную спецификацию производителя требуемой или рекомендуемой [RFC2026]? Имеются ли ссылки на другие стандарты, которые требуют оплаты (можно ли обойтись без неё)? Известны ли какие-либо патенты, препятствующие полной реализации стандарта [RFC8179] [RFC6701]?

Пояснения

Сеть Internet смогла стать глобальной сетью сетей благодаря наличию открытых, не патентованных (non-proprietary) стандартов [Zittrain], которые имеют решающее значение для функциональной совместимости. Однако открытые стандарты не определены явно в рамках IETF. По этому поводу в [RFC2026] сказано:

> Различные национальные и международные организации (такие, как ANSI, ISO, IEEE, ITU-T) разрабатывают многочисленные спецификации протоколов и услуг, подобные определенным здесь [в IETF] техническим спецификациям (Technical Specifications). Национальные и международные группы также публикуют «соглашения разработчиков», аналогичные определенным здесь заявлениям о применимости (Applicability Statement) и содержащие детали зависящих от реализации практических применений своих стандартов. В рамках процесса стандартизации Internet все эти документы рассматриваются, как открытые внешние стандарты (open external standards).

В [RFC3935] также нет определения открытых стандартов, но подчёркнута важность «открытого процесса»:

> ... любое заинтересованное лицо может участвовать в работе, знать, что решается, и высказывать [своё] мнение по данному вопросу.

Открытые стандарты (и программы с открытым кодом) позволяют пользователям собирать сведения о работе применяемых инструментов, включая их свойства в части безопасности и приватности. Они также позволяют совершенствования без получения разрешений, что важно для поддержки свободы и возможности свободно создавать и внедрять новые протоколы в имеющихся коммуникационных конструкциях. Это основа Internet с современном состоянии и для сохранения открытости требуется помнить о необходимости разработки открытых стандартов.

Все стандарты, требующие реализации, следует делать доступными свободно и обеспечивать им разумную защиту от патентных претензий, чтобы эти стандарты можно было реализовать в программах с открытым кодом или бесплатных программах. Патенты зачастую сдерживают открытую стандартизацию или используются против тех, кто внедряет открытые стандарты, особенно в сфере криптографии [Newegg]. Иногда делаются исключения, если стандартизованный протокол нормативно полагается на спецификации, разработанные другими органами стандартизации (Standards Development Organization или SDO), к которым нет свободного доступа. Патентам в открытых стандартах и нормативных ссылках на другие стандарты следует содержать раскрытие [Note-well], бесплатное лицензирование [Patent-policy] или иной вариант разумных, справедливых и недискриминационных условий.

Пример

В [RFC6108] описана система предоставления критических уведомлений конечным пользователям web-браузеров, которая была внедрена провайдером (Internet Service Provider или ISP) Comcast. Такая система уведомлений служит для практически мгновенного информирования клиентов, например, о том, что их трафик имеет поведение, характерное для наличия вредоносного кода или заражения вирусом. Имеются и другие фирменные системы, поддерживающие такие уведомления, но в них применяется технология глубокой проверки пакетов (Deep Packet Inspection или DPI). В упомянутом документе описана система, не использующая DPI и основанная на открытых стандартах IETF и приложениях с открытым исходным кодом.

Влияние

- Право на свободу выражения
- Право на участие в культурной жизни, искусстве и науке

4.8. Поддержка неоднородности

Вопросы

Поддерживает ли протокол неоднородность (гетерогенность) по своему устройству? Позволяет ли протокол использовать несколько типов оборудования? Разрешает ли протокол использовать несколько типов прикладных протоколов? Насколько строг протокол в отношении того, что он принимает и обрабатывает? Останется ли протокол пригодным для использования и открытым при смене контекста?

Пояснения

Сеть Internet является неоднородной на многих уровнях - устройства, узлы, алгоритмы планирования в маршрутизаторах, механизмы управления очередями, протоколы маршрутизации, уровни мультиплексирования, версии и реализации протоколов, базовые канальные уровни (например, «точка-точка», каналы с множественным доступом, FDDI и т. п.) в картине трафика и уровнях перегрузки в разное время в разных местах. Кроме того, Internet состоит из автономных организаций и ISP со своими интересами, поэтому имеется значительная неоднородность административных доменов и структур ценообразования. В результате при проектировании требуется поддерживать [FIArch] принципы неоднородности, предложенные в [RFC1958]. Таким образом, поддержка неоднородности протоколом может позволить широкому кругу устройств и (как следствие) пользователей участвовать в работе сети.

Пример

Поддержка неоднородности оказала существенное влияние на успех архитектуры Internet [Zittrain]. Есть знаменитая цитата, часто приписываемая Нильсу Бору: «Предсказывать очень трудно, особенно, когда речь идёт о будущем.» Это справедливо и для будущего архитектуры и инфраструктуры Internet. Поэтому, как правило, важно, насколько это возможно, разрабатывать протоколы для разных устройств и приложений, особенно на нижних уровнях стека. Если же это не делается, следует описать причины такого решения в соответствующем документе.

Влияние

- Право на свободу выражения
- Право на участие в политической жизни

4.9. Адаптивность

Вопросы

Является ли протокол модульным, возможно ли расширение протокола? Влияет ли в этом смысле протокол на инновации без получения разрешения? (см. параграф 4.7)

Пояснения

Адаптивность тесно связана с инновациями без получения разрешений - то и другое поддерживают возможность и свободу создания и внедрения новых протоколов на основе имеющихся коммуникационных конструкций. Это является основой Internet и для сохранения фундаментальной открытости требуется учитывать влияние протоколов на поддержание или сокращение инноваций без получений разрешений на них, чтобы обеспечить дальнейшее развитие Internet.

Адаптивность и инновации без разрешений можно применять для формирования информационных сетей в соответствии с предпочтениями групп пользователей. Более того, предварительным условием для адаптивности является способность людей приспособить (адаптировать) сеть, знать и понимать её. Именно поэтому адаптивность и инновации без согласования неразрывно связаны с правами на образование и науку, а также правом на свободу собраний и ассоциаций, поскольку они позволяют пользователям сети самим решать, как им собираться, сотрудничать и выражать своё мнение.

Пример

WebRTC генерирует голосовые и/или визуальные (видео) данные и может использоваться в разных местах различными сторонами. Разработаны стандартные интерфейсы прикладных программ (Application Programming Interface или API) для поддержки приложение от различных поставщиков голосовых услуг. Разные участники (стороны) получают близкие возможности. Чтобы все стороны могли опираться на имеющиеся стандарты, эти стандарты должны быть адаптивными и должны позволять инновации без специального разрешения.

Влияние

- Право на обучение
- Право на науку
- Право на свободу выражения
- Право на свободу собраний и ассоциаций

4.10. Целостность

Вопросы

Обеспечивает ли протокол поддержку, гарантию и/или проверку целостности данных в содержимом? Обеспечивает ли протокол поддержку и гарантии согласованности данных? Позволяет ли протокол (преднамеренно или нечаянно) изменить данные?

Пояснения

Целостностью называют поддержку и гарантии точности и согласованности данных, чтобы их невозможно было изменить (преднамеренно или нечаянно).

Пример

Проверка целостности важна для предотвращения уязвимостей и атак от злоумышленников на пути данных. Такие атаки происходят, когда посторонние лица (часто по злонамеренным причинам) перехватывают коммуникации между двумя сторонами, внедряясь в процесс и меняя содержимое данных. На практике это выглядит так:

> Алиса хочет взаимодействовать с Бобом и передаёт ему сообщение, которое Корин перехватывает и изменяет. Боб не может знать о перехвате и изменении сообщения Корин. Сообщения между Алисой и Бобом могут перехватываться и изменяться Корин, обеспечивая контроль содержимого при обмене информацией.

Влияние

- Право на свободу выражения
- Право на безопасность (защиту)

4.11. Подлинность

Вопросы

Достаточны ли меры подтверждения подлинности отдельной атрибутов части данных или сущности (объекта)? Могут ли атрибуты быть искажены в пути (см. параграф 4.13)? Применяется ли стандарт защиты IPsec, DNS Security (DNSSEC), HTTPS и т. п., если это уместно?

Пояснения

Аутентичность говорит о получении данных из того источника, который заявлен. Это важно для предотвращения некоторых атак и несанкционированного доступа к данным и использования их. Проверку подлинности не следует применять для препятствования поддержке гетерогенности, как это зачастую делается для блокировки отдельных производителей или управления цифровыми правами.

Пример

Аутентификация данных важна для предотвращения уязвимостей и атак в пути доставки. Такие атаки происходят, когда посторонние перехватывают (зачастую с враждебными целями) коммуникации между двумя сторонами, внедряясь в них и выдавая себя за обе стороны. На практике это выглядит так:

> Алиса хочет взаимодействовать с Бобом и передаёт ему сообщение, которое Корин перехватывает (и может изменять). Боб не может знать, что данные поступили от Корин, а не от Алисы.

При надлежащей аутентификации сценарий может выглядеть, как показано ниже.

> Алиса хочет взаимодействовать с Бобом и передаёт ему сообщение. Корин перехватывает данные, направленные Бобу. Корин читает и изменяет направленное Бобу сообщение. Боб не может проверить, поступили ли данные от Алисы.

Влияние

- Право на приватность
- Право на свободу выражения
- Право на безопасность (защиту)

4.12. Конфиденциальность

Вопросы

Раскрывает ли протокол передаваемые в линию данные? Раскрываются ли сведения, связанные с идентификаторами или данными? Если да, то что раскрывается каждому элементу протокола (получателям, посредникам, организаторам) [RFC6973]? Какие возможности предоставляются разработчикам для ограничения

сведений, раскрываемых каждому элементу? Какие средства оперативного контроля доступны для ограничения сведений, передаваемых каждому объекту?

Какие механизмы контроля или согласования определяет или требует протокол до передачи или раскрытия персональных данных или идентификаторов? При отсутствии таких механизмов и элементов управления предполагаются ли внешние механизмы контроля или согласования?

Предусмотрены ли в протоколе возможности передачи инициатором разных частей информации разным получателям? Если нет, существуют ли внешние механизмы для такой дифференциации?

Предусматривает ли протокол средства для ограничения обмена информацией или выражения индивидуальных предпочтений в части сбора, использования или раскрытия персональных данных? Если нет, имеются ли внешние механизмы, предоставляющие пользователям такой контроль? Предполагается ли, что пользователи поддерживают отношения (соглашения или иные способы), регулирующие использование информации сторонами, которые управляют посредниками? Предпочитает ли протокол использовать шифрование, а не открытые данные?

Пояснения

Конфиденциальность означает сохранение данных в тайне от непредусмотренных лиц [RFC3552]. Рост Internet зависит от уверенности пользователей в защите сетью их персональных данных [RFC1984]. Возможность повсеместного мониторинга и наблюдения подрывает доверие пользователей и может быть снижена за счет гарантий конфиденциальности, т. е. пассивные атакующие не смогут получить информации (или получат очень мало сведений) из своих наблюдений и выводов об активности протоколов [RFC7258] [RFC7624].

Пример

Протоколы, не шифрующие содержимое, делают сообщения доступными для идеализированного злоумышленника на пути. В соответствии с [RFC3365] большинство таких протоколов имеет защищённый вариант с шифрованием содержимого для обеспечения конфиденциальности и такие варианты применяются все шире. Примечательным исключением является протокол DNS [RFC1035], поскольку DNSSEC [RFC4033] не включает требований конфиденциальности. Это означает, что без применения более современных стандартов, таких как DNS через TLS [RFC7858] или HTTPS [RFC8484], все запросы и отклики DNS, создаваемые при работе любого протокола, будут доступны злоумышленникам. При использовании протоколов пересылки с промежуточным хранением (store-and-forward, например, SMTP [RFC5321]) посредники оставляют сохранённые данные доступными для взломавших посредника злоумышленников, если только не применяется сквозное шифрование данных в протоколах прикладного уровня или реализация не помещает данные в шифрованное хранилище [RFC7624].

Влияние

- Право на приватность
- Право на безопасность (защиту)

4.13. Безопасность

Вопросы

Знакомы ли вы с «Руководством по написанию текста RFC по вопросам безопасности» [RFC3552]? Обнаружены ли какие-либо атаки, в той или иной степени связанные с протоколом (спецификацией), но считающиеся выходящими за рамки этого документа? Относятся ли эти атаки к свойствам Internet, связанным с правами человека (как описано в этом документе)?

Пояснения

Безопасность не является монолитным свойством протокола или системы, а скорее состоит из ряда связанных, но в определённой степени независимых свойств. Не все эти свойства нужны каждому приложению. Поскольку взаимодействия происходят между системами, а доступ к этим системам осуществляется по каналам связи, цели безопасности очевидно будут взаимосвязанными, но могут быть достигнуты независимыми путями [RFC3552].

Обычно любой протокол, применяемый в Internet, может стать целью пассивных (злоумышленник имеет доступ в сеть и способен просматривать пакеты) и активных (злоумышленник способен осуществлять запись в пакеты) атак [RFC3552].

Пример

См. [RFC3552].

Влияние

- Право на свободу выражения
- Право на свободу собраний и ассоциаций
- Право на недискриминацию
- Право на безопасность (защиту)

4.14. Приватность

Вопросы

Ознакомились ли вы с рекомендациями раздела 7 «Вопросы приватности для протоколов Internet» [RFC6973]? Поддерживает ли протокол конфиденциальность метаданных? Может ли протокол противостоять анализу трафика? Придерживается ли протокол принципам минимизации данных? Указаны ли в документе потенциально чувствительные данные, записываемые (log) протоколов и как долго их нужно хранить по техническим причинам?

Пояснения

Приватность относится к праву субъекта (обычно человека), действующего от своего имени, определять степень взаимодействия с окружением, включая уровень готовности делиться своей персональной информацией с другими [RFC4949]. Если протокол не обеспечивает достаточной защиты приватности, он может негативно влиять на свободу выражения, поскольку пользователи будут применять самоцензуру, опасаясь слежки, или сочтут невозможным свободное выражение своего мнения.

Пример

См. [RFC6973].

Влияние

- Право на свободу выражения
- Право на приватность
- Право на недискриминацию

4.15. Анонимность и псевдонимы

Вопросы

Использует ли протокол идентификаторы? Являются ли идентификаторы постоянными? Применяются ли идентификаторы в разном контексте? Может ли пользователь сбросить или поменять идентификатор без негативного влияния на работу протокола? Видны ли идентификаторы за пределами конечных точек протокола? Связаны ли они с идентификаторами из реального мира? Рассматривался ли документ «Вопросы приватности для протоколов Internet» [RFC6973], особенно параграф 6.1.2?

Пояснения

Большинство протоколов зависит от использования тех или иных идентификаторов для сопоставления действий в пространстве и времени, например:

- адреса IP служат для идентификации отправителей и получателей дейтаграмм IP;
- идентификаторы соединений QUIC служат для распознавания пакетов, относящихся к соединению;
- в HTTP применяются cookie для сопоставления запросов HTTP с клиентом;
- в электронной почте применяются адреса вида example@example.com для указания отправителей и получателей.

В общем случае такие идентификаторы выполняют функции, требуемые для работы протокола, однако они могут вносить риск для приватности. Этот риск проявляется в основном двумя способами.

- Идентификатор может сам раскрывать личность пользователя, как в случае применения (телефонных) номеров E.164 в системах мгновенного обмена сообщениями.

- Идентификатор может не раскрывать пользователя, но позволять собрать достаточно подробные сведения о его поведении, чтобы поставить под угрозу его приватность, как в случае с HTTP cookie.

Поскольку идентификаторы нужны для работы протоколов, полной анонимности достигнуть сложно, но имеются методы, способствующие сохранению приватности пользователей даже при наличии идентификаторов.

Влияние

- Право на недискриминацию
- Право на свободу выражения
- Право на участие в политической жизни
- Право на свободу собраний и ассоциаций

4.15.1. Псевдонимы

В общем случае для повышения уровня приватности в качестве идентификаторов применяются псевдонимы, не связанные с отождествлением пользователей в реальном мире.

Пример

При разработке протокола IPv6 рассматривался вопрос встраивания адреса канального уровня (Media Access Control или MAC) в уникальный адрес IP. Это позволило бы прослушивающим трафик и другим сборщикам сведений сопоставлять адреса из разных транзакций с конкретными узлами. По этой причине были предприняты усилия по стандартизации, такие как «Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6» [RFC8981] и рандомизация адресов MAC [MAC-ADDRESS-RANDOMIZATION].

Отметим, что зачастую представляется привлекательным создание псевдонимов из постоянных идентификаторов. Очень сложно сделать это так, чтобы невозможно было раскрыть такой постоянный идентификатор.

Пример

Распространённой практикой web-отслеживания является «шифрование» адресов электронной почты путём их хэширования, что якобы делает адреса не связанными с персональным идентификатором. Однако функции хэширования являются общедоступными и можно провести поиск по словарю возможных адресов и найти исходный адрес электронной почты [Email-hashing].

4.15.2. Невозможность привязки

Даже тщательно подобранные идентификаторы-псевдонимы могут представлять риск для приватности, если они применяются достаточно широко. Приватность пользователей обеспечивается лучше, если область действия идентификаторов ограничена как в пространстве, так и во времени.

Пример

Примером является протокол динамической настройки хостов (Dynamic Host Configuration Protocol или DHCP), где передача постоянного идентификатора в качестве имени клиента не была обязательной и на практике многие реализации делали это ещё до появления DHCP [RFC7844].

Пример

Сторонние cookie кв HTTP позволяют отслеживающим сопоставлять трафик HTTP с разными сайтами. Это является основой целой системы web-отслеживания. Браузеры web все чаще ограничивают использование сторонних cookie для защиты приватности пользователей.

4.16. Стойкость к цензуре

Вопросы

Способствует ли цензуре архитектура протокола? Включает ли она специальные точки (choke point), которые легко применить для цензуры? Раскрываются ли идентификаторы, которые можно использовать для селективной блокировки некоторых видов трафика? Можно ли сделать протокол более стойким к цензуре? Раскрывает ли протокол ограничения доступа к ресурсам и причины таких ограничений?

Пояснения

Правительства и поставщики услуг блокирует или фильтруют содержимое или трафик, зачастую в тайне от конечных пользователей [RFC7754]. Обзор применяемых методов цензуры приведён в [RFC9505], где описаны свойства протоколов, используемые для цензуры доступа к информации. Стойкость к цензуре относится к методам и мерам предотвращения цензуры в Internet.

Пример

В современной структуре Web имеется ряд архитектурных точек, допускающих вмешательство цензоров. Это включает получение контроля над доменным именем, блокировку DNS на уровне протокола или распознавателей,

блокировку адресов IP и блокировку web-серверов. Ведётся активная работа по системам распространения содержимого, которые предполагаются более стойкими к цензуре, и некоторые из таких систем (например, BitTorrent) получили широкое распространение. Однако эти системы могут обладать меньшей надёжностью и производительностью по сравнению с Web (например, не поддерживают активное содержимое на серверах).

Пример

Идентификаторы содержимого, раскрываемые в протоколе, могут применяться для облегчения цензуры, позволяя цензорам определять, какой трафик блокировать. Запросы DNS, заголовки host в запросах HTTP и индикация имён серверов (Server Name Indication или SNI) в ClientHello протокола TLS являются примерами протокольных элементов, которые передаются в открытом виде и применяются цензорами для идентификации содержимого, к которому пользователь пытается получить доступ [RFC9505]. Механизмы вроде Encrypted ClientHello [TLS-ESNI] и DNS через HTTPS [RFC8484], которые шифруют метаданные, обеспечивают некоторую стойкость к этому типу инспекции протоколов. Для доступа к подвергаемым цензуре ресурсам могут также применяться системы с полным шифрованием трафика, такие как Tor <https://torproject.org>.

Пример

Как отмечено выше, одним из способов цензуры web-трафика является требование к серверам блокировать трафик или требование к ISP блокировать запросы к серверам. В HTTP отказ или ограничение доступа могут быть замечены в результате возврата кода состояния 451, который позволяет операторам серверов и посредникам более прозрачно выполнять операции в условиях, когда на их работу оказывают влияние законы или политика государств [RFC7725]. Если протокол потенциально допускает цензуру, разработчикам следует стремиться к заданию кодов ошибок, отражающих различные варианты (например, блокировку по административным правилам, недоступность в соответствии с законом и т. п.) для минимизации двусмысленности на стороне пользователей.

Влияние

- Право на свободу выражения
- Право на участие в политической жизни
- Право на участие в культурной жизни, искусстве и науке
- Право на свободу собраний и ассоциаций

4.17. Понимание результатов

Вопросы

Документированы ли предполагаемые влияния протокола и понятны ли они? Описаны ли основные варианты применения протокола с чётким указанием ожидаемого поведения и возможного влияния на другие протоколы, реализации, ожидания и поведение пользователей? Рассмотрены ли другие протоколы, решающие сходные задачи или использующие похожие механизмы, чтобы понять, можно ли извлечь уроки из их применения?

Пояснения

Некоторые технические решения могут приводить к непредвиденным последствиям.

Пример

Отсутствие проверки подлинности может приводить к нарушению целостности и негативным последствиям, например, к возможности спама. Отсутствие данных, которые можно использовать для учёта и выставления счетов, могут приводить к «бесплатным» соглашениям, когда скрываются фактические расходы и их распределение. Примерами являются бартерные соглашения на межоператорских соединениях Internet и коммерческое использование персональных данных для целевой рекламы, которое является наиболее распространённой моделью для так называемых «бесплатных» услуг поисковых машин и социальных сетей. Неожиданные результаты могут оказаться не техническими, а архитектурными, социальными или экономическими, поэтому важно документировать ожидаемые результаты и другие возможные последствия.

Влияние

- Право на свободу выражения
- Право на приватность
- Право на свободу собраний и ассоциаций
- Право на доступ к информации

4.18. Доступность

Вопросы

Предназначен ли протокол для обеспечения благоприятной среды для всех? Обращались ли разработчики к W3C Web Accessibility Initiative за примерами и рекомендациями [W3CAccessibility]?

Пояснения

Иногда при разработке протоколов, web-сайтов, web-технологий и инструментов создаются барьеры, препятствующие людям в использовании Web. Internet следует организовывать так, чтобы все люди, независимо от их оборудования, программ, языка, культуры, физических и умственных возможностей, могли пользоваться сетью. При соответствии технологий Internet этим целям сеть станет доступной для людей с разными возможностями слуха, зрения, подвижности, а также разными познавательными (когнитивными) возможностями [W3CAccessibility].

Пример

Протокол HTML, определённый в [HTML], требует, чтобы каждое изображение (с некоторыми исключениями) имело атрибут alt, чтобы изображения были доступны для людей, не способных самостоятельно разобраться с нетекстовым содержимым web-страниц.

Другим примером может служить работа групп AVT и AVTCORE в IETF по прочтению текста в multimedia, текстовой телефонии, беспроводным системам multimedia, и видеосвязи для языка жестов и чтения по губам (см. [RFC9071]).

Влияние

- Право на недискриминацию
- Право на свободу собраний и ассоциаций
- Право на обучение
- Право на участие в политической жизни

4.19. Децентрализация

Вопросы

Можно ли реализовать протокол без единой точки контроля? Можно ли, если это применимо, развернуть протокол федеративным образом? Создаёт ли протокол дополнительные централизованные точки контроля?

Пояснения

Децентрализация является одной из основных технических концепций Internet и принята в таком качестве IETF [RFC3935]. Это означает отсутствие или минимизацию централизованных точек управления, что, как предполагается, упростит присоединение новых пользователей и использование новых возможностей [Ziewitz]. Децентрализация также смягчает проблемы, связанные с критическими точками отказа и обеспечивает функционирование сети даже при отключении одного или нескольких узлов. С коммерциализацией Internet в начале 1990-х годов начался медленный отход от децентрализации в ущерб техническим преимуществам децентрализованной сети Internet. Более подробно этот вопрос рассматривается в [Arkko].

Пример

Данные (биты), передаваемые через Internet, становятся все более чувствительными к отслеживанию и цензуре со стороны правительств и ISP, а также третьих лиц (злоумышленников). Возможности мониторинга и цензуры становятся более доступными с ростом централизации в сети, создающей централизованные точки для подключения. Создание одноранговых сетей и разработка протоколов передачи голоса по IP (voice-over-IP) с использованием одноранговой технологии в сочетании с распределенными хэш-таблицами (Distributed Hash Table или DHT) для масштабируемости является примером сохранения децентрализации [Pouwelse].

Влияние

- Право на свободу выражения
- Право на свободу собраний и ассоциаций

4.20. Правовая защита

Вопросы

Может ли протокол способствовать реализации прав стороны, подвергшейся негативному воздействию, средствами правовой защиты без непропорционального ущемления прав других сторон (особенно в части их прав на приватность)?

Пояснения

Предоставление государствам и корпорациям доступа к средствам защиты является частью Руководящих принципов ООН для предпринимательской деятельности в аспекте прав человека (UN Guiding Principles on Business and Human Rights) [UNGP]. Доступ к средствам правовой защиты может способствовать жертвам нарушений прав человека в достижении справедливости или позволить правоохранительным органам установить личность возможного нарушителя. Однако имеющиеся в протоколах механизмы, пытающиеся разрешить «атрибутирование» отдельных лиц, препятствуют осуществлению права на приватность. Бывший специальный докладчик ООН по вопросам свободы выражения мнений (UN Special Rapporteur for Freedom of Expression) утверждал, что анонимность является неотъемлемой частью свободы выражения мнений [Kaye]. С учётом возможного влияния атрибутирования на право на приватность и свободу выражения мнений возможность атрибутирования на уровне отдельных лиц скорей всего не будет соответствовать правам человека.

Пример

Добавление идентифицирующих лицо сведений в потоки данных для реализации прав человека на правовую защиту может способствовать выявлению нарушителей прав человека и обеспечить доступ к средствам правовой защиты, но может оказывать непропорциональное влияние на право на приватность, анонимность выражения и участие в ассоциациях других пользователей. Кроме того, в последнее время были достигнуты успехи в части выявления злоупотреблений в системах обмена со сквозным шифрованием, с которыми также связан определённый риск нарушения приватности пользователей [Messenger-franking] [Hecate].

Влияние

- Право на правовую защиту (возмещение)
- Право на безопасность (защиту)
- Право на приватность

4.21. Прочие вопросы

Вопросы

Рассмотрены ли возможные негативные последствия внедрения протокола или документа на отдельных лиц и общество?

Пояснения

Публикация RFC с определенным статусом имеет последствия. Публикация в качестве Internet Standard как часть Standards Track может говорить об определённой зрелости спецификации, опыте её внедрения и согласия на применение. Публикация в качестве экспериментального документа в рамках Standards Track будет указывать сообществу, что документ «может быть не рассчитан на применение как Internet Standard или предназначен для будущей стандартизации, но ещё не готов» для широкого внедрения [RFC2026]. Область внедрения и, следовательно, суммарное влияние на конечных пользователей могут зависеть от статуса документа, указанного в RFC. Более полное описание приведено в [RFC2026] и дополнениях к этому документу.

5. Статус документа

В этом документе исследовательской группы представлен опыт и рекомендации в части экспертизы влияния на права человека сетевых протоколов, архитектур и других документов Internet-Draft и RFC.

6. Вопросы безопасности

Третья статья Всеобщей декларации прав человека гласит: «Каждый человек имеет право на жизнь, свободу и личную неприкосновенность» [UDHR]. В этой статье подчёркнута важность безопасности и её связь с жизнью и свободой человека, а, поскольку права человека неделимы, взаимосвязаны и взаимозависимы, безопасность человека тесно связана с другими правами и свободами. Данный документ нацелен на укрепление прав человека, его свободы и безопасности путём сопоставления и трансляции этих концепций в концепции и практику при разработке протоколов и архитектуры Internet. Целью является соблюдение прав человека и соответствующее повышение устойчивости, эффективности и удобства использования сети. Документ стремиться достигнуть поставленных целей путём предоставления руководящих принципов в разделе 3.

7. Взаимодействие с IANA

Этот документ не предполагает действий IANA.

8. Сведения об исследовательской группе

Дискуссионная конференция исследовательской группы IRTF Human Rights Protocol Considerations доступна по адресу <mailto:hrpc@ietf.org>. Сведения о группе и способах подписки на рассылки доступны по ссылке <https://www.irtf.org/mailman/listinfo/hrpc>, архивы почтовой конференции - по ссылке <https://mailarchive.ietf.org/arch/browse/hrpc/>.

9. Литература

[Arkko] Arkko, J., Trammell, B., Nottingham, M., Huitema, C., Thomson, M., Tantsura, J., and N. ten Oever, "Considerations on Internet Consolidation and the Internet Architecture", Work in Progress, Internet-Draft, draft-arkko-iab-internet-consolidation-02, 8 July 2019, <https://datatracker.ietf.org/doc/html/draft-arkko-iab-internet-consolidation-02>.

[Email-hashing] Acar, G., Englehardt, S., and A. Narayanan, "Four cents to deanonymize: Companies reverse hashed email addresses", April 2018, <https://freedom-to-tinker.com/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/>.

[FIArch] Papadimitriou, D., Zahariadis, T., Martinez-Julia, P., Papafili, I., Morreale, V., Torelli, F., Sales, B., and P. Demeester, "Design Principles for the Future Internet Architecture", The Future Internet, pp. 55-67, DOI 10.1007/978-3-642-30241-1_6, January 2012, <https://link.springer.com/chapter/10.1007/978-3-642-30241-1_6>.

[FREAK] University of Michigan, "Tracking the FREAK Attack", Wayback Machine archive, March 2015, <https://web.archive.org/web/20150304002021/https://freakattack.com/>.

[Hecate] Issa, R., Alhaddad, N., and M. Varia, "Hecate, Abuse Reporting in Secure Messengers with Sealed Sender", 31st USENIX Security Symposium (USENIX Security 22), pp 2335-2352, August 2022, <https://www.usenix.org/conference/usenixsecurity22/presentation/issa>.

[Hill] Hill, R., "Partial Catalog of Human Rights Related to ICT Activities", May 2014, <http://www.apig.ch/UNIGE%20Catalog.pdf>.

[HR-RT] "IRTF-HRPC / reviews", commit 3f5fbff, December 2020, <https://github.com/IRTF-HRPC/reviews>.

[HTML] WHATWG, "HTML Living Standard", August 2024, <https://html.spec.whatwg.org/multipage/>.

[HTTPS-interception] Durumeric, Z., Ma, Z., Springall, D., Barnes, R., Sullivan, N., Bursztein, E., Bailey, M., Halderman, J., and V. Paxson, "The Security Impact of HTTPS Interception", NDSS Symposium 2017, DOI 10.14722/ndss.2017.23456, February 2017, <https://doi.org/10.14722/ndss.2017.23456>.

[ICCPR] United Nations General Assembly, "International Covenant on Civil and Political Rights", December 1966, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.

[ICESCR] United Nations General Assembly, "International Covenant on Economic, Social and Cultural Rights", December 1966, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights>.

[IRP] Internet Rights and Principles Dynamic Coalition, "10 Internet Rights & Principles", <https://internetrightsandprinciples.org/campaign/>.

[Jorgensen] Jørgensen, R. F., "An internet bill of rights", Research Handbook on Governance of the Internet, edited by Ian Brown. Cheltenham: Edward Elgar Publishing, DOI 10.4337/9781849805025.00022, April 2013, <https://doi.org/10.4337/9781849805025.00022>.

[Kaye] Kaye, D., "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye", A/HRC/29/32, May 2015, <https://digitallibrary.un.org/record/798709?v=pdf>.

[Logjam] Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J., Heninger, N., Springall, D., Thomé, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Béguelin, S., and P. Zimmerman, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice", CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp 5-17, DOI 10.1145/2810103.2813707, October 2015, <https://doi.org/10.1145/2810103.2813707>.

[MAC-ADDRESS-RANDOMIZATION] Zúñiga, J. C., Bernardos, C. J., Ed., and A. Andersdotter, "Randomized and Changing MAC Address State of Affairs", Work in Progress, Internet-Draft, draft-ietf-madinas-mac-address-randomization-15, 15 July 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-madinas-mac-address-randomization-15>.

[Messenger-franking] Grubbs, P., Lu, J., and T. Ristenpart, "Message Franking via Committing Authenticated Encryption", Cryptology ePrint Archive, Paper 2017/664, July 2017, <https://eprint.iacr.org/2017/664>.

[Newegg] Mullin, J., "Newegg on trial: Mystery company TQP rewrites the history of encryption", Ars Technica, November 2013, <https://arstechnica.com/tech-policy/2013/11/newegg-on-trial-mystery-company-tqp-re-writes-the-history-of-encryption/>.

[Note-well] IETF, "Note Well", <https://www.ietf.org/about/note-well/>.

[Orwat] Orwat, C. and R. Bless, "Values and Networks: Steps Toward Exploring their Relationships", ACM SIGCOMM Computer Communication Review, vol. 46, no. 2, pp 25-31, DOI 10.1145/2935634.2935640, May 2016, <https://doi.org/10.1145/2935634.2935640>.

[Patent-policy] Weitzner, D., "W3C Patent Policy", W3C Recommendation, February 2004, <https://www.w3.org/Consortium/Patent-Policy-20040205/>.

[Penney] Penney, J., "Chilling Effects: Online Surveillance and Wikipedia Use", Berkeley Technology Law Journal, vol. 31, no. 1, pp 117-182, DOI 10.15779/Z38SS13, September 2016, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645>.

[Pouwelse] Pouwelse, J., Ed., "Media without censorship (CensorFree) scenarios", Work in Progress, Internet-Draft, draft-pouwelse-censorfree-scenarios-02, 22 October 2012, <https://datatracker.ietf.org/doc/html/draft-pouwelse-censorfree-scenarios-02>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996, <https://www.rfc-editor.org/info/rfc1958>.

[RFC1984] IAB and IESG, "IAB and IESG Statement on Cryptographic Technology and the Internet", BCP 200, RFC 1984, DOI 10.17487/RFC1984, August 1996, <https://www.rfc-editor.org/info/rfc1984>.

[RFC2026] Bradner, S., "The Internet Standards Process — Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <https://www.rfc-editor.org/info/rfc2026>.

[RFC2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, DOI 10.17487/RFC2277, January 1998, <https://www.rfc-editor.org/info/rfc2277>.

[RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", BCP 61, RFC 3365, DOI 10.17487/RFC3365, August 2002, <https://www.rfc-editor.org/info/rfc3365>.

[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>.

[RFC3724] Kempf, J., Ed., Austein, R., Ed., and IAB, "The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture", RFC 3724, DOI 10.17487/RFC3724, March 2004, <https://www.rfc-editor.org/info/rfc3724>.

[RFC3935] Alvestrand, H., "A Mission Statement for the IETF", BCP 95, RFC 3935, DOI 10.17487/RFC3935, October 2004, <https://www.rfc-editor.org/info/rfc3935>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4101] Rescorla, E. and IAB, "Writing Protocol Models", RFC 4101, DOI 10.17487/RFC4101, June 2005, <https://www.rfc-editor.org/info/rfc4101>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/info/rfc5321>.

[RFC5646] Phillips, A., Ed. and M. Davis, Ed., "Tags for Identifying Languages", BCP 47, RFC 5646, DOI 10.17487/RFC5646, September 2009, <https://www.rfc-editor.org/info/rfc5646>.

[RFC6108] Chung, C., Kasyanov, A., Livingood, J., Mody, N., and B. Van Lieu, "Comcast's Web Notification System Design", RFC 6108, DOI 10.17487/RFC6108, February 2011, <https://www.rfc-editor.org/info/rfc6108>.

[RFC6365] Hoffman, P. and J. Klensin, "Terminology Used in Internationalization in the IETF", BCP 166, RFC 6365, DOI 10.17487/RFC6365, September 2011, <https://www.rfc-editor.org/info/rfc6365>.

[RFC6701] Farrel, A. and P. Resnick, "Sanctions Available for Application to Violators of IETF IPR Policy", RFC 6701, DOI 10.17487/RFC6701, August 2012, <https://www.rfc-editor.org/info/rfc6701>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/info/rfc7301>.

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <https://www.rfc-editor.org/info/rfc7624>.

[RFC7725] Bray, T., "An HTTP Status Code to Report Legal Obstacles", RFC 7725, DOI 10.17487/RFC7725, February 2016, <https://www.rfc-editor.org/info/rfc7725>.

[RFC7754] Barnes, R., Cooper, A., Kolkman, O., Thaler, D., and E. Nordmark, "Technical Considerations for Internet Service Blocking and Filtering", RFC 7754, DOI 10.17487/RFC7754, March 2016, <https://www.rfc-editor.org/info/rfc7754>.

[RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", RFC 7844, DOI 10.17487/RFC7844, May 2016, <https://www.rfc-editor.org/info/rfc7844>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8179] Bradner, S. and J. Contreras, "Intellectual Property Rights in IETF Technology", BCP 79, RFC 8179, DOI 10.17487/RFC8179, May 2017, <https://www.rfc-editor.org/info/rfc8179>.

[RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <https://www.rfc-editor.org/info/rfc8280>.

[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>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC8558] Hardie, T., Ed., "Transport Protocol Path Signals", RFC 8558, DOI 10.17487/RFC8558, April 2019, <https://www.rfc-editor.org/info/rfc8558>.

[RFC8890] Nottingham, M., "The Internet is for End Users", RFC 8890, DOI 10.17487/RFC8890, August 2020, <https://www.rfc-editor.org/info/rfc8890>.

[RFC8980] Arkko, J. and T. Hardie, "Report from the IAB Workshop on Design Expectations vs. Deployment Reality in Protocol Development", RFC 8980, DOI 10.17487/RFC8980, February 2021, <https://www.rfc-editor.org/info/rfc8980>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

[RFC9071] Hellström, G., "RTP-Mixer Formatting of Multiparty Real-Time Text", RFC 9071, DOI 10.17487/RFC9071, July 2021, <https://www.rfc-editor.org/info/rfc9071>.

[RFC9293] Eddy, W., Ed., "Transmission Control Protocol (TCP)", STD 7, RFC 9293, DOI 10.17487/RFC9293, August 2022, <https://www.rfc-editor.org/info/rfc9293>.

[RFC9420] Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", RFC 9420, DOI 10.17487/RFC9420, July 2023, <https://www.rfc-editor.org/info/rfc9420>.

[RFC9505] Hall, J. L., Aaron, M. D., Andersdotter, A., Jones, B., Feamster, N., and M. Knodel, "A Survey of Worldwide Censorship Techniques", RFC 9505, DOI 10.17487/RFC9505, November 2023, <https://www.rfc-editor.org/info/rfc9505>.

[Saltzer] Saltzer, J. H., Reed, D. P., and D. D. Clark, "End-to-end arguments in system design", ACM Transactions on Computer Systems, vol. 2, no. 4, pp 277-288, DOI 10.1145/357401.357402, November 1984, <https://doi.org/10.1145/357401.357402>.

[TLS-ESNI] Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-20, 4 August 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-20>.

[UDHR] United Nations General Assembly, "Universal Declaration of Human Rights", December 1948, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

[UNGP] United Nations, "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", January 2012, <https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights>.

[UNHR] United Nations, "The Core International Human Rights Instruments and their monitoring bodies", <https://www.ohchr.org/en/core-international-human-rights-instruments-and-their-monitoring-bodies>.

[UNHRC2016] United Nations Human Rights Council, "The promotion, protection and enjoyment of human rights on the Internet", A/HRC/32/L.20, June 2016, <https://digitallibrary.un.org/record/845728?ln=en>.

[W3CAccessibility] W3C, "Accessibility", <https://www.w3.org/standards/webdesign/accessibility>.

[W3Ci18nDef] Ishida, R. and S. Miller, "Localization vs. Internationalization", December 2005, <https://www.w3.org/International/questions/qa-i18n.en>.

[Ziewitz] Ziewitz, M. and I. Brown, "A Prehistory of Internet Governance", Research Handbook on Governance of the Internet, edited by Ian Brown. Cheltenham: Edward Elgar Publishing, DOI 10.4337/9781849805025.00008, April 2013, <https://doi.org/10.4337/9781849805025.00008>.

[Zittrain] Zittrain, J., "The Future of the Internet and How to Stop It", Yale University Press, 2008, <https://dash.harvard.edu/handle/1/4455262>.

Благодарности

Спасибо:

- Corinne Cath-Speth за работу над [RFC8280];
- Reese Enghardt, Joe Hall, Avri Doria, Joey Salazar, Corinne Cath-Speth, Farzaneh Badii, Sandra Braman, Colin Perkins, John Curran, Eliot Lear, Mallory Knodel, Brian Trammell, Jane Coffin, Eric Rescorla, Sofía Celi и почтовой конференции hrpc за рецензии и предложения;
- лицам, выполнившим обзоры прав человека, за их рецензии и отклики - Amelia Andersdotter, Shane Kerr, Beatrice Martini, Karan Saini, Shivan Kaul Sahib.

Адреса авторов

Gurshabad Grover
Email: gurshabad@cis-india.org

Niels ten Oever
University of Amsterdam
Email: mail@nielstenoever.net

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru