

Спецификация OpenChain

Версия 1.2

Содержание

1) Введение	3
2) Определения.....	4
3) Условия	6
Цель 1: Знание своих обязанностей в отношении FOSS	6
Цель 2: Возложение ответственности за обеспечение соответствия	8
Цель 3: Проверка и утверждение содержания FOSS	9
Цель 4: Предоставление документации содержимого FOSS и Артефактов.....	10
Цель 5: Понимание Взаимодействия Сообщества FOSS.....	11
Цель 6: Подтверждение соблюдения требований OpenChain.....	12
Приложение I: Переводы на другие языки:	13

Авторское право © 2016-2018 Linux Foundation. Этот документ лицензирован на условиях лицензии Creative Commons Attribution 4.0 International (CC-BY 4.0). Копия лицензии доступна по адресу: <https://creativecommons.org/licenses/by/4.0/>.

1) Введение

Проект The OpenChain Initiative берет свое начало в 2013 году, когда группа поставщиков программного обеспечения с открытым исходным кодом заметила две появившиеся модели: 1) существуют значительные сходства между развитыми программами соответствия открытого исходного кода различных организаций; и 2) по-прежнему остается огромное количество организаций, обменивающихся программным обеспечением, с менее развитыми такими программами. Последнее замечание приводит к недоверию в части согласованности и качества Артефактов Соответствия, сопровождающих реализованное программное обеспечение. Как следствие, на каждом уровне цепочки организации более нижних уровней часто повторяют работу по соответствию, уже выполненную вышестоящими организациями.

Исследовательская группа была сформирована, чтобы определить, может ли быть создана стандартная программная спецификация, которая бы: i) способствовала повышению качества и согласованности информации о соответствии открытого исходного кода, будучи распространенной в отрасли; и ii) снизила высокие издержки, связанные с открытым исходным кодом в результате выполнения дополнительных работ по соответствию. Исследовательская группа превратилась в рабочую группу, и в апреле 2016 года была официально сформирована как совместный проект фонда Linux Foundation.

Видение и Миссия проекта The OpenChain Initiative следующие:

- **Видение:** Цепочка поставок программного обеспечения, где свободное/открытое программное обеспечение (FOSS) поставляется вместе с надежной и последовательной информацией о соответствии.
- **Миссия:** Установить требования к обеспечению эффективного управления программного обеспечения со свободным/открытым исходным кодом (FOSS) для программной поддержки участников цепочки, таких как требования и связанные гарантии разрабатываются совместно и открыто участниками цепочки поставок программного обеспечения с открытым исходным кодом, сообществом и научными кругами.

В соответствии с Видением и Миссией, эта спецификация («**Спецификация**») определяет набор требований, которые если выполняются, то значительно возрастает вероятность того, что программа соответствия с открытым исходным кодом достигла достаточного уровня качества, согласованности и полноты; хотя программа, которая удовлетворяет всем требованиям Спецификации, не гарантирует полного соответствия. Требования представляют собой базовый (минимальный) набор требований к программе, которая должна им удовлетворять, чтобы считаться соответствующей OpenChain. Спецификация фокусируется на качествах программы соответствия типа “что” и “почему”, в отличие от соображений типа “как” и “когда”. Это обеспечивает практический уровень гибкости, что позволяет различным организациям разрабатывать свои стратегии и процессы, которые наилучшим образом соответствуют их целям.

Раздел 2 вводит определения ключевых терминов, используемых в Спецификации. Раздел 3 представляет требования Спецификации, где каждое имеет перечень одного или более Материалов проверки. Они представляют собой доказательства, которые должны существовать для того, чтобы данное требование считалось выполненным. Если все требования были

выполнены по данной программе, она будет определена как Соответствующая OpenChain в соответствии со Спецификацией версии 1.2. Материалы проверки не предназначены быть открытыми, но могут быть представлены в рамках соглашения о неразглашении или по частному запросу от организации OpenChain для проверки соответствия.

Дополнительные пояснения о том, как толковать Спецификацию, могут быть получены путем ознакомления с часто задаваемыми вопросами (FAQ) по Спецификации, доступными по адресу: <https://www.openchainproject.org/specification-faq>.

2) Определения

Артефакты соответствия - набор артефактов, которые представляют собой результат программы управления FOSS для релиз-версии Предоставленного программного обеспечения. Набор может включать (но не ограничиваясь указанным) один или несколько объектов из следующего: исходный код, уведомления атрибуции, уведомления об авторских правах, копии текстов лицензий, уведомления об изменениях (модификациях), письменные оферты, спецификации компонентов FOSS, документы SPDX и тому подобное.

FOSS (Свободное и Открытое Программное Обеспечение) - программное обеспечение, в отношении которого применяется одна или более лицензий, удовлетворяющие определению Открытого исходного кода (Open Source Definition), опубликованному проектом Open Source Initiative (OpenSource.org), или определению Свободного программного обеспечения (опубликованному Фондом Free Software Foundation) или подобной лицензией.

Посредник FOSS - лицо, которое уполномочено принимать внешние запросы в отношении FOSS.

Идентифицированные Лицензии - набор лицензий FOSS, выявленных в результате соответствующего метода определения лицензии, которые применимы к Предоставленному программному обеспечению.

Программа, Соответствующая OpenChain - программа, которая удовлетворяет всем требованиям данной спецификации.

Персонал по программному обеспечению - любой сотрудник или подрядчик, который определяет, способствует или несет ответственность за подготовку Предоставленного программного обеспечения. В зависимости от организации, может представлять собой (но не ограничиваясь указанным) разработчиков программного обеспечения, инженеров, ответственных за выпуск релизов, инженеров по качеству, маркетингу и управлению продуктами.

SPDX или Обмен Данными о Пакете Программного Обеспечения - стандартный Формат, созданный рабочей группой SPDX для обмена информацией о лицензии и авторском праве для предоставленного пакета программного обеспечения. Описание спецификации SPDX можно найти по адресу: www.spdx.org.

Предоставленное программное обеспечение - программное обеспечение, которое организация предоставляет третьим лицам (например, другим организациям или физическим лицам).

Материалы проверки - доказательства, которые должны существовать для того, чтобы данное требование считалось выполненным.

3) Условия

Цель 1: Знание своих обязанностей в отношении FOSS

- 1.1** Существует письменная политика FOSS, регулирующая соответствие лицензий FOSS в отношении Предоставленного программного обеспечения. Политика должна быть передана внутренним образом.

Материал(ы) проверки:

- ☐ 1.1.1 документированная политика FOSS.
- ☐ 1.1.2 документированная процедура, которая информирует Персонал по программному обеспечению о наличии политики FOSS (например, посредством обучения, внутренней базы знаний или иным практическим способом связи).

Обоснование:

Для обеспечения принятия мер по созданию, записи и информированию Персонала по программному обеспечению о существовании политики FOSS. Хотя нет требований о том, что именно должно быть включено в политику, другие разделы могут налагать на нее требования.

- 1.2** Обязательное обучение FOSS всего Персонала по программному обеспечению следующим образом:

- Обучение, как минимум, охватывает следующие темы:
 - Политика FOSS и где найти ее текст;
 - Основы права интеллектуальной собственности, касающиеся FOSS и лицензий FOSS;
 - Основные понятия лицензирования FOSS (включая понятия разрешительных (permissive) и т.н. копилефтных (copyleft) лицензий);
 - Модели лицензирования проекта FOSS;
 - Роли и обязанности Персонала по программному обеспечению, касающиеся соблюдения FOSS, в частности, и политики FOSS в целом; и
 - Процесс выявления, записи и/или отслеживания компонентов FOSS, содержащихся в Предоставленном программном обеспечении.
- Персонал по программному обеспечению должен пройти обучение в отношении FOSS в течение последних 24 месяцев ("Уже Обученные"). Для выполнения требований к обучению Персонала по программному обеспечению может использоваться тест.

Материал(ы) проверки:

- ☐ 1.2.1 учебные материалы FOSS по вышеуказанным темам (например, презентации, онлайн-курсы или другие учебные материалы).
- ☐ 1.2.2 документированный способ для отслеживания завершения обучения Персонала по программному обеспечению.
- ☐ 1.2.3 по крайней мере 85% Персонала по программному обеспечению в настоящее время прошли подготовку, как это изложено выше. Показатель 85% не обязательно

должен относиться ко всей организации, но полностью к Персоналу по программному обеспечению, которое регулируется Программой соответствия OpenChain.

Обоснование:

Для уверенности в том, что Персонал по программному обеспечению прошел в последнее время обучение по FOSS и что основной набор соответствующих тем по FOSS был изучен в рамках такого обучения. Цель - быть убежденным в том, что основной базовый набор тем охвачен, но типовая учебная программа, вероятно, будет более объемной, чем та, что изложена здесь.

1.3 Существует процесс анализа Идентифицированных Лицензий для установления обязательств, ограничений и прав, предусмотренных каждой лицензией.

Материал(ы) проверки:

- ☐ 1.3.1 документированная процедура для проверки и документирования обязанностей, ограничений и прав по каждой Идентифицированной Лицензии.

Обоснование:

Убедиться, что существует процесс для анализа и идентификации лицензионных обязательств каждой Идентифицированной Лицензии для различных практических случаев.

Цель 2: Возложение ответственности за обеспечение соответствия

2.1 Определите функцию внешнего Посредника FOSS («Посредник FOSS»).

- Назначьте лицо (лиц), ответственное(ых) за прием внешних запросов в отношении FOSS;
- Посредник FOSS должен прикладывать все коммерчески разумные усилия для ответов на запросы о соответствии FOSS в необходимых случаях; и
- Доведите до общего сведения контакты Посредника FOSS для связи.

Материал(ы) проверки:

- ☐ 2.1.1 публично видимая идентификация Посредника FOSS (например, через опубликованный контактный адрес электронной почты или раздел Open Compliance Directory фонда Linux Foundation).
- ☐ 2.1.2 внутренняя документированная процедура, которая возлагает ответственность за получение запросов по соблюдению FOSS.

Обоснование:

Для уверенности, что это разумный вариант для запросов третьих лиц в организацию о совместимости FOSS и что эта обязанность была фактически назначена.

2.2 Определение внутренней роли (ролей) по соответствию FOSS.

- Назначьте лицо(лиц), ответственное(ых) за прием внешних запросов в отношении FOSS; выполнять роль по соответствию FOSS и Посредника FOSS может одно и то же лицо.
- Деятельность по управлению соответствию FOSS достаточно обеспечена ресурсами:
 - выделено время для выполнения роли; и
 - выделен коммерчески обоснованный бюджет.
- Распределены обязанности по развитию и поддержке политики и процессов по соблюдению FOSS;
- Правовая экспертиза, касающаяся соответствия FOSS, доступна для роли соответствия FOSS (например, может быть внутренней или внешней); и
- Процесс существует для разрешения вопросов о соблюдении FOSS.

Материал(ы) проверки:

- ☐ 2.2.1 имя лица, подразделения или должности по роли(ям) Соответствию FOSS внутренне определены.
- ☐ 2.2.2 Определение юридической помощи, доступной для роли(ей) по Соответствию FOSS, которая может быть внутренней или внешней.
- ☐ 2.2.3 Документированная процедура, которая назначает внутренние обязанности по Соблюдению FOSS.
- ☐ 2.2.4 Документированная процедура по рассмотрению и устранению случаев несоответствия.

Обоснование:

Для обеспечения эффективного распределения внутренних обязанностей по FOSS.

Цель 3: Проверка и утверждение содержания FOSS

3.1 Процесс существует для создания и управления списком материалов компонентов FOSS, который включает в себя каждый компонент (и их Идентифицированные Лицензии), включенный в состав Предоставленного программного обеспечения.

Материал(ы) проверки:

- ☐ 3.1.1 документированная процедура для определения, отслеживания и архивирования информации о наборе компонентов FOSS, из которых состоит релиз-версия Предоставленного программного обеспечения.
- ☐ 3.1.2 записи о компонентах FOSS для каждой релиз-версии Предоставленного программного обеспечения, которые демонстрируют, что документальная процедура должным образом соблюдается.

Обоснование:

Для обеспечения процесса создания и управления списком материалов компонентов FOSS, используемых для создания Предоставленного программного обеспечения. Список материалов необходим для поддержки систематической проверки условий лицензии каждого компонента в целях понимать, какие обязательства и ограничения применимы к дистрибуции Предоставленного программного обеспечения.

3.2 Программа управления FOSS должна быть способна обрабатывать типичные случаи использования лицензии FOSS, с которыми сталкивается Персонал по программному обеспечению в отношении Предоставленного Программного обеспечения, которое может включать в себя следующие варианты использования (следует отметить, что этот перечень не является исчерпывающим и не может применяться ко всем случаям использования):

- распространяется в двоичной форме;
- распространяется в форме открытого исходного кода;
- интегрировано с другими FOSS, которые могут вызвать копилефтные обязательства;
- содержит модифицированные FOSS;
- содержит FOSS или другое программное обеспечение под условиями несовместимой лицензией, взаимодействующее с другими компонентами в пределах Предоставленного программного обеспечения; и/или
- содержит FOSS с требованиями атрибуции.

Материал(ы) проверки:

- ☐ 3.2.1 документированная процедура для обработки самых распространенных случаев использования лицензий FOSS в отношении FOSS-компонентов Предоставленного программного обеспечения.

Обоснование:

Для обеспечения достаточной надежности программы для обработки распространенных случаев использования лицензий FOSS в организации, существования процедуры для поддержки этой деятельности и соблюдения процедуры.

Цель 4: Предоставление документации содержимого FOSS и Артефактов

4.1 Процесс существует для создания набора Артефактов Соответствия для каждого релиза Предоставленного программного обеспечения.

Материал(ы) проверки:

- ☐ 4.1.1 документированная процедура, обеспечивающая подготовку и распространение Артефактов Соответствия вместе с Предоставленным программным обеспечением в соответствии с требованиями Идентифицированных Лицензий.
- ☐ 4.1.2 копии Артефактов Соответствия Предоставленного Программного обеспечения архивированы и легко извлекаемы, и запланировано существование архива по крайней мере до тех пор, как реализуется Предоставленное Программное обеспечение или как того требуют Идентифицированные лицензии (в зависимости от того, какой срок длительнее).

Обоснование:

Для обеспечения полного набора Артефактов Соответствия в комплекте с Предоставленным программным обеспечением в соответствии с требованиями Идентифицированных лицензий наряду с другими отчетами, созданными в рамках процесса проверки FOSS.

Цель 5: Понимание Взаимодействия Сообщества FOSS

- 5.1 Существует письменная политика, которая определяет вклад организации в проекты FOSS. Политика должна быть передана внутренним образом.**

Материал(ы) проверки:

- ☐ 5.1.1 документированная политика содействию FOSS;
- ☐ 5.1.2 документированная процедура, которая информирует Персонал по программному обеспечению о наличии политики FOSS (например, посредством обучения, внутренней базы знаний или иным практическим способом связи).

Обоснование:

Для обеспечения подхода, что организация разумно рассмотрела создание политики в отношении публичных вкладов (контрибьютов) в FOSS. Политика вкладов в FOSS может стать частью общей политики FOSS в организации или иметь свою собственную отдельную политику. В ситуации, когда вклады ограничены или не допускается вообще, политика должна существовать, чтобы явным образом обозначить такую позицию.

- 5.2 Если организация разрешает вклады в проекты FOSS, тогда существует процесс, который применяет политику вкладов для FOSS, описанную в разделе 5.1.**

Материал(ы) проверки:

- ☐ 5.2.1 предоставленная политика по вкладам в FOSS разрешает вклады, документированная процедура регулирует вклады в FOSS.

Обоснование:

Для обеспечения в организации документированного процесса о том, как организация публично способствует FOSS. Политика может существовать таким образом, что вклады не допускаются вовсе. В такой ситуации понятно, что процедуры может не быть, и тем не менее, это требование будет выполнено.

Цель 6: Подтверждение соблюдения требований OpenChain

- 6.1 Для того, чтобы организация была сертифицирована со стороны OpenChain, она должна подтвердить, что обладает программой управления FOSS, которая отвечает критериям, описанным в данной Спецификации OpenChain версии 1.2.**

Материал(ы) проверки:

- ☐ 6.1.1 подтверждение существования программы управления FOSS, которая отвечает всем требованиям этой Спецификации OpenChain версии 1.2.

Обоснование:

Для обеспечения того, что если организация заявляет о наличии Программы, соответствующей OpenChain, то такая программа соответствует всем требованиям этой Спецификации. Само по себе соответствие ряду этих требований не будет считаться достаточным.

- 6.2 Совместимость с этой версией Спецификации продлится 18 месяцев с момента достижения проверки соответствия. Требования проверки соответствия можно найти на сайте проекта OpenChain.**

Материал(ы) проверки:

- ☐ 6.2.1 организация подтверждает существование программы управления FOSS, которая отвечает всем требованиям этой Спецификации OpenChain версии 1.2 в течение последних 18 месяцев с момента подтверждения такого соответствия.

Обоснование:

Для организации важно быть в курсе о Спецификации, если организация желает декларировать о программе соответствия с течением времени. Это требование обеспечивает поддержку процессов программы и контролирует отсутствие ее распада, если подтверждающая организация продолжит утверждать о таком соответствии и далее.

Приложение I: Переводы на другие языки:

Для облегчения глобального принятия мы приветствуем усилия по переводу Спецификации на различные языки. Т.к. проект OpenChain функционирует как проект с открытым исходным кодом, переводы определяются теми, кто готов внести свое время и знания для выполнения переводов на условиях лицензии CC-BY 4.0 и политики перевода политики самого проекта. Подробности такой политики и имеющиеся переводы можно найти на [странице Спецификации](#) проекта OpenChain.