Уязвимости в лицензиях СПО

Андрей Савченко

XV Конференция разработчиков СПО
28 Сентября 2018

Правовая оговорка

- В данном докладе отражается моё личное мнение и видение проблемы
- Представленные материалы не являются официальной юридической консультацией

Четыре свободы ПО

По определению FSF [1]:

0. Свобода использования в любых целях
1. Свобода изучения и модификации
2. Свобода копирования
3. Свобода распространения модифицированных версий

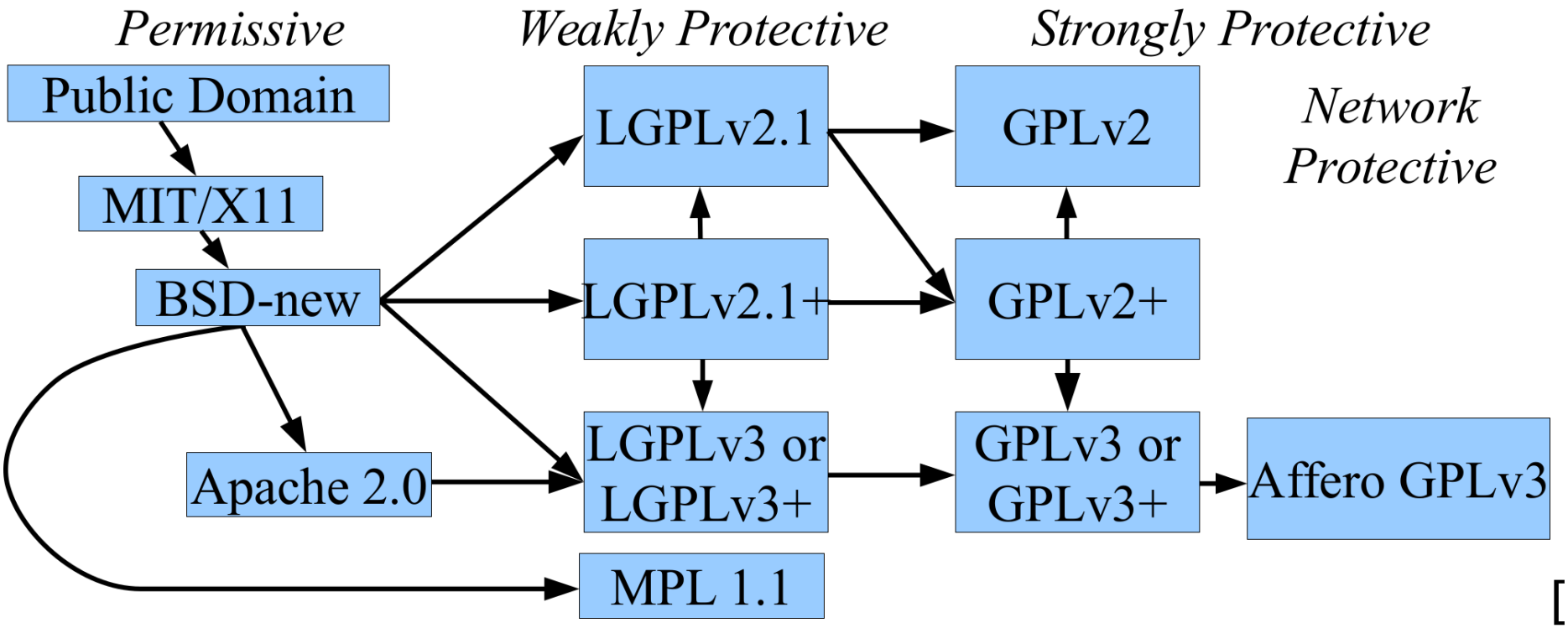
Четыре свободы ПО

[2]

Лицензии как ПО

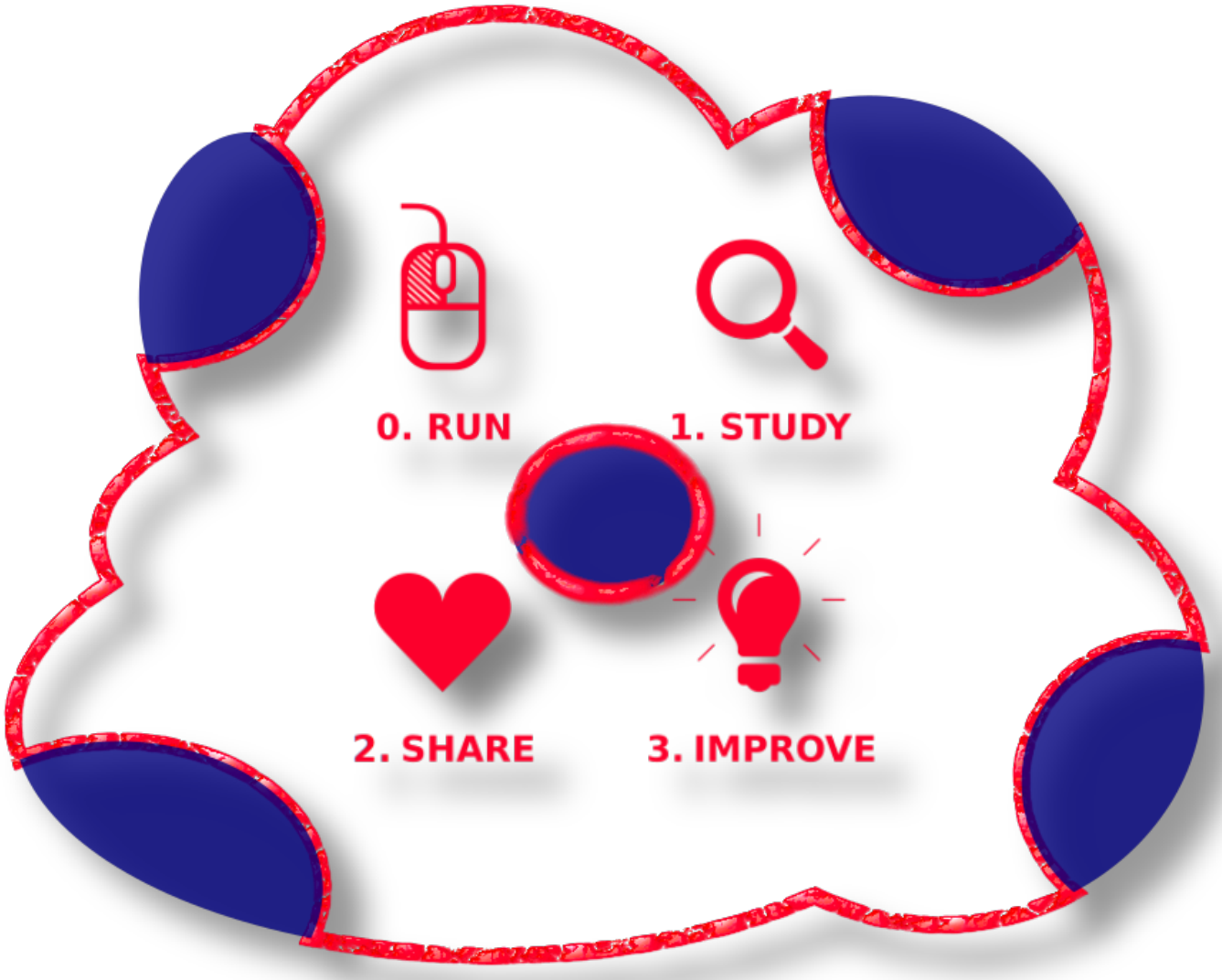
- Описывают набор правил и алгоритмов
- Идёт развитие и выход новых версий
- Есть наследование и вопросы совместимости
- Не идеальны, есть недоработки, дающие путь лазейкам

Классы свободных лицензий



[3]

Четыре свободы ПО в реальности



Как мы теряем нашу свободу

Вне зоны действия лицензий:

- микрокод
- мобильная экосистема
- SaaS
- java-script и прочее ПО на сайтах
- сетевое оборудование
- embedded
- ...

В рамках действия лицензий:

- нарушение лицензий и спорные случаи

Виды нарушений свободных лицензий

Прямые:

- явные и очевидные нарушения

Случайные:

- невнимательность
- недосмотр
- небрежность

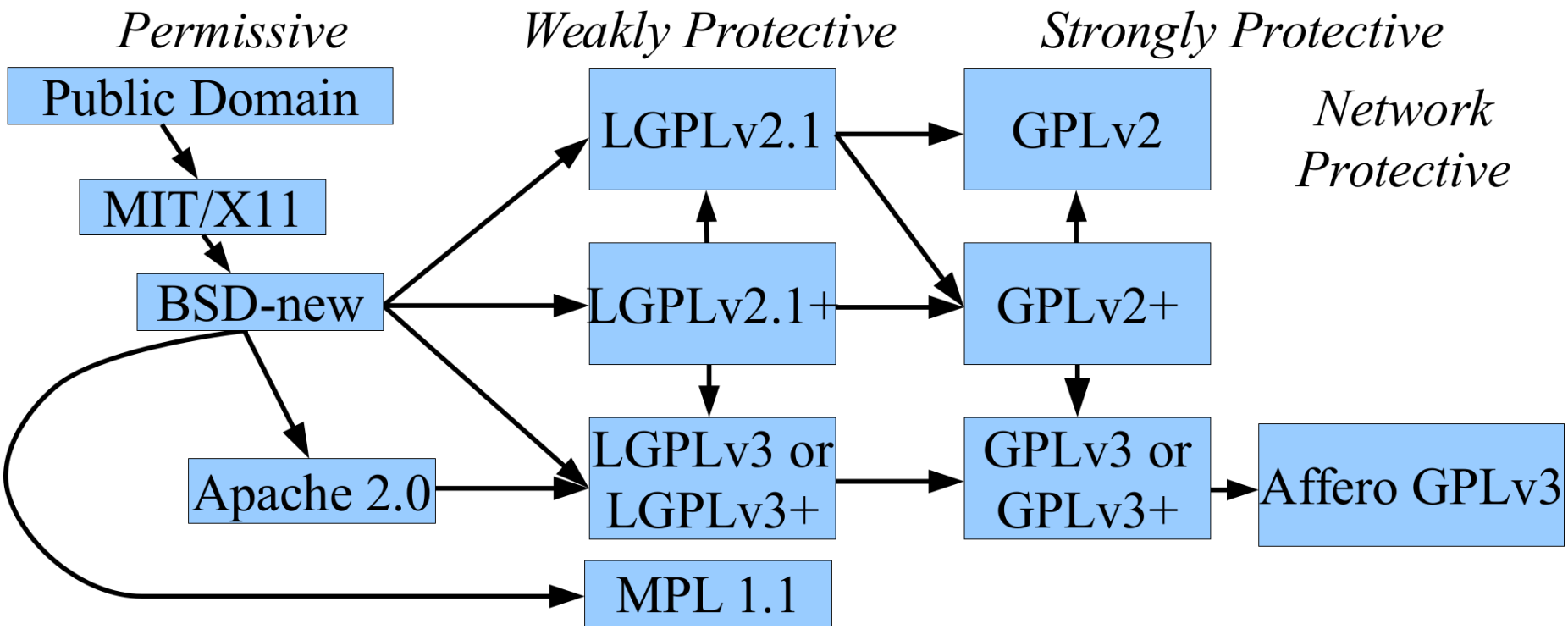
Злонамеренно спорные (серая зона):

- нарушение четырёх свобод СПО
- формальное соответствие лицензии
- использование обходных путей и лазеек

Случайные нарушения лицензий

- Забыли исходники для сгенерированных файлов
  - jar, flex, bison, *.am, ...
  - Даже GNU Emacs умудрился [4, 5]
- Недоступность исходных кодов
  - битые ссылки
  - упавший единственный сервер
  - просто потеряли
- Совместили несовместимое
  - Не все лицензии одинаково совместимы
- ...

В лицензиях можно запутаться!



[3]

Стрелками указан граф совместимости.

Примеры решённых проблем

Нарушение четырёх свобод при формально выполнении лицензии или законодательства:

- Tivo’изация [6]:
  - Пользователь не может устанавливать собственные модификации ПО, а производитель оборудования может
  - Основная причина выхода *GPLv3 [7]
- Патентный шантаж
  - Кросс-лицензирование патентных пулов (Microsoft – Novell и т.п.) [7, 8]
- DRM, DMCA и т.п.

Как были решены проблемы

Проблема	Решение
Тивоизация	Запрет блокировки использования модифицированных версий
Патентный шантаж	Патентная защита
DRM	У пользователей есть возможность отключать DRM

Выполненные изменения в лицензиях *GPL при переходе с v2 на v3.

Четыре свободы ПО: улучшение

Открытые проблемы

- Обфускация кода
- Форсирование несовместимых лицензий
- Дополнительные контрактные ограничения
- ...

Обфускация кода

Пример:

- RedHat выкладывает изменения к ядру единым патчем [9]
- Формально GPL-2 соблюдена
- Сотни (тысячи?) взаимно пересекающихся изменений
- Свободы изучения и модификации существенным образом ограничены.
- Открыто заявлено, что это ограничение конкуренции [10]

Форсирование несовместимых лицензий

Пример:

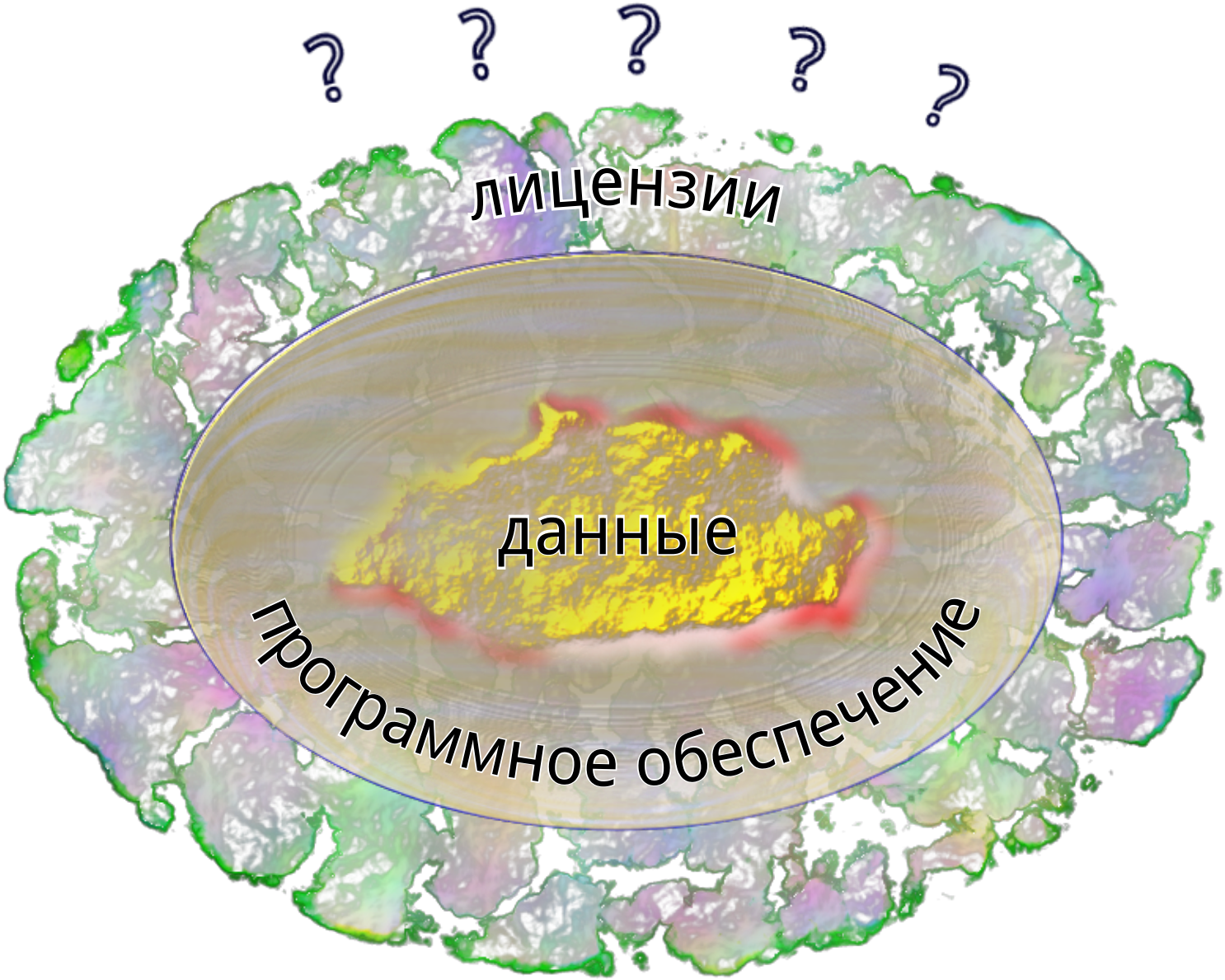
- Sun выпускает ZFS под CDDL
- CDDL несовместима с GPL: обе требуют, чтоб производные продукты были под родительской лицензией
- Предполагаемой причиной было ограничение конкуренции [11]
- Использование исходников без распространения полученных бинарников допустимо [11, 12]
- Распространять полученные бинарные файлы в рамках одного продукта *нельзя* [11, 12]

Контрактные ограничения

Пример:

- Grsecurity предоставляет патчи к ядру по платной подписке
- Проект основан на GPL-2 коде ядра и не имеет без него никакого смысла
- Подписка аннулируется при публикации исходных кодов
- Считается, что это нарушает GPL-2 [13]

Модель защиты



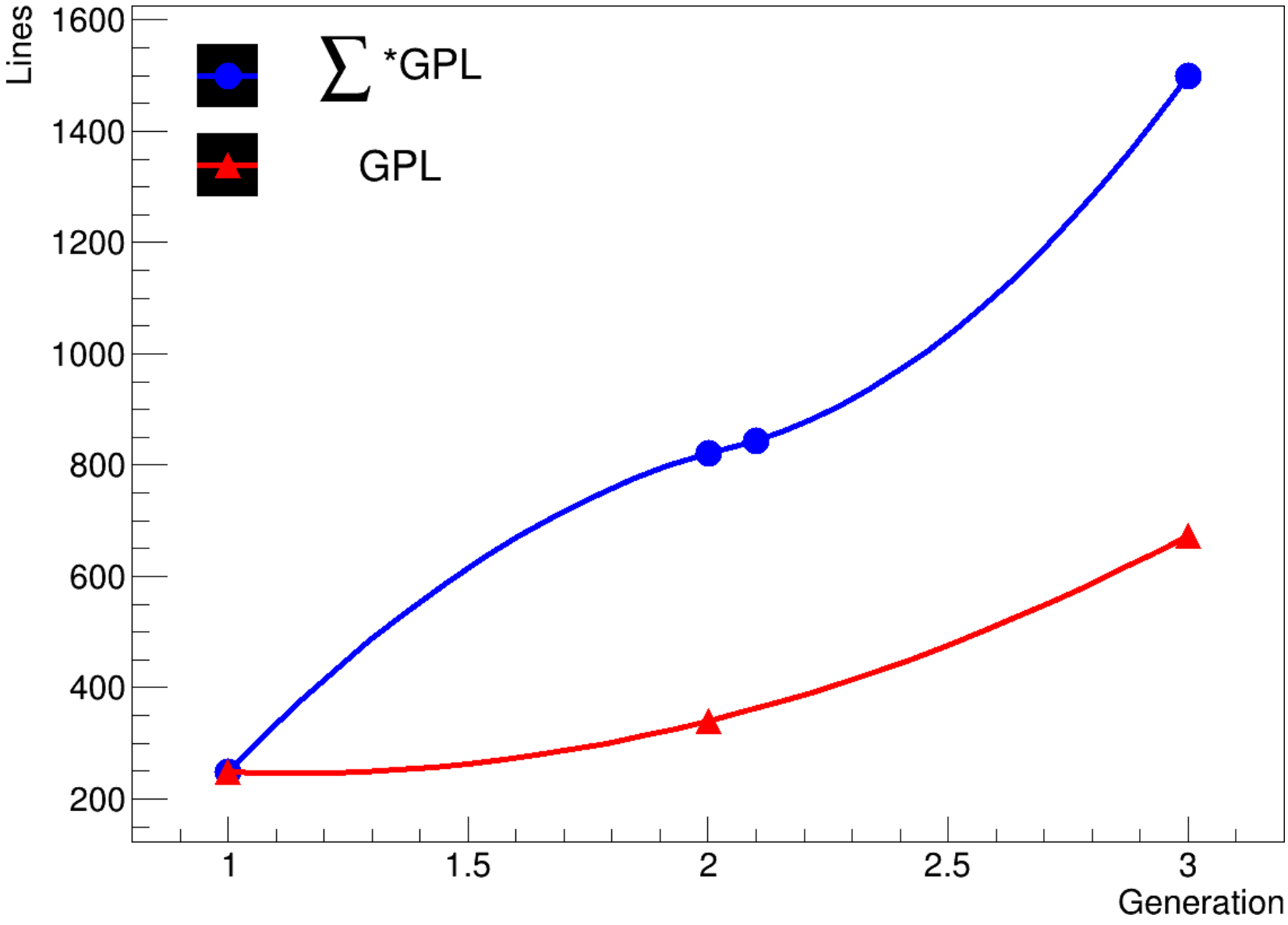
Пути решения

- Совершенствование лицензий
- Повышение общей культуры использования лицензий
- Использование альтернатив, наказание рублём
- Простых путей решения проблем нет

Совершенствование лицензий

- Уточнение лицензий $\rightarrow$ повышение сложности
- Чрезмерная сложность $\rightarrow$ отпугивание пользователей
- ! Инструменты выбора лицензий наподобие Creative Commons [14]
- Подготовка новых версий лицензий — очень сложная и кропотливая работа: на GPLv3 ушло $\sim$ 1.5 года [15].

Рост сложности лицензий



Повышение общей культуры

- В идеале: развитие до уровня, когда лазейками не пользуются.
- На практике: повышение грамотности при работе с лицензиями

Грамотное использование лицензий

- грамотный выбор
- предпочтение копилефта
- корректное заимствование кода
- использование последних версий лицензий
- использование лицензий по назначению:
  - лицензии для ПО плохо подходят для документации и мультимедиа
  - и наоборот :)

Заключение

Будьте аккуратны!

Уважайте лицензии СПО и труд разработчиков!

Спасибо за внимание!

Библиография I

Что такое свободная программа? — https://www.gnu.org/philosophy/free-sw.ru.html.

Why use Free Software? — https://www.softwarefreedomday.org/about/why-foss.

Wheeler David A. — The Free-Libre / Open Source Software (FLOSS) License Slide. — https://www.dwheeler.com/essays/floss-license-slide.html.

Stallman Richard M. — Re: Compiled files without sources???? — https://lwn.net/Articles/453374/.

Kastrup David. — Re: Compiled files without sources???? — http://article.gmane.org/gmane.emacs.devel/142405.

Что такое тивоизация? Как GPLv3 ее предотвращает? — https://www.gnu.org/licenses/gpl-faq.ru.html#Tivoization.

Stallman Richard M. — Why Upgrade to GPL Version 3. — http://gplv3.fsf.org/rms-why.html.

Библиография II


Evers Joris. —
Microsoft makes Linux pact with Novell. —
https://www.cnet.com/news/microsoft-makes-linux-pact-with-novell/.


corbet. —
Red Hat's "obfuscated" kernel source. —
https://lwn.net/Articles/430098/.


Metz Cade. —
Red Hat: 'Yes, we undercut Oracle with hidden Linux patches'. —
https://www.theregister.co.uk/2011/03/04/red_hat_twarts_oracle_and_novell_with_change_to_source_code_packaging/.


Kuhn Bradley M., Sandle Karen M. —
GPL Violations Related to Combining ZFS and Linux. —
https://sfconservancy.org/blog/2016/feb/25/zfs-and-linux/.


Stallman Richard M. —
Interpreting, enforcing and changing the GNU GPL, as applied to combining Linux and ZFS. —
https://www.fsf.org/licensing/zfs-and-linux.

Библиография III


Perens Bruce. —
Warning: Grsecurity: Potential contributory infringement and breach of contract risk for customers. —
https://perens.com/2017/06/28/warning-grsecurity-potential-contributory-infringement-risk-for-custo


Explore the Creative Commons licenses. —
https://creativecommons.org/choose/.


GNU General Public License Version 3. —
https://en.wikipedia.org/wiki/GNU_General_Public_License#Version_3.