

Васисусалий А.  
Пупкин

О технологиях  
И  
свободе слова в сети

# Правила использования документа

## 1. Для юр.лиц и их сотрудников

### (а) Запрещено:

- i. **Любое** использование документа

## 2. Для физ.лиц:

### (а) Разрешено:

- i. Скачивание, хранение, чтение цифровой копии
- ii. Распространение внутри P2P-файлообменных сетей
- iii. Печать одной физической копии для личного использования без права передачи третьим лицам

### (b) Запрещено:

- i. Распространение файла или средств (ссылок, torrent-файлов и т.п.) для получения файла на публичных ресурсах, на которых проводится показ рекламы
- ii. Всё, что не разрешено

# Оглавление

|          |                                                        |           |
|----------|--------------------------------------------------------|-----------|
| <b>1</b> | <b>Основные понятия</b>                                | <b>4</b>  |
| 1.1      | Акт свободного обмена информацией . . . . .            | 4         |
| 1.2      | Сеть . . . . .                                         | 4         |
| 1.3      | ПО . . . . .                                           | 6         |
| 1.4      | Централизация . . . . .                                | 6         |
| <b>2</b> | <b>Обзор протоколов</b>                                | <b>9</b>  |
| 2.1      | Асинхронные протоколы переписки . . . . .              | 9         |
| 2.2      | Синхронные протоколы переписки . . . . .               | 9         |
| 2.3      | Синхронные протоколы аудио-/видеоконференций . . . . . | 9         |
| 2.4      | Файлообмен . . . . .                                   | 10        |
| 2.5      | Сравнительные таблицы протоколов . . . . .             | 10        |
| <b>3</b> | <b>Угроза, исходящая от государств и корпораций</b>    | <b>12</b> |
| <b>4</b> | <b>Цифровой Гулаг</b>                                  | <b>14</b> |
| 4.1      | Причины доверия к сервисам ЦГ . . . . .                | 14        |
| 4.1.1    | Взгляд снизу . . . . .                                 | 14        |
| 4.1.2    | Взгляд сверху . . . . .                                | 14        |

# Глава 1

## Основные понятия

### 1.1 Акт свободного обмена информацией

Акт свободного обмена информацией можно представить в виде добровольной передачи информации и её добровольным получением между двумя участниками информационного обмена, не взирая на мнение третьих лиц. Для простоты иногда будем называть его *свободой слова*.

**Информационное насилие** — нарушение акта свободного обмена информацией.

### 1.2 Сеть

**Сеть** — среда информационного обмена компьютеров, не имеющая единого центра.

**Сервис** — услуга, обслуживание, служба, взаимодействующая с сетью.

**Степень доверия сервиса (от высшего к низшему):**

1. Свой компьютер-сервер, физически расположенный на частной территории
2. Арендованный удалённый компьютер-сервер, настроенный лично
3. Сервер знакомого админа
4. Чужой сервер, обслуживающий децентрализованный сервис
5. Чужой сервер, обслуживающий централизованный сервис

**Протокол** — набор соглашений для проведения сеанса информационного обмена. Протокол может быть:

- открытым
- закрытым.

**Открытый** протокол основан на наборе *стандартизаций*, т.е. соглашений, которые не имеют официального статуса — использование их сугубо добровольное.

**Закрытый** протокол основан на наборе *стандартов*, т.е. соглашений, которые имеют официальный статус. Как правило, такой вид протоколов жёстко завязан на организации его создавшей. Иногда использование такого протокола может требовать запроса на разрешение его использования, покупка лицензии на использование протокола и ПО, взаимодействующее с ним. Иногда информация о стандартах протокола закрыта, а её раскрытие, расшифровка протокола, разработка альтернативного ПО для него запрещена.

**Участники сети** (условные):

- Клиент
- Сервер

**Сервер** — программа, задача которой — получение информации от клиента и передача её серверу: себе или другому. Программа-сервер, как правило, всегда работает на компьютере, который всегда включен и имеет открытый порт в сети.

**Клиент** — программа, которой пользуется конечный пользователь для информационного обмена внутри сети, как правило с помощью сервера.

**Синхронность** протокола:

- Синхронный: пользователь может писать и читать новые сообщения другого пользователя, пока они оба в сети
- Асинхронный: пользователь может писать и читать новые сообщения другого пользователя, когда тот в сети или нет

Протокол может быть по способу **передачи** данных:

- потоковым
- пакетным.

Потоковые, как правило, бывают только синхронными, пакетные могут быть и синхронными, и асинхронными.

## 1.3 ПО

**Свободное ПО** — это такое Программное Обеспечение, которое

- имеет открытый исходный код, который свободно распространяется *через прямые ссылки с помощью свободных протоколов*
- позволяет собирать бинарные программы с помощью исходного кода
- позволяет вносить и распространять изменения в исходном коде
- не имеет ограничений по дизассемблированию (переводу бинарной программы в исходный код).

Противоположностью свободного ПО является *проприетарное*, т.е. несвободное ПО.

## 1.4 Централизация

**Централизация** архитектуры (её степень) информационной системы может быть *централизованной* и *децентрализованной*:

- клиентски федеративной.
- (серверно) федеративной,
- конфедеративной,

Начнём сверху вниз.

**Централизованная** — это такая архитектура, которая состоит из сервера(-ов), запущенного на оборудовании, управляемой одной организацией. Клиенты подключаются к одному серверу (ограниченному списку серверов) для взаимодействия друг с другом по средствам сервера.

Как правило, такая система жёстко завязана на организацию, занимающейся её обслуживанием, поэтому ПО и протокол постоянно изменяются, чтобы уменьшить количество альтернативных клиентов. Если этого не делать и не менять протокол, то со временем у протокола появится большое количество альтернативных клиентов, конкурирующих с официальным, что может сулить потерей денежного потока для официальных разработчиков. Но если всё-таки обновлять протокол, то это неизбежно будет снижать количество альтернативных клиентов, т.к. не у всех сторонних разработчиков есть такое количество времени/денег/желания на поддержание своего клиента. Такая архитектура не подразумевает использование внешних серверов. Она лишена стабильности, достижение свободы слова внутри такой системы невозможно. Невозможность объясняется тем, что держатель такого сервиса может менять правила по своему усмотрению и конечный пользователь никак не способен этого избежать.

Примеры можете поискать сами — в лишнем пиаре не нуждаются.

**Клиентски федеративная** — это такая архитектура, при которой клиент подключается по протоколу и взаимодействует с каждым сервером системы напрямую.

Напр., FTP, HTTP.

**(Серверно) Федеративная** — это такая архитектура, при которой клиент подключается по протоколу и взаимодействует с другими серверами системы через один сервер.

Напр., SMTP, IRC.

**Конфедеративная** — это такая архитектура, при которой один клиент напрямую взаимодействует с другим клиентом. Чистая конфедеративная коммуникация в сети является редкостью и, как правило, требует дополнительных средств (которые требуют дополнительного подключения к серверу) для подключения одного клиента к другому. К тому же ПО для такой архитектуры менее гибкое в настройке, т.к. код для сервера и клиента должен быть включён в каждый экземпляр программы. Внутри такой архитектуры информационный обмен между участниками может происходить только тогда, когда клиенты отправителя и получателя подключены к сети (синхронно).

Напр., BitTorrent.

## Глава 2

# Обзор протоколов

### 2.1 Асинхронные протоколы переписки

По моему мнению, лучшим асинхронным протоколом является SMTP — главный протокол электронной почты. С помощью него можно создавать конференции, можно передавать файлы.

### 2.2 Синхронные протоколы переписки

По моему мнению, лучшим синхронным текстовым протоколом является IRC. Он имеет встроенную поддержку модерирования конференций с тонкими настройками. Наименее удачным протоколом можно назвать XMPP, который основан на сложном и уродском языке разметки с рекурсивной вложенностью *XML*. К тому же за всё время жизни протокола так и не появилась нормальная синхронизация между клиентами.

### 2.3 Синхронные протоколы аудио- /видеоконференций

С видео/голосовыми протоколами всё печально. Есть SIP, но очень сложный и замороженный. К тому же очень кривой. Есть Mumble, но он требует SSL(!!!) на уровне протокола. Мало-мальски *приемлемым* можно считать только SIP.

## 2.4 Файлообмен

Из клиентски федеративных протоколов лучше всего подходит FTP. Этот протокол имеет аутентификацию, позволяет работать с файлами и директориями. Можно ещё использовать HTTP, но только в качестве протокола для скачивания файлов.

Из конфедеративных протоколов лучше всего подходит BitTorrent. Он требует внешнего сервера (трекер), задача которого обмен IP адресами между участниками раздачи. Ранее были распространены другие менее эффективные протоколы передачи — напр., Direct Connect.

## 2.5 Сравнительные таблицы протоколов

В таблице 2.1 перечислены некоторые протоколы по критериям:

- Тип (федеративность): *Централизованный, Серверно федеративный, Федеративный, Конфедеративный*
- Опенсорсность: *Закрытый, Клиент, Сервер*
- Коммутируемость (автоматическое подключение к другим участникам системы)
- Активность разработок
- Назначение: *Сообщения, Файлы, Звонки, Постинг*
- Примитивен в задумке и конечной имплементации

ВГулаге — это гипотетический цгшный сервис.

Дополнительным критерием по звонкам будет:

- возможность использовать *Конференции звонков* (с возможностью *Видео*) в таблице 2.2

| № | Название     | Т | О  | П   | К | А | Н       |
|---|--------------|---|----|-----|---|---|---------|
| 1 | ВГУлаге      | Ц | З  | -   | - | + | СФЗП    |
| 2 | Email (SMTP) | Ф | КС | +   | + | + | СФ(П?)  |
| 3 | IRC          | Ф | КС | +   | - | + | С(ФЗ?)  |
| 4 | XMPP         | Ф | КС | -   | + | + | СФЗ(П?) |
| 5 | FTP          | С | КС | +   | - | + | Ф       |
| 6 | HTTP         | С | КС | +/- | - | + | Ф       |
| 7 | SIP          | Ф | КС | -   | + | + | З(С?)   |
| 8 | Mumble       | С | КС | -   | - | + | ЗС      |
| 9 | BitTorrent   | К | КС | +   | + | + | Ф       |

Таблица 2.1: Основные критерии сервисов

| № | Название | К | В |
|---|----------|---|---|
| 1 | ВГУлаге  | + | + |
| 2 | SIP      | + | + |
| 3 | Mumble   | + | - |
| 4 | XMPP     | - | + |

Таблица 2.2: Возможность использования конференций звонков в системе

## Глава 3

# Угроза, исходящая от государств и корпораций

Государства представляют гигантскую угрозу для свободы слова. Пользуясь своим положением, они могут (и будут) использовать все виды информационного насилия. Государства тратят огромные средства на создание средств на цензурирование информационных потоков и выявление диссидентов. На практике уже было установлено, что используются не только лишь примитивные способы запрета доступа на ресурс путём бана по DNS и IP, но и по анализу сетевого трафика (DPI). Их первоочередная задача — это тотальный контроль за людьми, их мыслями и действиями. Они хотят знать всё: с кем вы обмениваетесь информацией, чем вы обмениваетесь, какими платёжными средствами пользуетесь и на что их тратите. В случае проведения следственных мероприятий, если человек оставлял некоторые зацепки, за которые бы могла зацепиться карательная система, его могут и **будут** пытаться привлечь по всей строгости закона. Будет использовано всё, даже самая безобидная информация, потому что задача государственного (и не только) обвинителя — получить очередную «палку», тем самым доказав необходимость в своём финансировании.

Корпорации, на первый взгляд, не представляют никакой угрозы для конечного пользователя их услуг, но это только так кажется. Такого огромного размера организации всегда сотрудничают со спецслужбами стран, чьи граждане пользуются корпоративными сервисами. Угроза так же исходит от стремления повлиять на свободное ПО и протоколы, которая заключается в продвижении сложных спецификаций (которые будут стремиться стать стандартами), которые трудно поддерживать независимым разработчикам и админам.

Примером влияния на свободное ПО может послужить стратегия корпорации Microsoft, которая получила название «Embrace, Extend and Extinguish» («Поддержать, надстроить и уничтожить»). Название говорит само за себя: ввести поддержку очередной свободной спецификации, надстроить поверх неё свои дополнения (которые, как правило, трудно поддерживать) и уничтожить изначальную спецификацию в пользу закрытого сервиса.

Этот подход использовали не только Microsoft, но и Google. Вспоминается их история с Google Talk. Изначально это был клиент для XMPP (Jabber), но постепенно гугловцы отключали часть межсерверного взаимодействия, чтобы конечному пользователю казалось, что админ не гугловского сервера лишает его функциональных возможностей, когда на самом деле это делал сам Google. Итогом сей эпопеи стало отключение Google Talk от сети XMPP и гугловский сервис стал полностью централизованным.

Единственная причина по которой существуют корпорации — разрешение на не добровольный показ рекламы. Я считаю, что реклама может быть допустима лишь в одном случае: когда получатель рекламы даёт **явное** согласие на её получение.

Главная цель корпораций (как и прочих (квази-)государственных образований) — это увеличение собственной власти. Именно, что власти, а не денег, потому что власть является более ценным ресурсом.

## Глава 4

# Цифровой Гулаг

Цифровой Гулаг (сокр., ЦГ) — это набор технических средств, направленных на полный контроль и ограничение, связанные с деятельностью пользователей в сети, со стороны государств и корпораций. Можно привести в пример великий китайский файрвол, а так же засилье несвободных корпоративных сервисов в сети.

### 4.1 Причины доверия к сервисам ЦГ

#### 4.1.1 Взгляд снизу

По мнению пользователей сервисов ЦГ они пользуются ими, потому что внутри них много знакомых контактов, а так же из-за «удобства» (привычки) по использованию именно этого сервиса. Рассматривать другие сервисы (что цгшные, что открытые сетевые) они не намерены. Причины этому ровно две: лень и стадный инстинкт. Потому что к новому сервису нужно привыкать, разбираться, как там всё устроено, зазывать знакомых. Кто этим будет заниматься? Они — точно нет.

С течением времени использования сервиса нарабатываются социальные связи, которые трудно разорвать и пользователи, которым уже давным давно осточертел сервис, всё равно будут продолжать им пользоваться. Такую ситуацию можно сравнить с наркотической зависимостью или с паросоциальными отношениями.

#### 4.1.2 Взгляд сверху

Пользователи сервисов ЦГ пользуются ими только лишь потому, что когда-то им непосредственно путём агрессивной рекламы или косвенно через их знакомых

рассказали об очередном новеньком сервисе. Самый главный аспект заключается в том, что им объяснили, т.е. весь маркетинговый пропагандистский аппарат был брошен на то, чтобы убедить и вдолбить в голову пользователя «удобность» использования сервиса.