

RetroShare — Urbanculture

Интернет Проекты
Криптоконспирология

Файлообмен



RetroShare — свободный клиент одноимённой сети, для частного обмена файлами, сообщениями, **анонимного** и нецензурируемого распространения контента. Это разновидность **P2P-сети** (Friend-to-Friend), в которой пользователи устанавливают прямые соединения только с людьми, которым они разрешают.

Аутентификация

Сразу после установки, программа предлагает пользователю сгенерировать пару **PGP-ключей** (публичный и приватный). Одновременно с этим, на основе публичного ключа, создаётся и т. н. сертификат RetroShare. После ввода пароля к приватному ключу происходит запуск программы. Поскольку RetroShare устанавливает соединения только с доверенными участниками сети (пирами), то далее пользователю необходимо обменяться сертификатами с действующим участником сети. Только, при условии, что оба пользователя добавили сертификаты друг друга в список доверенных, произойдёт соединение между ними.

Обмен файлами

Файлообмен в RetroShare даёт возможность анонимно распространять любое количество файлов, управлять доступом к ним, организовывать коллекции, автоматически загружать файлы друзей по подписке, осуществлять поиск файлов в сети.

Коммуникации

RetroShare как средство коммуникации включает:

- возможность отправки мгновенных сообщений,
- публичные и приватные чаты-комнаты,
- публичные и приватные форумы,
- собственный аналог электронной почты,
- плагин для аудио и видео связи.

Для всех видов связей применяется **сквозное шифрование** посредством библиотеки OpenSSL. Общение и файлообмен могут вестись как с доверенными участниками, так и с **любыми другими пирами**. Кроме того, информация может распространяться по т. н. каналу распространения контента, которые позволяют добавить к файлам описание, комментарии и прочее. Присутствует возможность анонимно подписываться и на внешние RSS-ленты. Имеется внутренний новостной сервис, где любой желающий может поделиться интересными ему Интернет-публикациями и обсудить их с участниками.

Пользовательский интерфейс

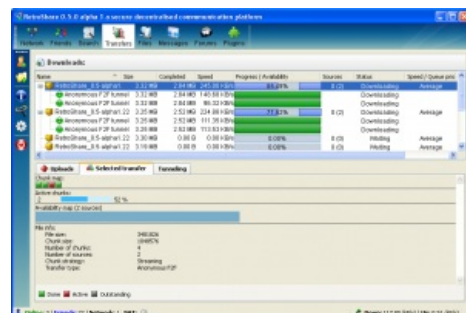
Ядро RetroShare основано на собственной библиотеке, к которой подключены два исполняемых файла:

- Интерфейс командной строки, который почти не предлагает управления;
- Графический пользовательский интерфейс, написанный на Qt. В дополнение к таким типичным функциям, как вкладка поиска и визуализация закачек, RetroShare даёт пользователям возможность управлять сетью, собирая дополнительную информацию о соседних друзьях, и отображает сеть как матрицу доверия или как динамический график сети.

Анонимность

Friend-to-friend структура сети затрудняет вторжение и делает невозможным контроль сети извне. Степень анонимности можно улучшить отключением DHT и сервиса обнаружения (discovery), что превратит RetroShare в самый настоящий дипнет.

Друзья друзей в сети не могут напрямую подключаться друг к другу, хотя анонимная раздача файлов



друзьям друзей возможна, если включена такая опция. В этом случае, соединение между сидером и личером происходит через общих друзей-посредников. Они не могут определить источник или конечный пункт назначения, а могут видеть только соседние звенья в цепи (друзей). Так как поток данных зашифрован, только источник данных и тот кому они предназначены могут видеть, какие именно данные передаются.

Клиент в настоящее время способен работать как в регулярном режиме на основе анонимного туннелирования данных, так и через сети [Tor](#) и [I2P](#). Поддержка I2P была реализована в сентябре 2015 года. Ожидается поддержка [IPv6](#).

Перспективы развития

Текущая версия (v0.6) платформы полностью несовместима с предыдущими, т.е. требует создания нового пользовательского сертификата. Пирры со старой версией не могут соединяться с пользователями новой.

Согласно [теории шести рукопожатий](#), в любом крупном неоднородном сообществе людей количество промежуточных связей никогда не превышает числа 6. Если верить ей, то при достаточном числе пиров, RetroShare может охватить ~~весь мир~~ сообщество любого объёма, при этом все соединения будут доверенными. Разумеется, для привлечения пользователей нужны печенки, а не голая теория. Но работа активно ведётся.

См. также

- [Zeronet](#)
- [Bitmessage](#)
- [IPFS](#)

Ссылки

- [Русскоязычный сайт](#)
- [Сборник статей на тему](#)