УДК 330.4:330.46

# *TOR И ЛУКОВАЯ МАРШРУТИЗАЦИЯ*

**И.Р. КИЯНОВ**

*Кубанский государственный технологический университет,*
*350002, Российская Федерация, г. Краснодар, ул. Московская, 2.*

Статья посвящена объяснению, что такое TOR (The Onion Router), и способу подключения к сети интернет по принципу «луковой маршрутизации». В современном мире, когда интернет присутствует во всех развитых регионах, актуальна проблема защиты личных данных от просмотра их посторонними лицами. Следовательно, анонимность актуальна не только от слежения государственными структурами, но и от использования персональных данных пользователя крупными корпорациями. Данная статья раскрывает, какие проблемы можно решить при помощи использования программного обеспечения TOR, а также I2P. Описывается, в каких случаях наиболее оптимально использовать определённую технологию. Также затрагивается проблема доступа к заблокированным провайдером сайтам, а также обход иных случаев блокировки. Описывается ключевой принцип работы «луковой маршрутизации» и «чесночной маршрутизации».

**Ключевые слова:** анонимность, TOR, луковая маршрутизация, прокси-сервер.

На сегодняшний день существует огромное число специальной и учебной литературы по сетевым и телекоммуникационным технологиям [1-3], а web технологии имеют широкое распространение во многих сферах деятельности человека. Поэтому сегодня разработка своего собственного web-сайта может занять всего несколько минут.

Сейчас правительства различных стран пытаются контролировать многие сферы деятельности человека, а так же доступность для просмотра и использования различного рода web-контент, иными словами проводят цензурирование информации. С каждым месяцем список заблокированных ресурсов пополняется. Политика цензуры постепенно проникает и в личную жизнь честных граждан, желающих защитить своё личное пространство. Такими же методами пользуются и киберпреступники.

Любой пользователь, находясь в сети интернет, надеется на то, что вся деятельность, которая им совершается за данную интернет-сессию не попадёт к ознакомлению третьим лицам. Увы, это отнюдь не так. Доступом к просмотру исходящего и входящего трафика могут обладать не только государственные

органы, но также круг некоторых лиц, что многих не устраивает. На выручку приходит бесплатное программное обеспечение TOR.

TOR (The Onion Router) – это открытое и свободное программное обеспечение, разработанное на свободном браузерном «движке» Gecko [4, 5]. Предназначено для реализации «луковой маршрутизации» второго поколения. Также выполняет функцию для анонимизации пользователя, посредством передачи зашифрованного выходящего трафика посредством виртуальных туннелей. Реализован на таких языках программирования как Python, C и C++. Иными словами, это браузер, получающий доступ в сеть интернет при помощи специального алгоритма подключения.

Данный алгоритм имеет название «луковая маршрутизация». Такое наименование произошло из-за принципа передачи информации между клиентом и сервером. Происходит это по принципу передачи сообщения между различными узлами (нодами) сети TOR. Где узлами в сети TOR являются специализированные прокси-сервера. Сообщение, которое необходимо передать серверу, шифруется несколькими слоями, самый первый слой шифра расшифровывает конечный узел, а самый последний слой – первый узел. Данная технология продемонстрирована на рисунке 1.

Цепочка из узлов такой сети обычно равна шести. Соответственно сообщение будет зашифровано шестью слоями информации. Именно из-за того, что с каждым переходом на новую ноду уходит один слой шифрования, словно снимается слой лука, технологию прозвали «луковой».

Преимущество данного способа передачи информации в том, что клиент и ресурс, на который посылается сообщение или запрос, не знают адресов друг друга. Клиент знает лишь адрес первоначального элемента цепи, а сервер, получивший сообщение, знает лишь адрес конечного элемента цепи, от которого было получено сообщение.

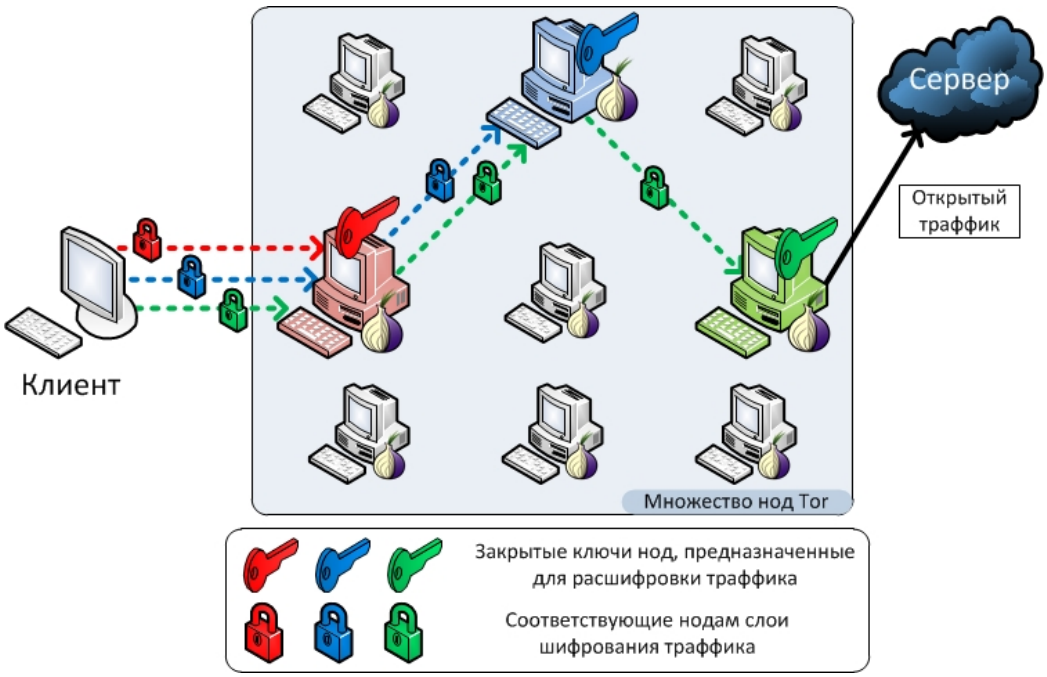


Рисунок 1 – Принцип работы луковой маршрутизации

По такому маршруту будет проходить весь трафик за всё время интернет-сессии через браузер TOR. Недостатком в данном методе является значительно уменьшенная скорость передачи и приёма трафика. Но в последних версиях TOR, разработчики добавили функцию выбирать страну с оптимальным значением отклика сервера, что может улучшить показатели скорости интернет соединения.

Если злоумышленник попытается получить доступ к трафику с клиентской части, то он получит только адрес первоначального прокси-сервера сети TOR и не сможет отследить его конечный пункт назначения. Также, если злоумышленник попытается перехватить трафик по каналу сервера, то он обнаружит только адрес конечного узла. Система спроектирована таким образом, что каждый из узлов после расшифровки слоя информации знает только адрес следующего звена, но при этом не обладает информацией, откуда было прислано ему сообщение.

С помощью данной технологии можно совершать обход блокировки множества интернет ресурсов, а также обезопасить свою работу в сети от просмотра третьих лиц.

Кроме посещения веб-страниц открытой интернет сети браузер TOR может переходить на сайты своей собственной сети. Домен имеет название .onion, но названия веб-страниц не имеют привычные названия, олицетворяющие контент сайта, а имеют длинное название из хаотично расположенных букв и цифр. Примером такого сайта может послужить многим известный торрент-трекер The Pirate Bay, который в связи с многочисленными блокировками переместил свой ресурс в сеть TOR и обладает адресом: uj3wazyk5u4hnvtk.onion. На веб-страницы с доменом .onion невозможно перейти из любого браузера кроме TOR. Веб-страницы такого типа не индексируются поисковыми системами общей сети интернет, но и аналогичные поисковые системы в сети TOR испытывают ряд проблем с поиском нужного запроса из-за того, что все веб-страницы сети TOR имеют длинное сложно индексируемое название, а также периодически меняют название из-за смены хостинга.

Однако не только сеть TOR обладает потенциалом анонимизации и обхода блокировок сайтов. Таким является сервис I2P.

I2P (Invisible Internet Project) «невидимый интернет» – это проект, разработанный для реализации анонимной компьютерной сети, работающей поверх сети интернет [6]. Доступ осуществляется с помощью специализированного бесплатного программного обеспечения.

Несмотря на схожесть выполняемых задач между TOR и I2P есть колоссальные отличия. Подавляющее большинство пользователей предпочитают использовать TOR из-за его простоты, тогда как использование I2P требует определённых знаний сетевых технологий для настройки входа.

TOR предназначен для клиентского использования. То есть основной задачей его использования является сокрытие истинного адреса клиента, обращающегося к серверу, тогда как перенос сайта на домен .onion является больше второстепенной задачей.

В случае I2P главной функцией является создание eepsite'ов (собственных сайтов внутри сети I2P), и для перехода на них клиенту необходимо иметь соответствующие программное обеспечение для обращения.

Разнятся также и способы передачи информации между клиентом и сервером. В случае TOR задействована луковая маршрутизация, где пакет дешифруется при переходе между прокси-серверами. I2P использует P2P (peer-to-peer), архитектуру и переменных посредников для передачи сообщения. Шифрование сообщений происходит по принципу «чесночного» шифрования. Данный принцип используют в том случае, когда зашифрованный сигнал переходит через несколько посредников. «Чеснок» формируется из нескольких зашифрованных сообщений, именуемых «зубчиками». К каждому зубчику прикреплена инструкция, на какой адрес должно быть доставлено сообщение. Каждый посредник может прочитать только адресованное ему сообщение в зубчике, к остальным зубчикам он не имеет доступа.

Каждый из описанных выше решений является актуальным, а выбор зависит от поставленной задачи для обхода. Если ваша задача сводится к «интернет сёрфингу» и вам необходим доступ ко всем ресурсам сети, а также анонимность во время обращения к определённым ресурсам, то в данном случае предпочтителен выбор программного обеспечения TOR. Но стоит отметить, что с популяризацией сети TOR, происходит и разработка методов вычисления подлинного IP-пользователя в данной сети. Поэтому использование данного программного обеспечения не гарантирует вашу анонимность в сети, и стоит воспользоваться дополнительными средствами. Самым популярным и надёжным является использование VPN подключения.

Если задача сводится к переносу сайтов в сеть из-за их блокировки по причине неприемлемости контента, то в данном случае актуальным является использование сервисов сети I2P. TOR в данном случае менее валиден по причине большей сложности переноса сайта на домен .onion, а также его дальнейшее продвижение внутри данной сети.

Приведённое в статье сравнение этих технологий позволяет взглянуть на дальнейшие перспективы развития свободного программного обеспечения, позволяющего сохранить анонимность перемещений и производимых действий в сети, а так же подобрать технологию, которая позволит защитить от киберпреступников личную и коммерческую информацию.

ЛИТЕРАТУРА

1. Попова О.Б. База данных раздела «Вычислительные системы» курса лекций «Вычислительные системы, сети и телекоммуникации» // Программы для ЭВМ. Базы данных. Топологии интегральных микросхем. 2015. №9. С. 88.

2. Попова О.Б. База данных раздела «Телекоммуникации» курса лекций «Вычислительные системы, сети и телекоммуникации» // Программы для ЭВМ. Базы данных. Топологии интегральных микросхем. 2015. №9. С. 72.

3. Попова О.Б. База данных раздела «Сети» курса лекций «Вычислительные системы, сети и телекоммуникации» // Программы для ЭВМ. Базы данных. Топологии интегральных микросхем. 2015. №9. С. 87.

4. Колисниченко Д. Н. Анонимность и безопасность в Интернете. От «чайника» к пользователю. – СПб.: БХВ-Петербург, 2012. – 240 с.

5. Разработка→Методы анонимности в сети. Часть 4. Tor&VPN. Whonix. Информационная безопасность, 2013 – [Электронный ресурс] – Режим доступа: https://habrahabr.ru/post/204266/

6. TOR - [Электронный ресурс] – Режим доступа: https://www.torproject.org

REFERENCES

1. Popova O.B. Baza dannykh razdela «Vychislitelnye sistemy» kursa lektsiy «Vychislitelnye sistemy, seti i telekommunikatsii» // Programmy dlya EVM. Bazy dannykh. Topologii integralnykh mikroskhem. 2015. №9. S. 88.

2. Popova O.B. Baza dannykh razdela «Telekommunikatsii» kursa lektsiy «Vychislitelnye sistemy, seti i telekommunikatsii» // Programmy dlya EVM. Bazy dannykh. Topologii integralnykh mikroskhem. 2015. №9. S. 72.

3. Popova O.B. Baza dannykh razdela «Seti» kursa lektsiy «Vychislitelnye sistemy, seti i telekommunikatsii» // Programmy dlya EVM. Bazy dannykh. Topologii integralnykh mikroskhem. 2015. №9. S. 87.

4. Kolisnichenko D. N. Anonimnost i bezopasnost v Internete. Ot «chaynika» k polzovatelyu. – SPb.: BKhV-Peterburg, 2012. – 240 s.

5. Razrabotka→Metody anonimnosti v seti. Chast 4. Tor&VPN. Whonix. Informatsionnaya bezopasnost, 2013 – [Elektronnyy resurs] – Rezhim dostupa: https://habrahabr.ru/post/204266/

6. TOR - [Elektronnyy resurs] – Rezhim dostupa: https://www.torproject.org

## TOR AND ONION ROUTING

**I.R. KIYANOV**

*Kuban State Technological University,*
*2, Moskovskaya st., Krasnodar, Russian Federation, 350002.*

The article focuses on explanation of what is TOR (The Onion Routing) and the way of connection to the Internet according to principle “onion routing”. In modern world, when connection to the Internet available in all developed regions of the world, there is a problem of protection of personal data from the view of outsiders. This article discovers what problems you can solve with using software TOR. Also address the problem of access to the blocked sites by the provider. Describes a key principle of the “onion routing”.
**Key words:** anonymity, tor, onion routing, proxy.