Обеспечение анонимности в сети Интернет

Ирышков М.М.

Пензенский государственных технологический университет, Пенза, e-mail: zshwarcz@mail.ru

Аннотация: в статье приведено описание средств повышения анонимности в сети. Показано, какими современными методами и подходами можно обезопасить доступ к глобальной сети начинающим пользователям Интернета. По результатам проведённого анализа выделены и сгруппированы технологии обеспечения безопасности для разных групп пользователей.

Ключевые слова: Интернет; безопасность; анонимность; анонимизация; браузер; сервер; прокси; сеть

При существующем темпе развития информационных технологий и внедрения их в нашу жизнь особое место необходимо уделять вопросам безопасности. Безопасность использования технологий – это проблема, которую решают корпорации, использующие их. Однако личная безопасность – это персональный вопрос, каждый начинающий и опытный пользователь сможет выбрать для себя один или несколько из предложенных вариантов защиты, изучив их достоинства и недостатки, описанные в данной статье.

Речь пойдет о безопасности использования Интернета. Однако эта статья коснется не безопасности компьютера, файлов, которые на нем хранятся или любых других данных, а о безопасности личности. Как известно, на сегодняшний день в России законы, касающиеся разных аспектов сети Интернет, а также различных информационных вопросов, лишь пополняются и ужесточаются. Так как не попасть под статью, за обычный интернет-серфинг?

Один из самых действенных способов – быть осторожным в выборе посещаемых сайтов. Но порой случайный клик приводит в неположенное место. Итак, как же избежать последствий в таких ситуациях?

Анонимность - это, возможно, не единственный, но самый действенный способ обезопасить себя, используя Интернет. Разберем несколько способов поддержания статуса anonymous.

Самый простой и доступный даже для неопытного пользователя метод – это использование браузера Tor. Данный метод не требует затрат и особых навыков. Этот браузер предоставляет возможность посещать любые ресурсы сети Интернет абсолютно анонимно. Принцип работы Tor-браузера предельно прост – прежде чем исходящий трафик выйдет в мир, он пройдет через цепочку серверов Tor’a. Более того, во время передачи данных между серверами происходит шифрование, что защищает информацию от прослушивания. Как правило, цепочку

серверов рассматривают как прокси-серверы, то есть на выходе вы не будете иметь ip адрес, присвоенный вам провайдером, однако вам будет присвоен другой ip – последнего сервера в цепочке.

Самая интересная особенность Tor браузера – это возможность серфинга сайтов с доменом .onion. В обычном интернете посещение ресурсов с доменом такого вида невозможно. Как правило, это всевозможные площадки и форумы с закрытой информацией, которая запрещена цензурой. Tor также работает и с обычными сайтами. Помимо этого, браузер имеет огромное количество настроек, среди которых можно выделить доступ по паролю, подключение сервера и т.д.

Наверное, данный метод является самым подходящим для большей части заинтересованной в анонимности аудитории, так как не имеет видимых недостатков и прост в использовании.

Следующий, довольно лёгкий и популярный способ – это использование прокси-серверов. Принцип их работы очень прост – прокси-серверы выступают неким посредником при передаче трафика между клиентом и адресатом (трафик во время передачи незашифрован, открыт). Однако существует несколько способов обеспечения анонимности с помощью прокси:

1) HTTP - пропускают через себя только HTTP-трафик, добавляя в передаваемый трафик данные о применении прокси, что уже говорит о невысоком уровне анонимности;

2) SOCKS. В отличие от HTTP, SOCKS передаёт всю информацию, ничего не добавляя от себя, то есть пропускает через себя весь трафик;

3) CGI-прокси или «анонимайзеры» по сути представляют собой web-сервер с формой, где клиент вводит адрес нужного сайта. После чего открывается страница запрошенного ресурса, но в адресной строке браузера виден адрес CGI-прокси. CGI-прокси, как и любой web-сервер может использовать https для защиты канала связи между собой и клиентом. Такую возможность предоставляет огромное количество сайтов, но доверять таким сервисам не стоит. По крайней мере в открытом доступе хороших анонимайзеров не найти. [1]

В интернете всегда можно найти большое количество бесплатных прокси-серверов, однако, чтобы пользоваться ими и не волноваться о том, что они не обеспечивают достойного уровня анонимности, нужно хорошо доверять сервису. Также существует множество сайтов, где можно приобрести прокси-сервер за 5-20$. Он будет отличаться большей степенью анонимности и скоростью работы.

Прокси-серверы не дают высокого уровня анонимности, но это не единственный их минус. Еще один недостаток – простота деанонимизации – ее возможно провести с помощью одного из

сервисов Google. Также к недостаткам можно отнести настройку прокси-сервера индивидуально для каждого приложения.

В общем, этот вариант подходит только для разового использования и не для каждого пользователя, так как это не совсем удобно и уходит больше времени на загрузку сайта, кроме того постоянно возникают ошибки.

Следующая технология - VPN. Virtual Private Network - это технология сложная в реализации как технически, так и теоретически (в плане понимания работы). Это связано с использованием всевозможных методов шифрования трафика, протоколов, применением криптографии и т.д. Однако, стоит обратить внимание на протоколы:

1) IPSec (IP security);

2) PPTP;

3) PPPoE;

4) L2TP;

5) L2TPv3;

6) OpenVPN SSL VPN с открытым исходным кодом, поддерживает режимы PPP, bridge, point-to-point, multi-client server;

7) freelan;

8) Hamachi;

9) NeoRouter.

Не нужно вдаваться в технические подробности их работы, но стоит отметить, что современные VPN-провайдеры, в основном, работают с OpenVPN, PPTP, L2TP+IPSec. Рядовому пользователю Интернета достаточно пользоваться OpenVPN.

В целом система работы VPN похожа на прокси, но если при использовании прокси передача трафика от клиента к серверу идет открыто, то в случае использования VPN сервера трафик передается в зашифрованном виде.

Не рекомендуется пользоваться бесплатными VPN-сервисами. Их серверы, как правило, очень перегружены, поэтому они не смогут обеспечить достойной скорости. Приобрести платную подписку можно у любого VPN-провайдера с помощью электронного кошелька.

Говоря о VPN, хочется упомянуть юридические аспекты, которые касаются работы сервисов, предоставляющих возможность анонимного использования сети Интернет. Дело в том, что зачастую, если дело доходит до уголовного масштаба, силовые ведомства вправе запросить у владельца VPN сервера данные о том или ином клиенте. Стоит помнить еще об одном – логи и

журналы. По заявлениям владельцев почти всех VPN-серверов никаких записей о действиях клиентов не ведется, а если и ведется, то хранятся они очень недолго.

Можно сделать вывод, что использование VPN довольно сложная и затратная (при желании пользоваться интернетом на высоких скоростях) процедура, но шифрование трафика, несомненно, является достоинством.

Последней из предложенных технологией анонимного доступа в Интернет будет I2P. Она самая нестандартная из всех существующих. Довольно сложно проникнуться полной схемой работы этой сети, но для ознакомления достаточно поверхностного понимания.

Технология работы I2P похожа на технологию работы torrent. Когда мы запускаем файл в клиенте, происходит автоматическое подключение к сети многих компьютеров, у которых этот файл тоже запущен, и взаимопомощью получаем необходимый файл. Подключение к I2P происходит аналогично – доступ в Интернет осуществляется посредством связи с другими компьютерами, подключенными к I2P. Причем стоит отметить, что обычные сайты в I2P не работают, точно так же, как и сайты I2P не работают в обычном Интернете. Собственно, I2P и нельзя назвать привычным словом “Интернет”, так как это некая сеть, которая работает по совершенно иным правилам.

Подключаясь к I2P, Вы теряете то, что имеете в обычном Интернете – IP адрес – именно поэтому и достигается очень высокая степень анонимности. Однако есть небольшое примечание – вычислить человека все равно можно: если вами заинтересуются силовые ведомства, то им будет лишь достаточно попасть в ту связку компьютеров, в которой находитесь и Вы. Вместо IP адреса в I2P существует адресная книга, по которой и происходят все обращения. Трафик, передаваемый в этой анонимной сети зашифрован случайными ключами, которые не имеют абсолютно никакой связи с реальными компьютерами.

Данный способ имеет ряд недостатков: медленная скорость работы, невозможность выходить на большое количество сайтов, неудобство в использовании. Но для создания скрытых от обычного пользования сайтов этот метод подходит, как никакой другой. В общем, подходит он для продвинутого пользователя с высокими навыками пользования сетью.

Каждый способ создания статуса anonymous хорош по-своему. Для выбора конкретного метода для себя, стоит проанализировать, какой аспект наиболее приоритетен: удобство, простота использования, низкие (или отсутствующие) финансовые затраты или максимальная защита при любых условиях.

Начинающему пользователю для максимальной безопасности в сети лучше всего подойдёт использование браузера Tor. Для разового доступа к сайту можно применять прокси.

Продвинутому пользователю подходит способ с использованием VPN. Для разработчиков сайтов незаменимым методом будет использование I2P.

Библиографический список:

1. Хабрахабр: Новостной сайт [Электронный ресурс]. URL: http://habrahabr.ru/post/190396/ (дата обращения: 13.01.2020)

2.ИНТУИТ: национальный открытый университет [Электронный ресурс]. URL: https://www.intuit.ru/studies/courses/120/120/lecture/13890?page=4