МАСКИРОВКА IP-АДРЕСА. ИСПОЛЬЗОВАНИЕ СПЕЦИАЛИЗИРОВАННЫХ ПРОГРАММ И СЕРВИСОВ

Даниловский О.А.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

В некоторых случаях возникает необходимость в сокрытии своего пребывания в Интернете. При подключении к сети Интернет, пользовательский компьютер имеет уникальный идентификационный IP-адрес, по которому всегда можно выяснить, кто вы такой и где вы находитесь, то есть получить всю подробную информацию об этом IP. Анонимный серфинг позволяет скрывать следы пребывания в интернете.

Для обеспечения анонимности пребывания в Сети, можно использовать специальные программы, такие как программы-анонимайзеры. *Анонимайзер* – средство для скрытия информации о компьютере или пользователе в сети от удалённого сервера.

Клиентское программное обеспечение может подключаться к анонимайзеру как к прокси-серверу или, например, как веб-сайту (веб-прокси). Прокси-сервер – промежуточный сервер в компьютерных сетях, выполняющий роль посредника между пользователем и целевым сервером, позволяющий клиентам как выполнять косвенные запросы к другим сетевым службам, так и получать ответы. На сегодняшний день веб-прокси наиболее популярны, так как не требуют каких-либо дополнительных настроек или программного обеспечения.

Работает веб-анонимайзер следующим образом: пользователь заходит на веб-сайт, предоставляющий услугу анонимайзера, вводит в адресную строку адрес веб-страницы, которую пользователь желает посетить анонимно. Анонимайзер загружает эту страницу себе, обрабатывает её и передаёт пользователю от своего имени (имени сервера-анонимайзера).

Одна из таких бесплатных программ – Surf Anonymous Free, которая предназначена для защиты идентичности онлайн пользователей и маскировки реального адреса IP-соединения, обеспечивая тем самым анонимность пользователя в сети.

Основные функциональные возможности Surf Anonymous Free:

- Анонимный серфинг в сети;
- Безопасный серфинг небезопасных сайтов;
- Запрет на отслеживание или контроля сетевого трафика;
- Скрытие IP-адреса компьютера пользователя;
- Отмена запрета ограничения посещений веб-сайтов;
- Отправка анонимной электронной почты;

- Поддержка браузеров Internet Explorer, Firefox, Opera.

Программа Surf Anonymous Free подключается к специальным серверам, где получает наиболее свежие и быстрые рабочие IP-адреса. Потом она размещает эту информацию IP в рабочий браузер компьютера пользователя. После этого реальный IP-адрес устройства пользователя и его местонахождение станут недоступными для других. Теперь можно находиться в сети Интернет с полностью скрытым от других новым IP-адресом и проводить анонимный серфинг онлайн.

Эта бесплатная версия может предоставить автоматически IP-адреса только в США, поэтому скорость серфинга будет ограничена, так как она частично зависит от качества и количества выбранных IP-адресов.

Другая бесплатная программа Mask My IP с таким же интерфейсом предназначена для анонимного серфинга в интернете. Mask My IP работает с Internet Explorer, Firefox, Opera, Maxthon, MyIE и совместима со всеми типами маршрутизаторов, межсетевых экранов, домашних сетей, беспроводных сетей и любых других устройств. Программа также использует для своей работы только свои прокси-серверы, за счёт чего достигается большая скорость соединения.

Проверить работоспособность программ и узнать свой реальный IP-адрес можно на сервисе Яндекса.

В настоящее время серфинг в Интернете становится всё более и более уязвимым и легко доступным для хакеров, которые без особого труда могут получить любую информацию о любом пользователе. Например, историю посещённых страниц, сайтов, пароли банковских счетов или другую важную информацию, хранящуюся на компьютере пользователя. Поэтому использование программ для анонимного серфинга в интернете значительно повышает личную безопасность и может служить, как определённое средство защиты.

Цели использования программ для анонимного серфинга должны быть законны. Нет ничего плохого в попытке скрыть свой IP-адрес. Однако использование этого программного обеспечения для незаконной деятельности не сможет защитить от ответственности.

Сфера использования анонимайзеров сегодня сместилась от обеспечения конфиденциальности информации о пользователе, в сторону предоставления доступа к запрещённым в локальной сети веб-сайтам.

Необходимо отметить, что использование анонимайзера не только не обеспечивает конфиденциальности передаваемых данных между пользователем и целевым веб-сервером, но и является дополнительным звеном возможности утечки персональной информации. Не рекомендуется при работе через анонимайзер использовать сколько-нибудь значимые

учётные записи, так как они могут быть легко скомпрометированы на сервере-анонимайзере.

При необходимости использования анонимайзеров, рекомендуется выбирать те, которые зарекомендовали себя как более-менее надёжные и работают уже на протяжении нескольких лет. Также необходимо отметить, что пользователям Рунета активно предлагаются плагины-анонимайзеры для основных используемых браузеров совершенно бесплатно. Практически, пользователь сам себя «сдаёт», используя данные плагины. Учитывая, что большинство запросов, при наличии желания правительства, перехватываются через список IP-адресов анонимайзеров, которые не особо скрываются, можно провести мониторинг, обработку статистики и прочие приёмы обработки информации, и при содействии местных провайдеров очень легко определить местоположение якобы спрятавшихся по MAC-адресам, которые можно изменить только при наличии специальной аппаратуры или старых сетевых или материнских плат с такой возможностью. Более новые варианты связи отслеживаются с такой же лёгкостью. Лучшим простым вариантом пока является SSL-запрос по IP-адресу вида «https://ddd.ddd.ddd.ddd», что тоже отслеживается, но не читается.

Примеры программ-аннонимайзеров: ProxySwitcher, HideIP NG, UltraReachUltraSurf, JonDosJonDo, TorBrowser, Anonymizer и другие.