УДК 004.7
DOI: 10.18101/978-5-9793-1626-0-106-111

АНОНИМНОСТЬ В СЕТИ

© **Молонтоев Амгалан Дугарович**
студент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
E-mail: molontoev@mail.ru

© **Тонхоноева Антонида Антоновна**
кандидат педагогических наук, доцент кафедры вычислительной техники и информатики,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
E-mail: ant_ton@mail.ru

Аннотация. В настоящее время пользователи интернета все чаще сталкиваются с проблемами блокировки доступа к веб-сайтам. Ограничений множество: работодатели блокируют доступ к сайтам с компьютеров работников, интернет-провайдеры и операторы связи запрещают доступ к ресурсам по распоряжению государственных органов, владельцы сайтов и хост-сервера блокируют или ограничивают доступ для отдельно взятых стран и регионов и так далее. Все это приводит к неудобствам в свободном использовании веб-ресурсов для обычных пользователей. Но более серьезная проблема заключается в том, что данные пользователей вне их желания остаются в Сети. Эти данные могут несанкционированно использоваться третьими лицами. В статье рассматриваются способы защиты личной информации.
Ключевые слова: анонимайзер, блокировка, веб-анонимайзер, Proxy-сервер, VPN-сервер

Для цитирования
Молонтоев А. Д., Тонхоноева А. А. Анонимность в сети // Информационные системы и технологии в образовании, науке и бизнесе: материалы региональной научно-практической конференции с международным участием (Улан-Удэ, 1 июля 2021 г.) / отв. ред. А. А. Тонхоноева, науч. ред. Е. Р. Урмакшинова. Улан-Удэ: Изд-во Бурят. гос. ун-та, 2021. С. 106–111.

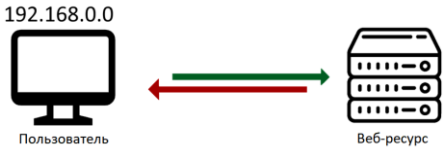
Сейчас доступ к веб-сайтам в Интернете может быть ограничен в силу ряда причин. Но есть проблема серьезней, пользователи сети оставляют за собой огромный шлейф из данных. То есть не просто какие-то разрозненные данные, а целый набор из разного рода информации, которая позволяет практически полностью идентифицировать пользователя и определить особенности его поведения. Эту информацию продают третьим лицам, например рекламодателям, которые ее используют для распространения точной таргетированной рекламы.

Можно ли защитить свою информацию или же получить доступ к ограниченному ресурсу?

В решении данного вопроса на помощь приходят анонимайзеры. Это специальные сервисы или службы, которые перенаправляют интернет-трафик пользователя через свои серверы и позволяют обеспечить анонимность путем скрытия

реального IP-адреса пользователя и удалением следящих за вами cookie-файлов, а также обход различных фильтров, как региональных, так и установленных интернет-провайдером или работодателем.

Как это работает?



Упрощенно интернет работает так: пользователь вводит адрес сайта в веб-браузере, формируется запрос и отправляется к серверу сайта. На этом пути могут быть различные фильтры, например провайдер, который обязан подчиняться местному законодательству и предотвращать доступ к запрещенным ресурсам. В итоге в зависимости от запроса пользователя, провайдер может как запретить, так и разрешить доступ к ресурсу. В случае отклонения пользовательского запроса юзер получит страницу, уведомляющую его о блокировке ресурса.

Также бывают и ограничения со стороны веб-сервера. Запрос пользователя успешно дойдет до сервера, но, проверив IP-адрес пользователя и определив, из какой страны он исходит, или посчитав его подозрительным, может заблокировать или ограничить доступ пользователю с соответствующим сообщением.

Рис. 1. Блокировка запроса

Можно обойти это ограничение, отправив запрос к другому серверу-анонимайзеру, который, допустим, находится за пределами страны или его нет в списке запрещенных. Сервер-анонимайзер принимает запрос пользователя и под своим IP-адресом отправляет запрос к нужному для пользователя ресурсу в интернете. Веб-ресурс отправляет назад данные к серверу и перенаправляет полученные данные пользователю. Именно так работает большинство средств для обеспечения анонимности веб-серфинга.

Но этот процесс приводит к некоторой задержке, пользовательские запросы могут возвращаться медленнее, чем при прямом обращении к веб-серверу.

Существует множество разных типов анонимайзеров, отличающихся используемыми технологиями и способами обхода блокировок. Кроме того, анонимайзеры могут быть бесплатными, условно-бесплатными, с рекламой или с ограничением объема трафика и полностью платными.

Бесплатными анонимайзерами стоит пользоваться с большой осторожностью. Нередки случаи, когда такие сервисы продавали конфиденциальные данные третьим лицам (злоумышленникам, рекламодателям). К надежным сервисам с большой опаской можно отнести только платные, но опять же не стоит доверять им на 100%.

Веб-анонимайзеры работают в виде сайтов и обеспечивают работу пользователя без установки ПО. Достаточно просто зайти на веб-анонимайзер, ввести адрес сайта, доступ к которому необходимо вам получить, и содержимое сайта будет доступно.

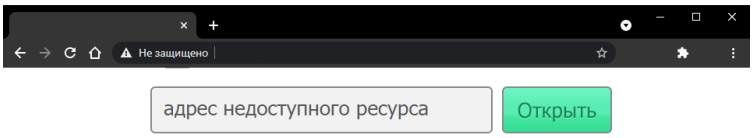


Рис. 2. Веб-анонимайзеры

Этот тип анонимайзеров имеет ряд ограничений — многие сложные сайты не могут быть перенаправлены таким образом из-за большого количества сложных ссылок, скриптов (JavaScript, PHP и т. п.). Или же сайты могут работать неполноценно, то есть некоторые функции не будут работоспособными, например проигрывание музыки или видео. Веб-анонимайзеры отлично подойдут для доступа к простым сайтам.

Proxy-серверы — технология прокси-серверов используется в среде анонимизации интернет-трафика, однако прокси-серверы подходят и для выполнения других функций:

повышение безопасности сети с помощью шифрования запросов;
предотвращение перехвата конфиденциальной информации;
блокировка вредоносных сайтов и рекламы;
кэширование сайтов для экономии трафика;
контроль использования сетевого канала;
блокировка доменов;
мониторинг и регистрация веб-запросов;
тестирование веб-ресурсов при заходе с различных IP

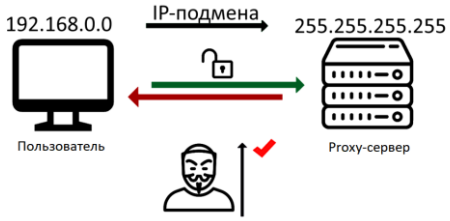


Рис. 3. Proxy-сервер

Достоинство такой технологии в том, что можно не устанавливать дополнительные программы, достаточно узнать адрес, прокси-сервера и указать его в настройках браузера пользователя. В отличие от веб-анонимайзеров прокси-сервер работает со всем содержимым сайта (скрипты, мультимедиа и т. д.). Однако есть и недостатки — проблемы с безопасностью. Прокси-серверы никак не шифруют интернет-трафик. HTTP трафик не будет шифроваться. А HTTPS будет зашифрован так же, как и при обычном интернет-соединении. Поэтому не стоит полностью доверять конфиденциальную информацию (пароли, банковские карты) прокси-серверу.

VPN-сервер — данная технология не создавалась как средство анонимизации трафика. Она обеспечивает защищенное подключение к удаленной локальной сети. Однако технологию применяют и для анонимизации интернет-трафика.

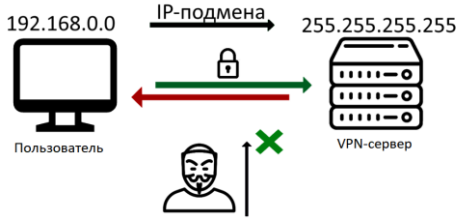


Рис. 4. VPN-сервер

Главным плюсом VPN и отличием от прокси является дополнительное шифрование всей сетевой активности пользователя. То есть никто не получит доступ к трафику пользователя, пока он доходит до VPN-сервера. Например, провайдер умышленно снижает скорость интернет-канала, когда пользователь использует слишком много интернет-трафика. Прокси не может предложить подобное, так как не использует шифрование.

Минусами технологии являются необходимость настройки доступа к VPN-сервису или установки дополнительного программного обеспечения и риск утечки конфиденциальной информации, владелец VPN-сервера может украсть данные пользователя. Также если сервис использует мощное шифрование, скорость отклика от веб-сервера до пользователя значительно снизится.

Специализированные браузеры — этот тип анонимизации отличается от остальных и представляет собой сборки популярных браузеров (Chromium или Firefox) с уже встроенными средствами анонимизации — через расширения для браузера, например браузер Opera имеет встроенный VPN.

TOR — этот тип анонимизации использует так называемую луковую маршрутизацию. Для анонимизации интернет-трафика пользователя TOR отправляет пользовательский трафик через серверы. В отличие от вышеуказанных способов, которые отправляют интернет-трафик через один сервер, здесь он проходит через 3 сервера, которые выполняют роль промежуточных узлов:

охранный (входной или сторожевой);

промежуточный;

выходной.

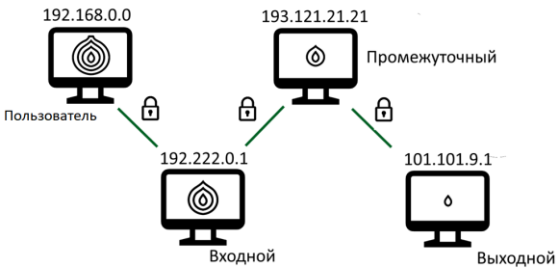


Рис. 5. TOR

Каждый узел знает IP-адрес только узла, который находится перед ним, например промежуточный не сможет узнать пользовательский IP-адрес. Трафик пользователя будет иметь три слоя шифрования. TOR шифрует данные юзера так, чтобы их мог расшифровать только выходной узел. Каждый слой шифрования расшифровывает один промежуточный узел.

Доступ к анонимной сети осуществляется через специальный браузер TOR Browser, основанный на браузере Firefox. В него встроили дополнения, запрещающие сайтам собирать любую информацию о пользователях.

В сети TOR передачей интернет-трафика занимаются множество маршрутизаторов. Они расположены по всему миру и работают благодаря обычным пользователям, которые разворачивают у себя промежуточные узлы.

Главный недостаток TOR — из-за многослойного шифрования сеть TOR работает очень медленно, даже по сравнению с VPN, половина сайтов просто отказываются или некорректно работают. Также есть вероятность, что ваши пользовательские данные могут быть украдены с выходного узла, так как на этом узле данные полностью расшифрованы. Также из-за обилия сложных технических терминов в настройках этот тип анонимизации не подойдет обычным пользователям.

Расширения для браузеров — этот тип анонимайзеров требует установки из специального магазина прямо в браузер пользователя, после чего можно настроить на определенных сайтах перенаправление интернет-трафика через сервер-анонимайзер.

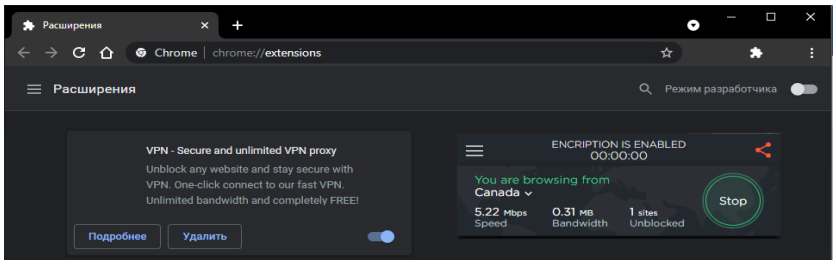


Рис. 6. Расширения для браузеров

Расширения для браузеров следует применять с наибольшей осторожностью. Существует множество расширений, созданных обычными пользователями. Стоит присмотреться к известным компаниям или же поискать информацию о репутации расширения.

Если возникает вопрос о безопасности данных в сети, то самым оптимальным способом их защиты будет VPN. В этом случае интернет-трафик пользователя будет надежно зашифрован и никто не сможет получить доступ к ним до достижения VPN-сервера. Но пользовательский трафик все равно будет расшифрован на VPN-сервере, в любом случае не стоит полностью доверять важную информацию VPN-сервису. Поэтому не стоит использовать сайты под своей учетной записью, тем самым можно скомпрометировать себя. В анонимной сессии в интернете будет разумным создать новую учетную запись, не имеющую актуальной информации о пользователе.

Литература

1. Новожилов Е. О. Компьютерные сети: учебное пособие. Москва: Academia, 2017. 288 с. Текст: непосредственный.
2. Таненбаум Э. С., Уэзеролл Д. Компьютерные сети. Санкт-Петербург: Питер, 2018. 512 с. Текст: непосредственный.
3. Шелухин О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Москва: ГЛТ, 2013. 220 с. Текст: непосредственный.

ANONYMOUS ON THE NETWORK

Amgalan D. Molontoev
Student,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: molontoev@mail.ru

Antonida A. Tonkhonoeva
Cand. Sci. (Education), A/Prof.,
Department of Computer Science and Informatics,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: ant_ton@mail.ru

Abstract. Now Internet users are increasingly faced with the problems of blocking access to websites. There are many restrictions: employers block access to websites from employees' computers, Internet providers and telecom operators prohibit access to resources by order of government agencies, website and host server owners block or restrict access for individual countries and regions, and so on. All this leads to inconveniences in the free use of web resources for ordinary users. But the bigger problem is that users' data, outside of their desire, remains online. This data can be used by by other people unauthorized. The article discusses ways to protect personal information.
Keywords: anonymizer, blocking, web anonymizer, proxy server, VPN server