

АНОНИМНОСТЬ В ИНТЕРНЕТЕ

ПОДГОТОВИЛ СТУДЕНТ 1 КУРСА

ПОЛЯКОВ ДМИТРИЙ



- Анонимность-сокрытие реальной идентичности “паспортных данных”. Явление, широко распространенное в интернете. Сейчас анонимность работает для свободного общения, пиратства, спама и многого другого.
- 28 Мая 2015 года Совет по правам человека ООН предоставил отчет заседания, посвященного анонимности и шифрованию в интернете, в котором сделан вывод, что возможность анонимного использования интернета и шифрование личных данных коммуникации необходимы и должны расцениваться как часть прав человека.

КАК ЗА НАМИ СЛЕДЯТ ?

- ОТСЛЕЖИВАНИЕ МЕСТОПОЛОЖЕНИЯ С ПОМОЩЬЮ ИНТЕРНЕТА
- СБОР ИНФОРМАЦИИ О ПОЛЬЗОВАТЕЛЕ ЧЕРЕЗ БРАУЗЕР
- СБОР ИНФОРМАЦИИ О ПОЛЬЗОВАТЕЛЕ ЧЕРЕЗ СОЦИАЛЬНЫЕ СЕТИ
- УТЕЧКА ИНФОРМАЦИИ ИЗ ЭЛЕКТРОННОЙ ПОЧТЫ

СБОР ИНФОРМАЦИИ ЧЕРЕЗ БРАУЗЕР
В АВГУСТЕ 2010 ГОДА ВНИМАНИЕ «THE WALL STREET JOURNAL» ПРИВЛЕКЛА ДЕЯТЕЛЬНОСТЬ КОМПАНИИ [X + 1]. «ВЫ МОЖЕТЕ НИЧЕГО НЕ ЗНАТЬ ОБ ЭТОЙ КОМПАНИИ, НО, ВПОЛНЕ ВОЗМОЖНО, ОНА ОЧЕНЬ МНОГОЕ ЗНАЕТ О ВАС», - ПИШЕТ АВТОРИТЕТНОЕ ИЗДАНИЕ

- По одному «клику» пользователя компания точно определяет его пол, возраст, семейное положение, годовой доход и другие «характеристики».
- Количество детей и любимая марка автомобилей, а также хобби и наличие высшего образования также не являются для нее секретом. Для этого вовсе не нужно отслеживать каждую деталь, простые технологии оценки и обработки информации дают достаточно точную характеристику отдельно взятого человека

COOKIES



- Куки — это файлы текстового формата. Поначалу они выполняли только полезные функции и предназначались для сохранения рабочей информации о пользователях интернет-ресурса. Например, посещал ли пользователь ранее данный ресурс. Но, чтобы не перегружать этой информацией сервера компании, куки сохраняются на жестком диске ПК самого пользователя. Позже куки стали использоваться для фиксации всей информации, т.е для шпионажа.

АНОНИМНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ



- ИНФОРМАЦИЕЙ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ МОГУТ ПОЛЬЗОВАТЬСЯ ЗЛОУМЫШЛЕННИКИ И СПЕЦ. СЛУЖБЫ

ВЗЛОМ ЭЛЕКТРОННОЙ ПОЧТЫ

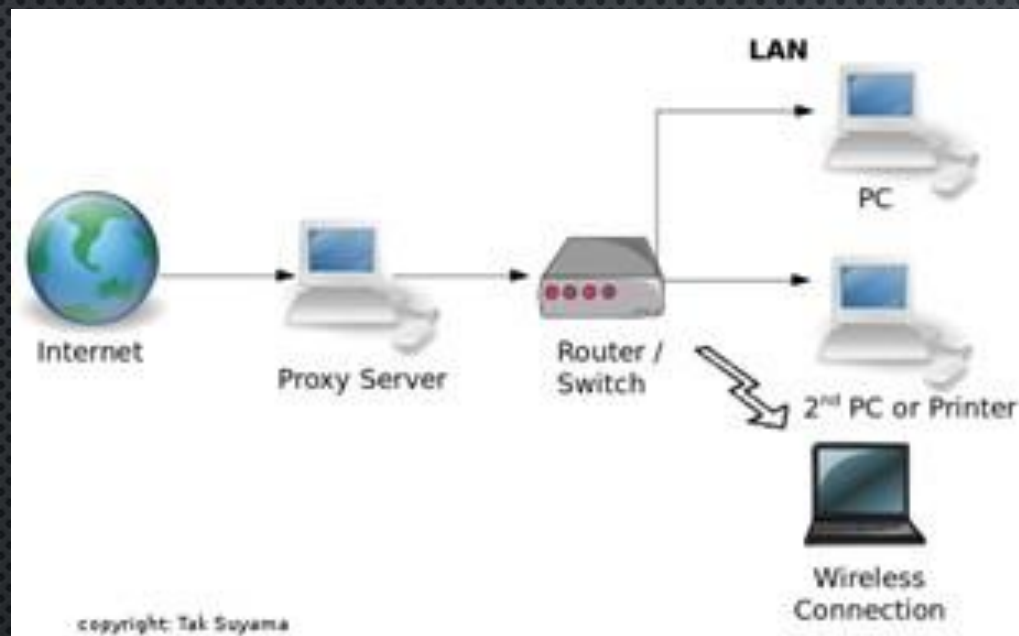


- СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ
- ТЕХНИЧЕСКИЕ СПОСОБЫ

СПОСОБЫ ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ В ИНТЕРНЕТЕ

- ПРОКСИ-СЕРВЕРА, АНОНИМАЙЗЕРЫ, VPN
- ШИФРОВАНИЕ ПОЧТЫ
- ОСТОРОЖНОСТЬ В РАЗМЕЩЕНИИ ЛИЧНОЙ ИНФОРМАЦИИ В ИНТЕРНЕТЕ

ПРОКСИ-СЕРВЕРА



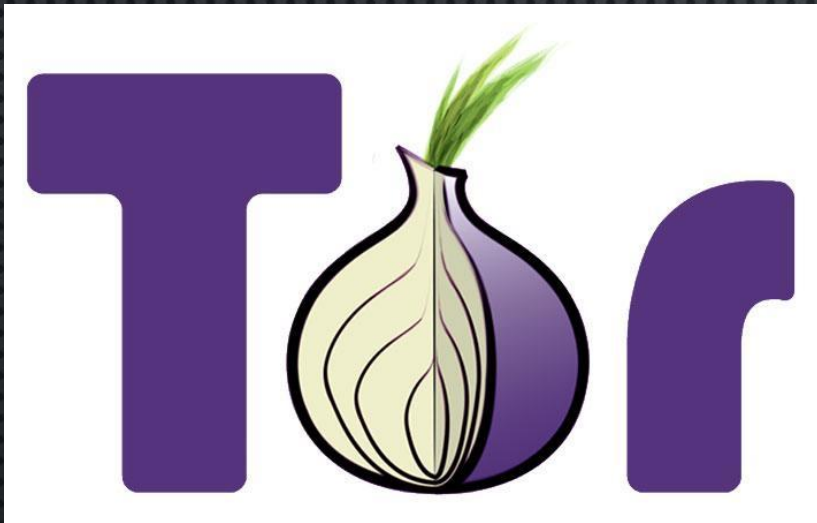
Когда вы набираете в строке браузера какой-нибудь адрес, то сначала запрос отправляется на сервер DNS, который преобразует строку символов в набор из 32 нулей и единиц — IP-адрес, использующийся для маршрутизации. Зная этот адрес, злоумышленник может выведать о человеке очень многое. Как себя защитить?

Для начала можно попробовать «спрятаться» с помощью прокси-сервера, который является как бы посредником между компьютером пользователя и серверами Сети. Главный «предатель» — это IP-адрес, от которого никак нельзя избавиться, потому что он необходим для маршрутизации данных. Но прокси-сервер отправляет запросы на веб-сервера как бы от себя. И он сам получает всю ответную информацию. Так что, на первый взгляд, использование прокси-сервера — гарантия анонимности. Но не так все просто. Оказывается, подавляющее большинство прокси-серверов в своих запросах передают в специальном поле (X-FORWARDED-FOR) IP-адрес конечного пользователя. Но есть и анонимные службы. Проверить любой прокси-сервер на анонимность можно на сайте

SOCKS-СЕРВЕРА

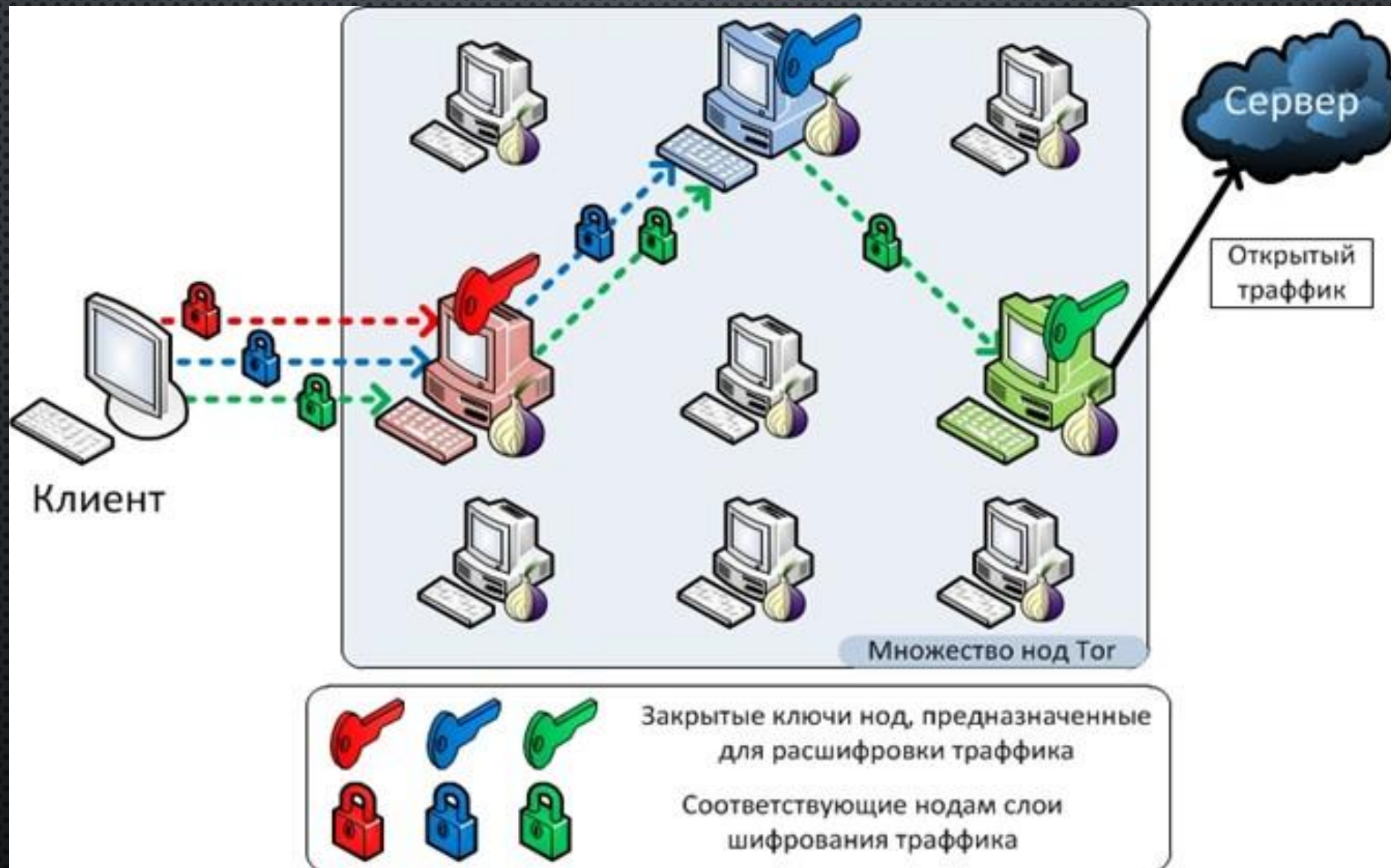
- Существует еще один способ обеспечения анонимности в Интернете — на сегодняшний день самый надежный. Речь идет о SOCKS-протоколах. Принцип действия этой технологии похож на работу прокси-сервера. SOCKS-сервер принимает данные от компьютера пользователя, отправляет их на веб-сервер, а затем перенаправляет ответную информацию обратно. Правда, здесь есть и несколько серьезных различий. Во-первых, «общение» клиентского компьютера и SOCKS-сервера происходит не по общепринятым, а по специальным протоколам (SOCKS4, SOCKS5 и т.д.). В результате передача IP-адреса пользователя невозможна в принципе. Кроме того, SOCKS-сервер сам преобразовывает информацию от пользователя в запросы для общепринятых протоколов. А это значит, что ни один сервер «не догадается», что отправляет данные не конечному пользователю, а посреднику.

TOR BROWSER.



- ТОР БРАУЗЕР ЭТО СИСТЕМА, ПОЗВОЛЯЮЩАЯ УСТАНОВЛИВАТЬ АНОНИМНОЕ СЕТЕВОЕ СОЕДИНЕНИЕ С ПОМОЩЬЮ ЛУКОВОЙ МАРШРУТИЗАЦИИ
- ЛУКОВАЯ МАРШРУТИЗАЦИЯ ЭТО СИСТЕМА МАРШРУТИЗАТОРОВ, В КОТОРОЙ ПОЛЬЗОВАТЕЛЬ ПОДКЛЮЧАЕТСЯ К СЕТИ ЧЕРЕЗ ЦЕПОЧКУ УЗЛОВ

СХЕМА РАБОТЫ TOR БРАУЗЕРА



СПАСИБО ЗА ВНИМАНИЕ

BIG BROTHER



**IS WATCHING
YOU**