№2(14)/2011

КОМПЬЮТЕР ДЛЯ НАЧИНАЮЩИХ

АНОНИМНОСТЬ В ИНТЕРНЕТЕ

КАК РАБОТАЕТ СЕТЬ

СКРЫВАЕМ СВОИ IP

ЧТО ТАКОЕ «БЕЛЫЕ» И «СЕРЫЕ» IP

КАК ПОЛЬЗОВАТЕЛЬ ОСТАВЛЯЕТ «СЛЕДЫ» В ИНТЕРНЕТЕ

Настоящий рай для шпионов...

Раньше слежка была делом хлопотным и опасным, теперь же поиграть в «агента 007» может любой. Для этого даже не придется выходить из дому: немного времени, навыков и терпения – и нужная информация легко отыщется в Интернете! Например, ваш коллега может посмотреть фотографии с вашей последней вечеринки, зайдя на популярный ресурс Flickr, сосед – узнать о ваших старых и новых друзьях на сайте «Одноклассники.ру», а жена – поинтересоваться, что за видеокассеты вы купили вчера в интернет-магазине...

Интернет – настоящий рай для шпионов. Эта гигантская губка впитывает в себя все сведения, которые вы оставляете в Сети! Кроме того, информацией о посещаемых вами сайтах владеет ваш провайдер или – в варианте с офисной сетью – системный администратор. При этом не важно, покупаете ли вы что-то в интернет-магазине, наводите справки о возможности получения банковского кредита или обсуждаете что-нибудь в форуме – ваши действия в Сети легко отслеживаются.

Многие компании специализируются на сборе сведений о пользователях, чтобы целенаправленно атаковать их рекламной рассылкой. Профессионалы в области компьютерного шпионажа составляют досье на вас, используя данные, полученные в Интернете. В первую очередь их интересует, какие сайты вы регулярно посещаете, что покупаете в интернет-магазинах и какие адреса электронной почты используете.

Найти «личную» информацию становится все проще. Такие службы, как www.zoominfo.com или www.spock.com, специализируются на поиске сведений о конкретном человеке. Сервисы эти бесплатны, и пользоваться ими не возбраняется никому. Радует одно – эти системы пока не добрались до российских пользователей, но это лишь вопрос времени.

Чтобы оградить себя от любопытных глаз, соблюдайте золотые правила работы в Сети и используйте специализированные программы-анонимайзеры, делающие вас невидимыми в Интернете.

Откуда данные попадают в Интернет?

Вы сами вводите сведения о себе! Вы много и с удовольствием рассказываете о себе любимых на социальных порталах типа «Мой круг» или «Одноклассники.ru». На вашей домашней странице наверняка можно найти семейные фотографии и адрес электронной почты, а на сайтах знакомств – узнать о ваших сексуальных предпочтениях. Порывшись же хорошенько на форумах по здоровью, можно найти вопросы, связанные с конкретным заболеванием, подписанные вашим именем.

Часто информация в Сеть попадает благодаря родственникам и знакомым, например, подруга может выложить в общий доступ фотографии вашего совместного пляжного отдыха или поместить на своей страничке рассказ о том, как здорово вы проводили время, со всеми нужными и ненужными подробностями. Вы являетесь членом клуба любителей музыки, общества переводчиков или вступили в партию? Тогда в Интернете можно найти информацию о ваших выступлениях, статьи, заметки, образцы творчества и прочие материалы.

Каким образом вас можно идентифицировать?

Сделать это можно с помощью IP-адреса вашего компьютера – это «удостоверение личности» во время вашего пребывания в Интернете. Его обычно назначает (когда вы выполняете подключение к Сети) и сохраняет в своих протоколах провайдер. При посещении той или иной веб-страницы сервер, на котором хранится сайт, тоже сохраняет ваш IP-адрес. Тот, кто сравнит протокол вашего провайдера с протоколом посещенного сервера, будет точно знать, что это именно вы заходили на сайт.

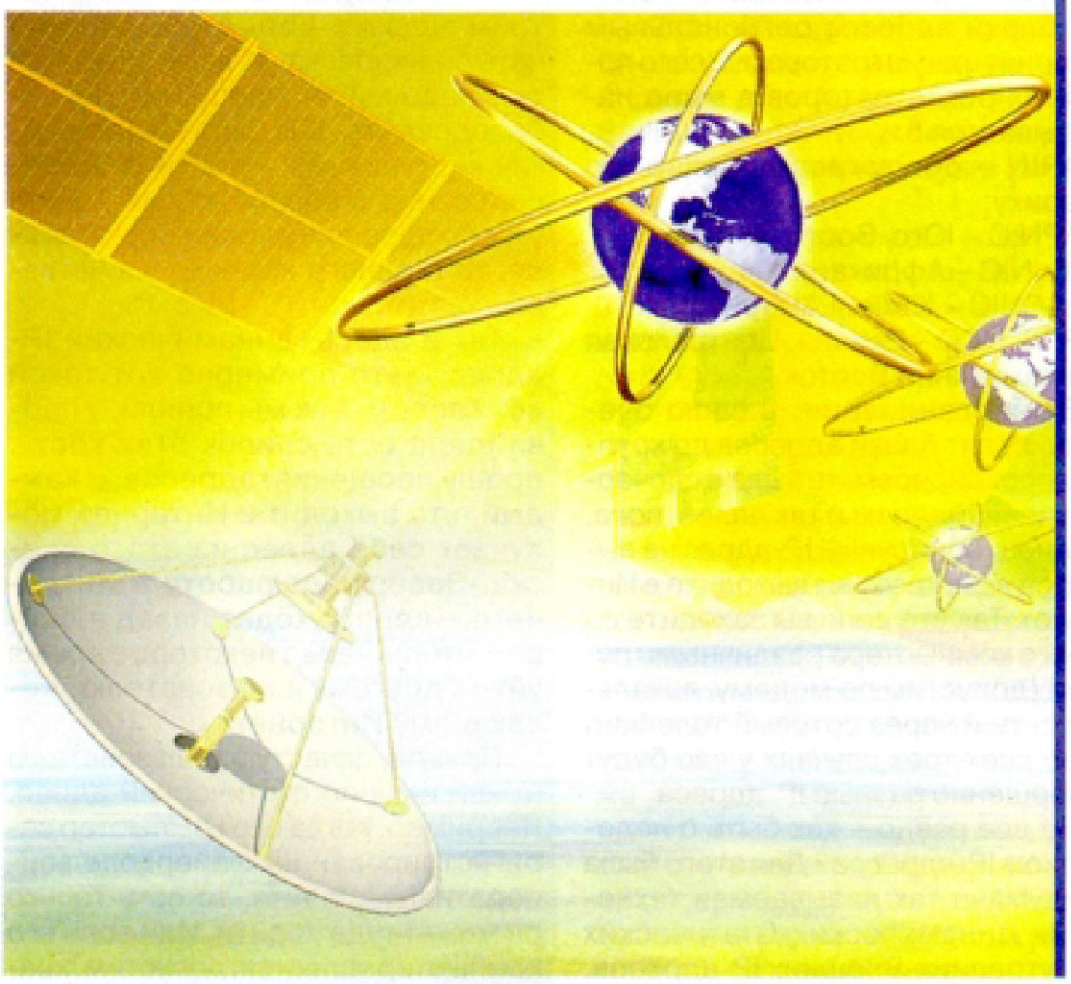
Какие следы пользователь оставляет в Интернете?

Когда вы просматриваете веб-страницу, ваш компьютер передает в Сеть следующую информацию:

* дату и время посещения веб-страницы;
* версию операционной системы и веб-браузера;
* адрес сайта, с которого вы перешли сюда, и ссылку, по которой двинулись дальше.

Кроме того, при посещении многих ресурсов cookies записываются на жесткий диск вашего ПК. С одной стороны, cookies – вещь полезная – например, именно благодаря им положенный в корзину на сайте интернет-магазина товар сохраняется там в течение всего времени «шопинга», несмотря на то что вы перемещаетесь по самым разным страницам. Кроме того, в «куках» сохраняются все пользовательские настройки, сделанные на данной веб-странице, и сведения, введенные в веб-формах. Плохо то, что на основании информации, содержащейся в cookies, можно отследить ваши привычки и предпочтения и составить небольшое, но весьма любопытное «досье».

http://www.computerbild.ru



КОМПЬЮТЕР ДЛЯ НАЧИНАЮЩИХ

№2 (14),февраль, 2011 г.

Подписной индекс
10188

Главный редактор
Михаил Андреев

Телефон (831) 432-98-16
E-mail friendcomp@gmi.ru

Учредитель
ЗАО «Издательство «Газетный мир»
Издатель
ЗАО «Издательство «Газетный мир»

Адрес издателя и редакции:
603126, Н.Новгород,
ул. Родионова, дом 192, корп.1
www.gmi.ru

Рекламное агентство
Телефон
(831) 434-88-20
факс (831) 434-88-22
e-mail reclama@gmi.ru

За достоверность рекламной информации ответственность несет рекламодатель

Служба продаж
Телефоны:
(831) 275-95-22,
438-00-54
e-mail sales@gmi.ru
Служба экспедирования и перевозок
Телефон (831) 434-90-44
e-mail dostavka@gmi.ru

Газета зарегистрирована Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Свидетельство о регистрации средства массовой информации ПИ № ФС77-37573 от 17 сентября 2009 г.

Подписано к печати
24 января 2010 г. в 16 часов
(по графику – в 16 часов).
Дата выхода в свет
7 февраля 2011 г.

Тираж 15207. Заказ № 5167002.

Цена договорная

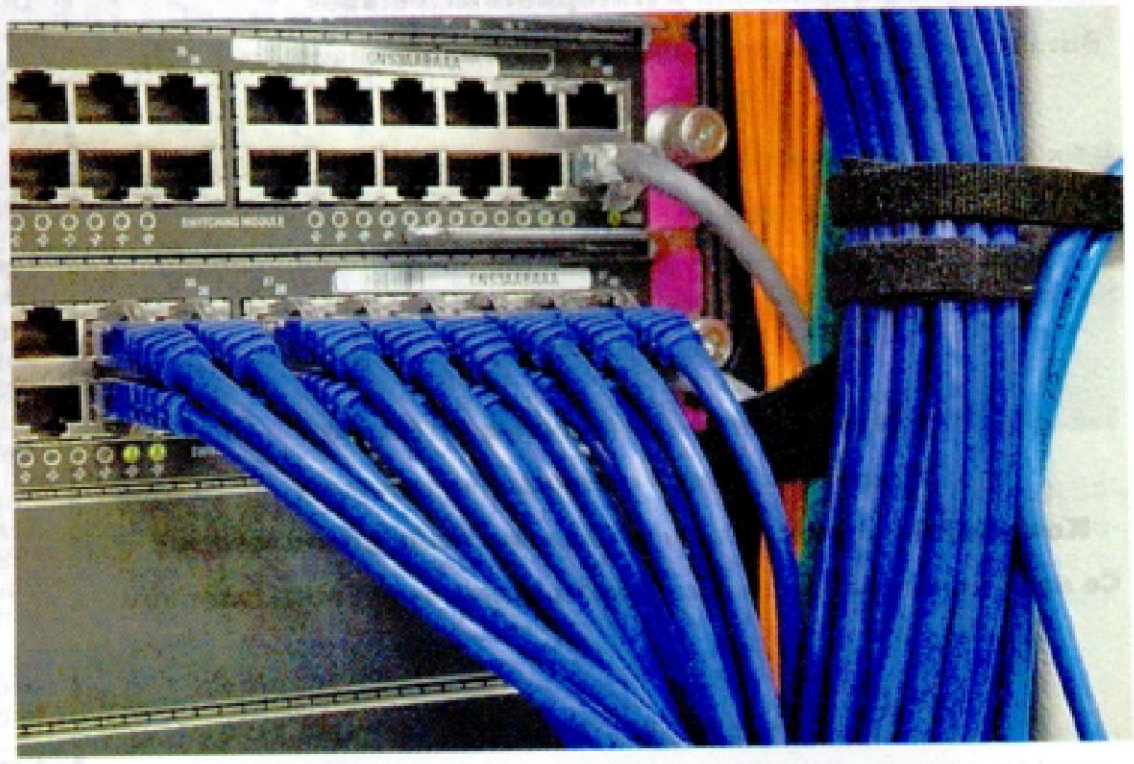
Отпечатано
в ОАО «Нижполиграф»,
603950, г. Н.Новгород,
ул. Варварская, 32

Дизайнер обложки
Андрей МАНИК

Технический редактор
Поль МАНИК

Что такое IP-адреса, откуда они берутся и какими бывают?

Вы включаете компьютер, заходите в Интернет, запускаете браузер и заходите на любимый сайт. Но не все задумываются – а что при этом происходит где-то там внутри компьютера. А происходит столько всего интересного.



К примеру, вашему компьютеру тут же выдают личный номер, и теперь все общение с другими компьютерами (скачивание файлов, прогулки по интернет-страницам, общение в ICQ) происходит строго по нему.

Что же это за номер? Это так называемый IP-адрес и каждое устройство, имеющее выход в Интернет, им обладает. Это ни много ни мало – основа всего Интернета.

IP-адрес (ай пи – от Internet Protocol)– это несколько цифр, вида 127.0.0.1 (это, грубо говоря, адрес компьютера, не подключенного к сети). В теории может варьироваться от 0.0.0.0 до 255.255.255.255. Правда, другие компьютеры видят эти цифры в несколько иной форме, точнее в виде нулей и единиц (допустим, тот адрес, который я написал выше, будет выглядеть как 01111111000000000000000000000001 – правда, неплохая строчка?).

Эти цифры можно сравнить с вашими паспортными данными, ведь именно по ним другие компьютеры понимают – куда нужно передать данные и откуда пришел запрос. Но паспортные данные это лишь с несколькими допущениями. Легко подсчитать, что всего IP-адресов может быть 4.228.250.625 (255 в четвертой степени), а сейчас, когда даже кофеварка может иметь доступ в Интернет, подобных номеров надо гораздо больше. А часть адресов уже зарезервированы под различные технические нужды, а часть уже жестко привязана к компьютерам. Как же тут быть? Над решением подобной задачи работы уже ведутся и даже есть решение, но пока мы вынуждены мириться с тем, что есть. Итак, как же люди выходят из положения?

В IANA (Internet Assigned Numbers Authority – «Администрации адресного пространства Интернета») следят, как эти адреса расходуются, собирают уже ненужные, чтобы вновь вернуть их в использование, выдавая блоки адресов региональным интернет-регистраторам. Всего подобных регистраторов в мире насчитывается 5:

ARIN – обслуживает Северную Америку;

APNIC – Юго-Восточная Азия;

AfriNIC – Африка;

LACNIC – Южная Америка;

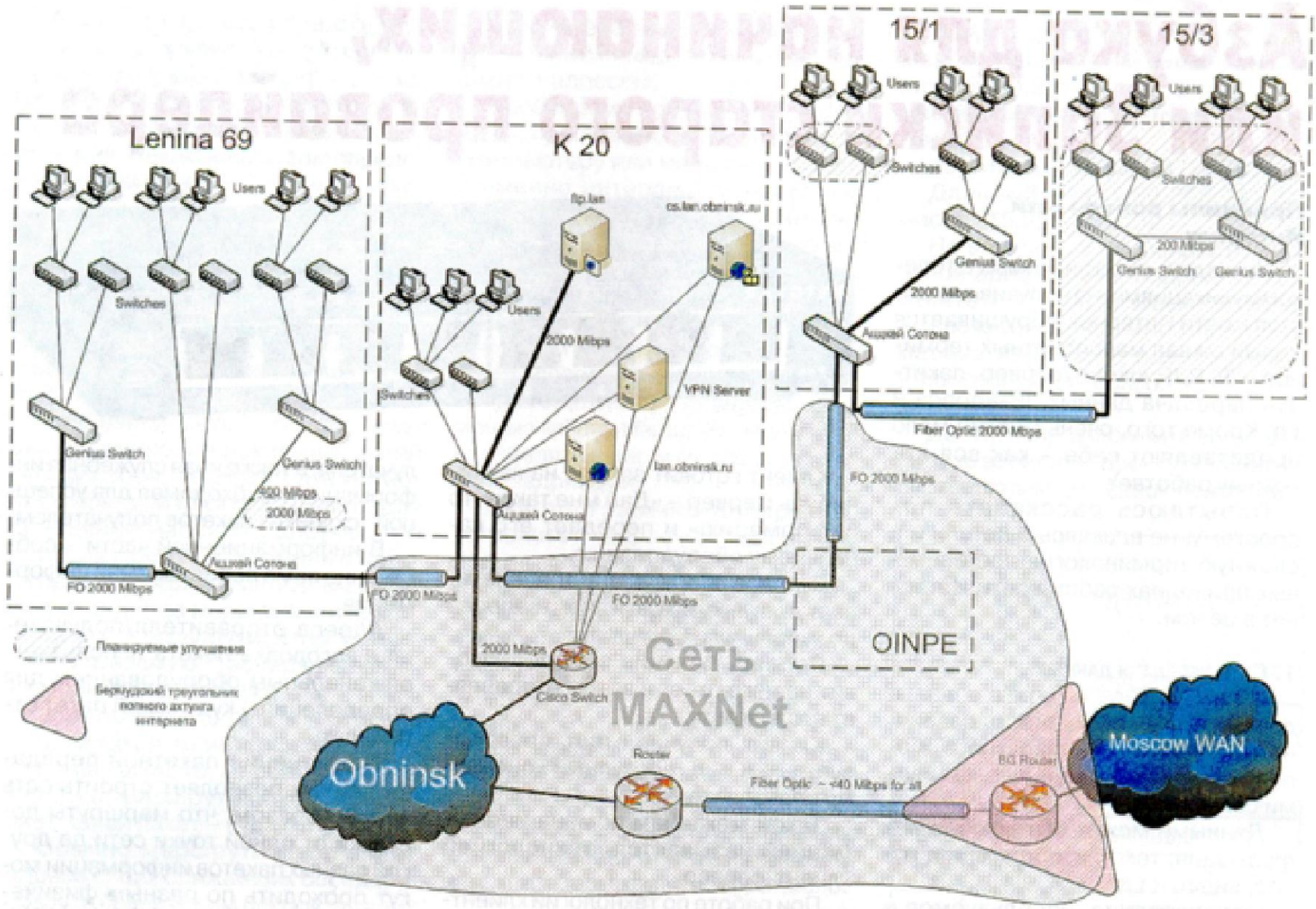
RIPE NCC – Европа, Центральная Азия, Ближний Восток.

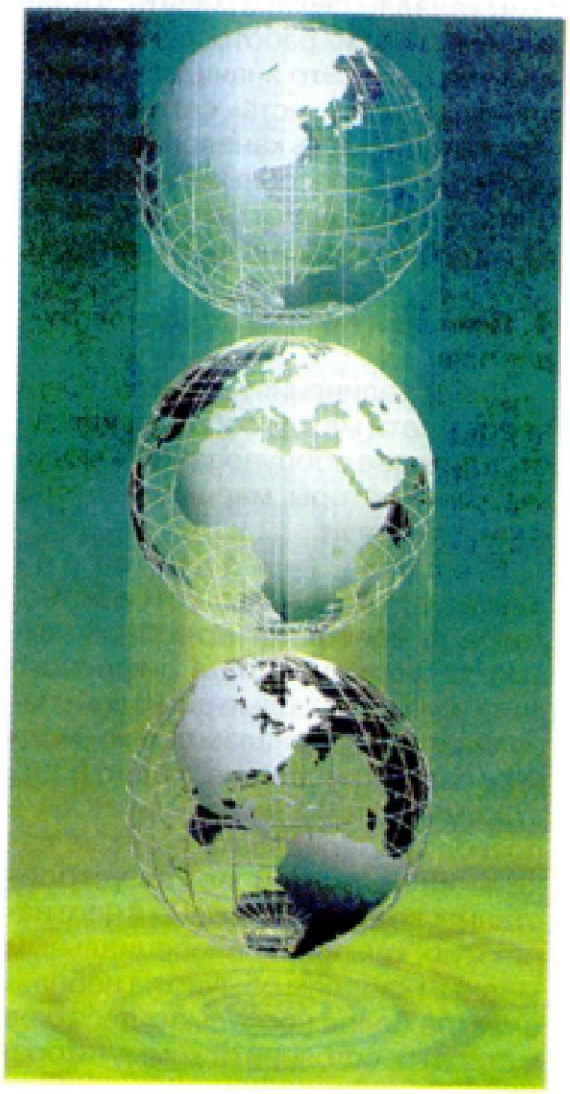
Эти организации, в свою очередь, делят блоки адресов по крупным провайдерам, те выдают дочерним провайдерам и так далее, пока, наконец, одиночный IP-адрес не выдается вам, когда вы выходите в Интернет. Так что если вы заходите со своего компьютера различными путями (допустим по модему, локальной сети и через сотовый телефон) то во всех трех случаях у вас будут совершенно разные IP-адреса.

Но все равно – как быть с недостатком IP-адресов? Для этого была придумана так называемая технология Динамических-Статических и Внутренних-Внешних IP-адресов. Что это за чудо? Давайте рассмотрим задачку. Есть два костюма и четыре человека. И всем этим людям надо пойти... допустим, на собеседование. Как быть? Самое логичное решение – пойти на собеседование в разное время – двое утром, двое днем. Если постараться, то и одного костюма на четверых хватит.

Так и здесь, динамический IP-адрес – это примерно вот такой вот костюм. Как мы поняли, у провайдера есть список этих кост... прошу прощения, адресов, и каждый, кто выходит в Интернет, получает себе адрес из этого списка. Завершает работу в Интернете – адрес уходит назад в список, чтобы через некоторое время уйти к другому пользователю, желающему Интернета.

Правда, зачастую пользователю нужен именно статический адрес. Например, когда его компьютер зарегистрирован на файерволе корпоративного сайта, то есть только он может туда пройти. Или если его компьютер является, допустим, хра-





нилищем базы данных или на нем находится сайт.

Хороший ход со сменой адресов? Вполне, но введение динамических адресов тоже не решает всех проблем, и их по-прежнему не должно хватать. Почему же эта система еще работает?

Давайте подумаем еще. У нас есть локальная сеть из, допустим, 10 компьютеров. Один из них подключен к Интернету, но и остальным нужно выходить в Интернет, пусть периодически, но надо. Что мы будем делать? Выкупать себе 10 IP-адресов? Или к каждому компьютеру тянуть соединение? Не стоит.

Тот один компьютер, у которого есть доступ в Интернет, будет у нас роутером, или маршрутизатором по-русски. Как мы помним, все компьютеры у нас в сети и, соответственно, у каждого из них есть внутрисетевой IP-адрес (у них такой же вид, как и у интернет-адресов и под них даже выделены специальные диапазоны 192.168.0.0, 172.16.0.0 и 10.0.0.0). Вот эти адреса будут у нас являться внутренними IP-адресами. Общаться с миром они будут через наш маршрутизатор, у которого есть доступ в Интернет и значит IP-адрес (а это уже будет внешний IP-адрес).

То есть пользователь со своего компьютера хочет выйти на сайт, набирает адрес сайта, и запрос уходит на маршрутизатор. Тот, в свою очередь, связывается с сайтом и загружает информацию, пересылая ее на компьютер пользователя.

И таких сетей может быть сколько угодно, в теории опять же. Ведь скоро ожидается такое нашествие компьютеров (да сейчас чуть не каждый телефон уже обладает IP-адресом), что и это ухищрение может не сработать. Именно поэтому разработана сеть IPv6 (мы работаем на IPv4), впрочем, это тема уже для другой статьи.

Ну а узнать свой собственный IP-адрес вы можете, если запустите Командную Строку (Меню Пуск – Программы – Стандартные – Командная Строка) и наберете в ней ipconfig.

Слава ЕЖИКОВ.
HTTP://SHKOLAZHIZNI.RU

Азбука для начинающих, или Записки старого провайдера

Принципы работы сети Интернет

На людей, мало знакомых с телекоммуникациями, но получивших доступ к сети Интернет, обрушивается целый шквал малопонятных терминов – TCP/IP, клиент/сервер, пакетная передача данных, IP-адреса и т.п. Кроме того, очень многие мало представляют себе – как вся эта «кухня» работает.

Попытаюсь рассказать попростому, не вдаваясь в детали и в сложную терминологию, об основных принципах работы сети Интернет в целом.

1. Сеть передачи данных

Итак. Сеть передачи данных – это совокупность различного программно-аппаратного оборудования, соединенного каналами связи.

Данными может быть любая информация: текст, изображение, голос, видео и т.д.

Оборудование, используемое в сети, можно разделить на три категории:

1) Клиентское оборудование (Клиент) – рабочая станция (персональный компьютер), ноутбук, телефон, телевизор... Т.е. любое устройство, которое может сформировать по команде пользователя или автоматически запрос на получение информации из сети, получить ответ на свой запрос и отобразить полученную информацию в вид, доступный для потребителя информации.

2) Серверное оборудование (Серверы) – это своего рода хранилища данных, которые получают запросы от Клиентов на получение нужной им информации, формируют и отправляют Клиентам ответы на их запросы или передают информацию другим Серверам для хранения или для передачи другим Клиентам.

3) Сетевое оборудование – оборудование, которое обеспечивает передачу информации по сети между Клиентами и Серверами, и собственно сами каналы связи.

2. Технология клиент-сервер

В общем случае сеть работает так:

Клиент готовит запрос на какой-нибудь Сервер – «Дай мне такую-то информацию» и передает его канальному оборудованию.

Сетевое оборудование обеспечивает доставку по сети этого запроса до указанного Сервера.

Сервер, получив запрос, готовит на него ответ и затем отправляет его Клиенту.

Клиент, получив ответ, преобразует его в вид, доступный конечному пользователю.

Такой механизм обмена информацией называется «технологией клиент-сервер».

При работе по технологии клиент-сервер Клиент является инициатором передачи данных и может сделать запрос когда ему вздумается. В перерывах между запросами Клиент может быть вообще выключенным.

Сервер же, напротив, должен быть включен всегда и должен постоянно «слушать» сеть – нет ли для него нового запроса от какого-нибудь Клиента.

3. Пакетная передача данных

Сеть Интернет относится к сетям пакетной передачи данных. Что это означает?

Вся информация в сети передается исключительно небольшими порциями – пакетами. Любой Клиент и любой Сервер умеют преобразовывать поток передаваемой информации в набор отдельных пакетов и «склеивать» полученные пакеты обратно в поток информации.

Обычно размер пакетов в сети небольшой – от нескольких байт до нескольких килобайт.

Каждый пакет состоит из заголовка и информационной части.

Заголовок – это аналог почтового конверта. В заголовке указывается кому и от кого этот пакет передан – адрес отправителя пакета и адрес получателя, а также иная служебная информация, необходимая для успешной «склейки» пакетов получателем.

В информационной части – собственно сама передаваемая информация.

Адреса отправителя/получателя в заголовке пакета используется канальным оборудованием для определения – куда какой пакет отправлять.

Применение пакетной передачи данных позволяет строить сеть таким образом, что маршруты доставки от одной точки сети до другой разных пакетов информации могут проходить по разным физическим каналам связи и меняться в зависимости от их работоспособности или загрузки. Это значительно увеличивает «живучесть» сети в целом – даже если часть каналов связи будут неработоспособными, информация все равно может быть доставлена по другим работающим каналам.

4. Принципы работы сетевого оборудования

Для объединения Клиентов и Серверов в сети между собой используется сетевое оборудование – модемы, коммутаторы, маршрутизаторы и каналы связи.

Модем («модулятор-демодулятор») – это устройство, которое позволяет преобразовывать информацию из/в цифрового вида в/из аналоговые сигналы и передавать ее по каналам связи – медным проводам, оптике, радио и т.д.

Коммутатор (Switch или HUB) – позволяет передавать сетевые пакеты информации между устройствами, которые включены в него напрямую, как правило, специальным медным кабелем обычно на небольшом (не более нескольких десятков метров) расстоянии от коммутатора.

Коммутатор имеет достаточно большое количество интерфейсов (портов подключения) – до нескольких десятков, автоматически может обнаруживать, какие устройства, в него включены, и сам определять, какой пакет информации какому устройству передавать.

Коммутаторы обычно применяются для организации локальных сетей по комнате или зданию и в принципе позволяют обмениваться информацией Клиентам и Серверам, к ним подключенным, даже без выхода в глобальную сеть.

Глобальная сеть – это фактически объединение локальных сетей между собой. А так как сеть Интернет сложная и многосвязная, то для выяснения маршрута доставки по сети для каждого конкретного пакета применяются специальные сетевые устройства маршрутизаторы.

Каждый маршрутизатор хранит так называемую «таблицу маршрутизации», в которой указано – пакеты для таких-то адресов – отправлять на такой-то интерфейс, а других – на такой-то, и, согласно этой таблице, маршрутизатор определяет, какой пакет – куда отправить.

Обычно маршрутизатор знает адреса своих ближайших соседей и сразу отправляет им пакеты, для них предназначенные. А все остальные – отправляет по т.н. default-маршруту (маршруту по умолчанию). Обычно им является «вышестоящий» маршрутизатор.

Таблицы маршрутизации могут быть как статическими, т.е. постоянными и неизменными, так и динамическими, меняющимися по определенным правилам.

Применение динамической маршрутизации значительно повышает «живучесть» сети, так как позволяет менять маршруты доставки пакетов в зависимости от исправности или перегрузки тех или иных каналов связи.

Адресация в Интернете

1. Что такое IP-адрес и зачем он нужен

Для того чтобы маршрутизаторы могли определять, куда направлять каждый конкретный пакет информации, передаваемый по сети, в заголовке каждого пакета обязательно указывается адрес отправителя и адрес получателя пакета.

Адресация в сети Интернет организована очень просто. Каждой точке подключения любого устройства к сети (интерфейсу) присваивается уникальный номер, который и называют IP-адресом.

Необходимо подчеркнуть, что IP-адрес присваивается не устройству (компьютеру или маршрутизатору), а именно интерфейсу, поскольку многие устройства могут иметь несколько точек подключения к сети, а следовательно и несколько различных IP-адресов.

Компьютеры и маршрутизаторы «знают» свои IP-адреса и адреса своих «соседей в сети», а маршрутизаторы еще и могут определять с помощью таблиц маршрутизации, куда направлять пакеты со всеми прочими IP-адресами.

Для программно-аппаратных устройств IP-адрес – это просто целое число, для хранения которого выделяется ровно 4 байта памяти. Т.е. число в диапазоне от 0 до 4294967295. Человеку запоминать такие громоздкие числа сложно. Поэтому для наглядности IP-адрес записывается в виде последовательности четырех чисел, разделенных точками в диапазоне от 0.0.0.0 до 255.255.255.255. Каждое из этих четырех чисел соответствует значению отдельно каждого байта из тех четырех, в котором хранится все число.

2. Что такое IP-сети и маски подсетей

Для обеспечения правильности работы маршрутизаторов и коммутаторов в сети IP-адреса распределяются между интерфейсами не произвольно, а, как правило, группами, называемыми сетями или подсетями. Причем IP-адреса могут группироваться в сети и подсети только по строго определенным правилам.

Количество IP-адресов (размер) в любой подсети всегда должно быть кратно степени числа 2. То есть – 4, 8, 16, 32 и т.д. Других размеров подсетей быть не может. Причем первым адресом подсети должен быть такой адрес, последнее (из четырех) чисел которого должно делиться без остатка на размер сети.

При использовании любой IP-сети нужно всегда помнить, что первый и последний адреса подсети – служебные и использовать их в качестве IP-адресов интерфейсов нельзя.

Для сокращения и упрощения описания подсетей существует понятие «маска подсети». Маска указывает на размер подсети и может быть описана двумя вариантами записи – коротким и длинным.

Например, описать подсеть размером 4 адреса, начинающейся с адреса 80.255.147.32, с помощью маски можно следующими вариантами:

Короткий – 80.255.147.32/30

Длинный – сеть 80.255.147.32, маска 255.255.255.252

Не вдаваясь в особенности двоичной арифметики, подробно объяснить – что такое маска довольно сложно, но знакомые с бинарной математикой могут разобраться в этом сами, а для большинства – это не суть важно.

Достаточно запомнить (или где-нибудь записать) простую табличку соответствия для масок подсетей:

Размер сети	Короткая маска	Длинная маска
4	/30	255.255.255.252
8	/29	255.255.255.248
6	/28	255.255.255.240
32	/27	255.255.255.224
64	/26	255.255.255.192
128	/25	255.255.255.128
256	/24	255.255.255.0

3. «Белые» и «серые» IP-адреса

К сожалению, общее количество возможных IP-адресов ограничено. Во времена создания сети Интернет и разработки основных протоколов ее работы никто и подумать не мог, что более чем 4 миллиардов допустимых адресов может быть мало. Но с развитием сети Интернет этого количества уже давно не хватает. Поэтому предпринимаются различные меры для жесткой экономии IP-адресов.

Одним из способов экономии является разделение всего пула адресов на так называемые приватные или «серые» и реальные или «белые» IP-адреса.

В Интернет-сообществе существует договоренность, что часть адресов разрешено использовать только для устройств, работающих в локальных IP-сетях, не имеющих выхода в глобальную сеть Интернет. Эти IP-адреса принято называть приватными или «серыми».

Вот полный перечень возможных «серых» адресов:

192.168.0.0 – 192.168.255.255 или 192.168.0.0/16

172.16.0.0 – 172.31.255.255 или 172.16.0.0/12

10.0.0.0 – 10.255.255.255 или 10.0.0.0/8

Все остальные IP-адреса называют реальными или «белыми».

Для того чтобы пакеты с «серыми» адресами в заголовке не попадали в глобальный Интернет, на устройствах, установленных на границах локальных и глобальных сетей (т.н. «граничных маршрутизаторах»), такие пакеты просто отфильтровываются. Поэтому в разных локальных сетях могут работать устройства с одним и тем же «серым» IP-адресом и друг другу они «мешать не будут».

4. NAT-сервис

Существует механизм, позволяющий устройствам с «серыми» адресами из локальных сетей все-таки получать доступ к информации из глобальной сети. Для этого на граничном маршрутизаторе устанавливаются программы, реализующие т.н. NAT-сервис.

Граничный маршрутизатор, как правило, имеет минимум два интерфейса, один из которых «смотрит» в локальную сеть с «серым» адресом, а другой, с «белым» адресом «смотрит» в глобальную сеть.

Суть работы NAT-сервиса заключается в следующем. Получив от устройства с «серым» адресом пакет с запросом на получение информации из глобальной сети, маршрутизатор запоминает, от какого «серого» адреса пришел запрос, и заменяет в заголовке пакета «серый» адрес на свой «белый», а затем отправляет его в глобальную сеть. Получив из глобальной сети ответ, маршрутизатор определяет – для какого «серого» адреса пришла эта информация, заменяет в пакете свой «белый» адрес на «серый» адрес локального устройства и передает ему этот пакет.

При использовании NAT-сервиса пользователь компьютера с «серым» адресом может получить по своим запросам полный доступ к любым ресурсам глобальной сети. Т.е. как Клиент может получать любую информацию от Серверов в сети.

А вот Сервер с «серым» IP-адресом «из-за NAT'а» работать не будет, так как из глобальной сети получить доступ к этому компьютеру просто не удастся. Но вообще-то это не совсем точно. Существует механизм т.н. «обратного NATа», с помощью которого можно обеспечить доступ из глобальной сети к серверам (MAIL, WWW, FTP и др.) клиента, работающим под «серым» адресом, но это требует не тривиальной настройки маршрутизатора клиента и далеко не каждый маршрутизатор это умеет делать...

Применение NAT-сервиса целесообразно для домашних подключений частных лиц и небольших организаций, которые не имеют своих информационных ресурсов.

5. «Динамические» и «статические» IP-адреса

Еще один способ экономии IP-адресов, используемый в основном провайдерами, – применение т.н. динамически выделяемых IP-адресов.

В идеальном случае каждое устройство в сети должно иметь постоянный (или «статический») IP-адрес. Но для устройств, подключающихся к сети только иногда – время от времени (на «сеанс связи»), закреплять на ними постоянные адреса слишком расточительно.

Для большинства клиентов, подключающихся только на сеанс связи, совершенно безразлично, какой именно IP-адрес им будет выделен, поэтому провайдеры обычно им выделяют т.н. «динамические» IP-адреса.

Суть приема заключается в следующем. Провайдер заранее выделяет некоторое количество адресов для подключения клиентов на сеанс связи. Причем общее количество таких адресов обычно значительно меньше, чем общее количество клиентов. При подключении очередного клиента ему выдается произвольный и на данный момент свободный IP-адрес из этого зарезервированного списка и он у провайдера помечается как «занятый». При отключении клиента признак заменяется на «свободный» и этот IP-адрес может быть выдан другому, вновь подключившемуся клиенту.

Если же клиенту важно, чтобы его IP-адрес был всегда один и тот же, то в этом случае провайдер «закрепляет» конкретный IP-адрес за клиентом, т.е. ему выделяется «статический» IP-адрес.

Такое подключение может потребоваться клиентам, которые со своих компьютеров обращаются к особым – защищенным – ресурсам сети, владельцы которых установили ограничение на доступ к своим ресурсам или хотят его контролировать, для чего проверяют, а с какого IP-адреса произошло обращение к ресурсу.

Например, если сотрудник какой-либо организации подключается из дома к сети Интернет «на сеанс связи» и хочет обращаться к компьютерам, установленным у него на работе. Как правило, в организациях строго контролируется доступ извне в сеть предприятия, но при наличии статического IP-адреса для этого адреса можно сделать исключение. В случае динамического адреса такое исключение сделать нельзя, так как заранее неизвестно, какой именно IP-адрес получит клиент после подключения.

6. Уникальность «белых» адресов и «подмена» IP-адреса

Для правильного функционирования всей сети Интернет необходимо строгое обеспечение уникальности «белых» IP-адресов. Для этого провайдеры тщательно контролируют адреса своих клиентов. Контроль обеспечивается двумя способами:

1) При постоянном подключении клиентов по выделенным каналам, провайдер так конфигурирует свое оборудование, что клиент может использовать только конкретные, выделенные только ему IP-адреса и при попытке использовать другие, клиент доступа в сеть просто не получит.

2) При подключении на сеанс связи оборудование клиента (модем или компьютер) прежде чем получит от провайдера IP-адрес, должен произвести авторизацию на сервере доступа провайдера по Логину/Паролю. И только в случае успешной авторизации сервер доступа выдаст оборудованию клиента «белый» «динамический» или «статический» IP-адрес.

Если клиент заменит выделенные ему IP-адреса на какие-нибудь другие, доступа в сеть он не получит, т.к. ближайшие к клиенту маршрутизаторы находятся под управлением провайдера и они эту смену адресов просто проигнорируют. Максимум (да и то далеко не всегда) клиент сможет отправить какие-то пакеты информации в сеть, но получить никакой информации он не сможет. Причем, если провайдер заметит такие действия клиента – он может быть строго на-

казан, вплоть до полного отключения от сети.

7. Что такое «домен» и «доменное имя»?

Уникальный «белый» IP-адрес точно идентифицирует любое устройство, подключенное к сети Интернет. Компьютерным программам работать с ними удобно, а вот людям – не всегда... IP-адреса непросто запомнить, да и понятной для человека информации в IP-адресе немного.

Для облегчения людям работы в сети придумана другая система идентификации устройств. Любому IP-адресу в сети можно присвоить какой-нибудь «словесный», более понятный для человека синоним, который называется «доменным именем» или просто «именем» устройства в сети.

Доменное имя – это последовательность из двух и более слов, разделенных точками. Слово, или, как оно еще называется, домен, может состоять из любой комбинации букв английского алфавита, цифр и знака «–» («минус» или «тире»). Другие символы в доменном имени использовать нельзя.

Последний домен в доменном имени называется «доменом первого уровня», второй от конца – «доменом второго уровня» и т.д.

Существуют две системы организации доменных имен – международная (национальная) и американская, однако в последнее время обе эти системы используются по всему миру и стали практически равнозначными.

По международной системе домен первого уровня должен состоять из двух символов – сокращения от названия страны, в которой зарегистрировано доменное имя. Например: .ru – Россия, .pl – Польша, .fr – Франция, .us – США, .ua – Украина и т.д.

Доменами второго и последующих уровней могут быть любые допустимые комбинации символов.

По американской системе домен первого уровня может состоять из трех или более символов, комбинация которых показывает принадлежность организации, пользующейся этим доменом, к тому или иному типу организации. Например: .com – коммерческая организация, .gov – государственная структура, .edu – образовательное учреждение, .mil – военная организация и т.д.

Доменные имена первого и второго уровня регистрируются и учитываются Техническими Центрами поддержки доменов. В России это – РосНИИРОС.

Любой желающий, как юридическое, так и физическое лицо, может (за умеренную плату) зарегистрировать у Регистратора любой (не занятый на момент регистрации) домен второго уровня, либо в своем национальном домене первого уровня (для России – .ru), либо в любом другом домене первого уровня.

Зарегистрировавший домен второго уровня становится его владельцем и может им пользоваться по своему усмотрению, а также определять принципы формирования поддоменов третьего и последующих уровней в своем домене.

В локальных сетях без доступа в глобальный Интернет и использующих серые IP-адреса никто не запрещает организовать свои собственные доменные имена по каким угодно правилам. Но обращаться к ресурсам по этим доменным именам можно будет только «изнутри» локальной сети. Из других сетей, в том числе и из глобального Интернета доступ по этим именам будет невозможен.

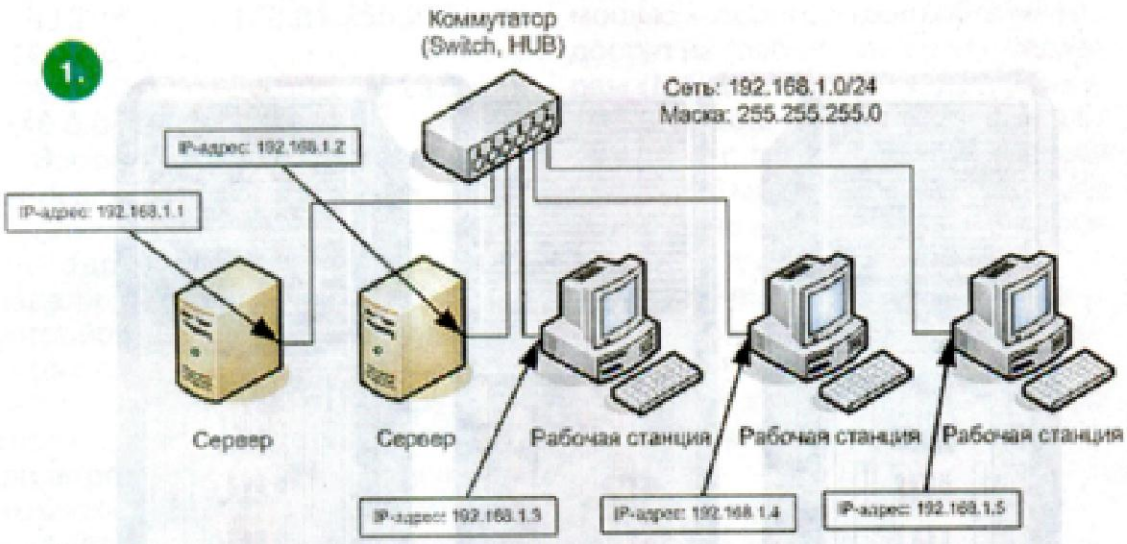
8. Как связываются между собой IP-адреса и доменные имена?

Связь между IP-адресами и доменными именами осуществляет международная распределенная база данных, основанная на использовании так называемых DNS-серверов.

Каждый владелец домена второго уровня должен иметь такой DNS-сервер или арендовать его у кого-либо.

На DNS-сервере в специальных файлах прописывается и хранится соответствие – какое доменное имя соответствует какому IP-адресу (прямая зона) и обратное соответствие IP-адрес – доменное имя (обратная зона) для всех доменных имен, находящихся в ведении владельца домена.

Любое изменение соответствия должно быть обязательно прописано на DNS-сервере, только после этого оно «вступает в силу». Например, вы можете на своем компьютере прописать для него какое хотите доменное имя, но знать об этом будете только вы. Если же такая запись появится на



DNS-сервере, через некоторое время (максимум – несколько часов) об этом узнает весь мир.

Каждая как прямая, так и обратная зона должна храниться как минимум на двух различных DNS-серверах. При этом, главный (как правило, расположенный у владельца) DNS-сервер называется MASTER DNS-сервером, второй или последующие называются SLAVE DNS-серверами.

Зоны, хранящиеся на MASTER-сервере, владелец домена может (и должен) заполнять и корректировать.

На SLAVE-серверах хранятся копии зон с MASTER-серверов, причем обновлениями зон MASTER и SLAVE-сервера обмениваются автоматически.

Все DNC-серверы, включенные в сеть Интернет, могут обмениваться между собой информацией о хранимых ими зонах и о других серверах, хранящих другие зоны.

Любому пользователю, подключенному к сети Интернет, его провайдер предоставляет доступ к своему DNS-серверу, IP-адрес этого сервера прописывается на оборудовании клиента и клиентские программы для работы в сети могут обращаться к этому серверу с запросами – какое доменное имя соответствует какому IP-адресу.

Если пользователь является владельцем зарегистрированного доменного имени он может установить у себя свой собственный DNS-сервер и пользоваться им, а не сервером провайдера.

Принцип работы любого DNS-сервера достаточно прост.

Любой Клиент или Сервер, которому необходимо определить соответствие доменное имя – IP-адрес или IP-адрес – доменное имя, обращается к DNS-серверу с запросом. И если DNS-сервер «знает» это соответствие из своих хранимых зон, то сообщает его сразу. А вот если DNS-сервер ничего не знает о запрошенном доменном имени или IP-адресе, он обращается к другим DNS-серверам «за помощью». Получив ответы на свои запросы от других DNS-серверов, сервер сообщает найденную информацию Клиенту.

Например. Вам необходимо узнать – какой IP-адрес соответствует доменному имени VASYA.PUPKIN.COM. Ваш DNS-сервер ни о зоне .COM, ни о зоне PUPKIN.COM ничего в данный момент не знает. Но сервер знает несколько «главных» в сети DNS-серверов, на которых хранится информация о серверах доменов первого уровня. По запросу вашего сервера «Главный» сервер сообщает ему IP-адрес того DNS-сервера, на котором хранится информация о доменах второго уровня в зоне .COM. Затем ваш сервер обращается к указанному серверу и спрашивает у него – «где хранится зона PUPKIN.COM». Этот сервер ему сообщает адрес очередного DNS-сервера. Далее ваш сервер спрашивает у последнего – «какой адрес для доменного имени VASYA.PUPKIN.COM» и получает точный ответ – доменное имя VASYA.PUPKIN.COM соответствует такому-то IP-адресу.

Схемы организации связи при подключении к Интернету

1. Простейшая схема организации локальной IP-сети

Прежде чем рассматривать схемы организации связи с подключением к сети Интернет, приведу пример схемы простейшей локальной сети.

Современное сетевое оборудование и системное программное обеспечение позволяют практически полностью автоматизировать настройку оборудования в локальной сети при однородном программном обеспечении. Для этого достаточно подключить все компьютеры к коммутатору и после минимальной настройки все они смогут передавать информацию друг другу.

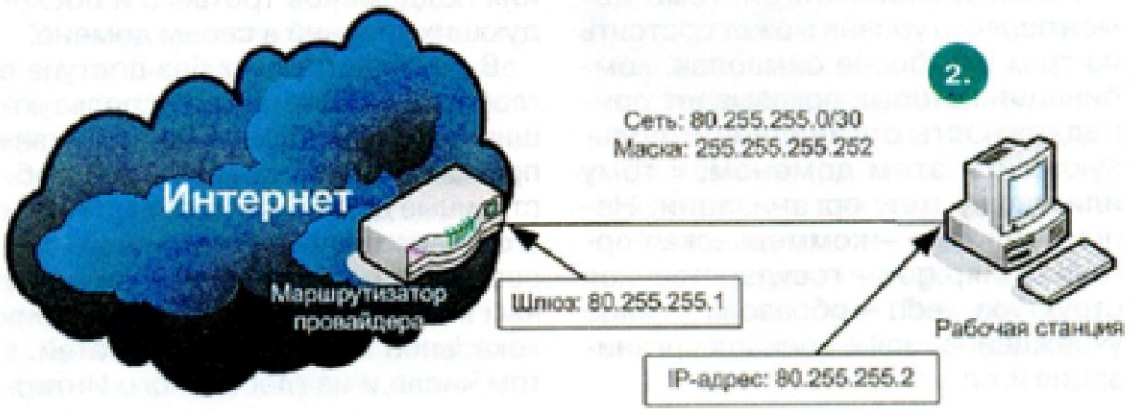
Но в этом случае будет создана локальная сеть, работающая по протоколам той операционной системы, под которой эти компьютеры работают, причем совсем не обязательно, что эта сеть будет IP-сетью, т.е. «кусочком» глобальной интернет-сети.

IP-сеть была разработана еще и для того, чтобы можно было объединять между собой совершенно разнородные «программные среды». Сейчас практически все существующие ОС понимают и умеют работать с протоколами IP-сетей и поддерживают систему адресации, применяемую в Интернете.

На рис. 1 приведен пример простейшей схемы локальной сети, причем не важно под какой «программной средой» (Windows, Lynux, MAC и т.п.).

Для настройки каждого из компьютеров этой сети необходимо задать минимум три параметра – IP-адрес, маску и адрес шлюза. На рисунке они указаны для «серой» сети – 192.168.1.0/24.

Замечу, что адресом шлюза в данном случае может быть любой



не занятый IP-адрес из этой сети, так как шлюз – это адрес, на который необходимо отправлять все IP-пакеты с адресами, не принадлежащими к этой сети, а раз сеть – локальная и ни с кем не связана, то пакеты с неизвестными адресами можно просто проигнорировать, все равно они доставлены никуда не будут.

2. Подключение к Интернету одного компьютера

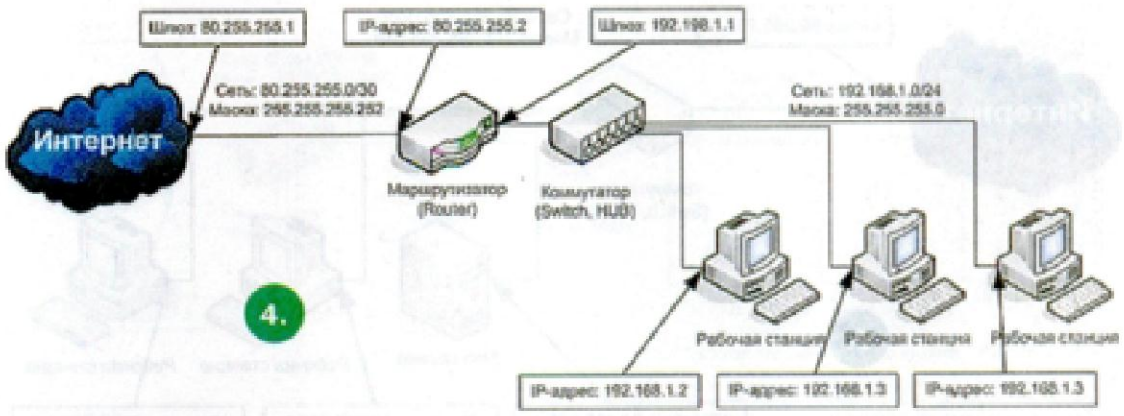
При подключении к Интернету одного компьютера обычно используют один из двух или несколько различных вариантов подключения: с выделением подсети из четырех «белых» IP-адресов («связной четверки») или с выделением одного IP-адреса.

Первый вариант применяется обычно в случае подключения к сети по выделенным каналам связи т.н. «корпоративных клиентов» – организаций, которые в дальнейшем предполагают подключать к сети более одного компьютера. Схема такого включения приведена на рис. 2.

Для пользователей – частных лиц, которые редко подключают к сети более одного компьютера, провайдеры чаще используют второй вариант – схему, приведенную на рис. 3. Эта принципиальная схема позволяет выделять клиентам как статические, так и динамические IP-адреса.

По такой схеме, как правило, подключаются клиенты т.н. «кампусных сетей», сетей FTTx и клиенты, подключающиеся на сеанс связи – DialUP и по технологии ADSL.

Необходимо подчеркнуть, что здесь приведены максимально упрощенные принципиальные схемы подключения – для понимания общего принципа организации связи. Реальные схемы обычно значительно сложнее.



3. Подключение нескольких компьютеров с одним «белым» IP-адресом

Если клиенту необходимо подключить несколько обычных компьютеров (рабочих станций) к сети Интернет, то можно использовать схему, представленную на рис 4. Она фактически является объединением схемы 1 со схемами 2 и 3 с помощью клиентского маршрутизатора.

Причем маршрутизатор должен уметь использовать NAT-сервис – механизм, который делает прямое и обратное преобразование «серых» IP-адресов локальной сети клиента (на схеме – сеть: 192.168.1.0/24) в один «белый» IP-адрес, под которым в Интернете «представляются» все компьютеры локальной сети клиента (на схеме – сеть: 80.255.255.0/30).

Такая схема оптимальна для домашней сети из 2-4 компьютеров или для небольших офисов компаний, в которых используются только обычные рабочие станции.

Достоинства этой схемы – экономия «белых» IP-адресов, независимость от провайдера (с ним не нужно согласовывать ни использование такой схемы, ни количество рабочих станций в ней). Количество одновременно работающих компьютеров, подключенных по этой схеме, может быт очень большое и оно зависит только от производительности маршрутизатора и «ширины» (пропускной способности) канала связи.

4. Подключения с использованием нескольких «белых» IP-адресов

4.1. Подключения с использованием только «белых» IP-адресов.

На рис. 5 приведена наиболее простая (для клиента сети) схема организации связи с использованием только «белых».

Однако провайдеры соглашаются на нее крайне неохотно, так как эта схема, требует чтобы ВСЕ устройства сети клиента имели «белые» адреса, что приводит к их неэкономичному использованию. Кроме того, маршрутизацией всех IP-пакетов передаваемых/принимаемых в Интернете приходится заниматься маршрутизатору провайдера.

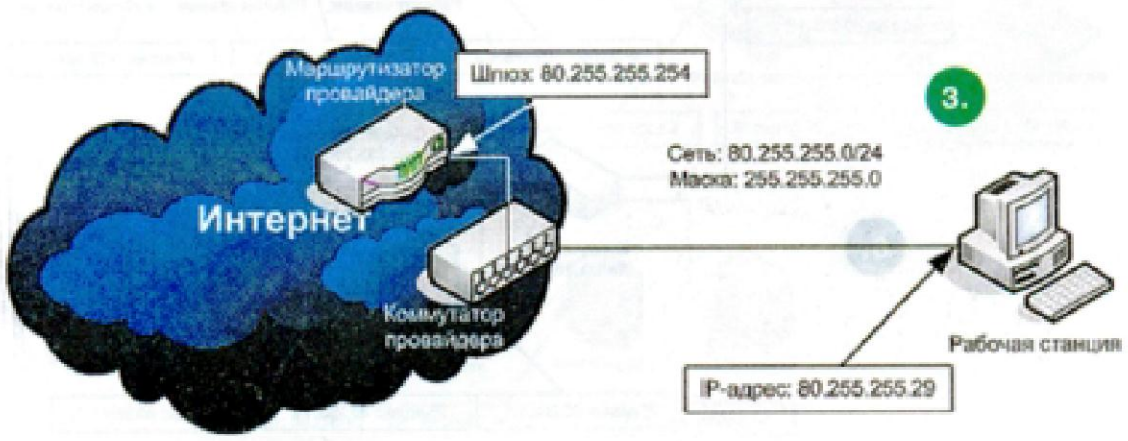
Применение этой схемы допустимо в случаях, когда клиент сети предполагает подключение небольшого количества компьютеров (от 2 до 13), причем часть из них предполагается использовать в качестве серверов.

4.2. Подключения с использованием и «белых», и «серых» IP-адресов

Для подключения большого количества рабочих станций под «серыми» адресами и некоторого количества серверов под «белыми» оптимальны схемы подключения, представленные на рис. 6, 7 и 8.

Схема 6 – более универсальна, но требует от клиента использования достаточно мощного и сложного в настройке маршрутизатора, который должен иметь не менее трех интерфейсов и поддерживать NAT-сервис.

Схема 7 – для клиента более удобна и не требует мощного и сложного маршрутизатора. Она фактически является объединением схем 4 и 5.



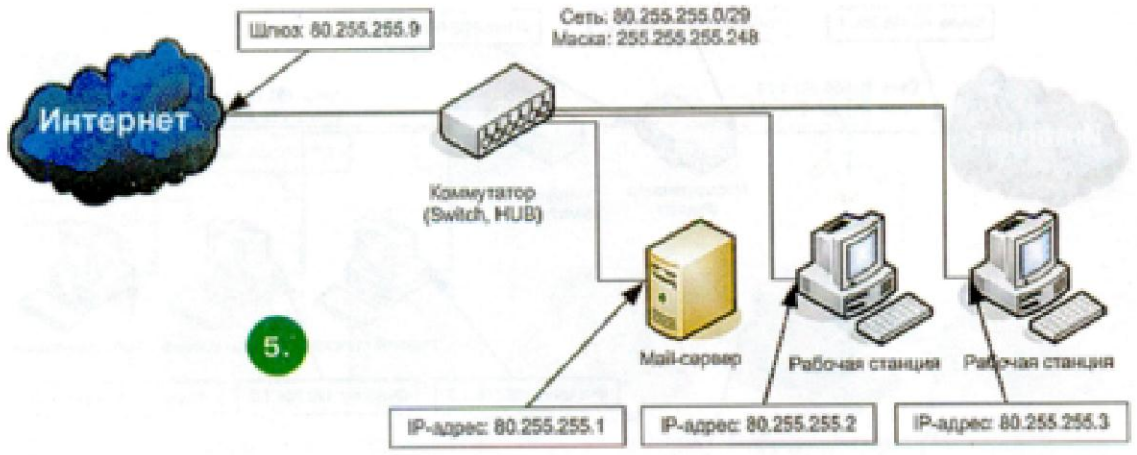


Схема 8 практически не отличается от схемы 7 и имеет смысл, если вы ранее были подключены по схеме 4 и хотите сохранить все «старые» настройки оборудования. Однако эта схема не слишком «экономична» по отношению к количеству белых адресов и не всегда может быть технически реализована провайдером.

Программы для анализа работы в сети

Для общего анализа работоспособности сети в любой операционной среде есть набор простых программ, с помощью которых клиент сети передачи данных может проверять состояние своего собственного подключения к сети, а также анализировать работоспособность сети в целом и отдельных ее компонентов.

Так как большинство клиентских компьютеров все еще работают под операционной системой Windows XP, то примеры здесь будут приводиться именно для этой ОС.

1. Режим командной строки

Большинство команд контроля за состоянием сети работают в «режиме командной строки». Для перехода в этот режим в Windows XP нужно сделать следующие действия:

Нажмите «Пуск» -> «Выполнить...»

В открывшемся окошке в строке ввода наберите слово из трех букв – CMD и нажмите кнопку «ОК».

Откроется новое окошко с черным фоном и мигающим курсором – это и будет «режим командной строки».

2. Программа PING

Для определения есть ли связь в принципе и доступен ли вам тот или иной ресурс сети используется команда PING.

Для всех версий ОС Windows эта команда является встроенной в систему. Для ее запуска перейдите в режим командной строки и наберите в нем:

PING ДОМЕННОЕ_ИМЯ

или

PING IP-АДРЕС

Если указанное в качестве аргумента доменное имя ресурса или его IP-адрес вам доступно по сети, вы получите примерно такое сообщение, которое приведено на **screen 1**.

Команда PING работает примерно таким образом.

Ваш компьютер посылает на указанный IP-адрес короткий пакет данных, который как бы спрашивает у ресурса – «ты живой?». Получив такой пакет, любое работающее в сети устройство, как правило, отвечает на него также коротким пакетом данных – «да, я живой».

Получив ответ, ваш компьютер вычисляет время, которое прошло с момента запроса и до получения ответа, и сообщает его вам.

Если ответ не пришел, то через некоторое время (примерно 1.5-3 сек.) программа считает, что пакет с запросом по какой-то причине «потерялся» и посылает запрос еще раз, а вам сообщает – «Превышен интервал ожидания для запроса».

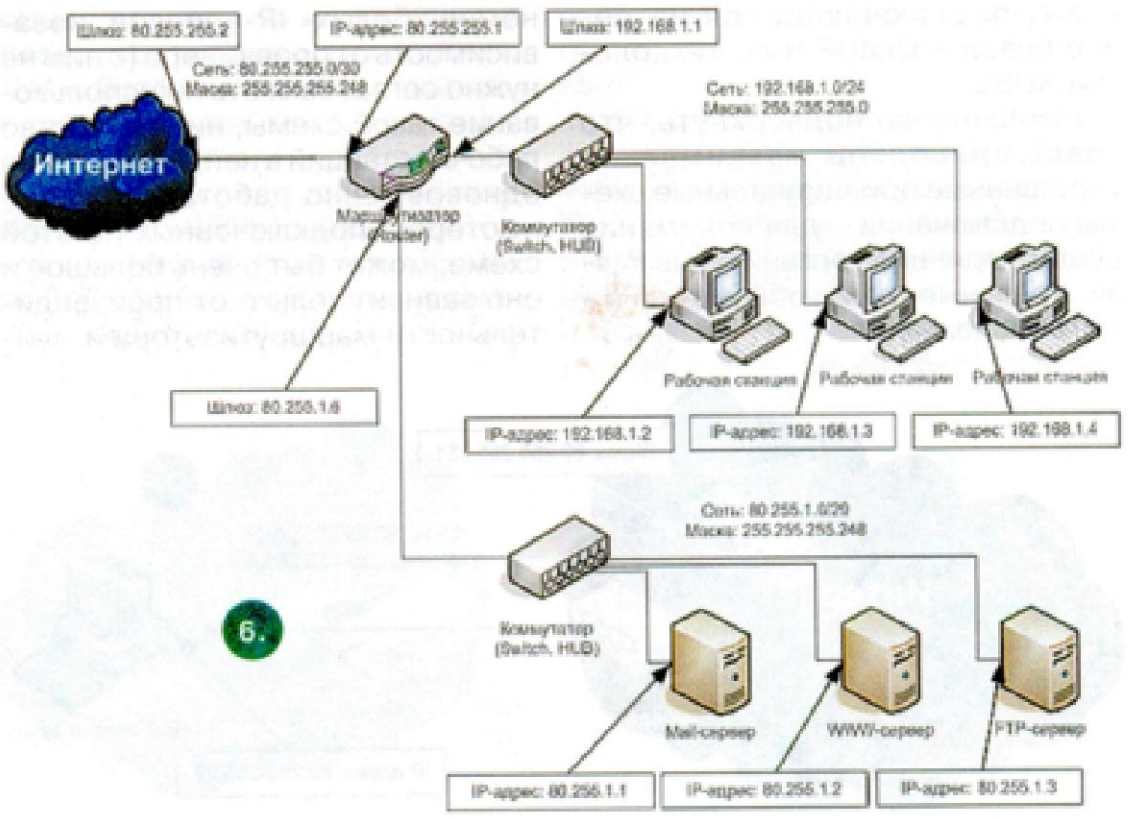
Если после запуска команды PING вы получили только такие строчки, значит, скорее всего, указанный вами ресурс – недоступен.

Необходимо подчеркнуть, что вся числовая информация, выдаваемая командой PING, является весьма приблизительной и позволяет только лишь оценить характеристики канала до указанного ресурса – примерное время задержки отклика указанного ресурса и примерный процент потерь отправленных IP-пакетов.

Причем более-менее точные значения программа PING сообщает ТОЛЬКО на заведомо «пустых» каналах, по которым кроме пакетов команды PING другая информация не передается.

То есть если вы запустили одну или несколько программ, которые активно потребляют ресурсы сети (что-то «качают»), и одновременно запустили PING до какого-нибудь ресурса, то он может показать очень большие задержки, а то и потери пакетов. Но это не означает, что канал очень плохой, а говорит лишь о том, что вы сильно загрузили свой канал (исчерпали его пропускную способность).

Кроме того, даже если PING сообщил вам о недоступности ресурса, совсем не обязательно, что этот ресурс вообще не работает. Вполне возможно, что указанный ресурс



запросы команды PING просто игнорирует.

Кстати сказать, любой компьютер под управлением Windows XP с включенным FireWall'ом именно так и делает!

3. Программа TRACERT

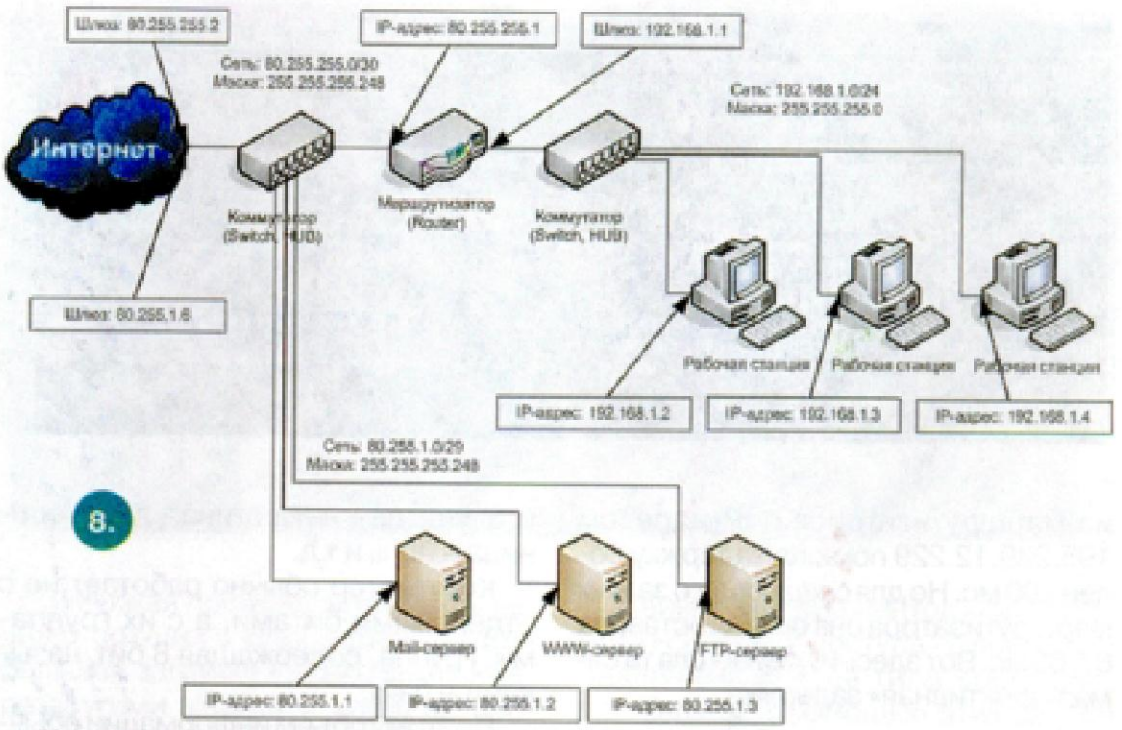
Как это ни странно, но маршруты перемещения информации по сети очень часто никак не связаны с географическим местоположением того или иного сетевого ресурса. Очень часто эти маршруты могут быть весьма экзотическими.

Например, несколько лет назад у нас в одном здании на разных этажах находились две организации, которые использовали сети передачи данных, но были подключены к разным провайдерам. Каково же было удивление сотрудников этих организаций, когда выяснилось, что электронное письмо, посланное с третьего этажа на пятый, попадает туда последовательно через Новосибирск, Москву, Копенгаген, Лондон, а потом обратно в Москву, Новосибирск и только потом в Красноярск в это же здание на пятый этаж.

Выяснить, каким маршрутом пойдут IP-пакеты до интересующего вас адреса, позволяет программа TRACERT (также являющаяся встроенной в ОС Windows). Во всех версиях ОС UNIX эта программа называется несколько иначе – traceroute.

Для запуска программы TRACERT в Windows перейдите в режим командной строки и наберите:

TRACERT ДОМЕННОЕ_ИМЯ
или
TRACERT IP-АДРЕС



8.

Принцип работы этой программы примерно следующий.

Ваш компьютер посылает несколько специальных коротких IP-пакетов до указанного ресурса. Каждый IP-пакет по сети передается последовательно от одного маршрутизатора к другому и каждый маршрутизатор, «пропустив через себя» IP-пакет программы TRACERT, посылает вашему компьютеру уведомление о том, что он этот пакет получил и переслал дальше, и свой IP-адрес.

Ваш компьютер, собрав все эти ответы, выдает вам список всех маршрутизаторов с указанием примерного времени задержки отклика от каждого из них.

Маршрутизаторы, как правило, отвечают на пакеты программы TRACERT, но это происходит не всегда. Некоторые сетевые администраторы по разным причинам запрещают своим маршрутизаторам это делать. В таком случае вместо времени задержки программа TRACERT отображает символы – * («звездочка»).

По величинам задержек ответов можно оценить загрузку каналов связи между маршрутизаторами и определить «узкие» места в общем составном канале от вашего компьютера до интересующего вас ресурса.

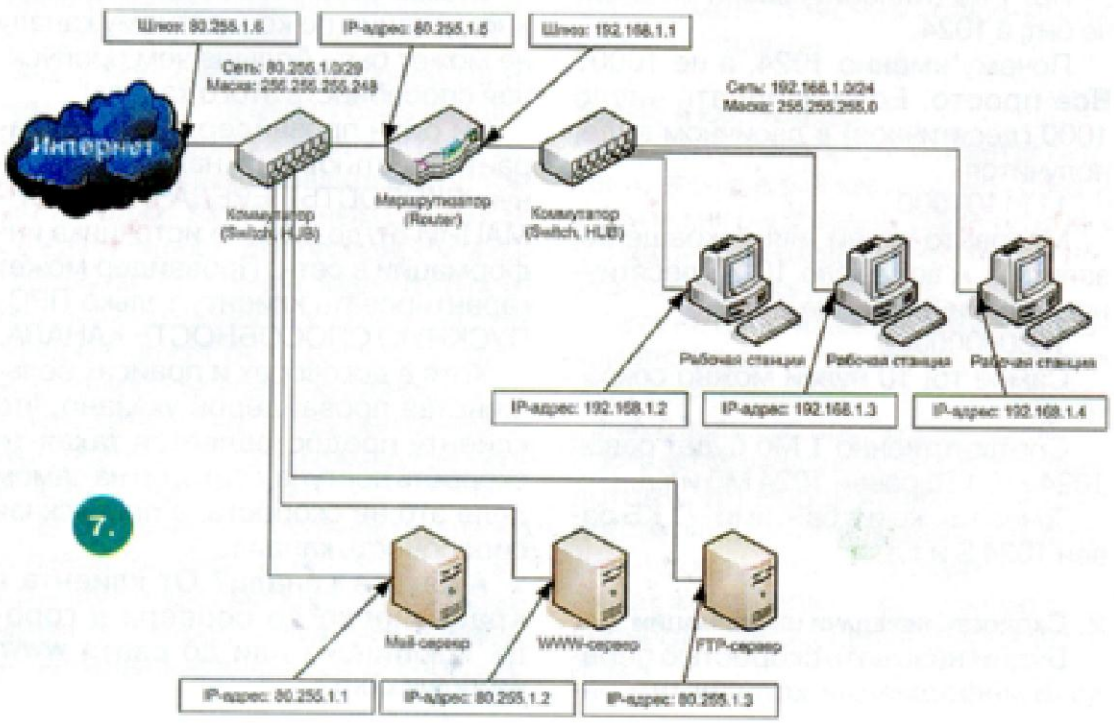
Однако следует иметь в виду, что некоторые маршрутизаторы (в частности, маршрутизаторы фирмы Cisco) обрабатывают адресованные им IP-пакеты программ TRACERT и PING в самую последнюю очередь и при значительной загрузке эти маршрутизаторы могут отвечать с заметным опозданием, а то и вообще не ответить на один или более пакетов.

Это совсем не означает, что в данном месте информация «тормозится» – транзитные пакеты эти маршрутизаторы пропускают без задержек.

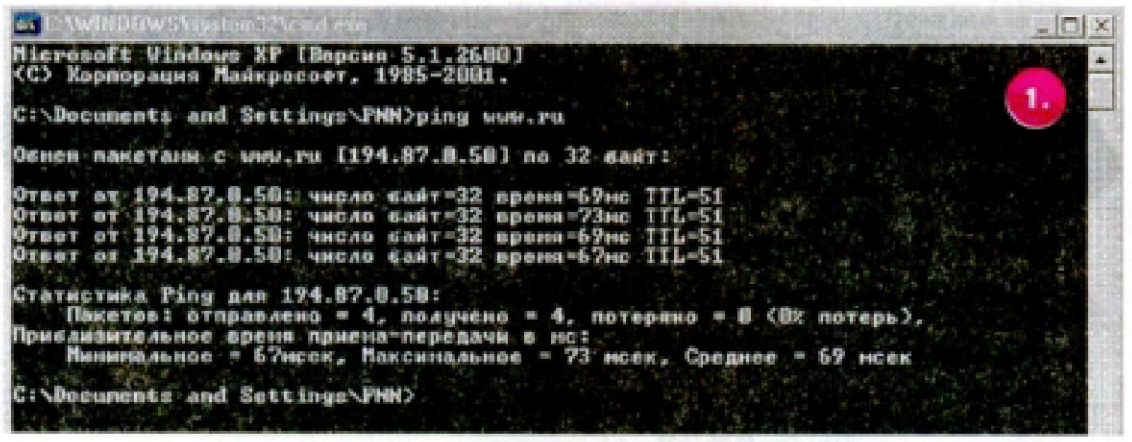
Отличить истинную задержку от вышеописанной (фиктивной) очень просто.

В примере первые четыре маршрутизатора находятся в Красноярске и связаны между собой достаточно быстрыми каналами, поэтому задержка для каждого из них примерно одинакова и составляет 9-11 мс (миллисекунд).

Пятый и последующие маршрутизаторы находятся уже в Москве, длина канала до которой около 4000 км, поэтому истинная задержка выросла и составила 65-80 мс. Однако один



7.



из маршрутизаторов с IP-адресом 195.239.12.229 показал задержку более 100 мс. Но для следующего за ним маршрутизатора она опять составила 67-68 мс. Вот здесь и произошла та самая «фиктивная» задержка.

4. Программа NSLOOKUP

Еще одна крайне полезная программа для работы в сети – NSLOOKUP.

Часто бывает необходимо, зная доменное имя ресурса определить его IP-адрес. Или наоборот – по известному IP-адресу ресурса, определить его доменное имя. Все это умеет программа NSLOOKUP.

Для ее применения в командной строке Windows наберите:

NSLOOKUP ДОМЕННОЕ_ИМЯ
или
NSLOOKUP IP-АДРЕС

Результат работы программы приведен на **screen 2** и, я думаю, никаких дополнительных объяснений не потребует.

Ох уж эта скорость...

1. Необходимый минимум информатики

Как известно, сети передачи данных предназначены для передачи информации.

Информация – особая сущность и измеряется она специфическими единицами.

Так как сеть передачи данных предназначена для передачи информации прежде всего между компьютерами, поэтому и методы ее измерения ориентированы прежде всего на компьютер. А так как все компьютеры используют для своей работы так называемую «двоичную» систему исчисления (а не «десятичную», которой обычно пользуются люди), то и измерение объемов информации тоже ориентировано на двоичную систему.

В информатике существует понятие бит – это минимальный объем информации и он может иметь два состояния: да – нет, истина – ложь, единица – ноль и т.д.

Компьютер обычно работает не с отдельными битами, а с их группами. Группа, содержащая 8 бит, называется байт.

Поэтому объем информации обычно измеряется в количествах бит или байт.

Чтобы избежать путаницы при сокращении наименований, буду далее обозначать маленькой русской буквой «б» или маленькой латинской «b» – «бит», а большими буквами «Б» или «B» – «байт».

В десятичном исчислении для сокращения «количества нулей» при записи больших чисел принято использовать приставки «кило», «мега», «гига» (или сокращенно «к», «м», «г»,) и т.д., которые соответсвенно означают тысячу (1000), миллион (1000000) и миллиард (1000000000).

В двоичной системе есть нечто подобное – «Кило», «Мега», «Гига» (или сокращенно «К», «М», «Г»,) и т.д..

Для того чтобы не путать десятичные «кило, мега, гига ...» с двоичными, двоичные – обычно пишутся с большой буквы.

Но! 1 Кб (Килобит) равен не тысяче бит, а 1024.

Почему именно 1024, а не 1000? Все просто. Если записать число 1000 (десятичное) в двоичном виде, получится -

1111101000

Маловато нулей для сокращения записи... А вот число 1024 (десятичное) в двоичном виде -

10000000000

Самое то! 10 нулей можно сократить.

Соответственно 1 Мб будет равен 1024 Кб, 1 Гб равен 1024 Мб и т.д.

Точно так же и с байтами – 1 КБ равен 1024 Б и т.д.

2. Скорость передачи информации

Будем называть скоростью передачи информации количество информации, выраженное в битах или байтах, переданное в единицу времени. Скорость передачи информации измеряется в битах в секунду – б/с, Килобитах в секунду – Кб/с или Мегабитах в секунду – Мб/с. Или в байтах в секунду – Б/с, Килобайтах в секунду – КБ/с и т.д., соответственно.

(Замечу в скобках – многие мало знакомые с информатикой люди часто путают б/с и Б/с (биты в секунду с байтами в секунду), а они различаются в 8 раз!)

Другое очень схожее понятие, которое часто путают, со скоростью передачи информации, – пропускная способность канала. Измеряется она в тех же единицах, что и скорость, но если скорость передачи информации показывает, как быстро передается информация от источника к получателю безотносительно к тому, как и по каким каналам эта информация передается, то пропускная способность канала показывает, как много информации можно передать по конкретному каналу передачи данных в единицу времени. Т.е. пропускная способность – это максимально возможная скорость передачи данных для конкретного канала.

В сетях передачи данных по одному каналу может одновременно передаваться информация от многих источников ко многим получателям и в зависимости от целого ряда факторов скорость передачи информации для каждой конкретной пары источник-получатель может быть разной, а вот пропускная способность для каждого канала величина, как правило, постоянная.

Сумма всех скоростей передачи информации по конкретному каналу не может быть больше чем пропускная способность этого канала!

Ни один провайдер не может гарантировать клиенту наперед заданную СКОРОСТЬ ПЕРЕДАЧИ ИНФОРМАЦИИ от/до любого источника информации в сети. Провайдер может гарантировать клиенту только ПРОПУСКНУЮ СПОСОБНОСТЬ КАНАЛА.

Хотя в договорах и прайсах большинства провайдеров указано, что клиенту предоставляется такая-то скорость доступа к сети, но на самом деле это не скорость, а пропускная способность канала.

А какого канала? От клиента в Красноярске до сервера в городе Урюпинске или до сайта www.windows.com?

Нет! Провайдер может гарантировать пропускную способность только тех каналов, которые ему принадлежат. Как правило, это канал от клиента до провайдерского канала доступа в глобальный Интернет, от клиента до центрального узла провайдера, на котором находятся его внутренние информационные ресурсы, или от одной точки подключения клиента до другой. Также в какой-то мере провайдер отвечает за пропускную способность его магистральных каналов до других провайдеров сети.

А вот дальше – извините, это уже «зона ответственности» других провайдеров, на которых ваш провайдер, как правило, повлиять никак не может. Так уж построена сеть Интернет...

3. От чего зависит скорость передачи информации?

Предположим, что вы как клиент измерили скорость передачи информации от себя (в Красноярске) до сервера, скажем, в Новосибирске. Для чего «закачали» с сервера файл большого размера и засекли время его «перекачки». Затем поделили объем файла на время и получили скорость.

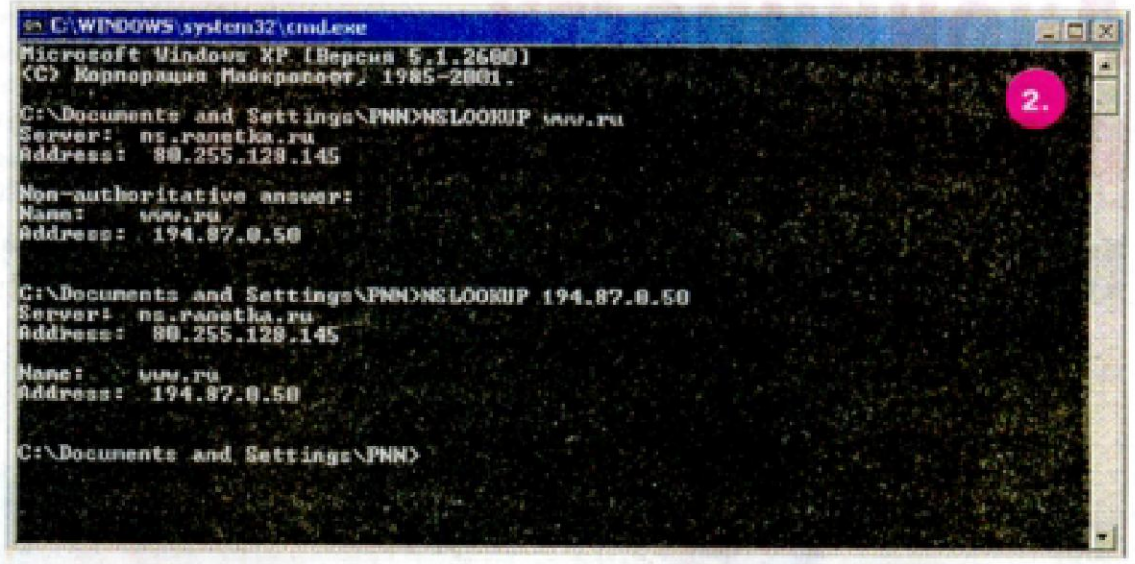
Только вот наверняка вы получите скорость меньше, чем ваша заявленная «скорость доступа» (то бишь – пропускная способность). И ваш провайдер в этом может быть абсолютно не виноват.

Попробую объяснить – почему.

Причин по большому счету может быть три:

1) Перегруженность какого-то канала связи между вами и новосибирским сервером. А каналов там может быть много: от вас до вашего провайдера, от провайдера до его UpLink'а («вышестоящего» провайдера), от UpLink'а вашего провайдера до UpLink'а провайдера, к которому подключен тот самый новосибирский сервер (причем в этом месте может быть довольно длинная цепочка каналов, принадлежащих разным провайдерам, в том числе даже зарубежным), а также между сервером и провайдером, к которому он подключен. Мало того пропускная способность каждого из этих каналов может быть разная, а «суммарная» пропускная способность всего канала будет не более, чем пропускная способность самого «медленного» из всех «подканалов».

2) Большая загруженность самого сервера (он просто медленно «отдавал» вам информацию) или ограничения на скорость «отдачи» данных, установленные владельцем сервера.



3) Низкая производительность вашего сетевого оборудования или большая загрузка вашего компьютера другими задачами, когда вы проводили измерения.

Кроме того, вы в этом случае измерили так сказать «чистую» скорость передачи информации, без всяких накладных расходов. А их тоже немало: служебная информация в заголовке каждого IP-пакета, команды соединения и установки процесса передачи информации, повторные посылки утерянных пакетов и т.д. В среднем эти накладные расходы составляют около 10-15%.

Причем чем больше заказанная вами у провайдера «скорость доступа», тем больше она может расходиться с измеренной таким образом скоростью передачи информации. Поскольку для того, чтобы просто сгенерировать информационный поток со скоростью более 5 – 10 Мб/с, нужны серьезные вычислительные мощности. С обычного персонального компьютера с бюджетной сетевой карточкой такие измерения будут иметь точность «плюс-минус большой лапоть»

4. Что и как мерить?

Почему-то многие клиенты считают, что каждый провайдер «спит и видит» как бы клиента обмануть, как бы дать ему «скорость доступа» поменьше, чем он заказал.

Это не так. Любой серьезный провайдер (кроме откровенных мелких жуликов) старается обеспечить гарантированную пропускную способность максимально точно и не только потому, что любой клиент может ее достаточно точно измерить и выставить провайдеру претензию.

Как же измерить пропускную способность канала связи с провайдером?

Сейчас среди клиентов модно мерить «скорость доступа» с помощью различных сайтов типа speedtest.net. Однако с помощью этих сайтов можно измерить только скорость передачи данных от вас до этого сайта, а никак не пропускную способность вашего канала.

Как я уже писал выше, это, во-первых, «две большие разницы», во-вторых, точность такого измерения «оставляет желать лучшего» (по причинам, изложенным в предыдущем разделе), в-третьих, показать они могут только так сказать «нижнюю границу» пропускной способности, т.е. что пропускная способность «не меньше» той, какую вы намерили.

Наиболее надежный способ измерения истинной пропускной способности вашего канала состоит в следующем.

Прежде всего вам необходимо иметь какую-нибудь программу, которая умеет подсчитывать объем передаваемой/получаемой информации прямо на интерфейсе вашего компьютера – типа TMeter, DUMeter и т.д.. (В сети Интернет их «навалом», можно свободно скачать как платные, так и бесплатные версии).

После запуска такой программы вам нужно любым способом «загрузить» максимально свой канал, например запустить «закачку» одновременно нескольких достаточно больших файлов с разных FTP-серверов (причем чем больше – тем лучше). Вот тогда вы сможете точно определить именно пропускную способность своего канала до провайдера, потому что больше, чем вам разрешил провайдер, до вашего компьютера информации «просто не пролезет».

Анонимности в интернете не бывает

Каждый, кто пользуется Интернетом, оставляет множество следов. Выявить эти следы, обобщить их и составить представление о человеке – задача чисто техническая.

Одно из самых удивительных свойств Интернета как коммуникационной среды заключается в том, что при формальной анонимности пользователей человек в этой среде парадоксальным образом оказывается даже более уязвим к разного рода злоупотреблениям, чем в реальной жизни.

Сейчас все больше стали говорить о нарушениях приватности, касающихся в основном (но не только) многочисленных участников различных социальных сетей...

Почти каждый интернетчик состоит в какой-нибудь социальной сети, а чаще и не в одной – суммарная аудитория только двух крупнейших российских ресурсов такого рода, «Вконтакте» и «Одноклассники», превышает общую численность пользователей Интернета в нашей стране. Кроме социальных сетей есть блогосфера и многочисленные форумы, поисковые ресурсы – в общем, каждый, кто активно пользуется Интернетом, даже только как справочником по кулинарным рецептам и сборником рефератов, оставляет множество следов. Выявить эти следы, обобщить их и составить более-менее полное представление о человеке – задача чисто техническая. И даже если вы тщательно следите за тем, чтобы не оставлять своего реального адреса, номера телефона и не разглашать деталей биографии, тем не менее можно узнать довольно много о ваших склонностях, привычках и предпочтениях, и даже прогнозировать ваше поведение.

А такая информация ценится на вес золота. Владимир Коровкин в своей статье (см. на этой же полосе) объяснил, почему сейчас буквально все – от гигантов вроде Google или Wal-Mart до мелких торговых и рекламных фирм – заняты сбором подобной информации. Она позволяет осуществлять адресную рекламу – такую, которая естественным образом вписывается в круг ваших личных интересов и потому не вызывает отторжения и раздражения, как обезличенная медийная реклама. И в такой постановке вопроса это действительно выгодно всем сторонам: и рекламодателям, которые получают значительно больший отклик, и пользователям, которых обычная реклама уже достала, и самим социальным сетям, которые наконец получают шанс монетизироваться и начать окупать свою деятельность.

Но пользователям почему-то в массе своей не нравится, что их тихо «посчитали», и они выступают против сбора персональной информации. Так, член Законодательного собрания Нью-Йорка Ричард Бродский выдвинул законопроект, запрещающий не только собственно сбор персональной информации, но и демонстрацию им адресной рекламы без предварительного согласия пользователей. Любопытно, что в то время как интернет-гиганты, живущие за счет рекламы (Google, Yahoo, AOL), разумеется, против законопроекта, Microsoft его поддержала, лишь попросив доработать так, чтобы он охватывал все компании, живущие за счет рекламы в Сети (а не только те, что демонстрируют адресную рекламу). Аналогичный проект был выдвинут в штате Коннектикут.

В Европе подобные настроения еще более распространены. Так, «отец Интернета» сэр Тим Бернерс-Ли возмущается сбором данных о пользователях: «Почтальон не вскрывает мои письма, телефонная компания не прослушивает мои разговоры. А ведь при использовании Интернета я сообщаю о себе намного более личные данные». Использование таких данных без разрешения, по его мнению, возмутительно. Эти настроения нашли поддержку на уровне Еврокомиссии, кото-

рая категорически запрещает сбор личных данных без согласия пользователей и сейчас ведет судебный процесс против ряда британских интернет-провайдеров, уличенных в сборе персональных данных.

Можно ли эту реакцию отнести только к разряду массовых фобий-«страшилок», как это квалифицирует Коровкин? Конечно, иррациональный протест против сбора обезличенной статистики ни на каких внятных аргументах не основан. Беда в том, что методы сбора такой информации позволяют не ограничиться статистикой, эти методы легким движением мышки дают возможность предельно детализировать и индивидуализировать получаемые данные.

А раз такая возможность есть, значит, ею кто-нибудь обязательно воспользуется, и не исключено, что в каких-нибудь неблаговидных целях. И будем откровенны: ранее, до появления коммуникационных сетей, такой сбор персональной информации всегда квалифицировался как шпионаж, персональная слежка, и не совсем понятно, почему нужно менять свое отношение к предмету с появлением цифровых технологий.

Причем в этих возможностях есть, конечно, и свои плюсы, и в них даже существует некая объективная необходимость, что трудно оспорить – смотря кто и зачем этим пользуется (об этом далее). Обратим также внимание на одно существенное отличие современных систем онлайновой слежки от традиционных способов – первые намного дешевле и проще в употреблении и хотя бы в теории доступны каждому, а не только спецслужбам или частным сыскным агентствам со специально обученными кадрами.

Чтобы не быть голословным, я связался с разработчиками одной из самых совершенных систем такого рода – компанией VS Lab. Ее подход отличается некоей глобальностью и универсальностью: разработанная там система под названием SkyPetr, основанная на передовых математических методах, одинаково годится для рекламщиков (для упомянутого выше анализа аудитории социальных сетей), государственных органов (например, для выявления и предупреждения экстремизма), для фильтрации «опасных связей» (например, для ограждения детей от нежелательных контактов) и многих других подобных вещей.

О перспективах, положительных и отрицательных сторонах системы SkyPetr я поговорил с Екатериной Должиковой, директором по развитию VS Lab.

— Какие реальные применения ваш проект уже находит?

— Увы, конкретных заказчиков я назвать не могу, скажу лишь, что это были коммерческие структуры, которым требовалась информация для проведения маркетинговых компаний. Сейчас к нам обратились специалисты (подразумеваются «специалисты» из спецслужб. – Ю.Р.), которым необходим анализ нескольких социальных ресурсов с точки зрения их безопасности и, скажем так, привлекательности для пользователей с «незаконными интересами и наклонностями», вроде детской порнографии и педофилии. Мы не стараемся ориентироваться на какой-то один сегмент рынка: считаем, что наши разработки могут найти применение в самых разных областях...

— Вы, наверное, понимаете, что ваши технологии могут также использоваться в качестве отличного инструмента для шпионажа за пользователями, в том числе со стороны не только спецслужб, но и криминальных элементов. В частности, декларированная вами защита детей от нежелательных контактов точно так же может использоваться в обратную сторону: скажем, для выявления подростков, склонных к определенного рода контактам. Ваши технологии легко использовать для выявления потенциальных объектов для шантажа и т.д.

— Вопрос, с одной стороны, вроде бы совершенно логичный, с другой – мне кажется, это старая, как мир, попытка переложить ответственность с человека на инструмент. Да, безусловно, любая технология, позволяющая так или иначе моделировать социальную структуру общества, прогнозировать поведение его членов и составлять их социальный и психологический портрет, может быть использована как во благо, так и во зло, и мы прекрасно осознаем свою ответственность.

Мы в своих выступлениях на «Инфофоруме» (конференция по информационной безопасности) в конце ян-

Не сообщайте пароли, явки и PIN-коды

Есть такое понятие – «кража идентификационной информации, удостоверяющей личность». В США «кража личности» уже давно является преступлением номер один. Типовой пример: злоумышленник узнает номер социального страхования какого-нибудь человека, заводит себе дюжину кредитных карточек на его имя, в результате платить по счетам приходится этому человеку.

Подоспела и свежая российская история. 20 мая сотрудники управления «К» МВД России задержали в Москве семейную пару, обманувшую более 10 тыс. абонентов сотовой связи примерно на 100 млн рублей. При помощи специальной программы мошенники отправляли SMS в платежную систему с номера, который идентифицировался как номер потенциальной жертвы. Система, в свою очередь, отправляла абоненту 4-значный ПИН-код для доступа в систему управления счетом. Чтобы его узнать, мошенники звонили абоненту, представлялись устроителями лотерей и предлагали получить денежный приз, который якобы выиграл абонент. Узнав PIN-код и паспортные данные абонента, мошенники получали полный доступ к его счету, переводили деньги через другие «электронные кошельки» на пластиковые карты, а затем обналичивали их. Сотрудники Управления «К» полагают, что сейчас они задержали организаторов обширной сети аферистов; исполнителей предстоит установить. Против задержанных возбуждено уголовное дело по ст. 272 УК РФ (неправомерный доступ к компьютерной информации) и ст. 159 УК РФ (мошенничество).

Это преступление – типичный пример «кражи личности», полный аналог того, что в Интернете носит название фишинга – рассылки подложных писем от лица реальных организаций.

ДЕТИ ШПИОНОВ

варя 2009 года подняли целый пласт проблем, связанных как раз с отсутствием на сегодняшний день инструментов определения «опасных связей» и прогнозирования возможности незаконных действий пользователя. Это и повсеместно встречающийся, особенно среди молодежи и школьников, моббинг (травля), и виктимизация (процесс превращения лица в жертву преступления. – Ю.Р.) интернет-пользователей, и, кстати, шантаж, и распространение нелегального контента. А рассуждая в духе «...ваша технология позволяет собирать сведения для шантажа», следует признать вредным и сам Интернет, и обезболивающие препараты, поскольку фактически все они могут служить и наркотиками.

Надо очень четко понимать, что наступает момент, когда НЕпоявление какого-либо средства или технологии куда опаснее, чем возможные последствия от его появления. Я думаю, ни для кого не секрет, что уже давно в Интернете используются разные виды информационного оружия, проводятся четко спланированные атаки. Отсутствие средств анализа и распространения контента и влияния Интернета на человека в целом приводит к тому, что Интернет с каждым днем становится все более опасным, что в нем применяются откровенно аморальные методы продвижения продуктов и услуг, разного рода пропаганда и проч. И если с этим ничего не делать, то ситуация будет только ухудшаться.

— Как вы относитесь к общим опасениям по поводу сбора данных о пользователях и сведения их в единые базы: понятно, что де-факто это уже не остановить, но многие возражают, квалифицируя это как нарушение приватности и высказывая опасения в связи с возможной утечкой таких баз и попаданием их в «плохие» руки?

— Во-первых, базы существуют на каждом ресурсе, где пользователь регистрируется, при этом большинство ресурсов никак не озабочены системой безопасности хранения этих баз. Данные пользователей лежат едва ли не в открытом доступе. Во-вторых, нельзя перекладывать всю ответственность на ресурсы. Люди должны наконец осознать, что понятие «виртуальная реальность» устарело. Вы же не оставляете, к примеру, свой кошелек на прилавке магазина, отходя в соседний отдел, и не диктуете номер своей кредитки по телефону, стоя посреди людной площади? Пора привыкать к тому, что и в Сети надо соблюдать те же правила безопасности. 80% пользователей имеют одинаковые логины и пароли на всех своих профилях и аккаунтах: электронной почты, социальных сетей, форумов и т.д. Киберпреступники, получив логин и пароль с незащищенного форума про «вышивание крестиком», совершенно спокойно получают доступ к почте и другим ресурсам, у которых как раз очень надежная защита данных.

Протестовать против создания баз, мне кажется, могут только ну уж совсем малообразованные люди. Весь Интернет, да что там Интернет – все общество строится на создании объединяющих баз. Никто же не возмущается по поводу обязательной регистрации по месту жительства, например (да ладно, еще как возмущаются. – Ю.Р.). А насчет утечек – опять же это вопрос не только к разработчикам. Пришло время, когда пользователям надо начинать задумываться о том, где и какую информацию о себе оставлять и, самое главное, какие действия совершать.

Конечно, Екатерина Должикова права: системы, подобные SkyPetr, есть всего лишь инструмент. Но о том, что он может быть использован и в преступных целях, не нужно забывать: классическим примером целой процветающей преступной отрасли, основанной на сборе данных о пользователях (как минимум об их адресах электронной почты), является рассылка незапрошенной корреспонденции – спама.

И зачем-то информацию о пользователях ведь собирают подпольно: так, в Великобритании зафиксирован сайт, собирающий резюме уволенных сотрудников. Оказалось, что за вполне законной на первый взгляд деятельностью стоит вымышленное кадровое агентство. И эксперты говорят, что большинство посланных резюме содержат по крайней мере восемь позиций персональных данных, которые могут быть теоретически использованы для «кражи личности». Аналогичная история случилась летом прошлого года и в России, где хакерская группировка Phreak предлагала спамерам на подпольных форумах за 600 долларов базу данных, содержащую тысячи резюме, собранных в автоматическом режиме с крупнейших сайтов по поиску работы. Такие базы могут использоваться, например, для адресных фишинговых атак – если клиенту поступает письмо якобы от банка, где он действительно имеет счет, вероятность успеха мошеннической операции резко возрастает.

Будем объективны: наверное, тенденцию к сбору персональных данных, как в маркетинговых целях, так и в интересах служб охраны порядка, уже не переломить. Но это не значит, что следует забывать о возможных негативных последствиях такой тенденции и пускать дело на самотек. Впрочем, сами пользователи тут могут себе помочь больше других, если действительно, как говорит Екатерина, начнут «задумываться о том, где и какую информацию о себе оставлять».

Юрий Ревич
обозреватель «Новой»

Защита конфиденциальных данных и анонимность в I-net

Это – руководство для пользователей Рунета по использованию криптографии, анонимайзеров, и по настройке операционной системы на защиту от утечки личных данных, слежения, внедрения в систему следящих или вредоносных программ. От читателя требуется начальный или средний уровень знаний о персональных компьютерах. Ориентировано на ОС Windows и использование бесплатного (freeware) или открытого/свободного (FOSS) программного обеспечения.

Зачем нужна анонимность?

Есть разные причины скрываться от опознания. Правительства, работодатели и преподаватели учебных заведений нередко ограничивают доступ к информации и ущемляют свободу выражения подчиненных им людей под всевозможными предлогами. Примеры таких случаев можно найти далее. Наблюдается тенденция усиления слежки в Сети и вообще. Кроме того, многим людям просто нравится ощущение приватности и невозможности слежки за ними через Сеть, это их право. Право, защищеное 23 и 24 статьями конституции Российской Федерации.

Программы для работы с интернетом

Программы, работающие с интернетом (браузеры, файловые менеджеры, Bittorent-клиенты и т. д.) для большей надежности от нарушений конфиденциальности должны иметь открытый исходный код.

Открытые браузеры:

* **Mozilla Firefox**
* **Flock**
* **Lolifox**
* **Mozilla Suite**
* **SeaMonkey**
* **K-meleon**
* **Google Chromium** (не путать с закрытым Google Chrome).
* **SRWare Iron**
* **Lynx**
* **Konqueror**
* **Html Viewer 3**

Не рекомендуется использовать для анонимного серфинга Google Chromium, так как он отсылает разную информацию Google. SRWare Iron, основанный на Google Chromium, этого недостатка лишен.

Открытые менеджеры закачек:

* **Free Download Manager** (может быть Bittorent и FTP клиентом).

Открытые FTP-клиенты:

* **FileZilla**

Открытые файлообменные клиенты:

* **ABC (Yet Another BitTorrent Client)**
* **aMule**
* **Anatomic P2P**
* **Arctic Torrent**
* **BitTornado**
* **BitTyrant** (BitTyrant – это разработка Университета Вашингтона по созданию эффективного BitTorrent клиента. BitTyrant базируется на коде Azureus 2.5.X и имеет практически идентичный интерфейс (немного изменена вкладка «Peers» – в ней появились столбики с действиями BitTyrant'а и статистические данные по каждому из peer'ов. Также изменения коснулись меню «Help»). При соединении пользователя, запустившего BitTyrant с Роем, другие участники видят клиент с именем «AzureusBitTyrant 2.5.0.0BitTyrant». Основные изменения произошли в механизме загрузки раздачи – BitTyrant собирает статистическую информацию на Пиров и на основе этого принимает решение о загрузке или раздаче файла. По данным разработчиков это увеличивает скорость загрузки на 70 %).
* **Blog Torrent**
* **Burst!**
* **Deluge**
* **DC++**
* **EMule**
* **G3 Torrent**
* **FlyLinkDC++**
* **KCeasy**
* **KTorrent**
* **LimeWire**
* **LeechCraft**
* **Localhost**
* **MLDonkey**
* **Rufus**
* **Shareaza** (Вы сможете загружать/выгружать файлы в следующих сетях: EDonkey, Gnutella (G1), BitTorrent и Gnutella2 (G2)).
* **Torrent Swapper**
* **TorrentFlux**
* **Transmission**
* **Vuze (старое название – Azureus).**
* **XBT Client**

Открытые IRC-клиенты:

* **Kvirc**
* **ChatZilla**

Открытые программы мгновенного обмена сообщениями:

* **Adium**
* **Instantbird**
* **Coccinella**
* **Exodus**
* **Gajim**
* **Jabbin**
* **Miranda IM**
* **Psi**
* **qutIM**
* **Tkabber**

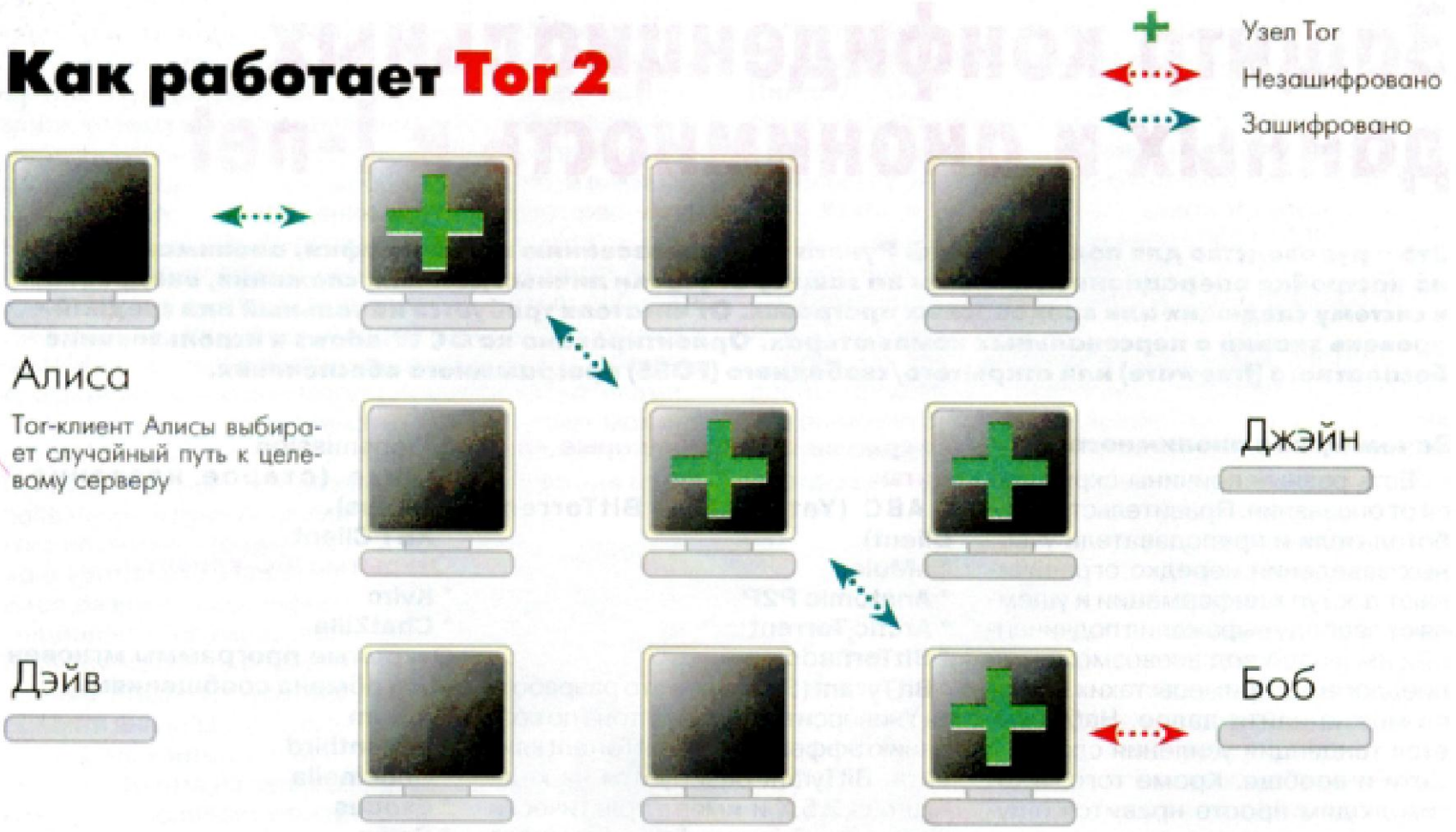
Открытые программа для работы с электронной почтой:

* **Mozilla Thunderbird** (может быть клиентом групп новостей)
* **Sylpheed** (Серьезный минус – в текущей версии (2.6.0) хранит пароли почтовых аккаунтов в открытом виде).
* **KMail**
* **Evolution**
* **Claws mail** (ранее известный как Sylpheed-Claws).

Распределенная анонимная сеть Tor

Tor – это Свободное программное обеспечение для анонимизации трафика. Открытый исходный код Tor'а проверяется многими людьми со всего мира, что обеспечивает своевременное выявление дефектов и невозможность тайного встраивания в него «черного хода» для государственных служб или кого-либо еще.

Tor обеспечивает надежную и бесплатную анонимизацию, защищая пользователя от слежки как за посетителями определенного сайта, так и за всей активностью самого пользователя. Когда пользователь передает данные, программа



Tor скрывает и настоящий пункт их назначения, и сами данные, перебрасывая данные в зашифрованном виде через цепочку промежуточных узлов сети.

Устройство

Узел сети «Алиса» общается с узлом «Боб» посредством анонимной сети Tor.

Работа Tor'а основана на взаимодействии многих серверов сети Tor, каждый из которых предоставляет часть пропускной способности своего интернет-подключения для нужд сети. Этот принцип работы близок к пиринговым сетям. Любой пользователь может быть сервером, отдавая часть пропускной способности для развития анонимной сети, и тем самым улучшая свою собственную анонимность (см. настройку сервера.)

Tor случайно выбирает несколько серверов из всех доступных (список которых он периодически скачивает с центрального сервера-директории) и строит «тоннель», проходящий через эти промежуточные точки. Ваш трафик будет пропускаться через этот тоннель; у него есть вход – приложение Tor на вашей машине и выход – последний из случайно выбранных для этого тоннеля серверов сети Tor.

Tor последовательно зашифровывает передаваемый пакет данных открытыми ключами серверов, входящих в цепочку, начиная с ее конца. При этом ваш компьютер (на диаграмме – «Алиса») непосредственно отсылает данные на первый сервер в этой цепи, который снимает с данных свой слой шифра и передает их далее, а с реальной точкой назначения (на иллюстрации – «Боб») непосредственно общается сервер, служащий точкой выхода из тоннеля.

Это защищает от слежки и возможных неприятных последствий посещения специфического сайта в интернете. В точке назначения нельзя выяснить ваш IP-адрес и местонахождение, ибо вы не связываетесь с ней напрямую. Даже серверы-посредники получают только необходимые сведения. Например, первый сервер сети Tor, выбранный для тоннеля, с которым вы взаимодействуете напрямую, не может точно определить, назначены ли данные для вас или вы, в свою очередь, являетесь всего лишь посредником для кого-то другого. Никакие узлы в цепочке, кроме сервера, служащего точкой выхода, не имеют доступ к собственно передаваемым данным (в незашифрованном виде), да это и не нужно для их работы. Им раскрывается только информация о том, кто есть следующий в цепи посредников, которому они перешлют скрытое от них содержимое.

Сокрытие информации так, чтобы каждый элемент цепи имел доступ только к той части, которая предназначена ему, реализуется с помощью криптографии с открытыми ключами. Подобный метод шифрования проработан и надежен, и даже если сервер сети Tor находится под контролем противника, он не сможет получить доступ к части информации, предназначенной для следующих серверов тоннеля.

Только последний сервер в цепи, который служит точкой выхода из тоннеля, способен расшифровать содержимое, которое он затем отсылает на пункт назначения. Полученный обратно ответ он может доставить на ваш компьютер аналогичным образом, с сохранением анонимности.

Сравнение сети Tor с другими системами и анонимными прокси

* Обычные бесплатные веб-прокси, как правило, не шифруют передаваемые данные, таким образом они не дают никакой защиты, если ваш канал связи уже находится под наблюдением противника (элементарный анализ трафика выявит все сайты, которые вы посещаете, а также многие действия, совершаемые вами). Tor всегда шифрует всю передаваемую информацию, поэ-

тому, даже если противник наблюдает за всеми передачами по вашему каналу связи, все что он получит – бессмысленные байты.

* Многие прокси, рекламирующие себя как «анонимные», на самом деле не являются таковыми (сообщают точке назначения информацию о пользователе через заголовки HTTP). Без специальной проверки пользователь не может быть уверен, что «анонимный веб-прокси» на самом деле является анонимным, и что при посещении веб сайта ваш IP-адрес не открывается для хозяев сайта или тех, кто имеет возможность наблюдать за каналом интернет связи этого сайта. При использовании Tor'а, при входе на пункт назначения (например, веб сайт), ваш IP всегда скрыт.

* Есть ограниченное количество по-настоящему анонимных веб-прокси, но никто не может гарантировать, что они не ведут логи активности пользователей и не передают эту информацию заинтересованным лицам. При использовании одного веб-прокси сервера вы полностью доверяете свою анонимность этому серверу. В случае использования Tor'а, вы доверяете анонимность нескольким случайным серверам из тысяч доступных, из которых многие запущены на обычных домашних компьютерах пользователей-волонтеров по всему миру. Для слежки за вами противник должен контролировать все из этих случайно выбранных Tor-серверов, вероятность чего крайне мала, даже если противник будет контролировать значительное количество Tor-серверов по всему-миру.

* Некоторые прокси и системы анонимизации, которые предлагают зашифрованный обмен данными и хорошую скорость, требуют денег. Tor абсолютно бесплатен.

* При этом, по простоте использования Tor стоит в одном ряду с самыми доступными для начинающего пользователя методами (такими как использование обычного веб прокси).

* Tor доступен для использования на многих операционных системах, например, Linux и других *nix системах.

* В отличии от веб-прокси, Tor в теории может поддерживать любые TCP соединения, а не только HTTP, благодаря этому вы можете анонимно использовать программы для сетевого общения и многое другое.

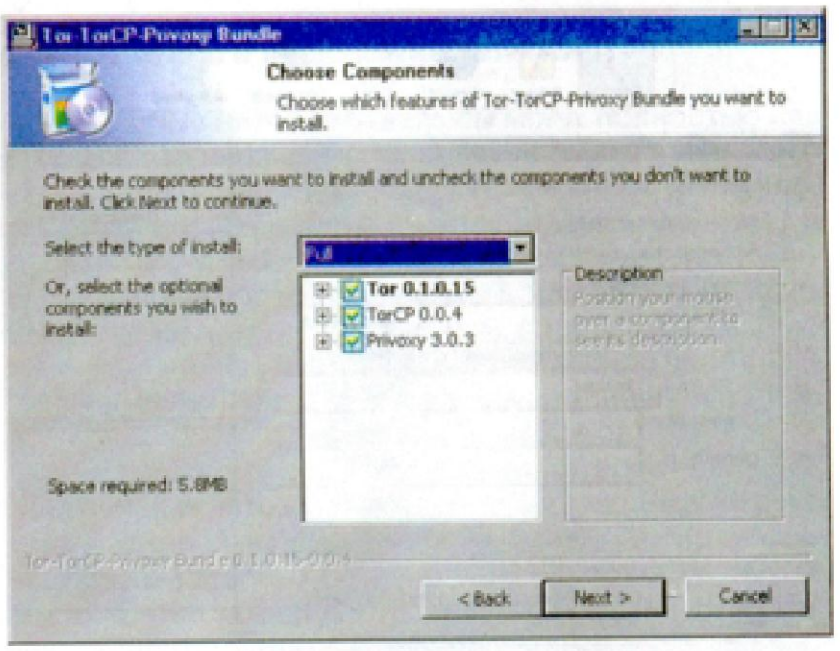
* Tor обычно работает медленнее, чем веб-прокси (плата за гораздо более качественную защиту).

* Теоретически, Tor по принципу действия приблизительно похож на систему JAP, но уступает последнему по скорости передачи. С другой стороны, Tor'у отдают предпочтение те, кто ценит его большую децентрализованность, открытость и «незапятнанную репутацию» (Tor всегда был открытым, тогда как разработчики JAP однажды были пойманы на внесении «черного хода» по запросу спецслужб).

Установка и использование

Tor, вместе с сопутствующим программным обеспечением (Privoxy, Vidalia), можно скачать с сайта программы. Для пользователей Windows ссылка на нужный файл находится в строчке «Windows: Tor & Privoxy & Vidalia в одном инсталляторе». Скачивайте стабильный выпуск.

Процедура установки проста: неопытным пользователям достаточно жать Далее, оставляя предлагаемые варианты выбора без изменения, ибо они хорошо подобраны и обеспечат правильную работу. После завершения установки, Vidalia и Privoxy автоматически запускаются и регистрируются в системе для автоматического запуска при входе пользователя Windows. Vidalia при старте запускает основное приложение, называющееся просто Tor. С этого момента система анонимизации трафика готова к работе.



Смысл установленных программ следующий:

Tor

Сердце системы анонимизации трафика. Эта программа будет строить тоннели, пропускать через них данные и получать ответы. Данные поступают от других программ, которым надо послать что-нибудь в интернет, им же передаются данные присылаемые в ответ с другого конца тоннеля. Способ общения программ, которым требуется интернет, с Tor'ом – SOCKS (широко используемый механизм взаимодействия сетевого программного обеспечения с прокси-серверами – сетевыми посредниками). Tor принимает локальные соединения на порт 9050, и обслуживает программы как прокси-сервер SOCKS.

Множество программ поддерживают использование прокси-сервера SOCKS. Если вы можете найти в сетевой программе настройки использования SOCKS прокси, значит, вы можете настроить эту программу для анонимной работы с интернетом через сеть Tor. В настройках как адрес прокси-сервера вводите localhost (для локального соединения), порт 9050. Теперь программа при попытке открыть соединение с интернетом будет подсоединяться к Tor'у, и благодаря этому обмен данных с точкой назначения будет проходить через тоннель сети Tor.

Учитывайте, что доступ к интернету через Tor может происходить ощутимо медленнее, чем доступ к интернету напрямую, в связи с этим, некоторым программам может потребоваться дополнительная настройка (например, продление допустимого времени соединения: такие опции, как «connection timeout» и тому подобное.)

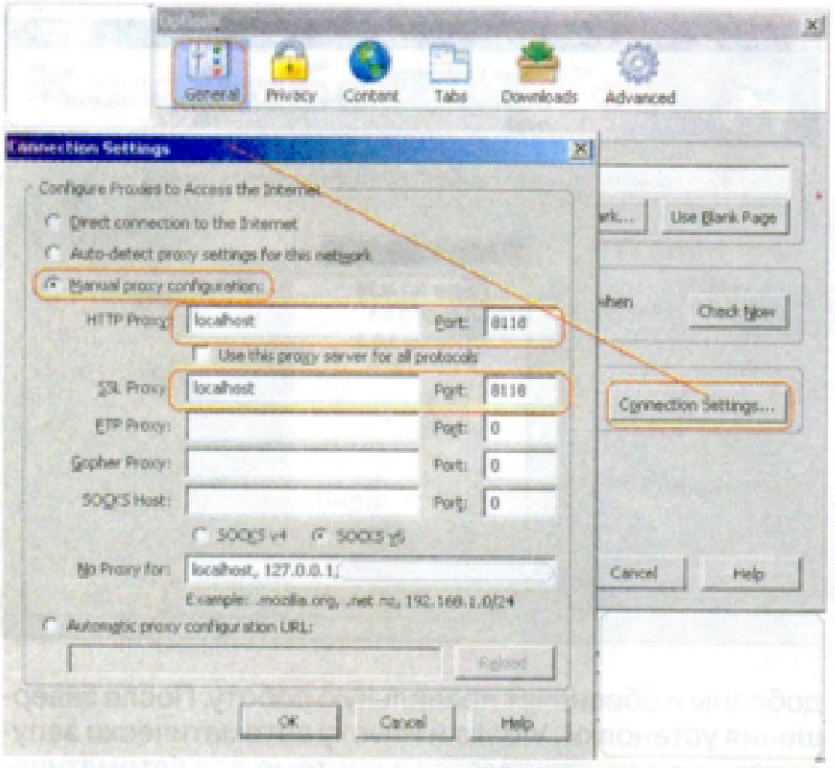
Vidalia

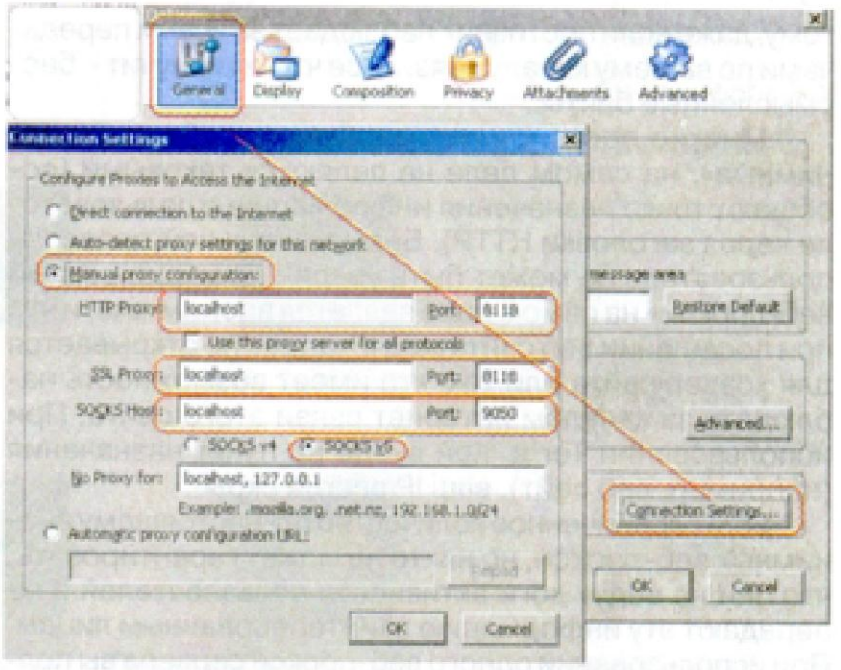
программа для автоматического запуска Tor'а при входе в операционную систему, настройки и наблюдения за работой Tor'а.

Privoxy

анонимизирующий HTTP/HTTPS прокси-сервер, использующий возможности основного приложения Tor для

ДЕТИ ШПИОНОВ





выполнения своих функций. Privoxy, по сути, будет работать как надстройка над Tor'ом, улучшающая защиту в программах, использующих протоколы HTTP и HTTPS (браузеры, любые другие программы, где используются URL, начинающиеся с http:// или https://). После выполнения дополнительной защитной обработки данных, Privoxy применяет Tor для работы с тоннелями, подсоединяясь к Tor'у через тот же порт 9050. Privoxy предотвращает утечку информации, нарушающей анонимность по вине браузера и других программ, использующих HTTP и HTTPS. Подробнее об этой проблеме можно прочитать далее.

Если программа использует протоколы HTTP и HTTPS, надо настроить ее для обращения к Интернету именно через Privoxy, если необходимо обеспечить анонимную работу с Интернетом. Privoxy принимает локальные соединения на порт 8118. Все широко используемые браузеры и большинство других программ, использующих HTTP и HTTPS, позволяют настроить использование прокси-сервера для HTTP и HTTPS (может обозначаться как SSL) соединений. Как адрес прокси-сервера, в таком случае вводится localhost (локальное соединение), номер порта – 8118 (порт Privoxy). Это можно (и нужно) вводить и для HTTP и для HTTPS (SSL). Далее приводятся примеры настройки конкретных приложений, например, Mozilla Firefox.

Настройка Firefox 1.5

Зайдите в настройки, через пункт меню Tools->Options, вкладка General, в области «Connection» нажмите «Connection Settings...». Это открывает окно настройки подсоединения к Интернету браузера Firefox. В нем надо выбрать «Manual Proxy Configuration» и заполнить две строчки: «HTTP Proxy» и «SSL Proxy». В каждой строчке в поле, расположенном левее, надо ввести localhost (локальное соединение), в поле правее 8118.

После такой настройки браузер будет пытаться открыть локальное соединение на порт 8118, где его примет приложение Privoxy и обеспечит выход в Интернет через основное приложение Tor.

Этого достаточно для работы основных функций браузера. Дополнительно можно записать localhost и порт 9050 в строчке «SOCKS Host» того же окна; это позволит, например, заходить на FTP-серверы в Firefox, общаясь с ними через посредничество основного приложения Tor; оно будет принимать локальные соединения на порт 9050.

В поле «No Proxy for:» выключается использование прокси для определенных адресов. Там обычно всегда перечислены хотя бы localhost и 127.0.0.1 – локальные соединения. Выключение прокси может потребоваться для каких-то других адресов, например, потому что они не пускают к себе пользователей из-за границы (при использовании Tor'а по-настоящему связываться с сайтом, на который вы заходите, может компьютер в любой точке земного шара с любым IP-адресом). Перечислите все адреса, для которых надо выключить прокси, через запятую. При этом можно использовать частичные адреса, например, .livejournal.com добавляет все адреса, заканчивающиеся на .livejournal.com.

Настройка Thunderbird 1.5

Работа с Tor'ом в Thunderbird похожа на работу в Firefox, ибо они из одного семейства программного обеспечения. Зайдите в настройки прокси (см. раздел о настройке Firefox).

Для получения почты главное прописать правильные значения в строчке «SOCKS Host», ибо Thunderbird будет использовать механизм SOCKS для взаимодействия с Tor'ом, при попытке скачать письма с сервера. В левом поле надо ввести localhost, а в правом – 9050 (номер SOCKS-порта основного приложения Tor), для того чтобы Thunderbird подключался к Tor'у.

«HTTP Proxy» и/или «SSL Proxy» могут понадобиться, скажем, при загрузке картинок в содержимом письма, в этих строчках надо записать localhost и 8118 (порт приложения Privoxy).

Thunderbird может обращаться к DNS-серверу, минуя Tor, поэтому вместо имен POP/IMAP/SMTP-серверов пропишите их IP-адреса. Их можно определить с помощью утилиты tor_resolve, которая находится в той же папке, что и Tor.

Строчка «No Proxy for:» – см. раздел о настройке Firefox.

После завершения окно опций может выглядеть как на иллюстрации.

Узлы сети Tor, как правило, блокируют трафик, связанный с отсылкой писем для противодействия спаму

(они блокируют трафик, идущий на порт 25, если почтовый сервер принимает соединения на другой порт (как, например, делает сервер GMail) то, вероятно, это не будет заблокировано). Если вам не удается послать письмо посредством Tor'a, добавьте ваш сервер выходящих сообщений (SMTP) в список «No Proxy for:». Работа с ним в таком случае будет происходить напрямую, без Tor'a, не анонимно.

Опасность утечки данных по вине программ

Tor защищает от угроз анонимности при проведении слежения за каналами связи и при слежении на другом конце соединения. Tor не помогает в случаях, когда проблема находится на вашем собственном компьютере.

При использовании браузера анонимность может частично или полностью нарушаться из-за ошибок в браузере, куки, и скриптов. Privoxy защищает от части таких проблем фильтруя данные, которыми обмениваются браузер и веб-сервер. Желательно не использовать браузер Internet Explorer, с которым связана львиная доля всех уязвимостей, а вместо этого использовать более безопасные Firefox или Opera. Если вы используете Firefox, запретите куки в настройках и установите расширения NoScript и Permit Cookies. После этого куки и скрипты надо разрешать отдельно для каждого сайта, которому вы доверяете, а на ненадежных сайтах они будут выключены. Разрешение (а также запрет) производится одним кликом на иконке «C» – для куки, или иконке «S» – для скриптов (в нижнем правом углу окна браузера).

Другие программы тоже могут представлять опасность. Отдавайте предпочтение программам от разработчиков с хорошей репутацией, предпочтительнее – открытым программам.

Личные данные могут утекать также из-за заражения компьютера вредоносными программами. Используйте брандмауэр и настройте Windows для предотвращения этого, установите защитное программное обеспечение (антивирус и тому подобное).

Ограничения и недостатки сети Tor

Некоторые интернет-ресурсы могут полностью или частично запрещать доступ из анонимной сети Tor. Пример, сайты Фонда Викимедиа (Википедия, Викиучебник и другие) запрещают редактирование при доступе из сети Tor, хотя это не всегда работает.

Некоторые порты, как правило, закрыты в выходной политике серверов Tor, поэтому определенные действия обычно не удается сделать анонимно через сеть Tor (например, часто запрещаются соединения на порт 25 – отсылка почты через SMTP протокол).

Некоторые веб-сайты и другие интернет-ресурсы могут определять местонахождения заходящих на них пользователей по IP-адресу и не пропускать пользователей из выбранных стран или регионов мира. Так как при анонимном доступе через сеть Tor с сайтом напрямую общается сервер-выходная точка, находящийся где угодно в мире, это может создавать проблемы при попытке доступа к подобным сайтам.

За анонимность, получаемую благодаря сети Tor, приходится расплачиваться понижением скорости передачи данных, а за интерактивность – возможностью раскрытия путем обнаружения синхронной активности (timing-атака).

Этика использования сети Tor

Не используйте Tor для действий, при которых не нужна анонимность (онлайн-игры, интернет-радио), или действий, перегружающих сеть Tor объемом трафика, который она пока не готова поддерживать (пиринговые сети).

Не используйте Tor для нанесения вреда сайтам, спама и т. д. Это приведет к тому, что у администраторов различных сайтов появятся дополнительные причины закрыть анонимный доступ к их ресурсам из сети Tor. Этим вы повредите людям во всем мире, которым необходима анонимность из-за возможного или реального преследования правительством или кем-то еще. К сожалению, на вики-сайтах, таких как Википедия и Викиучебник, это уже сделано для борьбы с вандализмом.

HTTP://RU.WIKIBOOKS.ORG

За нами следят?

Государство, крупные компании и мошенники контролируют каждый ваш шаг в Сети. Но вы можете защититься.

В наше время мало кто может поспорить с тем, что спецслужбы тщательно следят за интернет-трафиком. Но не только государственные ведомства интересуются частной жизнью пользователей. Интернет-индустрия – начиная с гиганта Google и заканчивая самым мелким интернет-магазином – тоже хочет знать точно, какие страницы вы посещаете и чем вы интересуетесь.

Защита от преследования в Интернете

Не оставляйте следов во Всемирной паутине: вашу анонимность может обеспечить подключение через каскад прокси, то есть цепочку из сотен серверов, вместе с надежным шифрованием трафика. Все это вы сможете реализовать либо с помощью специальной версии Firefox – xB Browser, либо посредством службы анонимизации серфинга JAP/JonDo.

xB Browser. Ранее этот браузер назывался Torpark. Он создан на базе Firefox, но упор в нем сделан на безопасность и анонимность серфинга в Интернете. Если вы не хотите, чтобы кто-то знал, по каким сайтам вы путешествуете или из какой точки мира вы это делаете, xB Browser поможет в этом.

Исполняемые файлы доступны только для Windows, поэтому пользователям других ОС придется «собирать» браузер из исходного кода.

JAP/JonDo (www.jondos.de/en/jondofox) представляет собой специальный сервис, позволяющий скрыть IP-адрес с помощью прокси-серверов. Название слегка сбивает с толку: пока вы выходите в Интернет через набор прокси технического университета Дрездена (anon.inf.tu-dresden.de), разработчики говорят о JAP. Если в главном окне программы в качестве «службы» вы выберете более быстрый платный набор прокси, напри-

мер Ramses-Lilie-Jupiter, программа будет называться JonDo. Проще всего использовать эту службу с помощью JonDoFox, модифицированной и предварительно сконфигурированной версии Firefox.

Защита от контроля за электронной почтой

Службы: Hushmail, SafE-mail, OpenPGP

На данный момент большинство бесплатных почтовых сервисов может предоставить данные вашей переписки спецслужбам. Корпоративная почта также ненадежна: ведь вы храните почту в незашифрованном виде, так что любой, кто получит доступ к вашему почтовому серверу, легко сможет прочитать ваши письма. Если вы хотите обезопасить свою переписку, воспользуйтесь услугами почтовых сервисов, использующих шифрование. Пожалуй, лучшие из таких служб – Hushmail (www.hushmail.com) и SAFe-mail (www.safe-mail.net). Они пока не настолько популярны, чтобы до них уже успели добраться спецслужбы.

Одним из интересных вариантов осуществления закрытой переписки является система шифрования OpenPGP, которая поддерживается многими почтовыми клиентами, например Mozilla Thunderbird. Для того чтобы расшифровать письмо, зашифрованное с ее помощью, вам необходимо будет получить от его отправителя файл с ключом.

Защита от определения местоположения мобильных телефонов

ПО: LocateProtect

Все, наверное, помнят услуги типа «узнай, где находится твой собеседник», предоставляемые провайдерами телефонии. Местоположение вашего телефона легко определить с помощью сигналов IMSI, который обычно посылается поставщиком телефонных услуг, но может быть имитирован специальным оборудованием. Однако обладатели аппаратов под управлением Symbian могут засечь эти запросы.

Установите LocateProtect с помощью ПО для вашего мобильного телефона, например Nokia PC Suite. Программа запустится автоматически, как только вы включите мобильный телефон. Если аппарат поймает запрос от службы радиосвязи, LocateProtect спросит, хотите ли вы на него ответить – то есть определить свое местоположение. В обычном случае вы ответите «Нет». Но если вы лежите со сломанной ногой в расщелине ледника, правильным ответом будет «Да». Ведь только так служба спасения сможет найти вас.

Защита от обнаружения Whois

Служба: active-domain

Хотите решительно высказываться в отношении действий правительства и нечистых на руку коммерческих структур? Тогда стоит позаботиться о том, чтобы скрыть от чужих глаз информацию о вашем сайте. Чтобы замаскировать свою запись в банке данных Whois, необходимо прибегнуть к услугам Private Whois Protection, которые предоставляют некоторые регистраторы доменных имен. Такая услуга, конечно, не бесплатна, но цена на нее редко когда переваливает за $20 за год. Система работает очень просто – доменное имя как бы перерегистрируется на фиктивное лицо. Однако стоит помнить, что пользоваться такими сервисами, расположенными в нашей стране, не слишком разумно.

Защита от личной слежки

ПО: WebFerret

В Интернете остается все. Все данные, которые вы там когда-либо оставляли, где-то сохраняются и могут быть найдены, например, любопытным начальником отдела кадров. Чтобы отыскать давно забытые грехи молодости, вам придется прочесать Сеть с помощью специальных инструментов.

Поскольку вы не знаете, с помощью какой именно поисковой машины шпион попытается разыскать информацию о вас, вы должны провести метапоиск, при котором будут показаны результаты многих известных поисковиков от Google до Yahoo! Если вы частый гость в Сети, вхождений может быть до 10000, и все их нужно будет просмотреть и оценить. WebFerret (скачайте на сайте www.webferret.com) сделает и то, и другое.

После ввода своего имени в строку поиска сначала ликвидируйте все дублирующиеся результаты с помощью «Search Lype | Duplicate Removal». Теперь отсортируйте результаты с помощью «View | Arrange Icons». Если вы наткнетесь на компрометирующую информацию, возможно, запрос у владельца страницы позволит ее удалить. Однако помните, что эта информация, хотя бы частично, еще некоторое время будет светиться в индексах поисковиков.

Защита от сбора данных

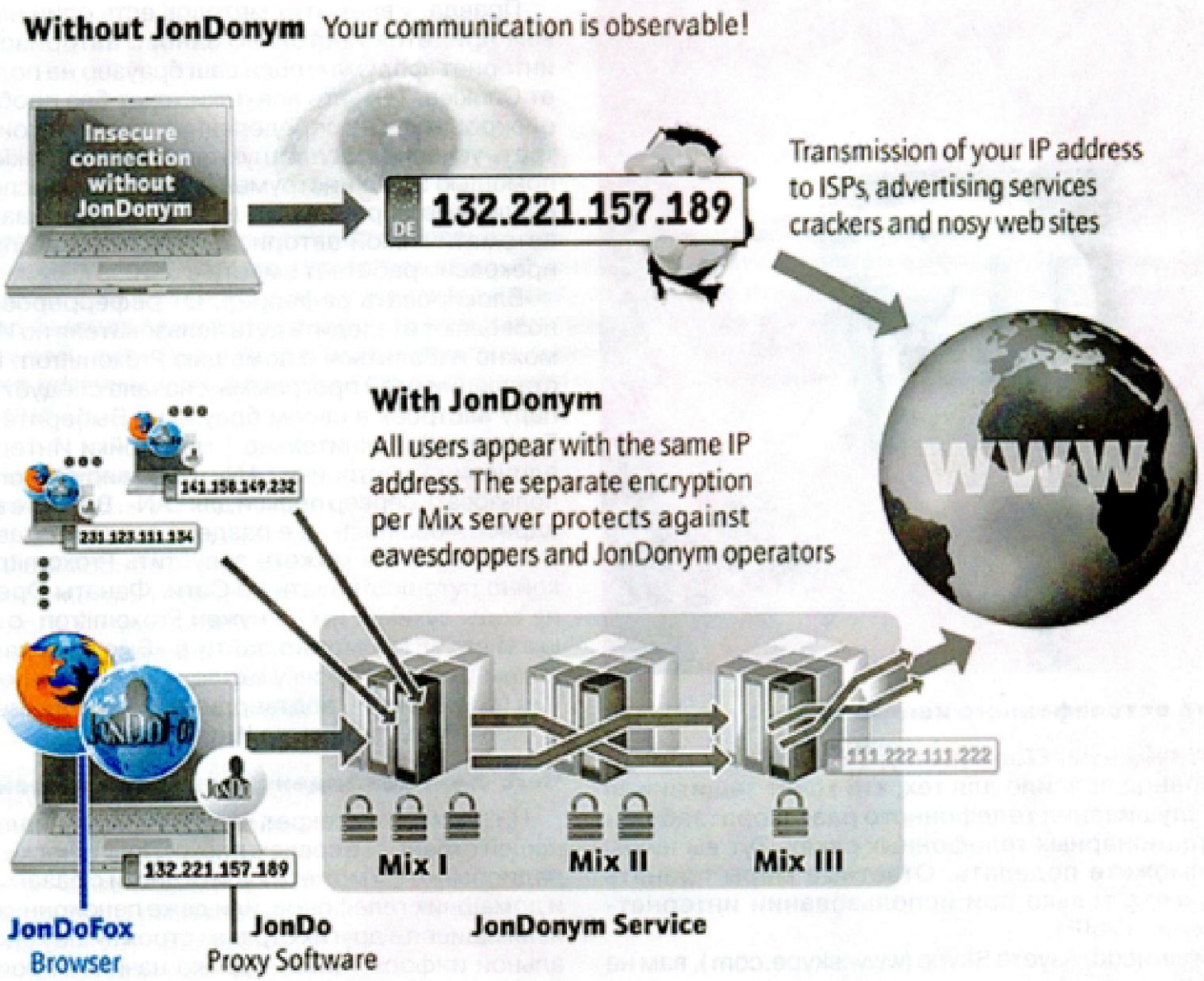
Службы: Googlonymous, http://spammotel.com, www.spamgourmet.com

В Интернете существует множество сервисов, собирающих информацию о пользователях и предоставляющих ее за деньги заинтересованным компаниям. Защититься от них поможет только осторожность – оставляйте в разных учреждениях и особенно в Сети как можно меньше информации о себе.

Поисковую машину Google вы обманете с помощью веб-сайта googlonymous.com. Она позволяет «обезличить» ваши запросы к этому сервису.

Другая интересная возможность защититься от сбора информации – воспользоваться сервисами временной почты (Disposable e-mail addresses, DEA), такими как http://spammotel.com или www.spamgourmet.com. Эти службы позволят вам создавать «псевдонимы» для своего реального ящика, без проблем отключая «засве-

ДЕТИ ШПИОНОВ



ченные» адреса. Это, во-первых, защитит вас от спама, а во-вторых, не позволит идентифицировать вас по адресу электронной почты.

Защита от записи разговора

Программы: Scatter Chat, P2P Messenger .NET

Знаете ли вы, что вашу переписку в системах мгновенных сообщений легко может перехватить ваш босс, спецслужбы или конкуренты? Чтобы иметь возможность продолжать общаться без проблем, зашифруйте соединение и скройте ваш IP-адрес. Сделать это можно двумя способами.

Чат с использованием Tor. Программа Scatter Chat, которую можно скачать по адресу http://scatterchat.en.softonic.com, – это клиент мгновенных сообщений, который шифрует разговоры с помощью библиотеки libcrypt, а также специального модуля Scatter-Chat. Вся переписка ведется через сеть анонимных прокси-серверов Tor.

Разговор P2P. Система мгновенных сообщений P2P Messenger .NET использует для скрытия IP-адреса технологию p2p, известную всем по сервисам файлообмена типа BitTorrent. Она также поддерживает шифрование с помощью ключа.

Защита от шпионажа

Программы: TrueCrypt 5.1a, Bitlocker (Vista Ultimate)

Чтобы избежать получения информации шпионскими программами, следует зашифровать ваш жесткий диск.

Windows XP. Для XP мы поместили на наш диск приложение TrueCrypt 5. С его помощью вы можете защитить жесткий диск от доступа без вашего ведома. Для этого TrueCrypt перед запуском Windows спросит пароль (PreBoot-Authentification). Чтобы зашифровать системную область, выберите в программе «System | Encrypt System partition/drive». В мастере активируйте «Encrypt the Windows system partition | Single Boot». В качестве алгоритма шифрования (Encryption algorithm) лучше выбрать «AES-Twofish-Serpent». Остальное понятно интуитивно.

VistaUltimate. Новая Windows имеет собственное шифрование в виде BitLocker, который вы можете включить в «Центре управления» в разделе «Шифрование диска BitLocker». С помощью него также можно защитить компьютер с самого момента запуска. Если ваш компьютер оснащен TPM-чипом (Trusted-Platform Module), вы сразу же можете зашифровать жесткий диск, нажав правой кнопкой мыши на системном диске и выбрав соответствующую функцию. Если у вас нет чипа TPM, сначала введите в командной строке команду gpedit.msc. В окне «Редактора объектов групповых политик» выберите «Конфигурация компьютера | Административные шаблоны | Компоненты Windows | Шифрование диска Bitlocker». Теперь дважды нажмите в правом окне на «Установки панели управления: включить дополнительные параметры запуска» и потом выберите «Активировать | Разрешить Bitlocker без TPM». Затем вставьте USB-накопитель, на котором должен быть сохранен ключ запуска, и закройте мастер. Теперь и Vista Ultimate защищена.

ДЕТИ ШПИОНОВ

Защита от телефонного контроля

Инструменты: Zfone (Beta), Skype

Основное правило для тех, кто хочет защититься от прослушивания телефонного разговора: забудьте о стационарных телефонных сетях. Тут вы ничего не сможете поделать. Ответные меры принять вы сможете только при использовании интернет-телефонии (VoIP).

Если вы используете Skype (www.skype.com), вам не придется принимать никаких дополнительных мер. Этот поставщик услуг IP-телефонии автоматически шифрует разговоры, используя 256-битный стандарт шифрования AES. Если же вы пользуетесь услугами другого провайдера, зашифровать свое соединение можно с помощью Zfone. Этот инструмент встраивается в известные программы интернет-телефонии, например X-Lite, как плагин. Этот инструмент тоже шифрует данные по стандарту AES. Чтобы все прошло успешно, сначала запустите Zfone и только после этого VoIP-клиент вашего провайдера.

Защита от охотников за интернет-профилями

Инструменты: CookieCooker, Proxomitron

С помощью cookies и реферреров шпионы могут узнать, какие веб-сайты вы посещаете и что на них скачивали или просматривали. Так как вы сами создаете персональный профиль, который содержит ваши интересы и покупательские привычки. Но с помощью пары трюков вы можете стать незаметными.

Отключить Cookies. В Internet Explorer в меню «Дополнительно | Настройки Интернет | Защита данных» переключите регулятор в положение «Высоко», чтобы удалить предательские текстовые файлы. Для Firefox скачайте плагин Remove Cookie(s) from Site. Как только он будет инсталлирован, нажмите на правую клавишу мыши на странице, где вы находитесь, и выберите «Remove Cookie(s)». Пользователи Opera должны выбрать «Дополнительно | Настройки | Расширенные | Cookies» и активировать пункт «Никогда не записывать Cookies».

Правда, у всех этих методов есть один недостаток: вам придется постоянно заново авторизоваться на интернет-форумах, если ваш браузер не поддерживает Cookies. Тем, кто все-таки хочет без проблем авторизироваться на определенных сайтах, стоит рассмотреть условно-бесплатную программу CookieCooker. С помощью этого инструмента вы можете использовать различные виртуальные личности, не отказываясь от автоматической авторизации. К тому же программа прекрасно работает вместе с JAR.

Блокировать реферрер. От реферреров, которые позволяют отследить путь пользователя по Интернету, можно избавиться с помощью Proxomitron. После инсталляции этой программы сначала следует изменить пару настроек в своем браузере. Выберите в Internet Explorer «Дополнительно | Настройки Интернет | Соединения | настройки LAN» и активируйте опцию «Использовать сервер прокси для LAN». Внесите в качестве адреса «localhost», а в разделе порта поставьте 8080. После этого вы можете запустить Proxomitron и спокойно путешествовать по Сети. Фанаты Opera вышли из воды сухими: им не нужен Proxomitron, с помощью клавиши «F12» можно зайти в «Быстрые настройки», потом удалить галочку около «Передать происхождение (реферрер)», подтвердить свое решение – и можно спокойно бродить по Интернету.

Чего стоит конфиденциальность в нашей стране?

Ни для кого не секрет, что с конфиденциальностью в нашей стране все совсем плохо. Практически на любом радиорынке вы можете купить диски с базами адресов и домашних телефонов, или даже пенсионные данные, являющиеся в других странах строжайше конфиденциальной информацией. Однако начинают говорить об этом лишь в том случае, когда это оказывается у всех на виду, как в случае скандального интернет-ресурса Radarix, предоставляющего информацию любому желающему о любом гражданине. И кто уж позаботился о своей конфиденциальности – так это создатели ресурса. Сайт оказался зарегистрирован на неизвестное лицо из далекой страны, а информация об истинных владельцах не появилась до сих пор. В этих условиях особо важно, чтобы ваши личные данные не были связаны с интернет-данными о вас. Это позволит значительно снизить потенциальный вред, который могут принести действия злоумышленников на просторах Глобальной сети. В особенности это касается фишинговых махинаций.

Лучшие инструменты для вашей личной безопасности

xB Browser защищенная версия Firefox

JAP/JonDoскрывает данные вашего браузера

JonDoFox позволяет анонимно путешествовать по Интернету

TrueCrypt 5 шифрует раздел Windows

ZfoneBeta шифрует VoIP-разговоры (SIP)

Skype шифрует VoIP-разговоры собственными средствами

CookieCooker скрывает ваши действия в Интернете

Proxomitron скрывает информацию через браузер

LocateProtect препятствует получению информации о местоположении вашего телефона

Источник: HTTP://WWW.ICHIP.RU

Как оставаться анонимным в сети: скрываем свой IP-адрес

Сеть Интернет все глубже проникает в нашу жизнь, в то время как компьютеры уже стали неотъемлемой частью нашего существования. И уже большинство ценной информации мы храним не в тетрадках или блокнотах, а на жестком диске, считая, что никто никогда не посягнет на нее. Но как бывает печально, когда это оказывается не так. Цель данной статьи затронуть умы пользователей, которые еще не задумывались о своей безопасности – ведь обновление Windows и установка антивируса с фаерволлом очень часто не защищает нашу конфиденциальную информацию.

Для начала узнаем немного про IP-адреса

IP-адрес (ай-пи адрес, англ. Internet Protocol Address) – уникальный идентификатор устройства, подключенного к локальной сети, или Интернету. Короче говоря, это адрес вашего компьютера в сети.

IP-адрес представляет собой 32-битовое (по версии IPv4 – наиболее распространенная версия) или 128-битовое (по версии IPv6) двоичное число. Удобной формой записи IP-адреса (IPv4) является запись в виде четырех десятичных чисел (от 0 до 255), разделенных точками, например, 192.168.0.1. IP-адреса представляют собой основной тип адресов, на основании которых сетевой уровень протокола IP передает пакеты между сетями.

А зачем скрывать свой IP-адрес?

В независимости от вашего желания или отсутствия оного, каждый ваш шаг в Интернете, будь то просмотр ваших любимых сайтов, или покупка в онлайновом магазине, или тот же треп в чатах, оставляет следы в регистрационных журналах интернет-серверов. Запуская свой браузер и посещая один сайт за другим, ваш слуга добровольно сообщает всем, кто у него просит, IP-адрес, под которым вы находитесь в сети, также выдает информацию о своем наименовании и версии, тип операционной системы, и множество другой информации о вашем компьютере. Может быть, для вас эта информация и является бесполезной, но для более-менее компетентного человека она является дверью в ваш компьютер, нужно лишь подобрать ключи (а это уже дело техники). Много может проблем и финансовых расходов свалиться на вашу голову, будь на месте этого человека злоумышленник.

С помощью чего можно скрыть свой IP-адрес?

Скрывать свой IP-адрес мы будем с помощью прокси (proxy) сервера. Прокси-сервер – это промежуточный компьютер, который является посредником («proxy» – от англ. посредник) между вашим компьютером и глобальной паутиной. Через него проходят все ваши обращения в сеть, он их обрабатывает, и результаты (скаченные файлы) передает вам. Прокси-сервер может повысить скорость связи, сделать присутствие в сети анонимным, обходить ограничения, поставленные вам (бан на форуме и чате).

Классификация прокси-серверов

Существует несколько типов proxy-серверов. Каждый тип proxy предназначен для решения своего круга задач, однако у них есть много общего, их возможности во многом совпадают.

HTTP (Hyper Text Transfer Protocol) proxy:

Это «обычный» прокси-сервер, встречающийся наиболее часто, и говоря просто «прокси», подразумевают именно его. С этим типом proxy умеют работать браузеры любых версий.

Socks proxy:

Эти прокси-серверы умеют работать практически с любым типом информации в Internet, одна-

ко для их использования в программах должна быть явно указана возможность работы с socks прокси. Многие браузеры не умеют самостоятельно использовать socks прокси, но существует множество программ, направленных на решение данной проблемы (к примеру FreeCap). Также указывается версия socks прокси сервера: socks 4 или socks.

CGI proxy (анонимайзеры):

Данным типом прокси-серверов можно пользоваться только с помощью браузеров. Он является web-страницей, адрес которой нужно просто набрать в панели адреса браузера, и не надо менять какие-либо настройки программ.

Как настроить браузер для работы с прокси-сервером?

Рассмотрим настройку прокси в нескольких наиболее распространенных браузерах.

Internet Explorer:

1. Выбираем меню «Сервис», пункт «Свойства обозревателя»;
2. Кликаем на вкладку «Подключения»;
3. Ставим галочку рядом с опцией «Использовать прокси-сервер»; в поле «Адрес» вводим имя прокси-сервера, а в поле «порт» – номер порта прокси;
4. Жмем везде «ОК».

Mozilla Firefox:

1. В меню «Инструменты» выбираем пункт «Настройки»;
2. Подменю «Дополнительно», вкладка «Сеть»;
3. Нажимаем «Настроить»;
4. Активируем функцию «Настроить параметры подключения прокси вручную», и вписываем прокси в соответствующие поля;
5. Жмем «ОК».

Opera:

1. В меню «Инструменты» выбираем «Настройки...» (Ctrl+F12);
2. Вкладка «Дополнительно», категория «Сеть»;
3. Кликаем по кнопке «Прокси-серверы»;
4. Указываем прокси для соответствующих протоколов;
5. Жмем «ОК».

Где взять анонимный прокси-сервер?

Итак, мы разобрались, как и с помощью чего можно скрыть наш реальный IP-адрес, подменив его адресом анонимного (не передающего наш реальный IP-адрес и прочую информацию о нас) прокси-сервера. Но теперь надо решить следующую задачу: где собственно взять этот прокси.

Доступ к этим прокси-серверам можно купить, а можно и бесплатные найти. Конечно, основную помощь нам окажет поисковик (пример запроса – «анонимный прокси-сервер», или лучше вбить в поисковик какой-либо прокси-сервер – 210.0.202.30:8080). Можно пройтись по найденным сайтам, где мы найдем списки прокси. Но в найденных списках не все прокси будут рабочими, а проверять их вручную далеко не лучший вариант. Тогда сбиваем все списки проксей в один файл и проверяем на работоспособность с помощью программы Proxy Checker.

Обеспечение анонимности в Интернете

От профессиональных шпионов в Интернете вас не спасет даже костюм Бэтмана, а вот новейшая версия программы-анонимайзера CyberGhost VPN справится с этой непростой задачей без особых проблем.

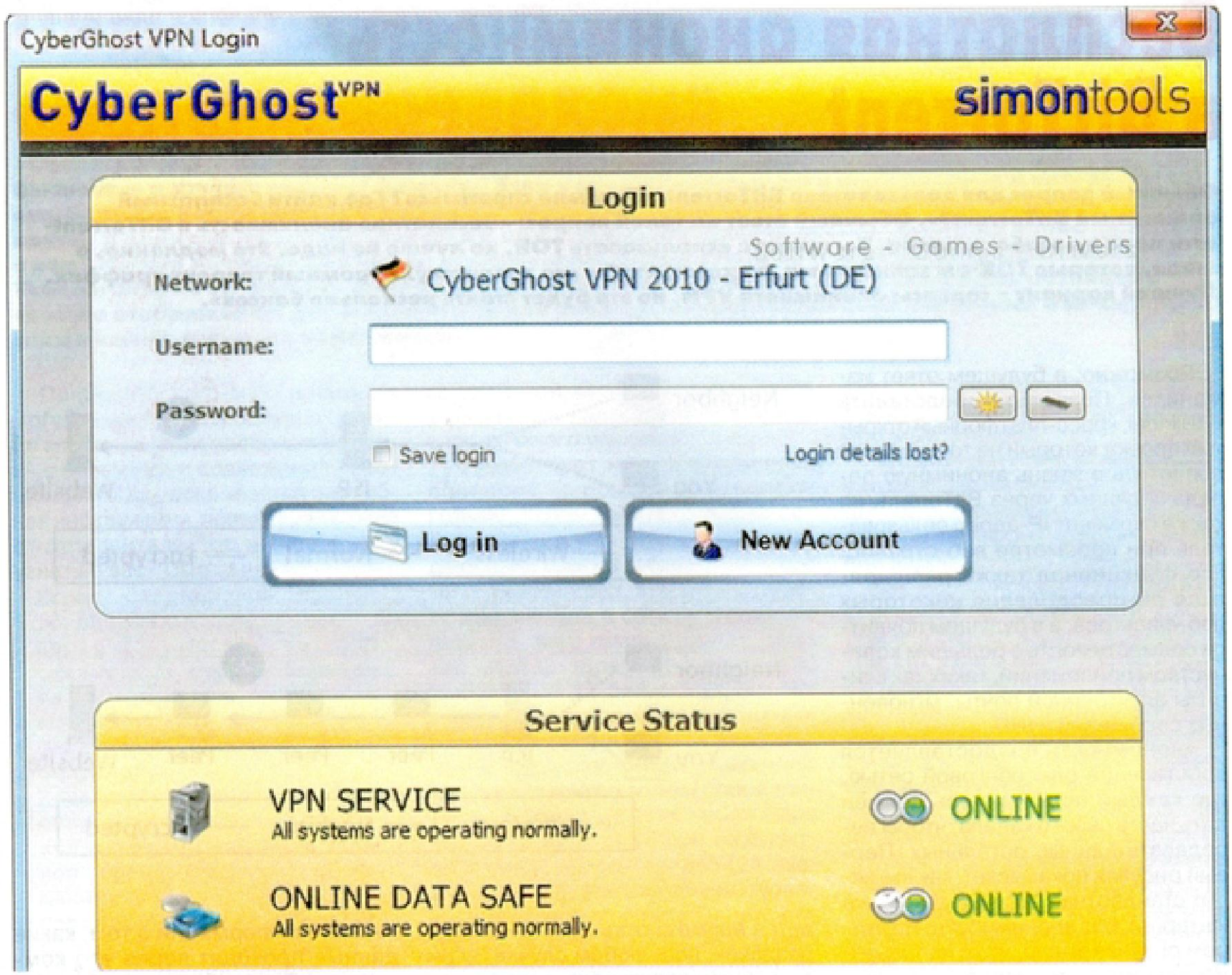
Вы никогда не чувствовали себя Нео? У вас не возникало ощущения, что за вами кто-то следит, читает ваши письма, слушает разговоры? «Я же не параноик!» – ответит нормальный человек и, казалось бы, будет прав. Однако в виртуальном мире оснований для паранойи значительно больше. Оказывается, администраторы интернет-сайтов знают о личной жизни пользователей удивительно много. С помощью этой информации они «бомбардируют» их целенаправленной рекламой. Защитить ПК от любителей «заглянуть в замочную скважину» можно с помощью специального ПО. Мы расскажем, как это сделать с помощью программы CyberGhost VPN.

Новейшая версия программы получила название CyberGhost VPN 2010. С сайта программы можно скачать бесплатный полнофункциональный вариант приложения (Basic), однако всегда есть возможность испытать всю мощь версии Premium, если купить годовую лицензию и продолжить анонимный серфинг.

* Платная версия Premium дает пользователю следующие преимущества:
* CyberGhost гарантирует анонимность работы в Интернете при скорости передачи данных не менее 2000 кбит/с.
* Доступ к ресурсу обеспечивает передачу 10 Гб информации в месяц – этого вполне достаточно для анонимного скачивания большого количества файлов из Интернета.
* Вам гарантируется полное отсутствие рекламы со стороны CyberGhost.
* Вы можете разместить в Интернете до 2 Гб личных данных и открывать их для скачивания другими пользователями программы CyberGhost (также анонимно).

Как информация о действиях пользователя попадает к посторонним лицам

В большинстве случаев администраторы сайтов могут узнать, по каким ссылкам щелкают их посетители. На основании IP-адреса через провайдера интернет-услуг можно даже соотнести эти клики с определенным компьютером. Если же вы оставляете и свои личные данные, такие как имя, адрес и рассказываете о



своих интересах, заполняя всевозможные анкеты или регистрационные формы, сведения о вас становятся еще более подробными.

Даже если вы не указываете личные сведения, неузнанным вы не останетесь, ведь так называемые cookies продолжают вас выслеживать. Веб-сайты сохраняют эти маленькие текстовые файлы на вашем компьютере – с их помощью администраторы интернет-магазинов всегда могут узнать, какие товары вы просматривали в ходе своего последнего визита.

Ничего хорошего в этом, разумеется, нет: вы не знаете, какие сведения о вас собираются и кто получает эти данные. Ловкие сборщики информации рано или поздно составят ваш полный портрет: они будут знать, какие проблемы со здоровьем вас беспокоят, за кого вы голосовали на последних выборах, вычислят, сколько денег вы тратите ежемесячно на покупку различных товаров.

И это касается практически каждого пользователя Глобальной сети.

Каким образом CyberGhost обеспечивает защиту вашего ПК

CyberGhost скрывает ваши действия в Интернете с помощью технологии маскирования. Процесс анонимизации ПК гарантирует, что установить, какие веб-сайты вы посещаете и что именно скачиваете из Сети, будет нельзя!

Серверы CyberGhost, обеспечивающие подстановку IP-адресов, расположены в Германии, что гарантирует российским пользователям непробиваемую защиту. Как сообщили нам коллеги из немецкой редакции ComputerBild, в Германии действовал «Закон о резервном копировании данных», который обязывал CyberGhost протоколировать визиты своих пользователей. Однако после того как Конституционный суд приостановил действие этого закона, все протоколы клиентов были немедленно удалены. Но даже в то время, когда закон о резервном копировании был в силе, CyberGhost никогда не выдавал никаких сведений о своих клиентах, несмотря на наличие свыше 200 запросов от органов власти Германии.

Что еще потребуется при работе с CyberGhost

Программа CyberGhost маскирует IP-адрес, однако через сохраненные на пользовательском компьютере cookies-файлы вас по-прежнему можно идентифицировать в Интернете. Если вы хотите скрыть эти следы, необходимо использовать специальное ПО.

Бесплатная анонимность в BitTorrent

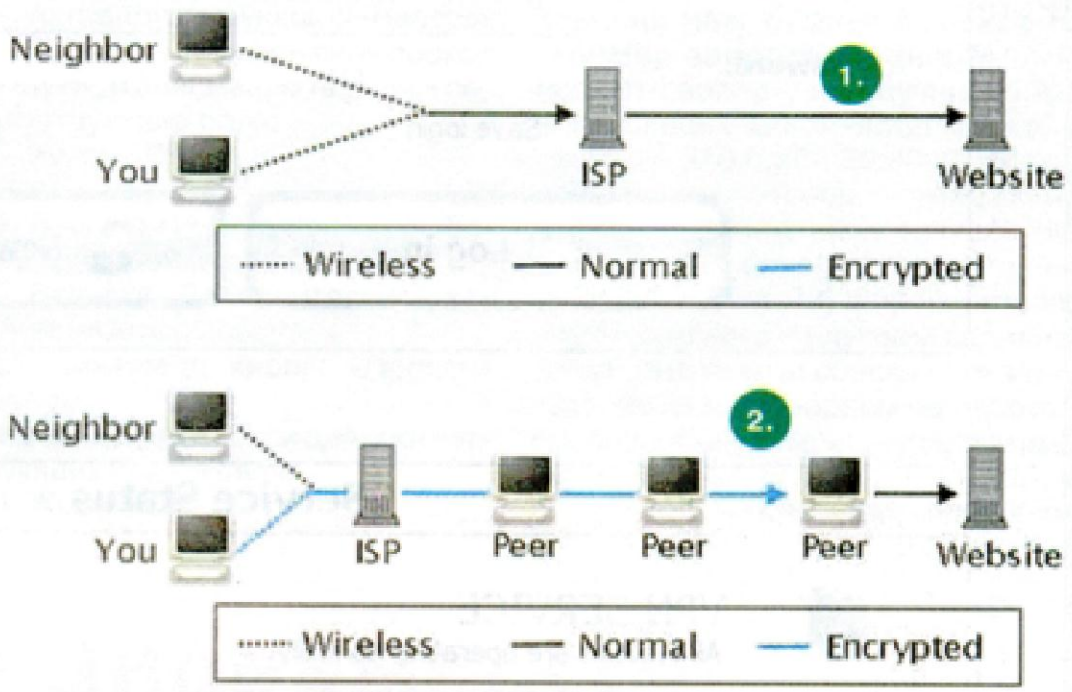
Обычный вопрос для пользователя BitTorrent: «Как мне спрятаться? Где найти бесплатный анонимный BitTorrent?». Обычный ответ на такой вопрос: «Бесплатная анонимность в BitTorrent-сети пока не особо реальна. Вы можете использовать TOR, но лучше не надо. Это медленно, а люди, которые TOR-ом занимаются, не хотят, чтобы его захлестнул огромный торрент-траффик. Лучший вариант – сервисы анонимного VPN, но это будет стоить несколько баксов».

Возможно, в будущем ответ изменится. Позвольте представить BitBlinder, кросс-платформный открытый проект, который не только готов воплотить в жизнь анонимную передачу данных через BitTorrent, но также скрывает IP-адрес пользователя при просмотре веб-страниц. Его функционал также расширяется до преодоления некоторых веб-фильтров, а в будущем появится совместимость с большим количеством приложений, таких как клиенты электронной почты, мгновенных сообщений и IRC.

Анонимность предоставляется собственной одноранговой сетью, где каждый пользователь должен дать часть своего канала, чтобы передавать данные остальных. Первый рисунок показывает, как выглядит стандартная система доступа в Интернет, без анонимности. На втором рисунке видно, что с использованием BitBlinder ваш запрос данных проходит зашифрованным через нескольких пиров. Каждый пир в цепочке знает лишь адрес следующего, но не изначального отправителя/запрашивающего.

Поскольку действительно доступные для использования в BitTorrent анонимизаторы стоят денег, как BitBlinder удается предоставлять то же самое бесплатно? Смысл в том, что сеть управляется очень похоже на закрытый BitTorrent трекер.

Для того, чтобы поддерживать хороший рейтинг на закрытом трекере, вам как минимум надо раздать столько, сколько скачали. В BitBlinder система та же – чтобы получить услуги бесплатно, вам надо передать X ГБ данных других людей сети, если вы хотите передать X ГБ своих анонимных данных. Как и на закрытых трекерах новичкам предоставляется стартовый запас – 2 ГБ. Если кто-то не хочет быть связанным рейтингом, то как и на многих закрытых трекерах скоро появится возможность купить «кредит раздачи», но в любом случае, если люди будут делиться каналом, никто не запретит им пользоваться сетью бесплатно.



Дистрибутив для пользователей Windows весит 17 мб. Торрент-клиент – модифицированная версия BitTornado, хотя в нем еще нет всех функций uTorrent, обещают со временем их добавить. Также в комплект входит анонимный браузер на основе Firefox.

Разумеется, в BitBlinder есть некоторые проблемы с анонимностью, они схожи с теми, что есть у пользователей Tor. Любой трафик в BitBlinder-сети должен рано или поздно попасть в Интернет. Чтобы это произошло, кто-то из пользователей должен стать точкой выхода, а значит, его IP-адрес будет ассоциирован с исходящим трафиком.

Не стоит паниковать, это не такая уж плохая новость. Работа с точкой доступа позволяет пользователю спокойно отвергать все обвинения, поскольку у него нет никакой информации о том, какие данные проходят через его компьютер. Также будет трудно доказать, что данные, вышедшие в Интернет с этого комьютера, изначально появились на нем или где-то еще, что позволит пользователю отказываться от обвинений, даже если данные его собственные. Да и до появления BitBlinder IP-адреса пользователей BitTorrent были отлично видны.

BitBlinder можно скачать здесь: http://www.bitblinder.com, не забудьте зарегистрироваться, а также прочитайте инструкции по открытию портов.

Новые пользователи должны учесть, что пригласительные высылаются с контролированной скоростью. Ранние пользователи смогут зарегистрироваться быстро, но чем больше будет людей, тем дольше придется ждать новичкам. Это сделано для построения здоровой сети с достаточным количеством хороших пользователей-прокси.

HTTP://P2P-PLANET.ORG.

Пишите письма «мелким почерком»

Вы любите получать письма? А писать? Если у вас есть компьютер и подключение к интернету, то есть большая вероятность, что у вас установлена почтовая программа и имеется адрес электронной почты. А коли так, то письма «летят» и к вам и от вас. Отправляя письмо, вы много о себе написали в нем? Ничего личного? Сейчас мы это проверим. Я пользуюсь почтовой программой Mozilla Thunderbird, но это можно выполнить почти в любом почтовике, с небольшой лишь разницей в способе отображения. Даже если кто-то для работы с корреспонденцией пользуется web-сервисом, также имеют такую же возможность.

Получив от кого-либо письмо, я могу щелкнуть по плюсику на границе между окнами содержания папки с письмами и содержания сообщения. Тогда раскрывается служебная информация, пришедшая ко мне от отправителя. Что из нее я могу узнать о вас? Смотрим:

```
From: отправитель данного письма;
Reply-To: адрес, который окажется в строке адресата при нажатии на кнопку «Ответить»;
Date: дата и точное время отправки;
Received: с какого IP было отправлено письмо, протокол передачи данных и точное время отправки сообщения;
Content-Type: text/plain; charset=koi8-r кодировка и форматирование сообщения;
X-Mailer: почтовая программа отправителя;
X-Originating-IP: IP отправителя;
X-Spam-Checker-Version: через какой антиспамовый фильтр прошло письмо;
X-Virus-Scanned: какой антивирусной программой было проверено письмо;
X-Virus-Status: Clean, т.е. вирусов не содержится.
```

Разумеется, это еще не полный список всего, что там содержится, но тем не менее, стоит задуматься перед отправкой любого письма, кому бы то ни было. Естественно, самой важной информацией в данном случае является «IP» отправителя. Обладая совершенными техническими и программными средствами, достаточно «подкованный» злоумышленник может причинить немалый вред любому написавшему ему письмо по электронной почте. Для абсолютной конфиденциальности в интернете надо прилагать очень и очень много усилий.

Существует много различных способов (с помощью спецпрограмм), чтобы узнать ip-адрес собеседника в чате или в аське. Надеюсь, вы еще не забыли, что такое «IP»? Каждый раз, выходя со своего компьютера в сеть интернет, вы (вернее, ваш компьютер) получаете свой ip-адрес. IP-адрес – это уникальный 32-битный адрес, используемый для идентификации узла (компьютера) в сети. Уникальный ip-адрес состоит из четырех чисел, разделенных между собой точками. Каждое из этих чисел (еще его называют октетом) находится в пределах от 0 до 255 (28 равняется 256). По значению первого октета можно подразделить все адреса на пять классов. Например: диапазон от 001.000.000.001 до 126.255.255.254 относится к классу «А» и предназначен для использования в больших сетях общего пользования. В нем первый октет обозначает сеть, а последние три октета – узел в сети. Диапазон от 128.000.000.001 до 191.255.255.254 относится к ip-адресам класса «В» и используется в сетях среднего размера, например, сетях университетов или крупных компаний. Первые два октета в нем обозначают сеть, последние два октета – узел в сети. Адреса класса «С» (диапазон от 192.000.000.001 до 223.255.255.254) используются в сетях с небольшим числом компьютеров. Первые три октета обозначают сеть, последний октет – узел в сети. И так далее. Так вот, у каждого провайдера имеется в своем распоряжении определенное количество арендованных ip-адресов, один из которых динамически присваивается одному из подключившихся компьютеров. В связи с чем не составляет большого труда определить, какому провайдеру принадлежит искомый ip-адрес.

Что это дает? Через провайдера уже можно вычислить всю информацию об определенном клиенте, его номере телефона и даже домашний адрес.

Как это происходит? Да просто на серверах ведется протокол, в котором фиксируется вся информация о том, кто, в какое время, с какого номера телефона заходил в интернет, какой протокол был использован, к каким сайтам были запросы, что запрашивалось, вплоть до каждой картинки (а иначе как вообще можно транслировать на ваш компьютер данные, не зная их адреса) и, разумеется, какое было использовано кодирование, если такое вообще имело место. По понятным причинам кому угодно подобная информация не предоставляется. Даже не надейтесь.

Но часто сервер, предоставляющий хостинг, сам ведет статистику, которую может предоставить вам, как своему клиенту. Чего не получится в случае использования услуги бесплатного хостинга. В этом случае можно на своем сайте установить какой-нибудь счетчик посетителей, по которому вы без труда сможете узнать ip-адрес посетителя, в том числе и время его посещения. Как это использовать? Располагая информацией об ip-адресе посетителя, можно без особого труда «отделаться» от его посещений, перекрыв ему доступ, что обычно и происходит, если посетитель начинает себя некорректно вести на чьем-то сайте. Выводы делайте сами.

Анонимность в интернете не бывает абсолютной. Помните об этом всегда, оставляя «честные» записи в Гостевых, на форумах и отправляя электронную почту.

Николай ГРУШИН.

Как узнать, чем занимался пользователь компьютера?

Зачем это нужно? Контролировать ребенка или проследить за второй половиной. Узнать, чем так занят ваш работник и не зря ли вы платите ему деньги. Выявить инсайдера или определить каналы утечки ценной информации. Или просто по долгу службы. Мотивов может быть много, и как вы договоритесь со своей совестью, вторгаясь в чужое пространство, уже ваше дело.

Немного конкретизирую задачу. Предположим, что на компьютере установлена ОС Windows XP, у пользователя свой логин с неизвестным вам паролем и у вас нет прав администратора. Нужно узнать, какие программы запускались, с какими файлами работал пользователь, что писал в аське и по почте, что хранит и хранил на жестком диске, пароли к сайтам и программам. На все не более часа. Программы, которые вы будете использовать, должны быть из класса «Portable», то есть работать без установки на исследуемый компьютер.

Поехали. Для начала надо получить доступ к учетной записи пользователя и зайти с его правами. И пароль тут не преграда. Существует масса программ по подбору паролей, но это требует значительного времени, и рассматривать их не будем. Самое простое – использовать загрузочный CD или флэшку с программой, способной изменить пароль пользователя без знания старого.

Например «CIA». Для загрузки с внешнего носителя у большинства современных компьютеров достаточно нажать специальную функциональную клавишу, указанную при включении компьютера на самом первом экране. Запускаете «CIA», выбираете каталог с Windows пользователя и обнуляете его пароль, затем устанавливаете новый. Перезагрузка в штатном режиме, ввод нового пароля – и вы уже в системе. Все просто. Для заметания следов достаточно обнулить пароль пользователя средствами системы, и большинство пользователей при следующей загрузке спишет все на «глюки дурацкой Винды».

Не теряя времени, запустите программу восстановления удаленных файлов. Советовать тут что-то сложно. На вкус и цвет. Попробуйте для начала «Active File Recovery», для большинства случаев ее хватит. Сначала быстрый поиск как менее затратный по времени.

Пока идет поиск, давайте вытащим все пароли. Лучшая из программ «Multi Password Recovery». Почта, аська, имена и пароли к сайтам и другим компьютерам. Какие программы установлены, что запускается при входе в систему – сохраните на флэшку, потом, в спокойной обстановке, можно полазить по форумам и почитать, что писал пользователь.

Пришла пора разобраться с почтой. Можно запустить почтовик, который используется, и почитать, а можно скопировать базы с письмами и разобраться потом. Если используется Outlook Express, то достаточно найти, где находится файл с именем «Входящие» и весь каталог скопировать себе на флэшку. Даже если пользователь аккуратно удалял все письма, то они все равно остаются в базе, пока он не применит команду «Сжать все базы». А кто это делает? Есть программы, которые восстанавливают такие удаленные письма.

Далее уже коротко:

- Всеми любимый QIP хранит всю переписку в C:\Program Files\QIP\Users\номер\History;

- С какими документами и файлами работал пользователь, смотрите в C:\Documents and Settings\имя \Recent;

- Какие программы запускал и когда, видно в C:\WINDOWS\Prefetch;

- В браузере (Internet Explorer, Opera и т.д.) можно посмотреть историю посещенных сайтов.

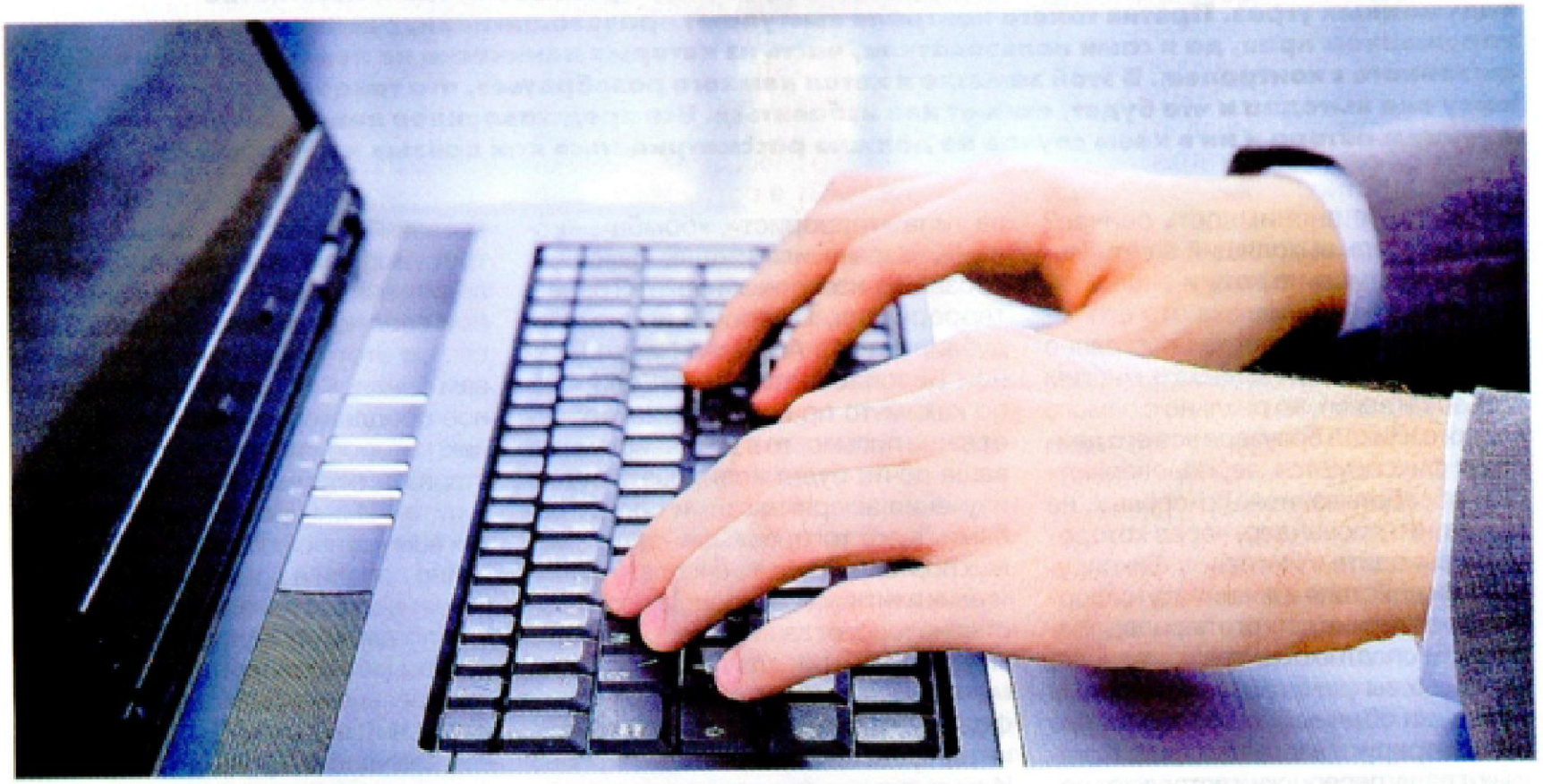
Есть простор, где поковырятся любопытному человеку. Как раз и поиск удаленных файлов закончился, там тоже много интересного можно найти. При большом желании это все можно сделать и удаленно, даже не подходя к компьютеру. Windows, установленная по умолчанию, довольно дырявая система, и защитить ее обычному пользователю практически нереально. Это труд, который должны делать специалисты.

Так что анонимность, тайна переписки, приватные данные и пароли в век компьютеров – не более чем самообман, уверяю вас.

Олег МИХАЙЛЕЦ.
HTTP://SHKOLAZHIZNI.RU

Со всех пользователей Интернета сняты отпечатки пальцев

Для однозначного опознания пользователя не надо, чтобы он регистрировался, не надо писать ему своих cookies – не надо делать ничего, что не нравится многим людям, озабоченным проблемами собственной безопасности. Достаточно просто посмотреть на доступные любому веб-сайту данные.



Каждый пользователь, ходящий по Сети, в своем браузере имеет уникальный «отпечаток пальцев» и даже не задумывается об этом. Как показало исследование Panopticlick, 84% браузеров, выходящих в Сеть, можно достоверно опознать. Настройки Javascript и Flash, язык системы, версия браузера (включая номер сборки), язык браузера – есть масса настроек компьютера, доступных для изучения сторонним сайтам. Ввиду того, что настроек этих очень много, а люди все разные, набор настроек почти всякого пользователя уникален.

Собирая такие данные, сайт может «опознавать» пользователя, даже если он меняет cookies или выходит с компьютера, изменив IP. Потенциально именно такие «отпечатки пальцев» являются источниками наиболее массовых нарушений приватности. Если общая доля однозначно идентифицируемых браузеров составляет 84%, то среди браузеров с установленным Flash или Java эта доля составляет 94%.

Panopticlick смогла найти уникальные идентификаторы браузеров, исследовав лишь 8 переменных:

- Имя браузера (включает в себя номер сборки, версию ОС, язык, установленные тулбары, иногда – другую информацию);
- Заголовки HTTP ACCEPT;
- Информацию о том, включены ли cookies;
- Разрешение экрана;
- Часовой пояс;
- Плагины браузера, их версии и MIME-тип;
- Системные шрифты;
- Информацию о supercookies (различные расширенные аналоги cookies, подобные Flash cookies).

В реальности существуют еще переменные – использовав их, возможно, получится уточнить результаты и опознать еще большую долю браузеров.

Некоторые типы пользовательских машин оказались сравнительно устойчивыми к методике исследователей:

- браузеры с отключенным Javascript;
- компьютеры, подключенные к анонимной сети Tor;
- мобильные устройства на Android и iPhone;
- корпоративные компьютеры в рамках одной компании, неотличимые друг от друга (хотя есть методики, которые позволяют отличить и их).

Результаты этого исследования означают, что на самом деле анонимность в Сети недостижима не только по отношению к правительственным органам и спецслужбам. Практически любого пользователя может отслеживать произвольный сайт – удаление cookies не спасет. Однако эти методики никак не решают задач, которые не дают покоя рекламщикам и другим людям, готовым отдать душу за пользовательские данные. С помощью снятия «отпечатков пальцев» можно различить двух пользователей, но никак нельзя установить про них какую-либо информацию – предпочтения, доходы, любимые сайты.

HTTP://WWW.RUFORMATOR.RU

Анонимность в Интернете — а кому она реально нужна?

В последнее время все чаще поднимается вопрос о необходимости ужесточения контроля за пользователями в сети Интернет в связи с массовым распространением пиратства, порнографии, угрозам кибертерроризма, спама и множества других как реальных, так и абсолютно надуманных угроз. Против такого контроля выступают правозащитники, считающие это нарушением прав, да и сами пользователи, часть из которых панически не переносит чего-либо связанного с контролем. В этой заметке я хотел немного разобраться, что такое анонимность, кому она выгодна и что будет, если от нее избавиться. Все представленное ниже является личным мнением автора и ни в коем случае не должно рассматриваться как призыв к действиям.

Что такое анонимность сейчас? Пользователь выходящий в сеть Интернет формально хоть и анонимен (единственная привязка это его IP-адрес, который может как постоянно меняться, так и принадлежать многим пользователям), но реально с самого первого клика в браузере все его действия фиксируются, перепроверяются и обрабатываются. Во-первых, не секрет что провайдер, через которого вы выходите в Интернет, фиксирует ваши действия и хранит эту информацию в течение долгого периода времени. Бесплатные почтовые сервера, с которых вы скачиваете почту, кроме фиксации обычных логов, полностью перлюстрируют ваш e-mail трафик, изучают вашу переписку и вставляют рекламу, соответствующую тематике отправляемого или получаемого сообщения. Кто-то может удивиться – мол, сколько не пользуюсь бесплатной почтой, никогда такого не замечал. То, что вы не видели такую рекламу, совершенно не означает, что ваша почта не анализируется. Это объясняется лишь тем, что пока в России продажи контекста не так распространены, как на Западе (в США это один из самых доходных видов бизнеса, посмотрите для примера на рост компании Google). Попробуйте попользоваться hotmail.com или gmail.com и отправить письмо другу, например, с вопросом посоветовать, какой плазменный телевизор лучше купить (только делайте этот вопрос на английском языке). Будьте уверены, что в письме снизу появится реклама интернет-магазина, продающего плазменные телевизоры… Если в письме поинтересуетесь аквариумными рыбками, компьютерными игрушками или порносайтами, вы увидите специфическую рекламу в письме.

Ряд писем, в контексте которых достаточное число раз встречаются слова типа «террорист», «бомба», «ислам», «взрыв» или имена, фамилии, прозвища известных наркотоговцев, террористов, хакеров и политиков, дублируются в Агенство Национальной Безопасности США. Если АНБ по каким-то причинам заинтересует ваше письмо, то в дальнейшем вся ваша почта будет копироваться для изучения американскими спецслужбами. Хуже того, большинство крупных порталов, будь то бесплатный почтовик или поисковик google.com, бесстыдно торгуют вашими персональными данными и предпочтениями, незаметно навязывая и представляя информацию, которая способна вас заинтересовать. Разве это не контроль? И вы ведь в большинстве случаев даже не будете подозревать о нем.

А заходя на обычный сайт? Давайте рассмотрим пример этого сайта – SecurityLab.ru. Контроль каждого посетителя начинается с первого хита. Если вы впервые на сайте, вам вылезет popup окно (оно, конечно, будет «зарезано» в большинстве браузеров, но такое есть) с предложением принять участие в опросе, появится пусть и ненавязчивая, но реклама других разделов сайта или самых интересных статей, которые могли бы заинтересовать новичка и в будущем дать ему шанс вернуться на сайт и стать постоянным посетителем. Абсолютно все ваши клики по разделам сайта, форума, скачиваемых программ и т.п. тщательно регистрируются и затем на основании ваших предпочтений вы будете получать ту информацию, в которой вы заинтересованы. К счастью (или к сожалению) SecurityLab не зарабатывает на посетителях, не продает им подобранные персонифицированные товары или услуги и не торгует этими данными.

Но представьте, что происходит с вами, когда вы зашли в интернет-магазин? Достаточно только посмотреть информацию, к примеру, о холодильнике LG, и будьте уверены, что при следующем заходе через 3 месяца в этот магазин первым делом вам предложат скидку или специальное предложение на этот холодильник, которое «завтра перестанет действовать, если вы его прямо сейчас не купите». И вы наивно будете думать, как вам крупно повезло и что вы случайно попали в последний день действия некого специального предложения по данному холодильнику, который вы мечтали купить уже пол года. А владельцы магазина потирают руки и подсчитывают прибыль, в очередной раз удостоверившись в правильности покупки дорогостоящей системы слежения за потенциальными покупателями. И не будьте наивными в том, что если вы имеете постоянную привычку удалять куки или временные файлы магазина, что это вас не касается. Давно уже придуманы и повсеместно используются механизмы контроля вне зависимости от вашего IP, наличия или отсутствия куки при посещении сайтов. В принципе некоторые сайты, типа SecurityLab, честно сообщают в HTTP заголовках о том, какой контроль за посетителями используется на сайте согласно правилам Platform for Privacy Preferences Project (P3P). Но покажите мне кого-нибудь, кто хоть раз посмотрел на эти заголовки и изучил, что же там такого мы изучаем. Хорошо бы если 1 из 100 000 посетителей сайта.

Можно дальше приводить множество примеров, это лишь типичные из тех, с которыми сталкиваются большинство интернет-пользователей.

К чему я все это? Да к тому, что наивно предполагать, что сейчас в Интернете существует хоть какая-то анонимность и бороться с попытками якобы ее запретить. Однако в такой ано-

нимности кроме приведенных выше примеров существует множество отрицательных последствий:

* Повсеместное распространение информации и данных, вроде охраняемых законом. Миллионы пользователей P2P сетей, нелегально скачивающих программы, музыку, фильмы и книги, нанося «непоправимый ущерб» правообладателям и их представителям. И хотя это право пытаются отстоять многие пользователи, ссылаясь на анархистские лозунги типа «информация должна быть свободной», нужно понимать, что, скачивая mp3 трек или новую книгу про Гарри Поттера, мы автоматически нарушаем Уголовный кодекс РФ и даже воспитываем пренебрежительное отношение к нему ваших детей. Подумайте – что вырастет из вашего ребенка, который каждый день видит, как его папа с легкостью идет на преступление?!

* Угроза детям, которые могут легко получить доступ к информации, способной повлиять на их здоровье, нравственное или духовное развитие. У нас безуспешно пытаются пока бороться только с проявлениями детской порнографии или педофилии, а это лишь малая доля того, что угрожает ребенку, путешествующему по сети Интернет. Это и повсеместная пропаганда алкоголя, табака или наркотиков, реклама которых детям давно запрещена в обычной жизни в большинстве стран. Это и засилие радикальных организаций, объединений или сект, на каждом шагу пытающихся внушить свою идеологию, которая нередко делает из недавно веселого и жизнерадостного ребенка зомбированный инструмент, который начинает считать своим врагом соседа, которого он считал другом на протяжении многих лет, и только потому, что тот другой расы, вероисповедания или социального сословия. Это – легкость и доступность различных методов взлома, навеянных романтическим образом хакера-героя, навязываемого голливудскими фильмами и журналами типа «хакер». А ведь любой взлом является уголовно наказуемым преступлением, за которое можно получить реальный срок в реальной тюрьме с уголовниками, совершившими преступления в реальной жизни. Примеров можно привести множество, и количество угроз растет с каждым годом, месяцем, днем или часом, которые ребенок проводит в сети Интернет.

* Повсеместное распространение спама, сетевых червей или шпионских программ, от которых не защищен никто, хоть раз побывавший в Интернете.

* Это мнимые и реальные угрозы кибертерроризма, с которыми тоже нужно считаться. Многие террористические организации создали в Интернете свои собственные шпионские программы и базы разведывательных данных (в ряде случаев практически не уступающих даже системам спецслужб США), которые используются при подготовке атак. Например, печально известная японская террористическая группировка 'Аум Синрике', которая провела газовую атаку в токийском метро в 1995 году, перед этим создала компьютерную систему, которая перехватывала сообщения полицейских радиостанций, изучала почту полиции и отслеживала маршруты движения полицейских автомобилей. Хотя число таких примеров можно пересчитать по пальцам, это совершенно не означает, что угроза надуманна. Уже были примеры убийства людей при использовании только возможности сети Интернет. И что мешает в будущем террористам уничтожить город, вызвав аварию на плотине, взорвать атомную станцию или сбить с курса самолет? Возможные варианты потенциальных угроз тут ограничены лишь больной фантазией террориста и отследить, а тем более успеть предотвратить их совершенно невозможно...

А теперь давайте вместе задумаемся – кому выгодно существующее положение вещей, современная «анонимность», кто больше всех пострадает от введения контроля и цензуры?

Это, во-первых, различные группы криминальных сообществ, использующие сеть Интернет как средство для получения незаконных доходов. Во-вторых, это производители антивирусов, антишпионов и прочего софта, зарабатывающие огромные деньги на угрозах, с которыми они якобы борются. В-третьих, это производители операционных систем, вынуждающих пользователей тратить деньги на новую версию ОС только потому, что старая недостаточно справляется с интернет-угрозами. Это бизнесмены, способные следить за вами в виртуальном пространстве, за что их давно бы судили, если бы они пытались это делать в реальном мире. Это производители сомнительных товаров, оборот которых никак не контролируется в Интернете. Это представители игорного бизнеса, которые давно поняли, что неконтролируемый бизнес на человеческих слабостях намного выгодней постоянных ограничений, с которыми они сталкиваются в реальной жизни... Это представители радикальных организаций, открывшие для себя огромное поле потенциальных жертв в виртуальной сети... Наконец, это производители компьютеров, постоянно вынуждающие нас тратить деньги на то, чтобы все более требовательное к ресурсам ПО могло справляться с отражением существующих угроз. Это и чиновники ГОСУДАРСТВА, которым выгодно выбивать деньги из своих ГРАЖДАН чтобы пытаться бороться с хаосом, который сейчас творится в Интернете. ЭТО ВЫГОДНО ВСЕМ, кроме ЗАКОНОПОСЛУШНОГО человека, который хочет прожить жизнь в соответствии с принципами морали и духовности, а не опираясь на навязанные ему идеалы виртуального общества.

К чему это я скажете вы? Как можно решить все проблемы? Вариантов, конечно, множество и какой будет в конце концов применен не знает никто.

Мое личное мнение. Самый простой и самый эффективный метод (хотя я уверен, что 99% всех, кто читает эту статью, воспримут его в штыки) – это внести небольшую модификацию в существующие коммуникационные протоколы, которая позволяла бы на каждом сетевом устройстве аутентифицировать пользователей, откуда бы они не выходили в Интернет, аутентифицировать сетевые сервисы, где бы они не находились. А вся информация о пользователях, сервисах и т.п. будет храниться в некой глобальной базе (аналог ЭЦП только на весь Интернет). Теперь представьте – заходите вы на Web сайт – сайт сразу вам сообщает – какие персональные данные для получения информации на этом сайте (или на его разделах) он хочет от вас получить. Ваше право – согласиться предоставить ему эти данные, либо вообще не заходить на этот сайт. Все прозрачно и отсутствует поле для злоупотреблений. Полностью как класс исчезнут спам, вирусы и прочая гадость, которая просто не сможет распространяться. Владельцам Web-сайтов больше не придется тратить ресурсы серверов на то, чтобы их сайт нормально работал и не падал от непрекращающихся атак...

Но самое главное – все это можно реализовать в рамках текущей структуры Интернет, а не ждать внедрения новой разработки американских военных.

Александр АНТИПОВ.
http://www.securitylab.ru

Хакерам не под силу создать мировую катастрофу в одиночку

Кибератаки уже могут стать потенциальной причиной глобальных экономических катастроф. Однако для этого они должны проводиться в одно время с любым другим масштабным бедствием. Как сообщает BFM, к такому выводу пришли исследователи Организации экономического сотрудничества и развития (ОЭСР), изучая причины возможных будущих катастроф.

По мнению специалистов ОЭСР, хакеры способны создать действительно мировое бедствие лишь при удачных атаках на определенные объекты, такие как технические протоколы и ключевые спутниковые компоненты, от которых зависит работа Интернета.

Но даже при успехе подобных атак «идеальный шторм» не гарантирован, отмечается в сообщении. Для этого, по мнению профессора экономики Лондонского университета Питера Соммера и доктора Иэна Брауна из Оксфордского университета, необходимо подкрепление в виде такого же по масштабам бедствия.

http://softodrom.ru

11002
4 607074 331557