



Идентификация в Сети

Можно ли сохранить полную анонимность своих действий в Сети? Нет. Даже если вы не вводите свое имя и не оставляете адрес электронной почты, ваш компьютер идентифицируется по своему уникальному имени — IP-адресу.



Что это такое?

IP-адрес есть у любого компьютера, подключенного к сети. Именно этот адрес позволяет компьютеру осуществлять правильную работу в локальных и глобальных сетях, таких как сеть вашего офиса и Интернет. **IP-адрес** — это группа из четырех чисел, разделенных точками, например **213.157.22.171**. Он содержит в себе информацию о сети, в которой вы работаете, описание ее класса и так называемого узла сети, то есть компьютеров, которые находятся в одной сети с вами. Существование в одной локальной сети двух компьютеров с одинаковым адресом невозможно. Это необходимо хотя бы для того, чтобы отправленная почта точно дошла до адресата.

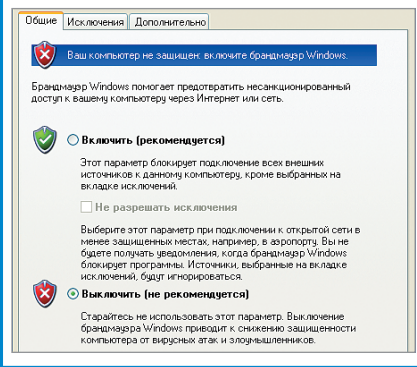
Каждый сайт в Сети также имеет свой **IP-адрес**, и чтобы эти адреса было легче запоминать, была введена система так называемых доменных имен, в которых числовому **IP-адресу** присваивается его буквенный аналог — **доменное имя**. Например, у сайта журнала **Enter** доменное имя — **ienter.ru**, хотя на самом деле его **IP-адрес** — **81.177.0.27** и хранится он в зашифрованном виде.

IP-адреса имеют принадлежность к сетям, которые, в свою очередь, разделяются на несколько классов: **A, B, C, D** и **E**. Самыми распространенными являются первые три категории. Сети класса **A** используются внутри больших офисов, где каждому компьютеру необходимо присвоить внутреннее имя. **IP-адреса** в таких сетях называют

СИСТЕМНЫЕ СРЕДСТВА

Брандмауэр представляет собой систему безопасности, действующую по принципу щита между вашим компьютером и внешним миром. Программа использует настройки ограничений, регулирующих обмен данными между Интернетом и домашней или офисной сетью. Брандмауэр позволяет вам защитить от различных сетевых угроз компьютер, а также другие машины, если они подключены к вашему ПК. Чтобы включить брандмауэр, вам необходимо выполнить следующие действия:

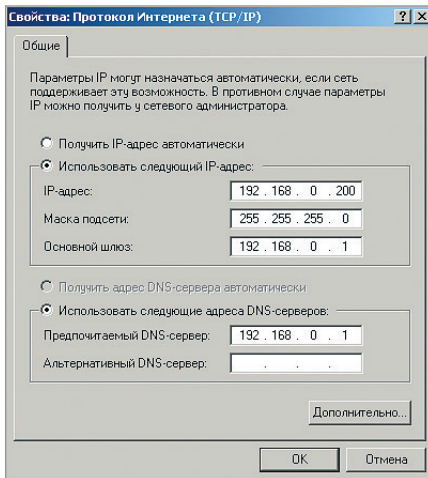
1. Выберите сетевое подключение, которое требуется защитить, и в группе **Сетевые задачи** щелкните по ссылке **Изменение настроек подключения**.
2. На вкладке **Дополнительные параметры** в группе **Брандмауэр подключения** к установите флажок **Защитить мое подключение к Интернету**.



локальными адресами, и они могут иметь следующий вид: **127.168.0.2**.

Чтобы узнать адрес своего компьютера, щелкните правой кнопкой мыши по иконке **Сетевое окружение** и выберите пункт меню **Свойства**. В открывшемся окне кликните правой кнопкой мыши по значку **Подключение по локальной сети** или **Сетевой мост** (в зависимости от ваших настроек), затем в поле **Компоненты, использующие данное подключение** найдите **Протокол Интернета (TCP/IP)** и дважды щелкните кнопкой мыши по этому пункту. На вкладке **Свойства: Протокол Интернета (TCP/IP)** вы сможете увидеть: свой **IP-адрес**, маску подсети, которая говорит о классе вашей сети и общем количестве адресов, а также **IP-адрес** шлюза (общего компьютера, через который осуществляется подключение к Интернету).

Система присвоения внутренних локальных **IP-адресов** настраивается вашим системным администратором и может быть произвольной. Такие адреса «не видны» че-



↑ IP-адрес ПК для подключения к Сети

рез Интернет, что и обеспечивает безопасность вашего компьютера. Правда, это вовсе не означает, что вы сможете оставаться анонимным пользователем в Сети. Дело в том, что компьютер (шлюз), с которого вы выходите в Интернет, имеет статический **IP-адрес**, принадлежащий сети класса **B** или **C**, и любые ваши действия в Интернете будут сохранены от лица этого **IP-адреса** и локального адреса вашего компьютера.

Предположим, ваш локальный адрес **127.168.0.2**, адрес шлюза **213.157.22.171**. Если вы оставите сообщение на форуме, система статистики зарегистрирует время вашего посещения и оба **IP-адреса** в таком порядке: шлюз/локальный адрес.

IP-адрес опасен

Сам по себе **IP-адрес** не представляет никакой опасности в сети. Но если злоумышленник захочет проникнуть именно в ваш ПК, то знание вашего статического **IP-адреса** открывает ему двери к вашему жесткому диску, общим ресурсам и ресурсам локальной сети.

Ваш компьютер имеет множество портов, через которые осуществляется работа с локальными и сетевыми дисками, подключение к Интернету и ftp-серверам и так далее. Так или иначе, **IP-адрес** связан со всеми этими портами, поскольку фактически он является проводником. Например, вам отправляется файл по локальной сети. Фактически он предназначается машине с вашим **IP-адресом**. Многие порты компьютера по умолчанию не защищены от атак вредоносных программ (вирусов, троянских коней и подобных), поэтому злоумыш-

ленники или вредоносные программы, зная ваш **IP-адрес**, могут не только нарушить работу компьютера, но и полностью перехватить управление машиной.

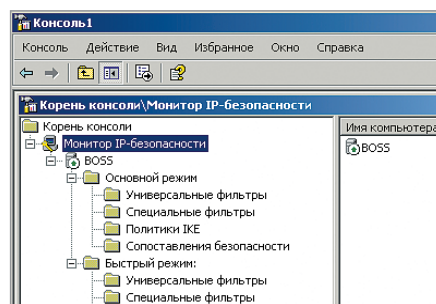
Как защитить IP-адрес?

Прокси-сервер

Самый простой способ защитить **IP-адрес** — использовать **прокси-сервер** для подключения к Интернету. **Прокси-сервер** обеспечивает так называемое сокрытие **IP-адреса** и препятствует внешним атакам на ваш компьютер. Узнать адрес своего прокси-сервера можно у провайдера, через которого осуществляется подключение к Интернету. Настроить браузер для работы через прокси-сервер можно с помощью меню **Свойства обозревателя → Подключение → Настройка**, где необходимо поставить галочку напротив пункта **Использование прокси-сервера**. При подключении вам нужно будет ввести адрес и порт прокси-сервера, который вы желаете использовать, например, **проху.имя_сервера.ru** (адрес вашего прокси-сервера) и порт 3128 (стандартный) для соединения с ним.

Управление политикой безопасности IP

В Windows XP встроены мощные средства обеспечения безопасности компьютера, например, в ОС есть функция **Управление политикой безопасности IP-адреса**. Для включения политики вам будет необходимо войти в систему через учетную запись **Администратор**. Управление политикой безопасности **IP-адресов** основано на протоколе **IPSec (Internet Protocol Security)** — «протокол интернет-безопасности». Он позволяет определить и блокировать как внутренние, так и внешние атаки на ваш ПК. Чтобы включить и настроить консоль **Управление политикой безопасности IP**, выполните следующие действия:



↑ Консоль управления IP-безопасностью

1. Нажмите на кнопку **Пуск** и выберите команду **Выполнить**.
2. В поле **Открыть** введите **mmc** и нажмите на кнопку **ОК**.
3. В меню **Консоль** выберите команду **Добавить или удалить оснастку**.
4. Нажмите на кнопку **Добавить**, а затем дважды щелкните **Управление политикой безопасности IP**.

После этого система будет автоматически отслеживать попытки атак на ваш компьютер через **IP-адрес** на основании специального алгоритма, позволяющего распознать вредоносные программы и хакерские атаки и вести журнал безопасности.

Леонид Николаев

ДОПОЛНИТЕЛЬНЫЕ СРЕДСТВА

a-squared (a_)

Версия ▶ 3.85

Разработчик ▶ Emsi Software GmbH

Сайт ▶ www.emsisoft.com

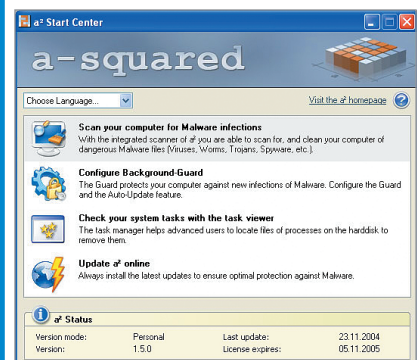
ОС ▶ Windows

Объем дистрибутива ▶ 3,26 Мбайт

Условия распространения ▶ shareware

Цена ▶ \$29,95

a-squared (a_) — одна из многочисленных разработок, предназначенных для защиты **IP-адреса** вашего компьютера от атак хакеров или вредоносных программ. Ранее она носила название



↑ Основное окно a-squared (a_)

Anti-Trojan. Программа поставляется в двух видах: **Free** — бесплатный сканер троянов; **Personal** — обеспечивает защиту от вредоносных программ в режиме реального времени. К особенностям **a-squared** следует отнести огромную пополняемую базу известных вредоносных программ, возможность производить сканирование не только жестких дисков, но и реестра на предмет наличия троянов в системе, а также сканирование всех портов компьютера.