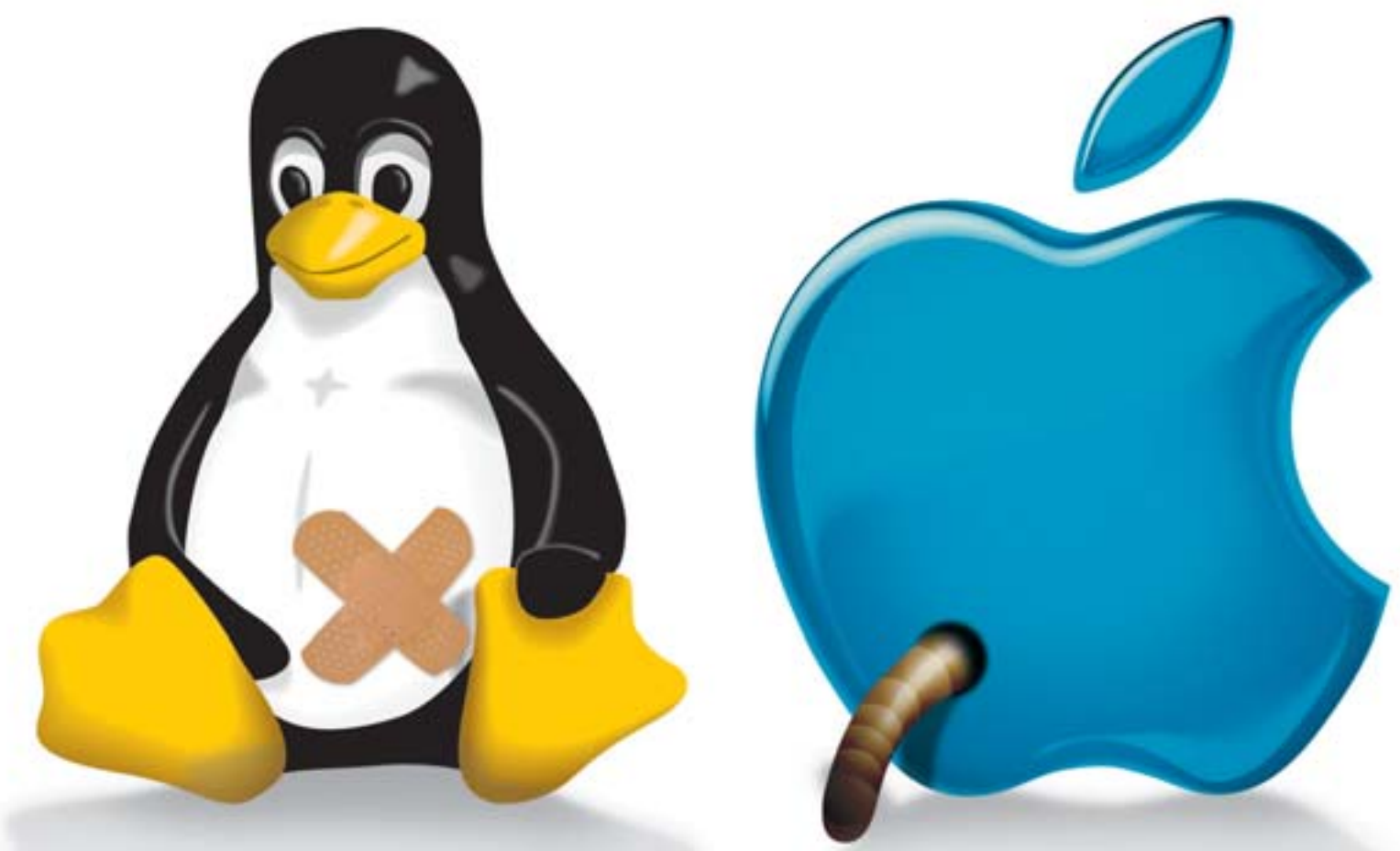
Тест защищенности ОС

# Linux, Mac OS

Действительно ли Mac OS и Linux безопаснее, чем Windows? CHIP проверил, насколько надежны эти операционные системы, и теперь готов рассказать своим читателям, как можно ликвидировать обнаруженные недостатки и бреши в защите.



# или Windows?

**Какая ОС защитит ваш компьютер лучше всего?**

Каждый раз, когда кто-то задает вопрос о самой безопасной операционной системе (неважно, какой именно), ответ вызывает просто шквал негодования. Так было и совсем недавно в случае с независимой компанией, регулярно проводящей исследования в сфере новых технологий, Forrester Research (www.forrester.com). На протяжении целого года аналитики сравнивали, какие бреши встречаются в безопасности ОС Windows и различных дистрибутивов Linux и насколько они в самом деле серьезны. Результат таков: согласно исследованию Forrester, только операционная система Microsoft оказалась способной закрыть все обнаруженные бреши, и к тому же быстрее всех! Разработчики различных производных Linux, таких как SuSE, Red Hat, Mandrake и Debian, справились с поставленной задачей «всего лишь» на 99%, причем реагируя не так оперативно. Едва только в марте 2004 года проведенное исследование было опубликовано, как тут же вызвало град критических высказываний со стороны дистрибьюторов Linux и ее приверженцев, которые ставили под сомнение практическую пользу методики Forrester.

Так что мы осознаем, на какой риск идем, но, тем не менее, отважимся провести сравнительное тестирование. Для нашего испытания мы выбрали по одному представителю каждого из трех миров: Windows XP Pro, SuSE Linux (наиболее простой, понятный и дружелюбный дистрибутив для начинающих Linux-пользователей) версии 9.1 Pro и Mac OS X версии 10.3.3 Panther. Все три системы проходили одни и те же стадии проверки. »


### Шаг 1: интернет-безопасность

Каждая операционная система сначала устанавливалась в так называемом режиме «out-of-the-box», то есть без патчей, и подвергалась онлайн-проверке профессионалов по безопасности Qualys. Эта проверка на прочность «простукивает» всю систему на предмет известных сбоев в безопасности — на тот момент их было около 3,5 тысяч — и структурирует их по пяти степеням опасности. Чем выше соответствующая степень, тем весомее пробел в системе безопасности.

В завершение мы задействовали все имеющиеся на момент тестирования сервисные пакеты, патчи и обновления. Если межсетевой экран не был включен автоматически, мы активировали его вручную. После этого еще раз прогоняли все три системы через то же самое горнило тестирования. Все результаты проверки, а также детальное описание теста вы найдете в итоговой таблице.

В каждой из трех операционных систем, которые мы рассматривали, был свой собственный браузер — их конфигурации, равно как и технологии, на которых основывается работа систем, различались довольно существенно. К примеру, браузер, поставляемый с ОС Linux, вообще не распознает такие языки программирования, как ActiveX или VBS. Поэтому браузеры, особенно уязвимые при работе в Интернете, мы отдельно посылали на детальную проверку специалистов из Scanit (http://bcheck.scanit.be/bcheck).

### Шаг 2: заштопываем все бреши вручную

Если даже, несмотря на патчи и обновления, бреши в безопасности браузера или ОС в целом остаются, мы закроем их самостоятельно — пока для этого будет достаточно имеющихся инструментов. В случае, если этого будет не хватать (к примеру, при защите от вирусов), мы расскажем, какие специальные утилиты следует использовать.

### Шаг 3: безопасность компьютера

Не всякая опасность приходит из Интернета. Иногда шпион находится совсем близко, в вашем же офисе. В этой связи мы тщательно рассмотрели стратегии безопасности трех операционных систем на уровне локальной сети. Насколько легко можно получить чужие регистрационные пароли и в какой степени они защищены шифрованием? Большую роль играет также распределение прав доступа и управление работой пользователей: какими возможностями обладают сетевые администраторы, чтобы, к примеру, сделать доступными отдельные секторы жесткого диска только для определенных групп пользователей? Безопасной работе с данными способствуют и ориентированные на пользователя функции резервного копирования реестра и системных файлов.

## Windows XP

С этой операционной системой Microsoft уж точно легко не приходится, ведь ежедневно в Сети появляются все новые сообщения о пробелах в системе безопасности Windows. Что из предрассудков о ненадежности этой ОС правда, а что нет, мы расскажем ниже. Кроме того, вы узнаете, как можно залатать найденные в системе дыры.

Логично, что самая распространенная система привлекает больше всего хакеров и тех, кто создает вирусы.

## Интернет-безопасность

«Out-of-the-box» корпорации Microsoft выглядит далеко не привлекательно. Проверка Qualys выявила более 25 пробелов в системе безопасности, что существенно хуже, чем у SuSE Linux и Mac OS X, причем пять из них относятся к самой опасной категории. Устранение этих недостатков возможно провести путем инсталляции новейших патчей и Service Pack 2. После их установки Windows XP в том же тестировании завоевывает совершенно незапятнанную репутацию.

### Инсталляция обновлений системы безопасности

Совсем необязательно каждый день заново искать обновления: специалисты из Редмонда вывешивают их в Интернете комплексно во второй вторник каждого месяца. С этого сайта (http://win-


С установкой Service Pack 2 межсетевой экран операционной системы Windows XP активируется автоматически


» dowsupdate.microsoft.com) вы можете скачать их либо вручную, либо используя встроенный в Windows XP модуль обновлений. Вы даже можете настроить модуль таким образом, чтобы ОС сама загружала и инсталлировала обновления.

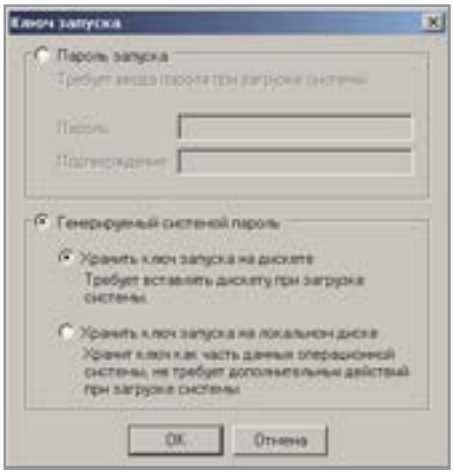
### Активация встроенного межсетевого экрана

Только начиная с Service Pack 2 межсетевой экран включается автоматически и защищает все важные сетевые соединения и передачу данных на удаленный узел. Система полностью блокирует все ICMP-пакеты, к примеру известную даже «чайникам» команду «Ping». Благодаря этому вы можете передвигаться по Интернету практически незамеченным: все запросы потенциальных атак на ваш компьютер XP препровождает в информационную «нирвану». Причем здесь не требуется никаких особых настроек, изначально задана оптимальная конфигурация. А в случае, если той или иной программе — к примеру, электронному биржевому брокеру — потребуется порт, Windows автоматически выдаст запрос, следует ли его открыть.

### Инсталляция дополнительной защиты от вирусов

Создатели вирусов уже пристрелялись к Windows: по данным известного разработчика антивирусных программ Sophos (www.sophos.com), в 2003 году было больше вирусов и червей, чем когда-либо ранее — явственно просматривается тенденция к нарастанию этого вала. Так как обычно авторы вирусов стремятся инфицировать как можно большее количество компьютеров, Windows является для них отличной мишенью, ведь ее доля рынка в области домашних компьютеров составляет более 90%.

Защиту от нарастающей опасности Windows XP сама по себе не может предложить, это становится задачей специальных программ, в данном случае — антивирусов. Неоценимыми помощниками в обнаружении так называемых вирусов in-the-wild служат прежде всего две программы. Коммерческий пакет AntiVirenKit 2003 Professional компании G Data (www.gdata.de/gdc/start) найдет любой вирус благодаря двум сканирующим движкам. Единственный его недостаток заключается в том, что за такую эффективную защиту приходится дорого платить: программа неимоверно требовательна к производительности системы. Гораздо быстрее действует бесплатная утилита AntiVir Personal Edition (www.free-av.com). Ее недостатком является то обстоятельство, что в области «зоовирусов» (вирусы, спрограммированные специально для исследовательских целей) она значительно отстает от AntiVirenKit производства G Data.




▲ Шифрованная файловая система (EFS) обезопасит вход в Windows XP Professional

Если вы хотите стопроцентной надежности, лучше всего установить к тому же и программу от PivX. Утилита Qwik-Fix (www.pivx.com) идет другим путем: она защитит ваш компьютер еще раньше, чем разработчик выдаст патч. Программа заранее устраняет пробелы в системе безопасности. К примеру, блокирует атакованные порты.

### Обезопасить браузер

В качестве браузера Windows XP предлагает Internet Explorer 6. Мы проводили тест браузера Browser security test компании Scanit (www.scanit.net). Как и в случае с проверкой Qualys, выяснилось, что абсолютно необходимо в обязательном порядке инсталлировать все обновле- »

**Глоссарий**

## Опасные службы

Многие проколы в безопасности касаются различных служб и протоколов. Ниже — самые важные из них.

- **ICMP:** протокол Internet Control Message Protocol транспортирует сообщения об ошибках для сетевых протоколов IP, UDP и TCP. Самое известное сообщение ICMP — команда «Ping». Разнообразие ICMP-сообщений (их около 20) позволяет атакующим собрать информацию о системе путем отправления соответствующих ICMP-пакетов.
- **RPC:** протокол Remote Procedure Call Protocol запускает функции на других компьютерах, к примеру, при Remote Computing.
- **UDP:** протокол Users Datagram Protocol является, как и TCP, протоколом коммуникации между компьютерами. Равно как и TCP, UDP действует через Internet Protocol (IP).
- **TCP/IP:** интернет-протокол (IP) фрагментирует и адресует данные и передает их. Протокол Transmission Control Protocol (TCP) его дополняет и заботится о сортировке пакетов в правильной последовательности, а также обеспечивает коммуникацию без помех.


ния. Только после того как с их помощью были закрыты все бреши, тест больше не указывал на точки потенциальных атак.

Чтобы быть готовым отразить потенциальные нападения в будущем, лучше всего деактивировать ActiveX, Java и JavaScript и включать их только по необходимости. Для этого откройте Internet Explorer и в меню «Tools» щелкните на «Internet Options». В появившемся окне выберите вкладку «Security» и нажмите на «Custom Level». Затем активируйте перед пунктом «Run ActiveX controls and plug-ins» опцию «Prompt». С этого момента Windows XP будет запрашивать в случае с каждым элементом ActiveX, должен ли Internet Explorer выполнить команду. Это же относится и к Java, нужно только в том же окне установить соответствующие настройки на «High safety».

## Безопасность компьютера

В Windows XP каждый пользователь может работать в отдельном профиле. Можно выбрать один из двух вариантов: или полные права доступа и свободное распоряжение операционной системой, или ограниченный доступ. Пользователи «второй категории» будут, таким образом, управлять в какой-то степени вашей ОС, но не смогут устанавливать программное обеспечение или изменять системные настройки. Однако на практике в распределении прав управления и доступа к паролям часто обнаруживаются лазейки.


▲ Тест браузеров мы проводили с помощью Browser Security Test компании Scanit

### Обезопасить профили пользователей

Вы можете еще перед запуском XP назначить запрос пароля BIOS. Тогда только те пользователи, которые знают пароль, смогут начать работу за компьютером. Конечно, это можно отменить, если снять батарею материнской платы, но при нормальных обстоятельствах у вас будет неплохая базовая защита.

Пароли входа в профили пользователей XP сохраняет как хеш-значения. Если вы вводите пароль, Windows его пересчитывает и сравнивает подсчитанное и сохраненное значения. Если они совпадают, вы получаете доступ к системе. Windows хранит эти значения в файле SAM, который находится в каталоге c:\windows\system32\config. Но это не так безопасно, как может показаться: нападающие, у которых есть локальный доступ к системе, могут всего лишь с помощью пары простых утилит из Интернета заменить хранимые хеш-значения своими собственными и причислить себя к пользователям.

Предотвратить подобные случаи поможет считающаяся вполне надежной система EFS (Encrypting File System), с помощью которой вы можете зашифровать файловую систему так, чтобы только «уполномоченные» пользователи могли ознакомиться с содержимым жесткого диска. Активируйте функцию


▲ Сделайте двойной клик на «nolmhash» и в пункт «Значение» вставьте цифру 1

«Пуск → Выполнить → syskey» и нажмите на кнопку «Enter». В последующем диалоговом окне выберите пункт «Обновить». После этого вы увидите список предлагаемых опций. Самый надежный и безопасный путь: пусть система сама сгенерирует пароль, который вам нужно будет затем сохранить на дискете. При каждом включении компьютера просто вставьте дискету в дисковод.

При управлении работой пользователей существует еще одна лазейка: если пользователь поменяет свой пароль, Windows сохранит его в двух хеш-значениях. Оба значения система XP опять-таки поместит в файл SAM. Второе значение носит имя файла LMHash (LAN Manager Hash) — это пережиток из времен Windows 3.1, который создается только из соображений совместимости. Хакерам такая ситуация дает все карты в руки: ведь LMHash распознает только заглавные буквы, следовательно, число возможных комбинаций знаков пароля резко сокращается. Следует дезактивировать второе хеш-значение. Для этого в меню «Пуск» выберите «Выполнить», наберите «regedit» и нажмите «OK». Перейдите к ключу «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa». В правой части сделайте двойной клик на «nolmhash» и в пункте «Значение» установите цифру 1.

# Windows XP

▲ С этого сайта вы можете скачать обновления для Windows XP вручную

### » Шифрование каталогов

Если вы используете XP Professional, можете зашифровать папки NTFS. Для этого нажмите правой кнопкой мыши на нужную папку и выберите пункт «Свойства». Под заголовком «Другие» активируйте опцию «Шифровать содержимое, чтобы защитить данные». Теперь информация будет защищена — хакеру целой жизни будет мало, чтобы взломать код.

Шифрование использует не пароль, а надежный сертификат, который должен быть установлен на вашем компьютере; именно он служит ключом. Только обладая им, хакер может получить доступ к вашим данным. Поэтому мы рекомендуем экспортировать сертификат и стереть его с жесткого диска. Действуйте следующим образом: в меню «Пуск» выберите пункт «Настройка», затем «Панель управления» и дважды щелкните на «Опции Интернета». На вкладке «Содержимое» выберите «Сертификаты». Нажмите на «Экспортировать» и выберите «Далее». Появится пункт «Да, экспортировать личный ключ», который вам нужно будет активировать. Следующее окно можете пропустить, нажав «Далее». Теперь введите пароль. В качестве места сохранения ключа вначале используйте жесткий диск. Подтвердите последующие сообщения. Затем вы снова обнаружите перечень сертификатов. Выберите «Удалить» и подтвердите запрос безопасности нажатием на «Да». Переместите экспортированный ключ с жесткого диска на какой-либо внешний носитель данных, к примеру на дискету или Memory Stick. Когда вы захотите воспользоваться зашифрованными файлами, импортируйте ключ с носителя.

Не забывайте после каждого сеанса Windows удалять сертификат с жесткого диска, так как Windows на нем каждый раз заново сохраняет ключ доступа.

## Итог: безопасность только при установленных обновлениях

Результат нашего теста оказался неожиданным: Windows не такая уж ненадежная операционная система. Если вы регулярно скачиваете обновления системы, не забываете про резервное копирование и шифруете файловую систему, можете не опасаться за безопасность XP.

Qualys

## Профессиональная проверка

Чтобы протестировать безопасность системы, CHIP вместе с экспертами американской компании Qualys провел обширную онлайн-проверку. Qualys является одним из мировых лидеров в сфере безопасности («Best Security Service 2004», SC Magazine Global Award); эта компания делает почти миллион анализов безопасности в квартал. В число ее корпоративных клиентов входит и американское правительство. Для частных клиентов Qualys предлагает бесплатное тестирование (**http://freescan.qualys.com**), которое позволяет выявить десять самых важных брешей в безопасности системы. Профессиональные проверки предназначены только для предприятий, их стоимость исчисляется пятизначными числами.

В использованной нами версии «для корпораций» тестирующая программа, разработанная Qualys, сканирует компьютер на предмет более 3500 известных и наиболее существенных брешей в безопасности системы.

При этом проверка проходит очень точно, доля ошибок составляет менее 0,003%. Программа тестирует все важные характеристики надежности компьютера в сфере интернет- и онлайн-безопасности. Выявленные пробелы структурируются по пяти категориям: первая степень обозначает наименьшую опасность, пятая степень предупреждает о наличии крайне опасных брешей в системе. Дальнейшая информация: ▸ **www.qualys.com.**


▲ Онлайн-проверка: Qualys выслеживает пробои в безопасности системы

# SuSE Linux

Пользователи Linux полагаются на безопасность этой системы, потому что ни вирусы, ни черви не представляют для них угрозы. Но действительно ли эта операционная система так надежна, или, может быть, просто не нашлось пока еще вредителей, которые внесли бы сумятицу в ее работу?

Образцово-показательным в Linux является разделение на пользователей без каких бы то ни было прав доступа и на администраторов — прямое наследие Unix. Как следствие, вирусы и черви могут в худшем случае посягнуть на ограниченные права только определенного пользователя, и «заражение» не выйдет за эти пределы.

## Интернет-безопасность

Уже в «голой» SuSE Linux онлайн-проверка Qualys выявила значительно меньше брешей, чем в Windows; к тому же большинство из найденных были отнесены к самой низкой степени опасности. Удивительно, что обновления никак не изменили эту статистику — только после того как мы вручную активировали встроенный брандмауэр, исчезли еще десять дыр. И все же пять пробелов, которые были причислены к самой низкой степени опасности, остались.

### Установка обновлений системы безопасности

Как и в случаях с Windows XP и Mac OS, обновления можно установить через Интернет. Правда, есть одна загвоздка: после установки автоматические обновления деактивируются, администратор должен их сначала включить. Эту настройку можно изменить: запустите Yast и активируйте в модуле «Программное обеспечение» опцию «Онлайн-обновление». В следующем окне выберите пункт «Конфигурация полностью автоматического обновления» и поставьте галочку напротив «Активировать автоматическое обновление».

### Включение и настройка брандмауэра

Так как брандмауэр SuSE не включается автоматически, первым делом следует заняться именно им. В менеджере конфигурации Yast вызовите пункт «Безопасность и пользователи». Нажмите на «Брандмауэр» и выберите сетевой интерфейс, который вы хотите защитить.

Тому, кто эксплуатирует сервер, нужно еще подумать и о том, чтобы фильтровать запросы пингования. Для этого надо отредактировать файл конфигурации SuSEFirewall2 в каталоге /etc/sysconfig. Как пользователь «Root» откройте этот файл в каком-либо редакторе и установите значение переменной «FW_ALLOW_PING_FW» на «no». Тем самым вы запретите брандмауэру отвечать на запросы пингования.

### Конфигурация браузера

Стандартная установка SuSE использует в качестве браузера Konqueror, который также может служить файловым менеджером и FTP-клиентом.

Тестирование браузера не выявило ни одной бреши в его безопасности. Проверка на Cross-Site-Scripting (межсайтовый скриптинг, сокращенно — XSS) была прервана сообщением об ошибке.

Java и JavaScript автоматически включены. Если вы можете без них обойтись, лучше всего отключить эти скрипты. Для этого перейдите в меню «Настройки → Konqueror → Java & JavaScript» и снимите галочки напротив «Полностью удалять Java» и «Полностью удалять JavaScript». Этот KDE-браузер не владеет небезопасными технологиями

▲ Надежность: в настройках браузера Konqueror можно удобно настроить работу Java и JavaScript

Microsoft ActiveX и VisualBasicScript. Наш совет: замените стандартный браузер на Mozilla Firefox — он такой же надежный, но значительно более удобный.

### Включение защиты от вирусов

Вредители в среде Linux — не самая большая головная боль. Евгений Касперский, эксперт в области компьютерной безопасности, уверен, что это обусловлено только ограниченным использованием ОС Linux. Однако факт остается фактом: на данный момент опасных червей под Linux не существует.

В стандартной установке нет сканера антивируса, однако в отличие от Windows здесь он, по крайней мере, присутствует в комплектации: на системных CD и DVD SuSE вы найдете AntiVir от H+BEDV. После его установки занесите в Root-Shell команду «antivir-update».

## Безопасность компьютера

При установке SuSE необходимо кроме профиля «Root» создать еще и как минимум один пользовательский. Если вы захотите войти в графический интерфейс как администратор, экран в знак предупреждения станет ярко-красным, и на »

# SuSE Linux

» нем появится изображение взрывающихся бомб. На правах администратора вы можете изменить в Linux практически все. SuSE четко проводит линию между профилями пользователей и профилем «Root», и если пользователь попытается внести в системные настройки какие-либо изменения, появившееся окно тут же запросит пароль «Root».

### Зашифровать пароли

Безопасность паролей в среде Linux заслуживает похвал: они кодируются с помощью алгоритма безопасности и сохраняются в файле /etc/shadows, который доступен только пользователю «Root». В дистрибутиве SuSE также есть возможность шифрования паролей: откройте модуль Yast «Безопасность и пользователи» и перейдите к подменю «Настройки безопасности». Для компьютера с одним пользователем при наличии доступа в Интернет подходит степень безопасности «Level 1». Выделите соответствующий пункт и нажмите «Завершить».

### Закодировать файловую систему

Шифрование — одна из функций SuSE. Уже при установке целые разделы системы можно снарядить шифрованной файловой системой.

Внимание: если вы хотите использовать шифрованную файловую систему, вам понадобится отдельно включить эту функцию сразу же при установке ОС, так как шифрование задним числом будет воспринято как форматирование файлов заново и приведет к полной потере данных.


▲ Выключите автоматический вход в систему и регистрируйтесь самостоятельно

Файлы и каталоги вы можете закодировать под KDE с «KGpg» (аналог PGP из Windows). В контекстном меню Konqueror выберите под заголовком «Действия» пункт «Упаковать и зашифровать папки». Если вы еще не создали пару ключей, программа автоматически подскажет, что это нужно сделать. Если вы раньше уже создавали работающие ключи, можете выбрать их через управление ключами «KGpg». Для декодирования нужно будет просто ввести пароль, который вы определили при создании ключа.

### Провести резервное копирование

Функции для резервного копирования и восстановления системы вы найдете в Yast под заголовком «Система». Мастер резервного копирования выборочно сохраняет системные файлы локально на жестком диске или на NFS-сервере. При восстановлении вам нужно только выбрать файл с сохраненными данными, все остальное система берет на себя.

К сожалению, в Yast вы не сможете подстроить автоматическое резервное копирование под свои нужды. Если вы захотите сохранять систему через регулярные промежутки, нужно будет создать Cron-Job — процесс, который система запускает автоматически и который, к примеру, может определять ежедневные или еженедельные задачи. Если вам нужно, чтобы какая-либо задача выполнялась ежедневно, оставьте в каталоге /etc/cron.daily Shell-Script. Он будет автоматически запускаться каждый день. Когда именно это будет происходить, указано в файле /etc/crontab.


▲ Взлому не подлежит: Linux может обезопасить файловую систему с помощью DSA-алгоритма

### Итог: безопасность с помощью нескольких приемов

Самая главная дилемма Linux: эта ОС должна быть достаточно простой и в то же время надежной. В дистрибутиве SuSE стремление к комфорту пользователей иногда заходит слишком далеко, и стандартная установка не всегда соответствует идеальным представлениям о безопасности. Из-за автоматического входа или предустановок службы SSH возникает вероятность потенциальных атак на в остальном надежную систему. То же самое относится и к выключенному брандмауэру. В случае с обновлениями, напротив, недостает комфорта, автоматическое обновление нужно сначала активировать. Одно из преимуществ SuSE — то, что на поставляемых дисках есть все необходимые программы для безопасной работы системы. Эпидемия червей для Linux и вовсе не проблема, она просто не может возникнуть из-за образцового разделения между администратором и обычными пользователями.

# Mac OS X

**Пользователи Apple абсолютно уверены: Mac OS X — безопасная операционная система. И это подтвердится, если посмотреть на результаты нашего тестирования. Но в самый последний момент пришло известие, что пользователям Mac необходимо как можно скорее установить «заплатки».**

В основе Mac OS X лежит Darwin, измененная Unix. До сих пор она считалась надежной, но с введением Panther и новым ядром ситуация может измениться. Вирусы для Mac вряд ли станут головной болью — доля рынка примерно в пять процентов не так уж сильно привлекает хакеров к Mac OS. На данный момент известно всего 30 вирусов, которые могут атаковать платформы ниже версии 9.2.2.

## Интернет-безопасность

Приверженцы Mac могут радоваться: даже при установке системы без «заплаток» наш тест выявил всего несколько брешей, причем все они относились к самой низкой степени опасности. После настройки брандмауэра открытыми остались только две безвредные дыры.

### Настройка брандмауэра

Брандмауэр включается автоматически; отчасти именно этим можно объяснить столь успешное прохождение первого теста. К сожалению, в меню «Firewall» вряд ли можно внести изменения в настройки: предварительные установки нельзя отладить, как и нельзя ограничить службы на определенном компьютере или в сети собственными правилами. Кроме того, все UDP-порты остаются открытыми для внешнего мира. Жаль, особенно учитывая, что в Mac OS X уже имеется пакетный фильтр BSD с ipfw для TCP, UDP, ICMP и IGMP. Очевидно, Apple решила предложить только брандмауэр с простой конфигурацией, который при старте таких служб, как Apple File Sharing или Windows Sharing, обеспечивает автоматический доступ.

Чтобы настроить ipfw, вам понадобится утилита BrickHouse (http://personal-pages.tds.net/~brian_hill/brickhouse.html). С ее помощью вы закроете четыре из шести обнаруженных Qualys брешей в безопасности системы.

Щелкните на «замочек», чтобы вас идентифицировали как администратора. Определите ваш тип интернет-соединения (Ethernet, DSL-модем, обычный модем), а также обозначьте способ, как вы получаете IP-адрес (как правило, это бывает адрес, динамически выделяемый провайдером). Следующее окно можно пропустить, по завершении процедуры нажмите на «OK».

Теперь вы можете активировать брандмауэр и добавить какие-либо правила, к примеру, закрыть оба еще открытых порта 514 и 1434. Для этого нажмите на «Add Filter» и добавьте «Deny» для входящего соединения UDP-порт 514. То же самое относится и к порту 1434. Чтобы защитить систему от запросов «Ping» и «Traceroute», нужно соответствующим образом настроить правила. Щелкните на «Advanced» и деактивируйте опции «Allow All ICMP Traffic» и «Allow FTP Data Port». Снять галочку надо и напротив надписи «Allow Network Time». Но при этом следует иметь в виду, что настройки в области ICMP в зависимости от провайдера могут вызвать проблемы при подключении. Чтобы определить настройки, щелкните на «Apply», затем на «Install» и «Save».

### Безопасность браузера

Вместе с OS X компания Apple поставляет браузер Safari. Apple принципиально


▲ **Совсем просто: как и в случае с конкурирующими ОС, в продукте Apple вы можете задействовать автоматическое обновление**

делает ставку на выключение всех опасных служб и разрешает их использование только тогда, когда пользователь в явном виде подтверждает их активацию. Так как ActiveX в среде Mac OS в любом случае не функционирует, в Safari нужно будет отключить только Java и JavaScript. В тестировании браузеров мы подвергли онлайн-проверке Safari со стандартными настройками. Результат — ни одной бреши! А вот после мая 2004 года обнаружились весомые пробелы в безопасной работе программы.

### Настроить защиту от вирусов

Есть ли у OS X иммунитет против вирусов, червей и троянских коней? Пока еще да. Но 8 апреля 2004 года работающая в сфере безопасности компания Intego обратила внимание общественности на то, что один программист разработал для тестовых целей троянца MP3Concept. При работе с iTunes инфицированный файл не причинит никакого вреда. Но если открыть его через Finder, вирус начнет фиктивную атаку.

Одни только макровирусы дают повод для беспокойства: они могут причинить »


» вред при работе с Office:mac, так что следует включить защиту от макросов в редакторе Word и тому подобных. На всякий случай в качестве антивируса подойдет VirusBarrier от Intego. Подробнее см. www.intego.com/virusbarrier.

## Безопасность компьютера

Пренебречь локальными регистрационными паролями в среде OS X, к сожалению, еще легче, чем в Windows XP: достаточно вставить в дисковод установочный диск, включить компьютер и удерживать нажатой клавишу «C». Этого вполне достаточно, чтобы злоумышленник мог получить полный доступ, не вводя пароли.

### Назначить Firmware-пароль

Именно из этих соображений вам потребуется установить Firmware-пароль (практически BIOS-пароль). Для этого нужно только, чтобы у вас была установлена одна из последних версий Firmware (4.1.7. и выше). Чтобы это проверить, щелкните в меню «Apple» на пункт «Через этот компьютер», затем «Дальнейшая информация» и выберите пункт «System-Profiler». В списке аппаратного обеспечения под пунктом «Boot-ROM-Version» указана версия Firmware. Теперь вставьте в привод первый диск и зайдите в каталог «Applications/Utilities». Запустите утилиту Open Firmware Password и нажмите на «Modify». После аутентификации вашего пароля администратора активируйте опцию «Требовать пароль» и введите Firmware-пароль.

### Использовать безопасные пароли

Mac OS X 10.2 и более ранних версий сохранял локальные пароли в службе каталогов Netinfo. Там их можно было достаточно легко взломать. Начиная с версии 10.3 OS X сохраняет пароли исключительно как «Shadow-Passwords», то есть они графически отображаются в виде звездочек. Так что прочитать их с помощью команды «nidump passwd.» уже невозможно. В версии 10.3 разрешены пароли длиной более чем в восемь знаков. Системы, которые представляют собой свежую версию, сделанную с помощью «заплаток» на основе 10.2, еще могут содержать старые хешированные пароли. Это можно проверить через команду «nidump passwd.». Если вы найдете хешированные записи, можете поменять все пароли в системной настройке «User».


▲ Утилита из дистрибутива OS X позволяет форматировать диск и разбивать его на части — партиции


▲ Предустановленный брандмауэр входит в набор стандартных программ для Mac OS

### Безопасная работа пользователей

OS X делит права доступа на три категории: «Standard-User», «Administrator» и «Root». Обычных пользователей можно «снабдить» индивидуальными ограничениями, чтобы они не смогли читать или удалять каталоги других пользователей. Администратору не разрешается стирать системные файлы, это привилегия пользователя «Root». Тем самым управление работой пользователей как минимум такое же безопасное, как и в среде Linux. Первый профиль пользователя, который вы регистрируете при установке, автоматически считается профилем администратора. Управление работой осуществляется централизованно через системную настройку «User». Если символ «замочка» закрыт, войдите в систему как администратор. Чтобы локальный злоумышленник даже не мог увидеть, какие профили пользователей существуют в системе, на всякий случай отключите автоматическую регистрацию: для этого щелкните на «Login-Options», деактивируйте автоматический вход и измените диалог регистрации на «Логин и пароль». Опции «Lazy», «Restart» и «Shut down» также лучше отключить. Это сделает невозможной ситуацию, при которой, для того чтобы уклониться от регистрации, достаточно будет перезагрузить компьютер. Дальнейшие настройки нужно будет задать в меню «System Settings → Security»: включите защиту паролем для заставки экрана и запрос авторизации администратора для всех системных настроек, а также определите автоматический выход из системы при ее простое.

### Зашифровать файлы и папки

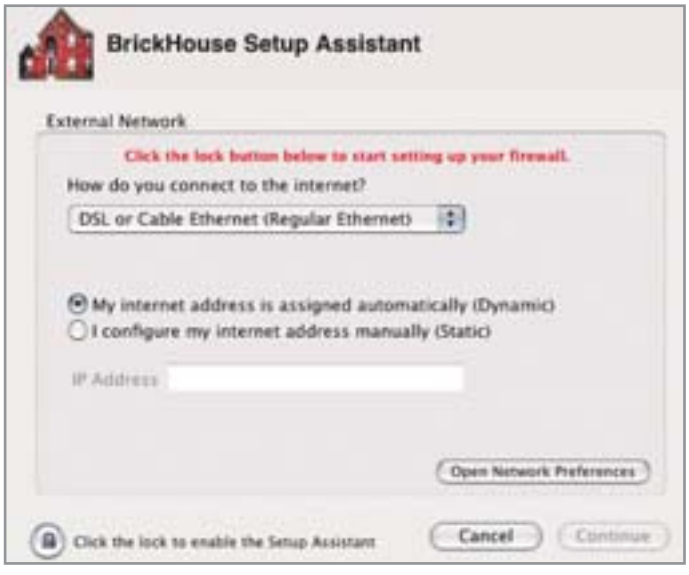
Для шифрования файлов в распоряжении OS X есть такое средство как OpenSSL. Для того чтобы работа протекала легко, воспользуйтесь специальной утилитой PuzzlePalace (http://personalpages.tds.net/~brian_hill/puzzlepalace.html). С ее помощью вы сможете настроить такие счита- »

» ющиеся надежными алгоритмы шифрования, как Blowfish Cipher, Triple DES, DEA, CAST или RC5. Выберите какой-либо метод, перетащите нужный файл в открытое окно программы и назначьте пароль.

Для наших мобильных современников оптимальным выбором будет «File Vault» в меню «System Settings → Security». Значок сейфа указывает на 128-битное шифрование каталога. При входе в систему «уполномоченного» пользователя зашифрованный домашний каталог откроется и будет в распоряжении пользователя в течение сеанса. Другие зарегистрированные пользователи не обладают правом доступа к этой области. Перед тем как приступить к работе с FileVault, нужно назначить главный пароль. Затем активируйте FileVault, и домашний каталог автоматически будет зашифрован.

### Создать автоматические резервные копии

В OS X нет утилиты, которая бы создавала резервные копии. Но вы можете спрограммировать Cron-Job, который будет выполнять данные команды. Для этого подходит программа CronX 2.1. Кликните на титульной планке в пункте «Новый». Выберите раздел «Простой/Стандартный» и задайте начало работы в графах «Минута», «Час» и «День недели». Запустите резервное копирование: «ditto-rsrc/Users/admin/Volumes/HD2/BU/admin». Тем самым home-каталог пользователя «admin» будет сохранен в раздел HD2 в каталоге BU. »




▲ Защита от проникновения: брандмауэр BrickHouse внесет свою лепту в безопасность вашей OS X

# Mac OS X

### » Зашифровать резервные копии

Служебная программа жесткого диска сохраняет все его содержимое — разделы, папки и файлы — в образ. Преимущество такого метода резервного копирования состоит в том, что образ можно зашифровать в 128-битном режиме. Запустите утилиту в меню «Programs/Service Programs». Выберите пункт «Images → New → Image of the Folder». С помощью файлового браузера выделите тот каталог, для которого вы хотите создать резервную копию, и нажмите «Open». Задайте имя каталога и определите место, где он должен быть сохранен. Теперь активируйте желаемый формат образа и собственно опцию шифрования. Нажмите «Save», и процесс резервного копирования в образ начнется. Двойным щелчком мыши образ можно монтировать в виртуальный дисковод.

**В последний момент**

## Новая брешь в OS X

После завершения нашего теста обнаружился один крайне значительный пробел в безопасности OS X, который помимо Safari затрагивает и все остальные браузеры, работающие в среде OS X. Через эту брешь нападающий на систему может, используя соответствующий URL, загрузить образ диска, который, к примеру, удаляет через скрипт весь домашний каталог — а пользователь этого даже не заметит. Apple подготовила «заплатку», но она на самом деле способна устранить не все проблемы. В безопасности вы окажетесь только с утилитой Paranoid Android. Эта бесплатная программа защитит ваш компьютер и от так называемого HelpViewer, который создает похожие проблемы. Подробнее см. ▸ **www.unsanity.com/haxies/pa**

### Итог: пока вполне безопасно

В «сыром виде» OS X вряд ли может подвергнуться нападению извне. Однако, что касается локальной сферы, эту систему можно брать голыми руками. Жаль, что Apple не слишком заботится, чтобы проинформировать своих пользователей о том, как можно защитить систему. Ведь большинство брешей в системе безопасности можно «заштопать» относительно легко и просто. Зато Apple поставляет новую Mac OS X Panther с весьма разумными опциями и с программным обеспечением Open Source. Если вы хотите еще больше обезопасить систему, задействуйте несколько freeware- или shareware-утилит.

## Общий результат

### Windows, Linux, Mac OS: какую ОС можно считать самой безопасной?

Вы также придерживаетесь мнения, что Windows крайне уязвима? Так думают многие — и, как выяснилось, ошибаются. Неожиданным результатом тестирования стало то, что ОС Windows показала себя очень хорошо. Конечно, для такой работы необходимо большое количество «заплаток» и новый Service Pack 2, что, в общем-то, делает результат довольно относительным. Ведь без них Windows демонстрирует наибольшее количество брешей. Однако после установки обновлений все они благополучно исчезают. Linux и Mac OS сами по себе менее уязвимы, но зато и обновления устраняют далеко не все дыры.

В чем заключается разница? Если речь идет о вирусах, червях и троянах, то с Windows XP ситуация обстоит хуже всего. Причина этого кроется в том, что с этой ОС не поставляется сканер-антивирус, а из-за распространенного использования она была и остается самой главной мишенью для хакеров.


▲ Утилита PuzzlePalace позволяет шифровать файлы «на лету»

Что касается локальной безопасности, Windows подкачала и здесь. Ведь в этой области конфигурацию практически нельзя изменить. Совсем другое дело с Mac OS и Linux: хотя в обеих ОС нужно вручную поработать с настройками, зато после этого они гораздо успешнее выдерживают атаки на локальном уровне. Дополнительную защиту обеспечивает шифрованная файловая система, однако ей может похвастаться только Linux.

Все три системы впечатляют работой с обновлениями. С их помощью ваша ОС всегда будет оборудована по последнему слову техники. В случае Windows это абсолютно необходимая мера, так как выходец из Редмонда остается основной целью всех хакеров. Но Apple тоже дает повод для беспокойства: обнаруженные бреши в безопасности «тяжеловесны», здесь безотлагательно бы понадобилась «заплатка». Между тем Apple и Microsoft (только с Service Pack 2) делают ставку на работающий по стандартным настройкам брандмауэр, а в среде SuSE Linux его надо активировать самостоятельно. CHIP

Qualys

# Результаты тестирования от Qualys-Guard

## Windows XP Prof.

### Стандартная установка

| Степень опасности | Количество брешей |
|---|---|
| высокая 5 | 4 |
| 4 | 1 |
| 3 | 5 |
| 2 | 4 |
| низкая 1 | 11 |

**Общий риск**

При первой проверке тест Qualys показывает, что Windows «out-of-the-box» открыта нараспашку, и это не вызывает особого доверия.

### Установка с обновлениями

| Степень опасности | Количество брешей |
|---|---|
| высокая 5 | 0 |
| 4 | 0 |
| 3 | 0 |
| 2 | 0 |
| низкая 1 | 0 |

**Общий риск**

Неожиданный итог: после установки патчей и обновлений Windows показывает блестящий результат — не осталось ни одной бреши.

## SuSE Linux 9.1 prof.

### Стандартная установка

| Степень опасности | Количество брешей |
|---|---|
| высокая 5 | 0 |
| 4 | 0 |
| 3 | 1 |
| 2 | 2 |
| низкая 1 | 12 |

**Общий риск**

Ситуация с SuSE Linux обстоит гораздо лучше, чем с Windows, и тем не менее значение риска слишком уж высокое для этой системы.

### Установка с обновлениями

| Степень опасности | Количество брешей |
|---|---|
| высокая 5 | 0 |
| 4 | 0 |
| 3 | 0 |
| 2 | 0 |
| низкая 1 | 5 |

**Общий риск**

После того как мы пустили в ход обновления и несколько раз щелкнули мышкой в системных настройках, SuSE Linux стала неуязвимой.

## Mac OS 10.3.3

### Стандартная установка

| Степень опасности | Количество брешей |
|---|---|
| высокая 5 | 0 |
| 4 | 0 |
| 3 | 0 |
| 2 | 0 |
| низкая 1 | 6 |

**Общий риск**

Apple не допускает компромиссов, и даже в «сыром» виде система почти на сто процентов безопасна — очень похвально.

### Установка с обновлениями

| Степень опасности | Количество брешей |
|---|---|
| высокая 5 | 0 |
| 4 | 0 |
| 3 | 0 |
| 2 | 0 |
| низкая 1 | 2 |

**Общий риск**

Установленные патчи оставляют ситуацию, в общем-то, такой же. Если устранить всего две бреши, Mac OS станет неподвластна атакам.

**Общий риск:** исходя из количества и значимости обнаруженных брешей Qualys рассчитывает показатель общего риска: от категории 0 до категории 5.

Тест Qualys обнаружил ни много ни мало 25 брешей в этой ОС, пять из которых относятся к самой высокой степени опасности. Общий риск компьютера с установленной на нем XP тем самым оценивается экспертами по безопасности как очень высокий (пять пунктов из пяти возможных).
Найденные Qualys пробелы — почти исключительно ошибки программирования в каких-либо службах Windows. К примеру, тест выявил брешь в безопасности Windows Messenger. Многочисленные дыры, вызванные печально известным переполнением буфера, продолжают черный список, составленный тестировавшей XP программой. Остальные пробелы, как и в случае с Linux, относятся к работе различных служб, которые выдают информацию о компьютере, например ICMP (Internet Control Message Protocol, см. глоссарий) — злоумышленник может, среди прочего, узнать, услугами какого провайдера вы пользуетесь.
Однако после установки обновлений и Service Pack 2 все потенциальные точки нападения, которых до этого было великое множество, были устранены.

Qualys выявил 15 брешей, хотя они и не такие опасные, как в Windows. Общий риск нападения на систему Qualys оценил как средний и поставил Linux 3 пункта. Недочеты относятся в основном к тем службам, которые видны во внешней среде. Целями атак они могут стать, только если в этих службах возникнут сбои.
Единственная брешь из третьей категории касается Secure Shell (SSH), основной задачей которого является обеспечение безопасного соединения. В версии OpenSSH есть баг, который открывает доступ хакерам в случае переполнения буфера. Две следующих бреши (степень опасности 2) относятся к RPC и ICMP-сообщениям. Злоумышленники могут воспользоваться Portmapper, который передает RPC-запросы системным службам.
Даже онлайн-обновление не исправило ситуацию. SuSE по-прежнему реагирует на запросы пингования: так можно выяснить, доступен ли компьютер. Можно проследить и путь пакетов данных. А через запрос «whois» на сайте www.ripe.net/perl/whois хакер может разузнать, клиентом какого провайдера вы являетесь.

После стандартной установки Mac OS X Qualys сообщил о наличии шести брешей самой низкой степени опасности.
Четыре пробела относятся к области добычи информации. Mac OS пропускает ICMP-запросы: к примеру, запрос «Ping» и ответ, что какие-либо порты закрыты. К тому же не представляет труда проследить путь пакета данных или получить информацию, используя «whois». В сфере TCP и UDP (см. глоссарий) Qualys нашел недостатки в двух открытых UDP-портах: 514 (syslog) и 1434 (ms-sql-m). Syslog обычно используется в сетевых устройствах (Hubs, Router), а порт 1434 — при SQL-аутентификации. Оба не представляют собой серьезной опасности. В общем, даже при стандартной установке ОС можно спокойно путешествовать по Сети.
Только после настройки правил межсетевого экрана при внутреннем пакетном фильтре BSD «ipfw» тест Qualys сообщает о наличии всего двух брешей самой низкой степени опасности — к примеру, Reachable Hostlist. Он позволяет увидеть IP и DNS провайдера, у которого зарегистрирован ваш Mac.