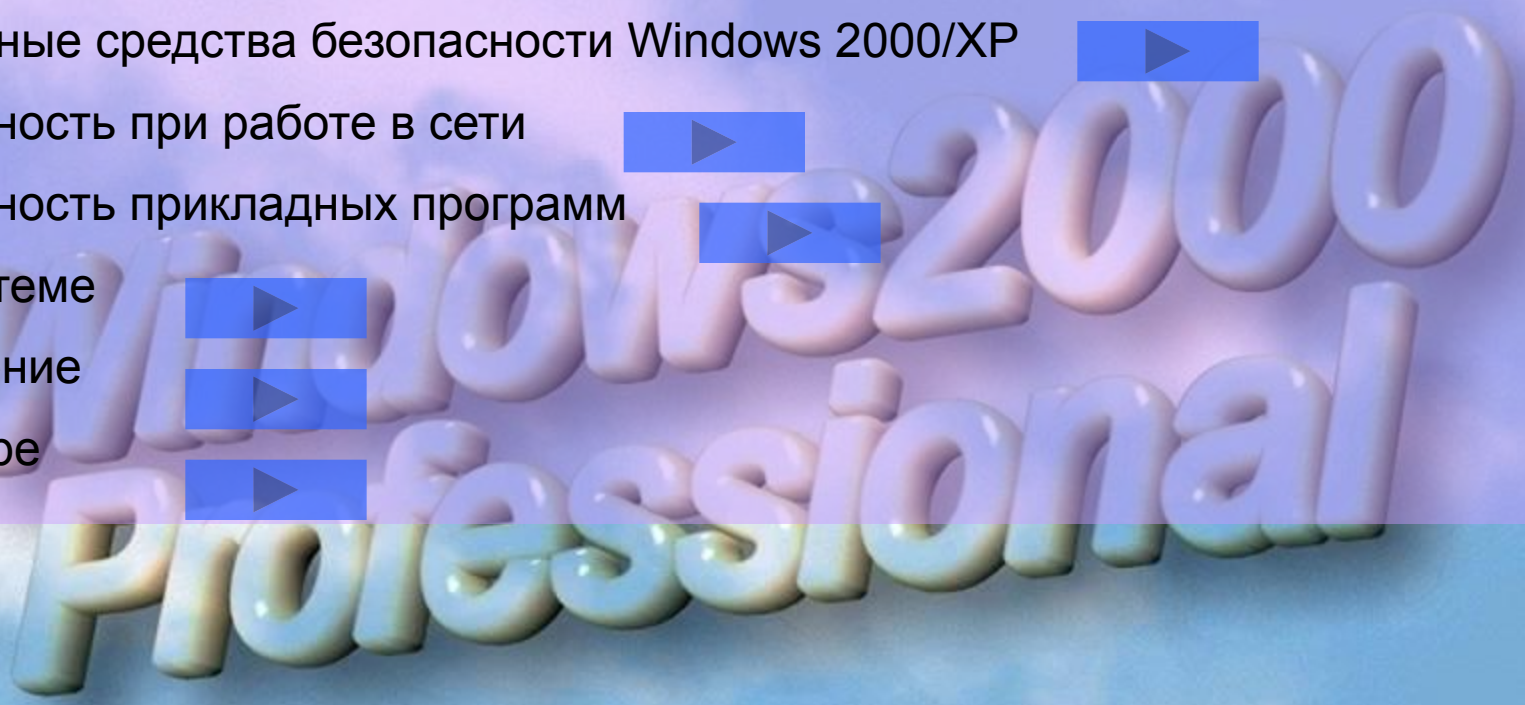
Безопасность Windows 2000/XP- это просто!

Выход

Дальше

СОДЕРЖАНИЕ:



Назад

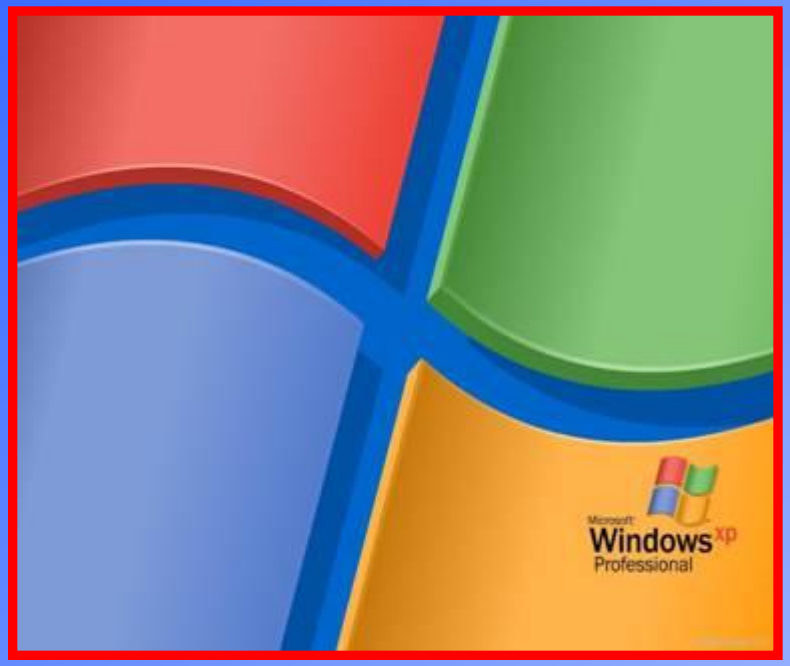
Дальше

Системные требования.

Для нормальной работы операционных систем Windows 2K/XP требуется: процессор Celeron/Pentium/Duron/K6 300 MHz, 32 Mb или 64 Mb ОЗУ (минимум).

Рекомендуемые требования соответственно удваиваются.

К содержанию | Назад | Дальше



Вступление

В настоящее время операционные системы Windows 2000 и Windows XP фирмы Microsoft, основанные на ядре Windows NT, получили очень широкое распространение. Процент этих ОС среди всех windows-систем очень велик и продолжает расти, поэтому проблема их безопасности является одним из важных аспектов современной компьютерной безопасности. В данной статье мы рассмотрим основы безопасности Windows 2000/XP и дадим практические советы по созданию максимально защищенного компьютера под управлением этих ОС.

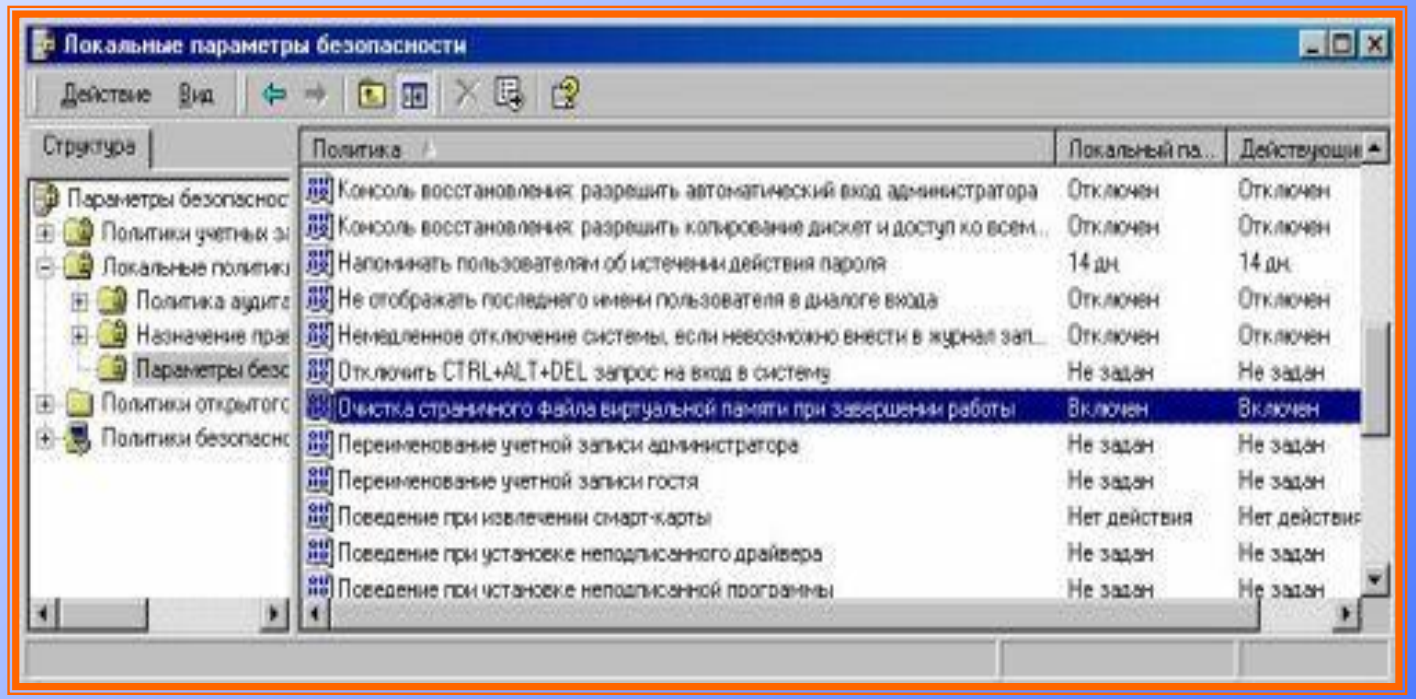
К содержанию

Назад

Дальше

Встроенные средства безопасности Windows 2000/XP

Несомненно, одним из главных инструментов для создания защищенного компьютера под Windows 2000/XP являются "Локальные политики безопасности", вызываемые из апплета "Администрирование". Множество параметров безопасности удобнее настраивать именно оттуда, а не через реестр или программы-твикеры - например, такие, как обнуление файла подкачки перед выключением компьютера или установка минимальной длины паролей. Не поленитесь, загляните в список параметров безопасности, и вы найдете много интересного.



К содержанию | Назад | Дальше

Безопасность при работе в сети

Если компьютер под управлением Windows 2000/XP подключен к сети, то, конечно же, он становится, уязвим и для сетевых атак. Поэтому безопасность при работе в сети также включает в себя несколько рекомендаций.

Даже когда вы не предоставляете свои каталоги в общий доступ, то можете заметить, что в системе существуют так называемые "административные" ресурсы 'C$', 'D$', 'E$' и так далее, а также 'Admin$' и 'IPC$'. Они предназначены для удаленного администрирования компьютера. Даже если их удалить, то при следующей загрузке они появятся снова. Чтобы запретить их создание, в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters нужно установить равным "0" параметр типа REG_DWORD "AutoShareServer" для сервера или параметр "AutoShareWks" для рабочей станции.

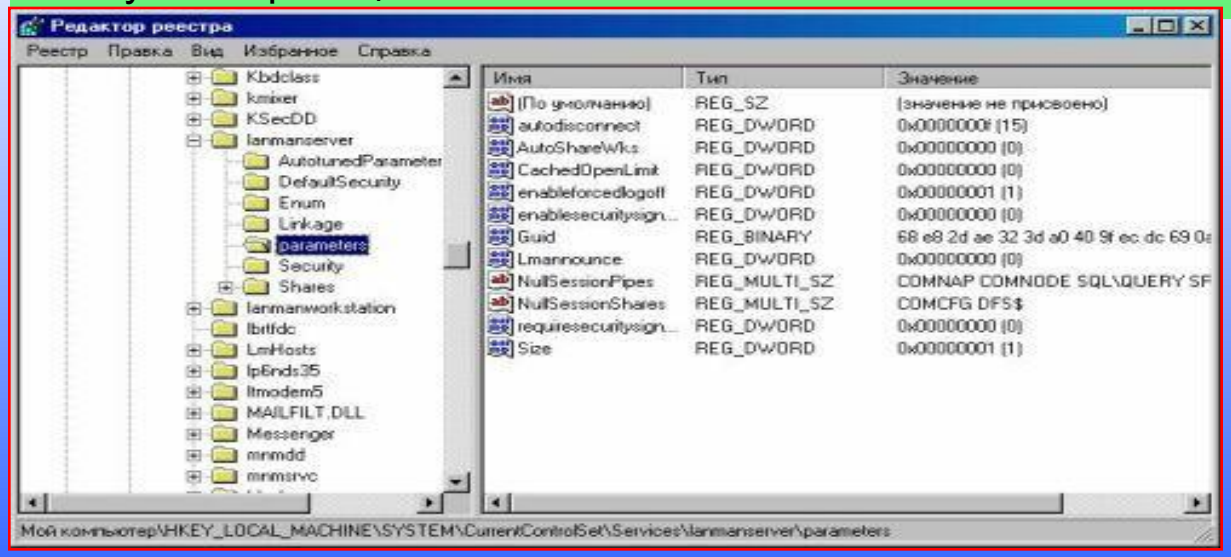
Однако этот метод не запретит создание ресурса IPC$, для этого нужно создать командный файл (BAT или CMD) файл со следующей строкой: **net share ipc$ /delete** и вставить запуск этого файла в Автозагрузку (кстати, таким же путем можно удалять и остальные ресурсы со знаком '$').

Теперь поговорим о таком распространенном сетевом явлении, как перехват паролей на вход в сеть. Не секрет, что обычно эти пароли также являются и паролями на вход в Windows, поэтому их перехват аналогичен воровству SAM-файла и восстановлению из него паролей пользователей.

К содержанию | Назад | Дальше

Ниже мы рассмотрим так называемую защищенную NT challenge/response (NTLM) аутентификацию, при этом процедура входа в сеть (если сетью управляет сервер) следующая:

1. Компьютер передает серверу запрос об аутентификации пользователя.
2. Сервер генерирует случайную 8-байтовую последовательность данных (так называемый "Challenge") и передает его компьютеру.
3. Компьютер, получив Challenge, на основе его и пароля, который ввел пользователь с помощью функций хеширования, генерирует LanMan Hash (а при отключении формирования LanMan Hash генерируется NT Hash). В этом случае длина хэша составляет уже 24 байта.
4. Компьютер передает полученный хэш серверу.
5. Сервер, в свою очередь, также генерирует хэш, используя те же входные данные (пароль, хранящийся на сервере, и Challenge, который в пределах одной сессии одинаковый для сервера и для компьютера-клиента).
6. Затем сервер сверяет оба полученных хэша и возвращает результат аутентификации.



К содержанию

Назад

Дальше

При данной схеме избегается передача пароля в незашифрованном виде. Но, несмотря на это, к этим хэшам также можно восстановить пароли. Перехват хэшей может происходить с любого компьютера в сети, работающего под любой ОС, и для этих целей используют программы LC4, PacketCatch, WinSniffer, NTSniffer и другие программы - «снифферы», то есть программы, анализирующие сетевой трафик. Для восстановления же паролей к перехваченным хэшам обычно используются программыLC4, Packet Inside и LC+4. **Для защиты от перехвата паролей используются следующие методы:**

Использование более защищенных методов аутентификации - NTLM v2 и Kerberos.

Использование в структуре сети свитчи или же полноценный маршрутизатор, тогда компьютер А (к примеру) физически не сможет перехватить пакеты, которыми обмениваются компьютер В и сервер С.

И, конечно же, обязательным условием для безопасной работы в сети является наличие файрвола. При грамотной настройке он практически на 100% защитит ваш компьютер от сетевых атак.

К содержанию Назад Дальше

Безопасность прикладных программ

Разумеется, безопасность Windows зависит не только от самой ОС, но и от программ, которыми вы пользуетесь. Никакая защита Windows не поможет, если, к примеру, через уязвимость в Internet Explorer можно закачать себе троян или несанкционированно выполнить вредоносный код.

- Не пользуйтесь Интернетом под аккаунтом Администратора - лучше создайте для этих целей отдельную учетную запись с правами обычного пользователя, чтобы попытки проникнуть на ваш компьютер через уязвимости браузеров или других интернет-утилит не принесли злоумышленнику успеха.
- По возможности пользуйтесь только последними версиями программ, с которыми вы работаете, следите за обновлениями этих программ, устанавливайте все патчи, хотфиксы (hotfixes) и заплатки для Windows, Internet Explorer и других программ, чтобы оперативно устранять возникающие уязвимости.
- Пользуйтесь антивирусом, периодически скачивайте антивирусные базы, не запускайте скачанные из Интернета программы без проверки на вирусы и трояны, не запускайте файлы, полученные по почте, если только они не получены из очень надежного источника, файлы же от подозрительных отправителей вообще удаляйте сразу.
- Настройте службы на вашем компьютере таким образом, чтобы работали только те сервисы, которые необходимы именно вам, в частности, желательно запретить удаленное управление реестром, остановив одноименную службу.
- Пользуйтесь возможностями шифрования данных средствами Windows 2000/XP с помощью EFS (Encrypting File System).

К содержанию | Назад | Дальше

К содержанию

Тест по теме

Что является одним из главных инструментов для создания защищенного компьютера под Windows 2000/XP ?

Замок с ключами

Ничего

Локальные политики безопасности

Неверно!

Назад

Правильно!

Дальше

К содержанию

Как называется программа, обеспечивающая

безопасность при работе в сети?

Фэйрволл

Word

ReGet

Неверно!

Назад

Правильно!

Дальше

К содержанию

Как называется процесс кодирования имени пользователя и пароля?

Кэширование

Инвентаризация

Хеширование

Неверно!

Назад

Правильно!

Дальше

К содержанию

Как называется файловая система шифрования данных средствами Windows 2000/XP ?

NTFS

EFS

FAT

Неверно!

Назад

Правильно!

К заключению

Заключение

Компания Microsoft, несомненно, проводит плановую политику по улучшению безопасности своих программных продуктов, но все равно главным элементом в создании максимально защищенного компьютера на базе операционных систем Windows 2000/XP остается пользователь. И ответственность за безопасность компьютера целиком лежит на администраторе или же пользователе с правами администратора. Практика администрирования компьютеров под управлением NT-систем показывает, что грамотно настроенный компьютер под Windows 2000/XP по надежности и защищенности не уступает компьютеру под управлением Linux.

Конечно же, тема безопасности Windows 2000/XP многогранна и включает в себя множество различных направлений, подробное описание которых может занять не одну книгу, поэтому наш совет вам, читатели, - активнее изучайте систему, на которой вы работаете, будьте в курсе всех последних новостей по компьютерной безопасности и постоянно повышайте свою квалификацию пользователя, тогда от работы за компьютером вы будете получать гораздо больше удовольствия, чем огорчений.

Корнев Александр

К содержанию | Выход | Об авторе

Корнев Александр, ученик 8Б класса лицея №43. Почти год занимается архитектурой систем безопасности операционных систем Windows 2000/XP/ Server 2003. Также занимается способами взлома удалённых систем и различными вариантами обхода Kerberos.

К содержанию

Выход


Необходимое условие