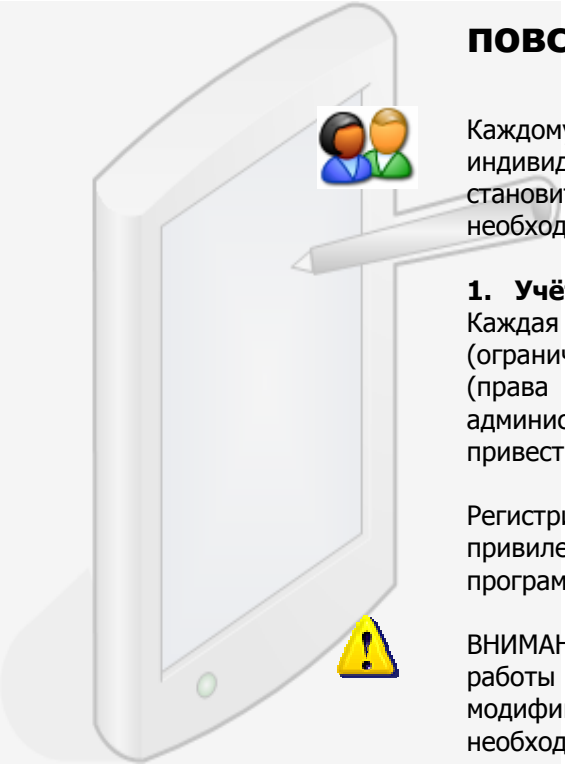
описание продукта

Добро пожаловать!

В настоящем Руководстве рассказывается о том, как использовать операционную систему Microsoft ® Windows ® XP Professional, сконфигурированную для безопасной работы.

Данный продукт содержит в себе стандартные меры безопасности и отказоустойчивости, которые, по мнению поставщика, должны широко применяться при настройке практически каждой компьютерной системы.

Неукоснительно выполняйте рекомендации, приведённые в данном Руководстве, и ваш компьютер надолго останется быстрым, надёжным и безопасным.



повседневное использование системы

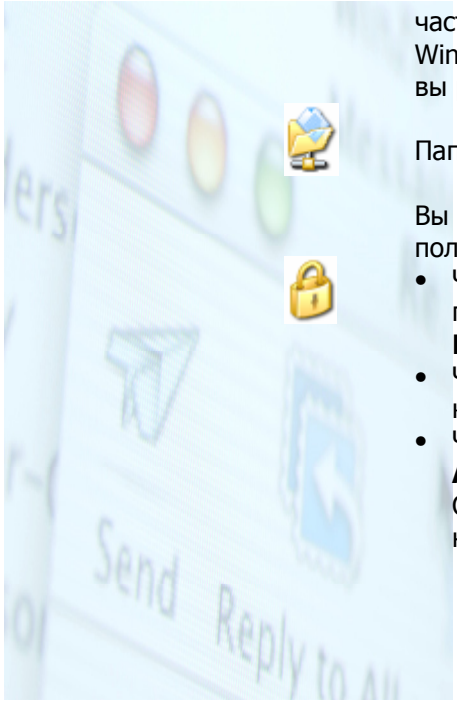
Каждому человеку, работающему с компьютером, выдаётся индивидуальная учётная запись (логин). Тем самым, компьютер становится способен различать людей, а также предоставлять им необходимые права и уровни доступа.

1. Учётные записи и уровни привилегий.

Каждая учётная запись может обладать либо правами обычного (ограниченного) пользователя, либо неограниченными привилегиями (права администратора). Не используйте учётные записи уровня администратора для повседневной работы, так как это может привести к случайному повреждению системы.

Регистрировать пользователей, а также настраивать уровень привилегий той или иной учётной записи вы можете в **Control Panel**, программа **User Accounts**.

ВНИМАНИЕ! Некоторые учётные записи необходимы для корректной работы системы, - например, пользователь **Backup**. Не модифицируйте настройки системных пользователей без необходимости.



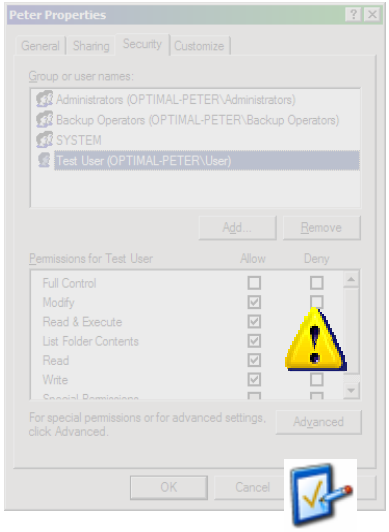
2. Программы, документы и права доступа.

Жёсткий диск в вашем компьютере поделен на несколько логических частей. Раздел C: предназначен для хранения самой системы Windows и основных программ, раздел **D:** - для файлов, с которыми вы работаете.

Папка **My Documents** также нацелена в **D:\Users**.

Вы можете защитить свои документы от вмешательства других пользователей:

- Чтобы посмотреть список допущенных лиц и их права, щёлкните правой кнопкой мыши поверх требуемой папки, выберите команду **Properties**, закладку **Security**.
- Чтобы расширить список допущенных лиц, просто добавьте их кнопкой **Add**.
- Чтобы сузить список допущенных лиц или их права, в меню **Advanced** отключите галочку „Inherit from parent..", выберите Copy, Ok и отредактируйте список доступа согласно текущим нуждам.



Регулируя права доступа, придерживайтесь следующих правил:

- Не используйте Запреты (**Deny**) для регулирования доступа к папке. Вместо этого, не давайте Разрешения (**Allow**) лицам, которые не должны получить доступ.
- Помните, что группа **Users** включает в себя всех пользователей. Назначая права группе Users, вы предоставляете тот или иной доступ всем пользователям вашего компьютера.
- Группа **Backup Operators** выполняет задачи резервного копирования, не снимайте с неё прав Чтения на документы.
- **ВНИМАНИЕ!** Не следует изменять права доступа системных папок C:\, C:\Documents and Settings, C:\Windows.

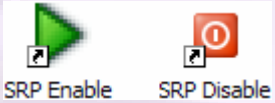
3. Общие рекомендации

- Работая с ограниченными привилегиями, вы надёжно защитите свой компьютер от случайного повреждения или вирусного заражения. Используйте вход Администратора только при явной необходимости.
- Храните документы и рабочие файлы в папке **D:\Users**, это обеспечит их регулярное резервное копирование
- Храните **медиа-файлы** и вещи, не требующие резервного копирования, за пределами папки D:\Users (например, F:\Movies).

установка и настройка программ

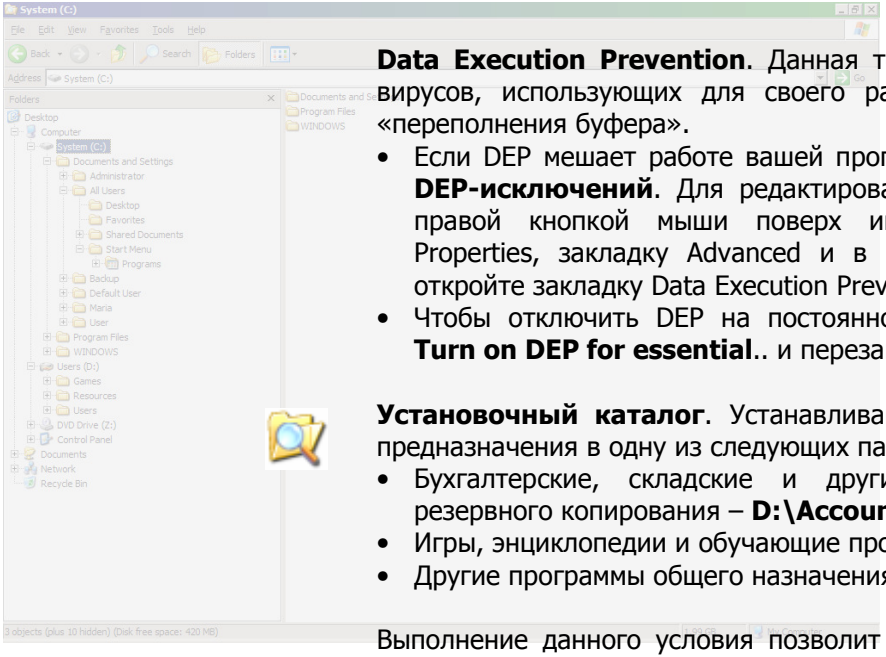
1. Установка новых программ

Система безопасности может блокировать установку некоторых программ. Ознакомьтесь с использованными в данной поставке Windows методами защиты, чтобы успешно установить и настроить необходимые вам программы.



Software Restriction Policies. Данная технология разрешает запускать только заранее согласованные Администратором программы, что позволяет предохраниться от множества почтовых червей и троянских программ.

- Временно отключайте SRP перед установкой новых программ (или обновления имеющихся) с помощью иконки **SRP Disable**.
- Список разрешённых SRP программ доступен в папке Additional Rules консоли **Local Security Policy**. Чтобы отредактировать этот список, вызовите Start -> Run -> gpedit.msc и откройте меню Computer Configuration -> Windows Settings -> Security Settings -> Software Restriction Policies.
- Чтобы отключить SRP на постоянной основе, выберите команду Set As Default, щёлкнув правой кнопки мыши поверх опции **Unrestricted** упомянутой выше консоли.



Data Execution Prevention. Данная технология блокирует работу вирусов, использующих для своего распространения методы т.н. «переполнения буфера».

- Если DEP мешает работе вашей программы, внесите её в список **DEP-исключений**. Для редактирования этого списка щёлкните правой кнопкой мыши поверх иконки Computer, выберите Properties, закладку Advanced и в секции Performance Settings откройте закладку Data Execution Prevention.
- Чтобы отключить DEP на постоянной основе, выберите опцию **Turn on DEP for essential**.. и перезагрузите компьютер.

Установочный каталог. Устанавливайте программы согласно их предназначения в одну из следующих папок:

- Бухгалтерские, складские и другие программы, требующие резервного копирования – **D:\Accounting**
- Игры, энциклопедии и обучающие программы – **D:\Games**
- Другие программы общего назначения – **C:\Program Files**

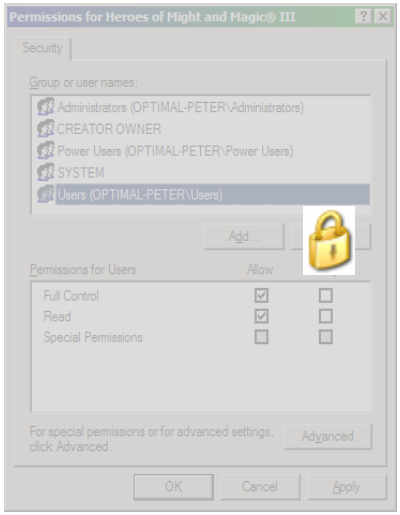
Выполнение данного условия позволит правильно назначить права доступа и обеспечить качественное резервное копирование программ и рабочих файлов.

2. Настройка программ для работы с ограниченными привилегиями

ВНИМАНИЕ! Данная процедура требует определённого опыта работы с компьютером. Неправильное изменение параметров безопасности может привести к серьёзным неполадкам, требующих переустановки системы.

Выполните следующую последовательность действий, в случае, когда установленная программа не запускается или работает некорректно от лица обычного пользователя, но успешно выполняется от лица Администратора:

- Зайдите в систему пользователем с ограниченными привилегиями и попытайтесь запустить программу или исполнить неработающую функцию. Запомните текущее время
- Зайдите в систему Администратором и откройте программу **Event Viewer** из Control Panel, Administrative Tools. Включите фильтр событий безопасности, щёлкнув правой кнопкой мыши поверх журнала **Security**, команда View, Filter. Снимите все галочки, кроме Failure audit; в поле **Event ID** введите "**560**" и нажмите Ok
- Найдите в журнале события, относящиеся к примерному времени тестирования программы и ознакомьтесь с их содержимым



- Некоторые из событий в поле **Object Name** будут указывать на файлы или ключи реестра, доступ к которым требуется программе для корректной работы. Например: ”Object Name: C:\Program Files\Winamp\Winamp.ini”, ”Object Name: \REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{43DF7A11-E7B8-11D0-A445-004095E1DAEA}”.
- Расширьте уровень доступа пользователей (группа **Users**) до **Modify** на требуемые файлы или каталоги, используя методику, описанную в п. 2 модуля «Повседневное использование системы».
- Если этого недостаточно, отрегулируйте права пользователей на реестр Windows с помощью программы **Registry Editor**, вызвав её командой Start, Run, regedit. Найдите требуемый ключ реестра в левой части окна, щёлкните поверх него правой кнопкой мыши и вызовите команду **Permissions**. Следуя аналогии с файлами на жёстком диске, расширьте уровень доступа до **Full Control** для группы **Users**.

Внимательно документируйте совершённые действия. В случае, если выполнение данной процедуры не привело к решению проблемы, обратитесь к поставщику системы.

3. Рекомендации безопасности

Тщательно ограничивайте список устанавливаемых программ, так как именно беспорядочные инсталляции в первую очередь влияют на скорость и надёжность работы вашего компьютера.

- Не устанавливайте программы, не являющиеся действительно необходимыми для работы.
- Приняв решение установить ту или иную программу, возьмите её файлы в надёжном источнике, лучше всего – на оригинальном сайте или компакт-диске производителя.
- Перед началом установки проверяйте инсталляционные файлы антивирусным пакетом. К примеру, многие бесплатно распространяемые в Интернете хранители экрана (screen-savers) содержат в себе троянские модули.
- Устанавливайте программы в предназначенные для этого каталоги (см. рекомендации выше), что облегчит их настройку и не помешает процедурам резервного копирования.

резервное копирование (опция)

Данный продукт может поставляться с настроенным модулем резервного копирования, что позволит вам восстановить систему и рабочие документы из страховой копии в случае сбоя.

1. Настройка резервного копирования

Автоматически создаются резервные копии рабочих документов и бизнес-программ (папки **D:\Users**, **D:\Accounting**), а также самой системы (**C:** и **SystemState**). Копируются все файлы, за исключением мультимедиа-ресурсов (музыки, фильмов и т.п.)

Изменить время начала резервного копирования вы можете в Control Panel -> **Scheduled Tasks**, вызвав свойства задач Backup System и Backup Documents соответственно. Примите во внимание тот факт, что само копирование занимает некоторое время (до нескольких часов) – не выключайте компьютер слишком рано.

Также, вы можете отменить резервное копирование вообще, убрав галочку **Enabled** в свойствах указанных выше задач.

За более подробными настройками модуля резервного копирования обращайтесь к поставщику системы.

2. Процедура съёмного копирования

Регулярно выполняйте копирование важных документов на съёмные носители (flash-устройство или мобильный диск), чтобы восстановить данные в случае полной утраты или повреждения компьютера.

- подключите съёмный диск и запустите программу копирования.
- введите пароль шифрования архива. **ВНИМАНИЕ!** В случае утери пароля, документы восстановить будет НЕВОЗМОЖНО!
- Убедитесь, что процесс копирования исполняется. Дождитесь завершения процедуры копирования и отключите съёмный диск в штатном порядке.

3. Восстановление данных.

Автоматически создаваемые резервные копии хранятся в папке **D:\Resources\Backup\Имя_Компьютера**. Для восстановления данных зайдите в систему с учётной записью, обладающей привилегиями Администратора.

- Для восстановления повреждённых рабочих документов или файлов бизнес-программ, найдите их копии в подпапке **\DAY01** и скопируйте в требуемую директорию.
- Для восстановления системы, программ или реестра воспользуйтесь программой **ntbackup.exe**, указав ей местонахождение файла резервной копии в подпапке **\WEEK01\Backup.bkf**.
- Для восстановления системы или данных со съёмного диска, найдите в папке \Resources\Backup\Имя_Компьютера этого диска файл **Backup.rar** и разархивируйте его, указав пароль шифрования, который вводили при создании копии.

ВНИМАНИЕ! Ответственность за качество копий и восстановление данных полностью лежит только на владельце компьютера.

Для более подробных инструкций по действиям в случае сбоя обращайтесь к поставщику системы.

рекомендации по обслуживанию системы

- Выполняйте обычную работу, заходя в систему с ограниченными привилегиями. Это гарантированно защитит компьютер от любой вирусной инфекции или случайного повреждения.
- Регулярно выполняйте обновление не только Windows, но и других пользовательских программ, для чего используйте сайт **Windows Update** (http://windowsupdate.microsoft.com), а также веб-сайты производителей соответствующих программ.
- Периодически проверяйте систему антивирусной программой. Помните, что существуют зловредные программы, которые не могут быть обнаружены таким путём.
- Регулярно меняйте пароль Администратора. Не используйте этот же пароль для доступа к другим системам (компьютерам, веб-сайтам, электронной почте). Сменить пароль вы можете в **Control Panel**, программа **User Accounts**.