

Лабораторная работа №4

Защита от несанкционированного доступа и сетевых хакерских атак

Цель работы:

Задание 1. Познакомиться с встроенными компонентами защиты операционной системы Microsoft Windows XP и настроить их.

Теоретическая часть

Брандмауэр Windows

Задачу защиты от несанкционированного доступа и сетевых атак домашнего компьютера успешно решает персональная программа-брандмауэр. Она может быть как встроенной в операционную систему (например, брандмауэр Windows), так и устанавливаемой отдельно (например Outpost FireWall).

Самая, пожалуй, популярная на сегодняшний день операционная система домашнего компьютера - Microsoft Windows XP содержит встроенный Брандмауэр Windows. Более поздние версии Microsoft Windows, Vista и Seven (находится в стадии разработки, в начале 2009 года будет представлена beta-версия) содержат в себе дополнительные компоненты защиты от несанкционированного доступа и шпионских программ, например Windows Defender.

Встроенные брандмауэры отличаются весьма ограниченной функциональностью, что с другой стороны компенсируется отсутствием конфликтов с операционной системой и бесплатностью. Брандмауэры же третьих производителей, устанавливаемые отдельно, обеспечивают обычно более удобную и приятную работу с возможностью более точной настройки различных параметров.

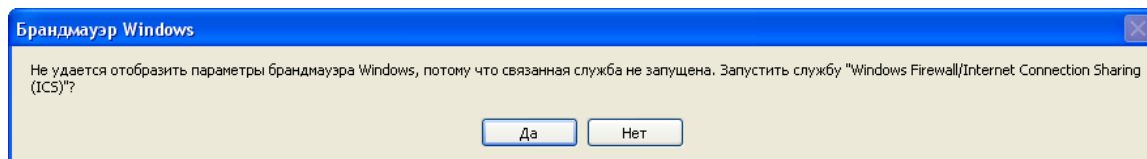
1. После загрузки операционной системы Microsoft Windows XP (в Microsoft Virtual PC), Брандмауэр Windows будет отключен. Для его включения выполните следующие действия:



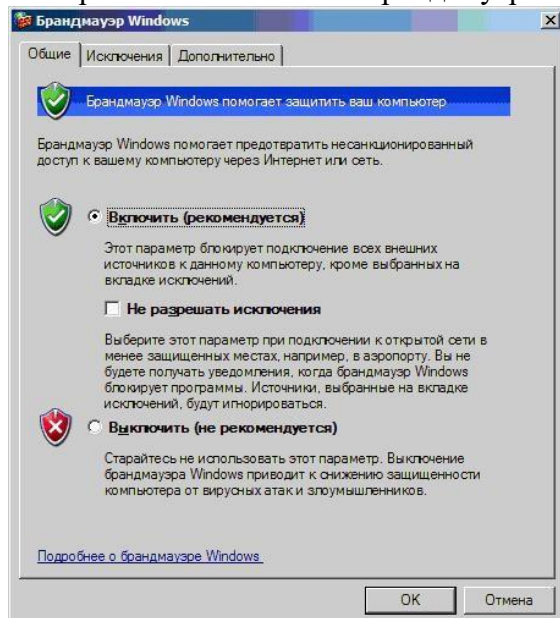
Брандмауэр
Windows

Нажмите Меню Пуск – Панель управления – Брандмауэр Windows

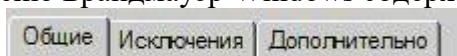
2. Появится сообщение операционной системы, информирующее вас о выключенной службе Брандмауэра Windows. Включите службу, нажав кнопку Да.



На экране появится меню Брандмауэр Windows

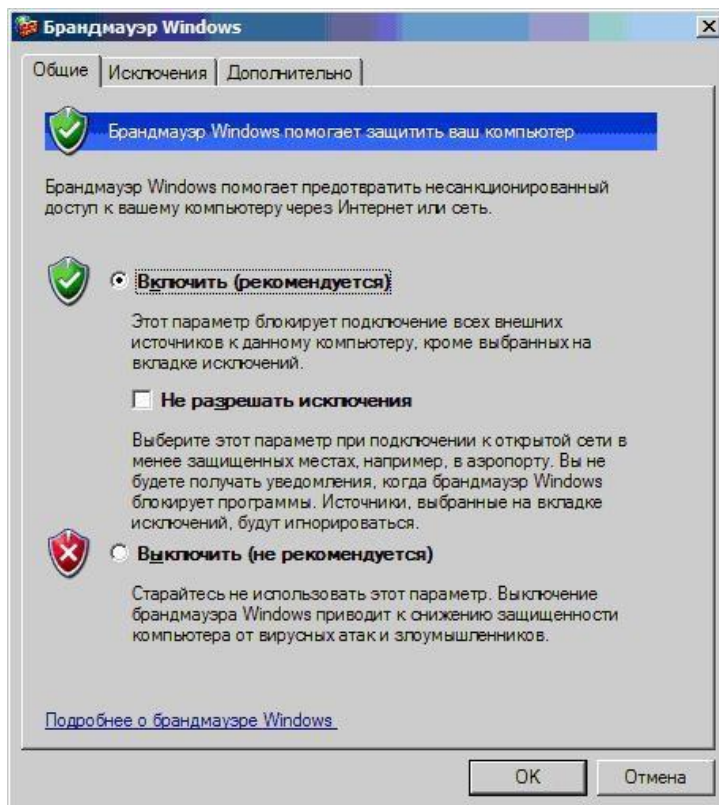


3. Меню Брандмауэр Windows содержит 3 вкладки – Общие, Исключения,



Дополнительно. Выберите каждую вкладку и просмотрите ее содержимое.

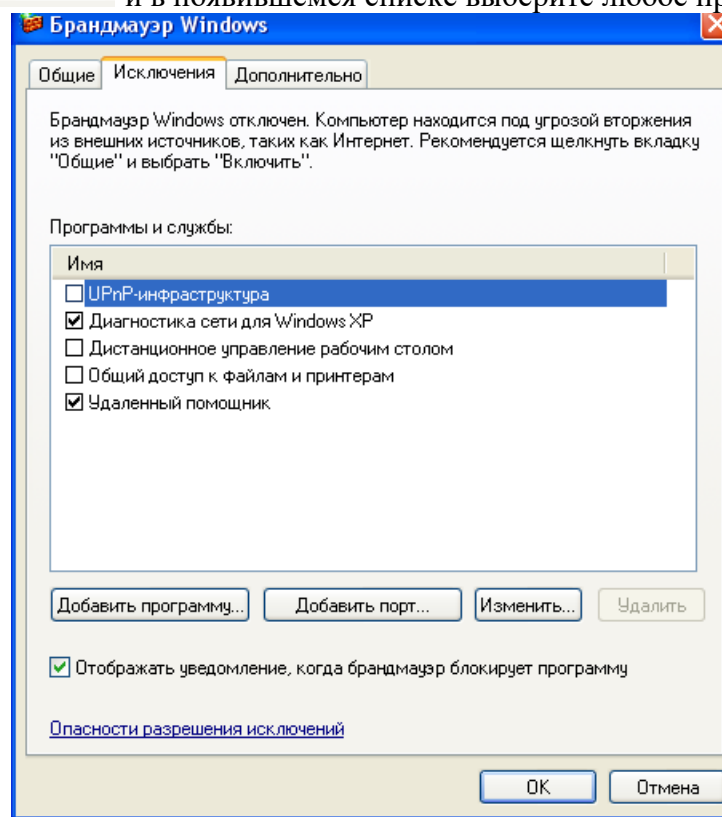
4. Вкладка Общие позволяет менять режим работы Брандмауэра Windows. Можно Включить брандмауэр (после установки Операционной системы Microsoft Windows XP, система автоматически включает Брандмауэр Windows) или Выключить его (при установке другого Брандмауэра на ваш компьютер, Брандмауэр Windows будет выключен автоматически). Отключите Брандмауэр Windows, а затем вновь включите его.



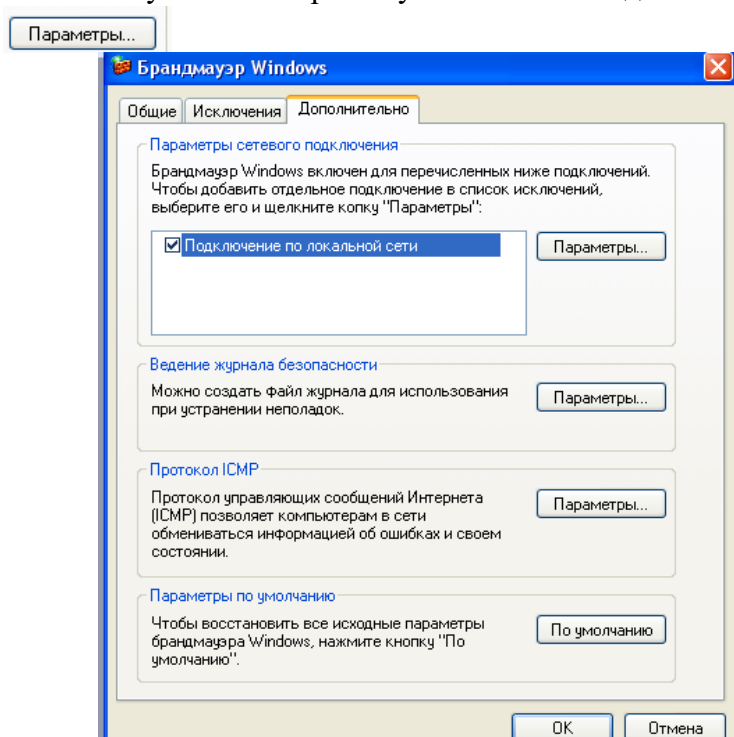
5. Вкладка Исключения позволяет создавать исключения для нужных служб и приложений. Например, если вы точно уверены, что конкретное приложение не будет выполнять несанкционированных удаленных соединений или Брандмауэр Windows заблокировал сетевой доступ приложения, можно создать Исключение и блокировка будет снята. Добавьте исключение для программы, нажав кнопку Добавить программу

Добавить программу...


и в появившемся списке выберите любое приложение.

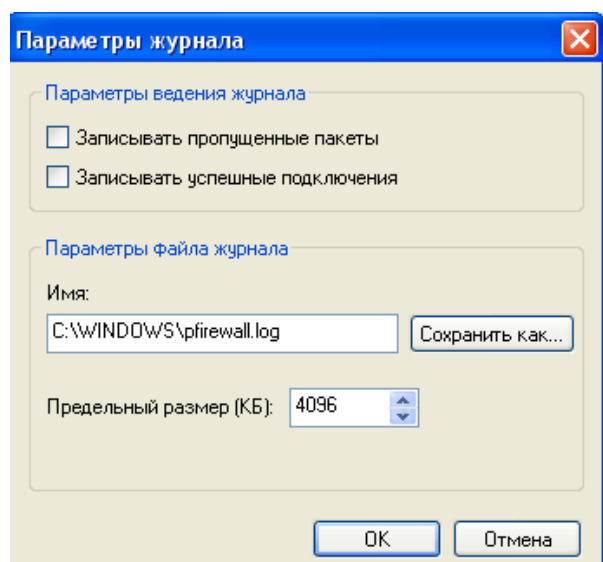


6. Вкладка Дополнительно позволяет включить или отключить Брандмауэр Windows для конкретных сетевых подключений, заблокировать или разблокировать сетевые службы. Выберите нужно сетевое Подключение и нажмите кнопку Параметры

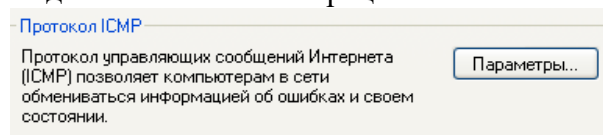


7. При устранении неполадок, можно воспользоваться Журналом Безопасности, для того, чтобы выяснить, когда произошла неполадка и при каких обстоятельствах.

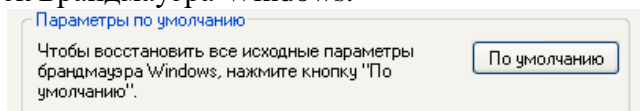
Нажмите кнопку Параметры  в блоке Ведение журнала безопасности. В появившемся окне произведите настройки, согласно предложенному рисунку и нажмите Ок.



8. Блок Протокол ICMP служит для приема и отправки сообщений об ошибках и состоянии компьютеров в сети. Так же этот протокол используют некоторые вредоносные программы, с периодичностью показывая различные сообщения о якобы произошедших ошибках в операционной системе.



9. Блок Параметры по умолчанию служит для восстановления исходных настроек Брандмауэра Windows.



Центр Обеспечения безопасности Windows

Если ваш компьютер подключен к компьютерной сети (неважно, Интернет это или Интранет), то он уязвим для вирусов, атак злоумышленников и других вторжений. Для защиты компьютера от этих опасностей необходимо, чтобы на нем постоянно работали межсетевой экран (брандмауэр) и антивирусное ПО (с последними обновлениями). Кроме того, необходимо, чтобы все последние обновления были также установлены на вашем компьютере.

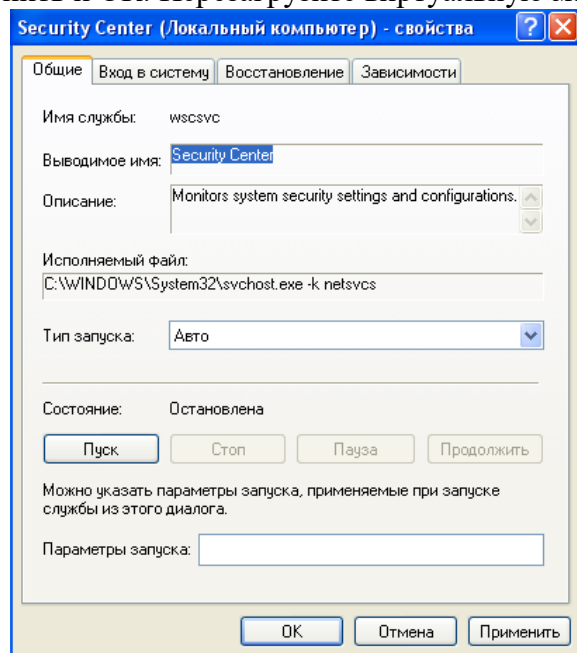
Не каждый пользователь может постоянно следить за этим. Не каждый пользователь знает, как это осуществить. И даже если пользователь компетентен в этих вопросах, у него просто может не хватать времени на такие проверки. Компания Microsoft позаботилась обо всех этих пользователях, включив в состав SP2 (и SP3) для Windows XP такой инструмент. Он называется Центр обеспечения безопасности Windows (Windows Security Center).

1. Нажмите Меню Пуск – Панель управления – Центр обеспечения

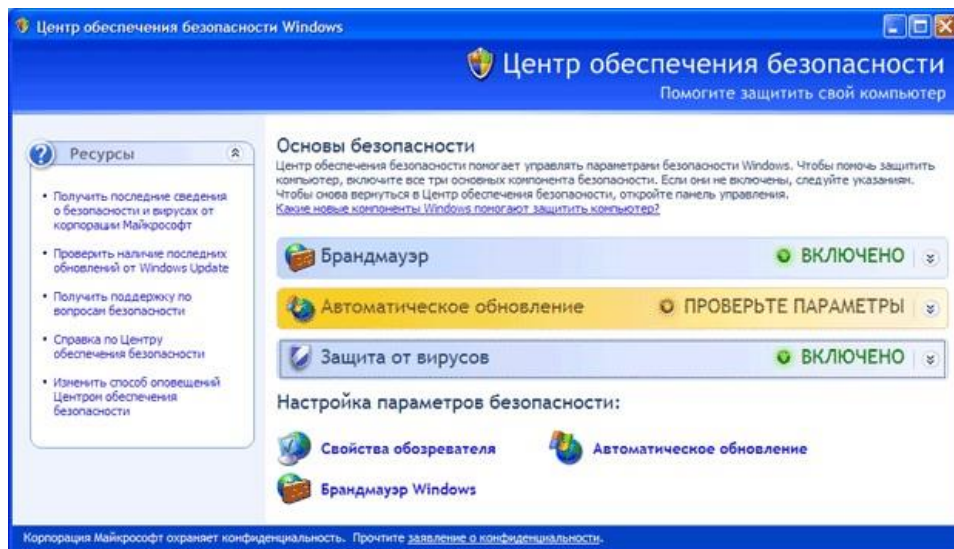


безопасности

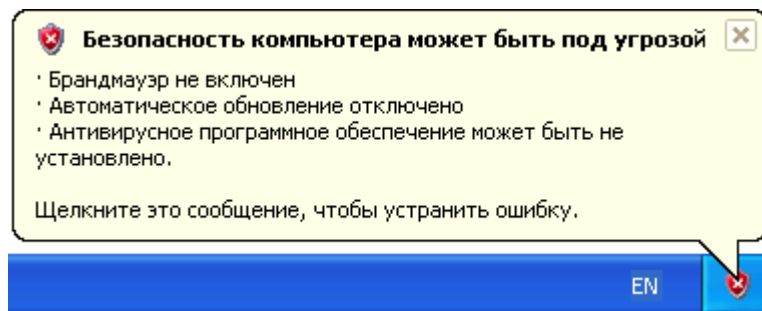
Для включения Центра обеспечения безопасности Windows, нажмите Пуск – Панель управления – Администрирование – Службы. В списке служб найдите службу Security Center, нажмите 2 раза на на этой службе, выберите тип запуска Авто, нажмите кнопку Применить и ОК. Перезагрузите виртуальную машину.



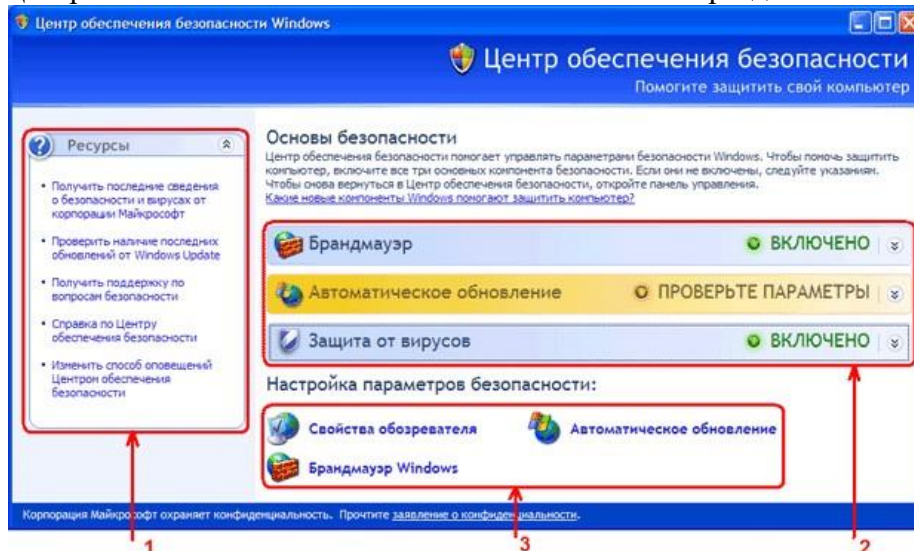
2. На экране появится меню Центра обеспечения безопасности Windows.



3. Основное назначение этого инструмента - информировать и направлять пользователя в нужном направлении. Во-первых, он постоянно контролирует состояния трех основных компонентов ОС (брандмауэр, антивирус, система автоматического обновления). Если параметры любого из этих компонентов не будут удовлетворять требованиям безопасности компьютера, то пользователь получит соответствующее уведомление.



Меню Центра обеспечения безопасности Windows можно разделить на 3 части

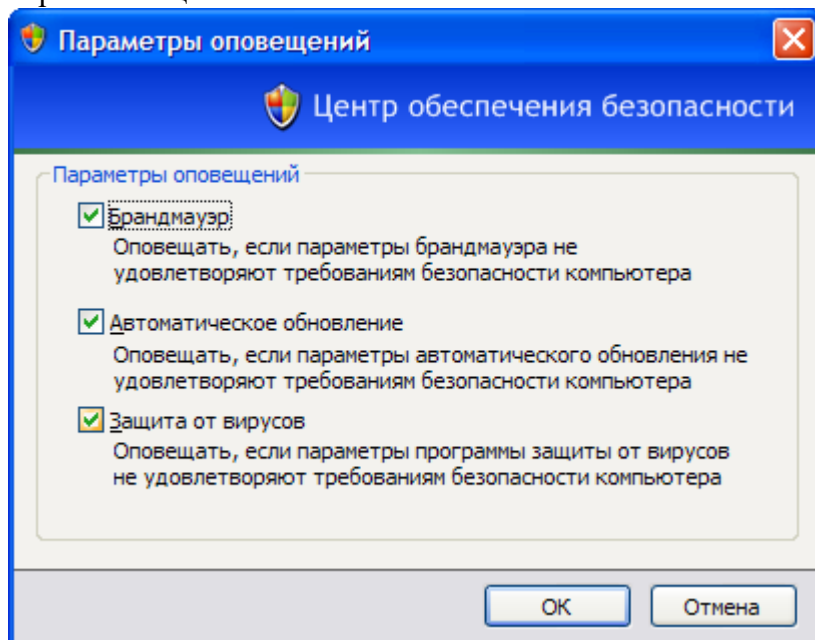


1. Ресурсы. Здесь располагаются ссылки для перехода к Интернет-ресурсам, к встроенной в Windows справочной службе и к окну настройки параметров оповещений.
2. Компоненты безопасности. Здесь располагаются информационные элементы трех основных компонентов безопасности: брандмауэр, автоматическое обновление, антивирусная защита.

3. Параметры безопасности. Здесь располагаются кнопки перехода к настройкам безопасности следующих компонентов: обозреватель Internet Explorer, автоматическое обновление, брандмауэр Windows.

Рассмотрим эти части более подробно.

4. В части 1 первые три ссылки предназначены для перехода на соответствующие страницы на сайте Microsoft. Предпоследняя ссылка предназначена для открытия справочной службы Windows на странице "Общие сведения о центре обеспечения безопасности Windows". Последняя ссылка предназначена для открытия окна "Параметры оповещений".



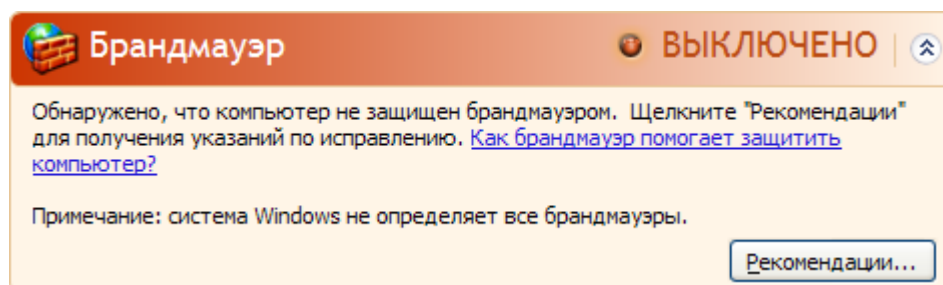
Если на компьютере установлен брандмауэр и антивирусное ПО, не определяемое Центром обеспечения безопасности, вы можете отключить соответствующие оповещения

5. В части 2 каждое информационное табло сообщает о состоянии соответствующего компонента. На рисунке представлены возможные состояния.

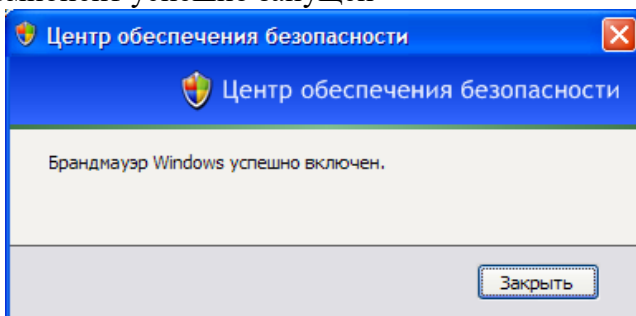
A	ВКЛЮЧЕНО
B	ПРОВЕРЬТЕ ПАРАМЕТРЫ
C	ВЫКЛЮЧЕНО
D	НЕ НАЙДЕНО
E	СРОК ИСТЕК
F	НЕ НАБЛЮДАЕТСЯ

Состояния A-C понятны без комментариев. Состояние D - "Не найдено" - соответствует невозможности определить присутствие соответствующего ПО (например, антивирус или брандмауэр). Состояние E - "Срок истек" - возможно для антивирусной защиты, когда обновления антивирусных баз устарели. Состояние F - "Не наблюдается" - соответствует отключенному контролю над соответствующим компонентом.

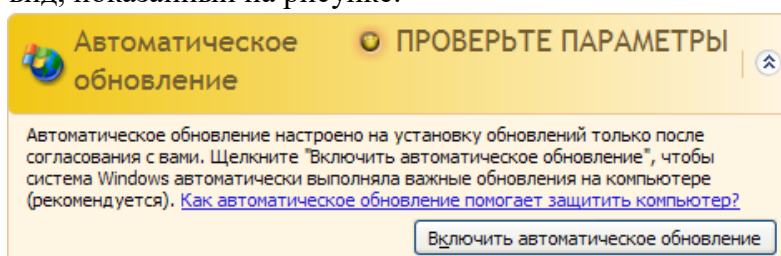
6. Выключите один из компонентов защиты. Состояние этого компоненты примет вид, показанный на рисунке (например, если отключить Брандмауэр Windows)



7. Включите отключенный компоненты защиты, на экране появится сообщение
Ваш компонент успешно запущен




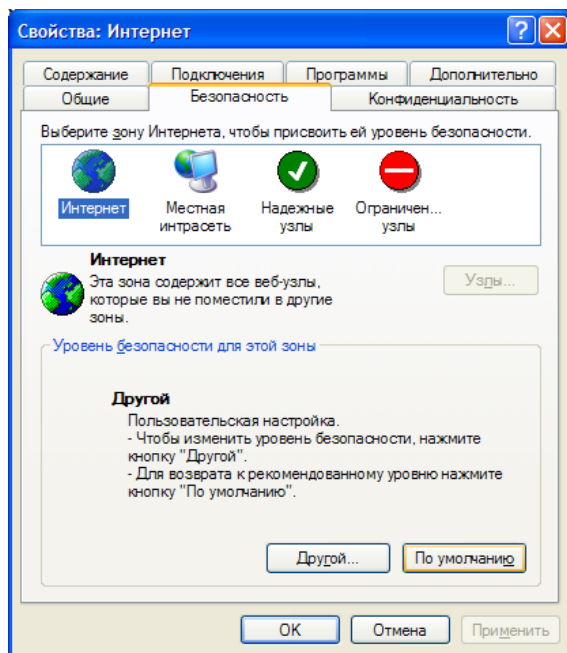
8. Если один из компонентов не может выполнить нужное действие (например, автоматические обновления устанавливаются по выбору пользователя), статус компонента примет вид, показанный на рисунке.




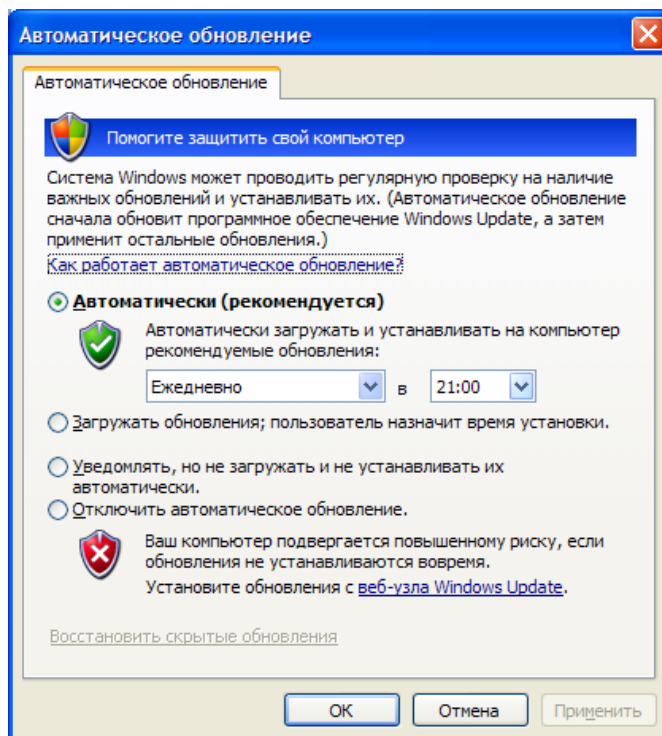
9. Как уже было указано ранее, в разделе 3 расположены кнопки перехода к настройкам безопасности следующих компонентов: обозреватель Internet Explorer, автоматическое обновление, брандмауэр Windows.



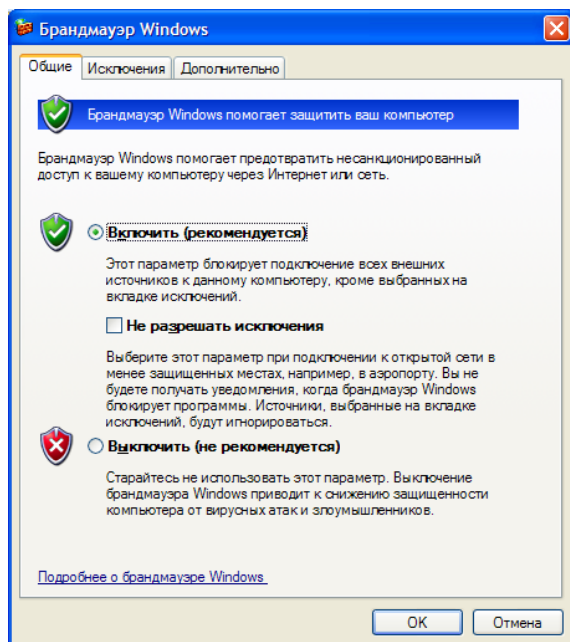
10. Нажав кнопку  **Свойства обозревателя**, вы попадете на закладку "Безопасность" в окне настроек обозревателя Internet Explorer.



11. Нажав кнопку  **Автоматическое обновление**, вы откроете окно настроек "Автоматического обновления".



12. Нажав кнопку  **Брандмауэр Windows**, вы попадете в соответствующее окно настроек.



Измените различные настройки безопасности компонентов Internet Explorer, Автоматического обновления и Брандмауэра Windows.

Контрольные вопросы:

1. Дайте определение «несанкционированный доступ», «хакерская атака».
2. Что такое персональная программа-брандмауэр? Какие задачи она решает?
3. Перечислите плюсы и минусы брандмауэров.
4. Как вкл/выкл брандмауэр?
5. Для чего нужен журнал безопасности брандмауэра?
6. Для чего служит блок протокол ICMP?
7. Как защитить компьютер от сетевых хакерских атак?
8. В чем заключается назначение Центра обеспечения безопасности Windows (Windows Security Center)?
10. Какие действия необходимо выполнить для активации Брандмауэра Windows?

Задание 2. Ознакомиться с процедурами создания учеников

Теоретическая часть

Пользователи

Локальный пользователь или группа - это учетная запись, которой могут быть предоставлены разрешения и права на вашем компьютере. Домен или глобальные пользователи и группы управляются сетевым администратором. Имеется возможность добавить локальных пользователей, глобальных пользователей и глобальные группы в локальные группы. Однако невозможно добавить локальных пользователей и локальные группы в глобальные группы.

Пользователи и группы важны для безопасности Windows XP, поскольку позволяют ограничить возможность пользователей и групп выполнять определенные Действия путем назначения им прав и разрешений. Право даст возможность пользователю выполнять на компьютере определенные действия, такие как архивирование файлов и папок или завершение работы компьютера. Разрешение представляет собой правило, связанное с объектом (например, файлом, папкой или принтером), которое определяет, каким пользователям и какого типа доступ к объекту разрешен.

Операционная система содержит несколько встроенных учетных записей пользователей и групп, которые не могут быть удалены.

Краткая информация о встроенных учетных записях.

Учетная запись администратора

Учетная запись пользователя с именем «Администратор» используется при первой установке рабочей станции или рядового сервера. Эта учетная запись позволяет выполнять необходимые действия до того, как пользователь создаст свою собственную учетную запись. Учетная запись администратора является членом группы администраторов на рабочей станции или рядовом сервере.

Учетную запись «Администратор» нельзя удалить, отключить или вывести ИЗ группы администраторов, что исключает возможность случайной потери доступа к компьютеру после уничтожения всех учетных записей администраторов. Это свойство отличает пользователя «Администратор» от остальных членов локальной группы «Администраторы»

Учетная запись гостя

Учетная запись гостя используется теми, кто не имеет реальной учетной записи на компьютере. Если учетная запись пользователя отключена (но не удалена), он также может воспользоваться учетной записью «Гость». Учетная запись гостя не требует пароля. Учетная запись гостя по умолчанию отключена, но не может включена.

Учетной записи пользователя «Гость», как и любой другой учетной записи, можно предоставлять права и разрешения на доступ к объектам. Учетная запись «Гость» по умолчанию входит во встроенную группу «Гости», что позволяет пользователю войти в систему с рабочей станции или рядового сервера. Дополнительные права, как любые разрешения, могут быть присвоены группе «Гости» членом группы администраторов.

1. Группы

Администраторы

Пользователи, входящие в группу «Администраторы», имеют полный доступ на управление компьютером. Это единственная встроенная группа, которой автоматически предоставляются все встроенные права и возможности в системе.

Операторы архива

Члены группы «Операторы архива» могут архивировать и восстанавливать файлы на компьютере, независимо от всех разрешений, которыми защищены эти файлы. Также они могут входить на компьютер и выключать его, но не могут изменять параметры безопасности.

Опытные пользователи

Члены группы опытных пользователей могут создавать учетные записи пользователей, но могут изменять и удалять только созданные ими учетные записи. Они могут создавать локальные группы и удалять пользователей из локальных групп, которые они создали. Они также могут удалять пользователей из групп «Опытные пользователи», «Пользователи» и «Гости»

Они не могут изменять группы «Администраторы» и «Операторы архива», не могут являться владельцами файлов, не могут выполнять архивирование и восстановление каталогов, не могут загружать и выгружать драйверы устройств или управлять журналами безопасности и аудита.

Пользователи

Члены группы пользователей могут выполнять наиболее распространенные задачи, например запуск приложений, использование локальных и сетевых принтеров, завершение работы и блокировка рабочих станций. Пользователи могут создавать локальные группы, но изменять могут только те, которые они создали. Пользователи не могут организовывать общий доступ к каталогам или создавать локальные принтеры.

Гости

Группа «Гости» позволяет случайным или разовым пользователям войти в систему со встроенной учетной записью гостя рабочей станции и получить ограниченные возможности. Члены группы «Гости» могут только прекратить работу компьютера.

2. Управление учетной записью пользователя

Для управления учетными записями используется компонент «Управление компьютером». Чтобы открыть окно этого компонента, нажмите Пуск-Панель управления.



Администрирование

Дважды щелкните значок Администрирование, затем дважды щелкните значок

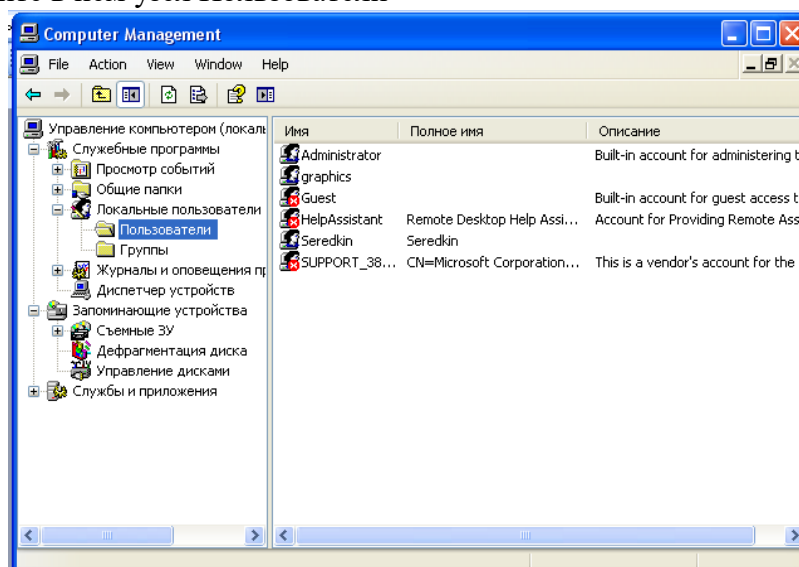


Управление компьютером
Shortcut
2 KB

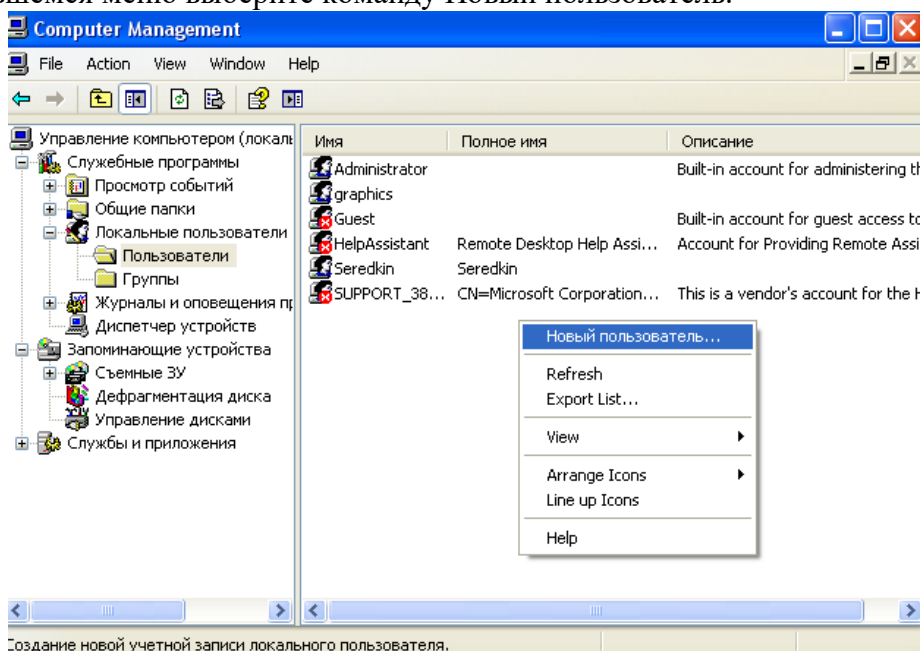
Управление компьютером

Создание новой учетной записи пользователя:

1. Откройте компонент «Управление компьютером».
2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Пользователи



3. Нажмите правой кнопкой мыши в окне со списком пользователей и в появившемся меню выберите команду Новый пользователь.



4. Введите соответствующие сведения в диалоговое окно.

Новый пользователь

Пользователь:

Полное имя:

Описание:

Пароль:

Подтверждение:

☒ Потребовать смену пароля при следующем входе в систему

☐ Запретить смену пароля пользователем

☐ Срок действия пароля не ограничен

☐ Отключить учетную запись

Создать Закрыть

5. Установите или снимите перечисленные ниже флажки.

☒ Потребовать смену пароля при следующем входе в систему

☐ Запретить смену пароля пользователем

☐ Срок действия пароля не ограничен

☐ Отключить учетную запись

Потребовать смену пароля при следующем входе в систему – при входе в систему пользователю будет выведено сообщение о смене пароля.

Запретить смену пароля пользователем – пользователь не сможет изменять пароли других пользователей в системе.

Срок действия пароля не ограничен – по истечению срока действия пароля, при входе в систему пользователю будет выводиться сообщение о блокировке учетной записи.

Отключить учетную запись – вход в систему для данного пользователя будет не возможен.

6. Выполните одно из следующих действий.

Чтобы создать дополнительного пользователя, нажмите кнопку Создать и повторите шаги 2 и 3.

Чтобы завершить работу, нажмите кнопку Создать, а затем Закрыть.

Изменение учетной записи пользователя

1. Откройте компонент «Управление компьютером».

2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем учет Пользователи

3. Выберите учетную запись, которую требуется изменить.

4. В меню Действие выберите команду Свойства и произведите изменения.

5. Внесите нужные изменения и нажмите кнопку ОК.

Изменение пароля для пользователя

1. Откройте компонент «Управление компьютером».

2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Пользователи.

3. Выберите учетную запись, которую требуется изменить.

4. В меню Действие выберите команду Установка пароли.

Отключение и активизации учетной записи пользователя

1. Откройте компонент «Управление компьютером».

2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Пользователи
3. Выберите учетную запись, которую требуется изменить.
4. В меню Действие выберите команду Свойства.
5. Чтобы отключить выбранную учетную запись пользователя, установите флажок

☐ Отключить учетную запись

Чтобы активизировать выбранную учетную запись пользователя, снимите флажок

☐ Отключить учетную запись

Удаление учетной записи пользователя

1. Откройте компонент «Управление компьютером».
2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Пользователи
3. Выберите учетную запись, которую требуется удалить.
4. В меню Действие выберите команду Удалить
5. В окне подтверждения удаления нажмите кнопку ОК.
6. В отвоз на приглашение подтвердить удаление нажмите кнопку Да.

Переименование учетной записи пользователя

1. Откройте компонент «Управление компьютером».
2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Пользователи
3. Выберите учетную запись, которую требуется переименовать.
4. В меню Действие выберите команду Переименовать.
5. Введите новое имя пользователя и нажмите клавишу ENTER.

Управление группами пользователей

Пользователь, принадлежащий группе, имеет все права на разрешения, предоставленные этой Группе. Пользователь, являющийся членом нескольких групп, имеет все права и разрешения, предоставленные каждой из этих групп.

При удалении локальной группы удаляется учетная запись группы. Учетные записи пользователей и глобальных групп, являющихся членами удаленной группы, при этом не удаляются.

Создание новой локальной группы

1. Откройте компонент «Управление компьютером».
2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Группы.
3. В меню Действие выберите команду Новая группа.
4. Введите имя новой группы в поле Имя группы
5. Введите описание новой группы в поле Описание
6. Выполните одно из следующих действий.
Чтобы создать другую группу, нажмите кнопку Создать и повторите шаги 2 и 3.
Чтобы завершить работу, нажмите кнопку Создать, а затем Заккрыть.

Добавление пользователя в группу

1. Откройте компонент «Управление компьютером».
2. В дереве консоли выберите компонент «Локальные пользователи и группы» и выберите в нем узел Группы.
3. Выберите нужную группу.
4. В меню Действие выберите команду Свойства.
5. Нажмите кнопку Добавить.
6. В нижнее поле введите имена пользователей или групп, которые нужно добавить, или выберите имена пользователей или групп из верхнего поля и нажмите кнопку Добавить.
7. Если необходимо проверить имена добавляемых пользователей или групп.

Нажмите кнопку Проверить имена.

8. Добавив имена всех требуемых пользователей, нажмите кнопку ОК.

Удаление локальной группы

1. Откройте компонент «Управление компьютером».

2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Группы.

3. Выберите Группу, которую следует удалить.

4. В меню Действие выберите команду Удалить.

5. В ответ на приглашение Подтвердить удаление нажмите кнопку Да.

Контрольные вопросы:

1. Дайте определение «локальный пользователь или группа».
2. Почему пользователи и группы важны для безопасности ОС?
3. Какие встроенные учетные записи вы знаете?
4. Расскажите об учетной записи администратора, гостя.
5. Поясните следующие группы: администраторы, операторы архива, опытные пользователи, пользователи, гости.
6. Как осуществляется управление учетной записью пользователя?
7. Как создать новую учетную запись пользователя?
8. Как изменить учетную запись пользователя?
9. Как осуществляется управление группами пользователей?
10. Как создать новую локальную группу? Как добавить пользователя в группу?