Министерство образования и науки РФ

Томский государственный университет систем управления и радиоэлектроники

Конев А.А., Костюченко Е.Ю., Сопов М.А.

Методические указания по проведению лабораторных работ для специальности 040101 «Социальная работа»

Семестр 9

Лабораторные работы 14 часов

2012

Содержание

1. Лабораторная работа №1 «Защита персональных данных»

Цель: получение основных навыков при работе с персональными данными.

Задание:

1. Определить полный перечень персональных данных, обрабатываемых в организации.
2. Определить категории обрабатываемых персональных данных.
3. Определить перечень сотрудников работающих с персональными данными и для каждого установить перечень ПДн.
4. Определить класс информационной системы обработки ПДн
5. Описать соответствующие меры по защите ПДн.

Описание:

Задание выполняется в соответствии с лекционным материалом и дополнительной литературой к данной лабораторной работе.

Контрольные вопросы:

1. Что такое персональные данные?
2. На основании, каких документов составляется перечень ПДн?
3. Перечислите все категории ПДн.
4. Какими критериями служат для определения категории ПДн?
5. На основании, каких документов определяется перечень сотрудников обрабатывающих ПДн.
6. Что такое класс информационной системы обработки ПДн?
7. Опишите методику определения класса информационной системы обработки ПДн.
8. Назовите основные организационные меры которые используются для защиты ПДн.
9. Назовите основные виды программных и программно-аппаратных средств, использующихся при защите ПДн.

Литература:

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных";

2. Приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»;

3. Постановление Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

4. Постановление Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

5. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»

2. Лабораторная работа №2 «Защита компьютерной информации на уроне доступа в систему».

Цель:

изучение основных средств администрирования учетных записей пользователей в семействе ОС Windows и групп пользователей. Настройка локальной политики безопасности: пользователей, паролей, блокировки учетной записей, прав пользователей и настроек безопасности операционной системы.

Задание:

1. Создать и настроить учетную запись пользователя.
2. Настроить локальную политику безопасности для пользователя.

Описание:

Управление учётными записями локальных пользователей

1.1 В контекстном меню значка «Мой компьютер» откройте «Управление». Выберите «Локальные пользователи и группы», рис. 1.

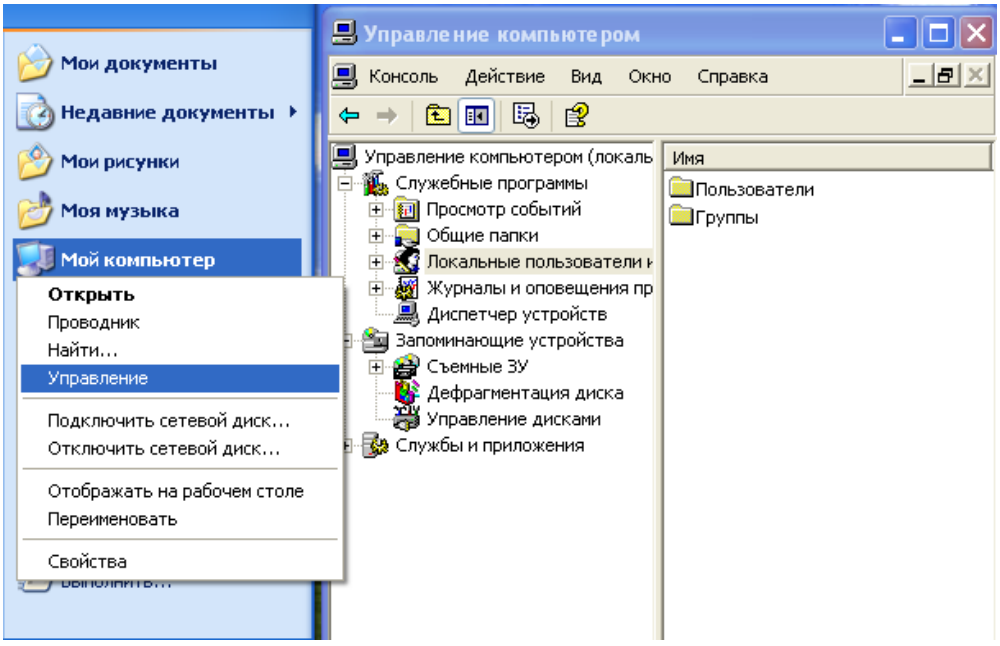


Рисунок 1 – Управление компьютером

1.2. В контекстном меню папки «Пользователи» правой половины окна (или в меню «Действие») выберите элемент «Новый пользователь», рис. 2.

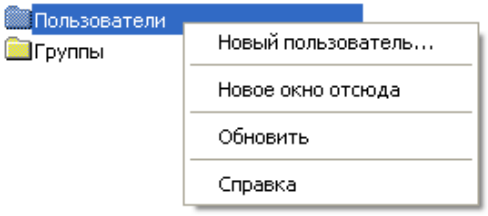


Рисунок 2 – Создание учетной записи

Введите имя учетной записи, а также пароль и его подтверждение. Создайте учётную запись пользователя, рис. 3. Если требуется смена пароля при следующем входе в систему, установите флажок «Потребовать смену пароля при следующем входе в систему». Сразу после успешной аутентификации пользователь получает запрос на смену пароля, в ответ на который он должен задать новый пароль. Этот подход необходимо использовать в тех случаях, когда администратор системы не должен знать пароли пользователей. Если установлен этот флажок, вы не можете установить флажки «Запретить смену пароля пользователем» и «Срок действия пароля не ограничен».

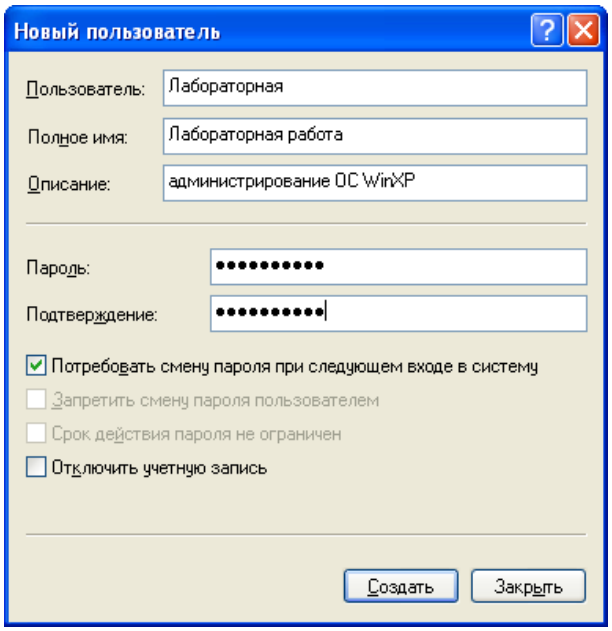


Рисунок 3 – Настройка параметров учетной записи

Если пользователь забыл свой пароль, то член группы «Администраторы» может сбросить старый пароль при помощи функции «Задать пароль», рис. 4.

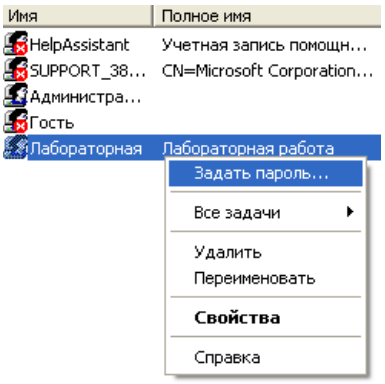


Рисунок 4 – Функция «Задать пароль»

1.3 Откройте «Свойства» созданной учётной записи. На вкладке «Членство в группах» добавьте пользователя в группу «Опытные пользователи», рис. 5.

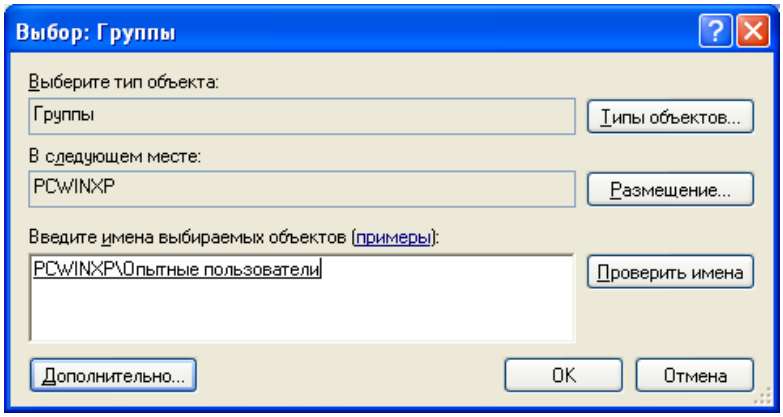


Рисунок 5 – Добавление пользователя в группу.

1.4 В папке «Группы» откройте свойства группы «Опытные пользователи» и проверьте наличие в группе только что добавленного пользователя. Создайте новую группу и добавьте в неё этого же пользователя, рис. 6.

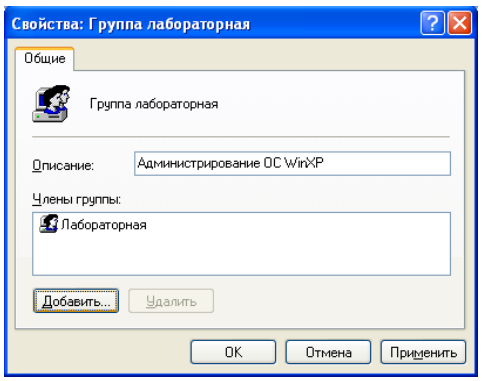


Рисунок 6 – Создание группы

2. Настройка локальной политики безопасности

2.1 Откройте оснастку «Локальная политика безопасности». (Пуск – Панель управления – Администрирование – Локальная политика безопасности). Главный вид окна оснастки представлен на рис. 7. Значения параметров, заданные при настройке политики, будут применяться ко всем пользователям локального компьютера.

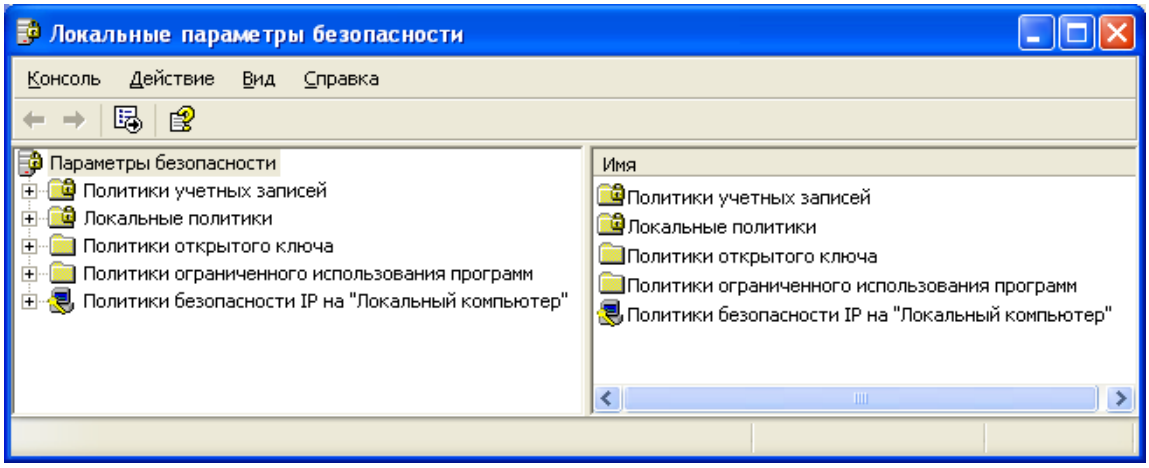


Рисунок 7 – Локальная политика безопасности

2.2 Выберите раздел «Политики паролей». (Параметры безопасности – Политики учётных записей – Политики паролей). Настройки, входящие в раздел «Политики паролей» представлены на рис. 8.

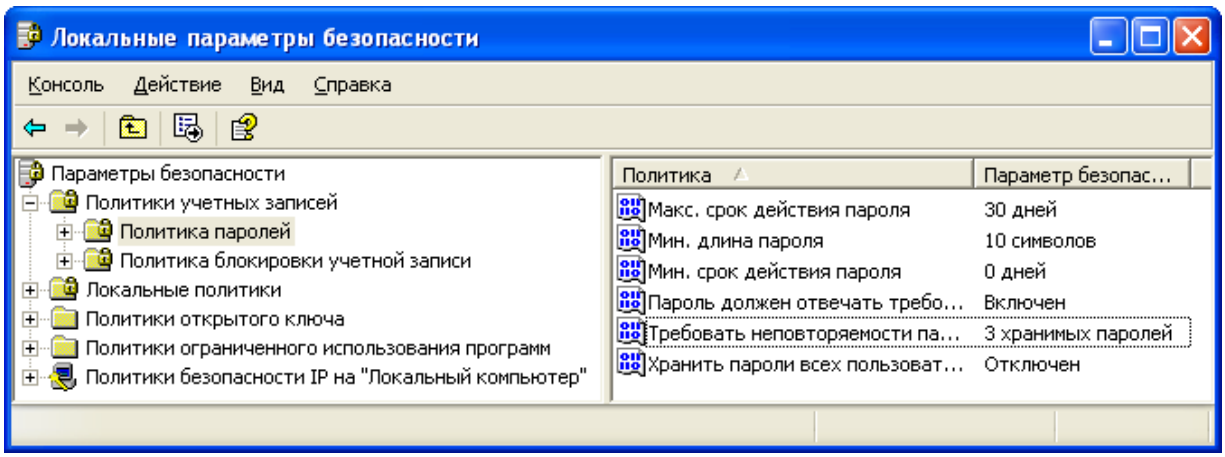


Рисунок 8 – Параметры раздела «Политика паролей»

– Установите максимальный срок действия пароля – 30 дней.

– Установите минимальную длину пароля – 10 символов.

– Для параметра «Требовать неповторяемости паролей» (рис. 9) установите значение 3 хранимых пароля, означающее, что новый пароль должен отличаться от 3 последних паролей пользователя.

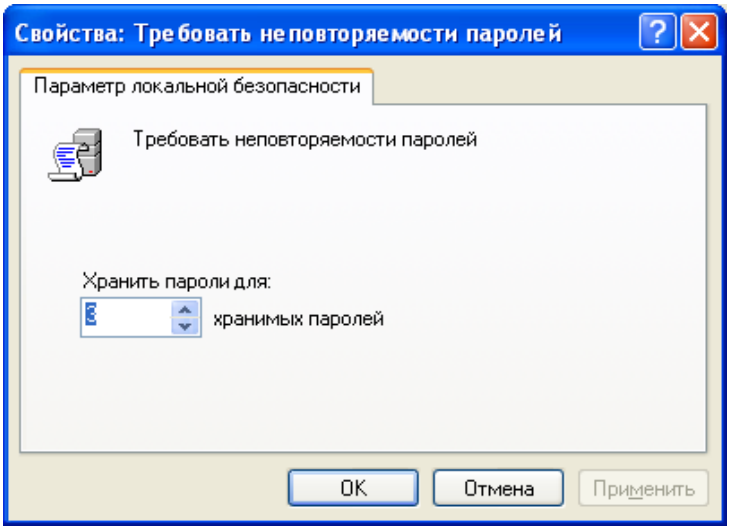


Рисунок 9 – Параметр «Требовать неповторяемости паролей»

– Включите параметр «Пароль должен отвечать требованиям сложности» (рис. 10).

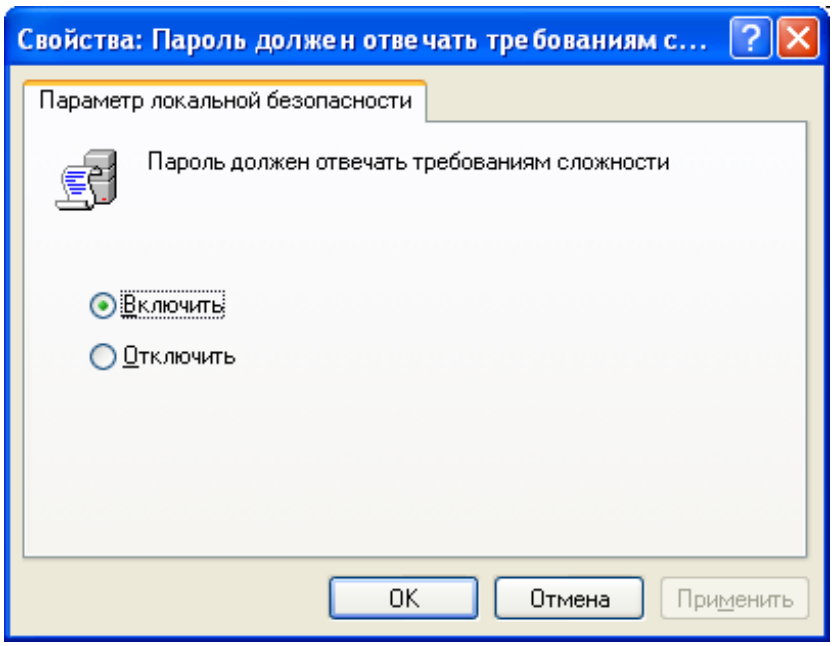


Рисунок 10 – Параметр «Пароль должен отвечать требованиям сложности»

Примечание: этот параметр безопасности определяет требования сложности для паролей. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям:

– пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

– пароль должен состоять не менее чем из шести символов;

– в пароле должны присутствовать символы трех категорий из числа следующих четырех:

1. прописные буквы английского алфавита от A до Z;

2. строчные буквы английского алфавита от a до z;

3. десятичные цифры (от 0 до 9);

4. неалфавитные символы (например, !, $, #, %).

Проверка соблюдения этих требований выполняется при изменении или создании паролей.

Таким образом, можно избавиться от легко подбираемых паролей типа «111», «qwerty», «12345» и т.д.

2.3 Выберите раздел «Политика блокировки учётной записи» (Параметры безопасности – Политики учётных записей – Политика

блокировки учетной записи). У созданной учетной записи попытайтесь заменить пароль на более простой (например: abc12345) после чего на пароль удовлетворяющий требованиям.

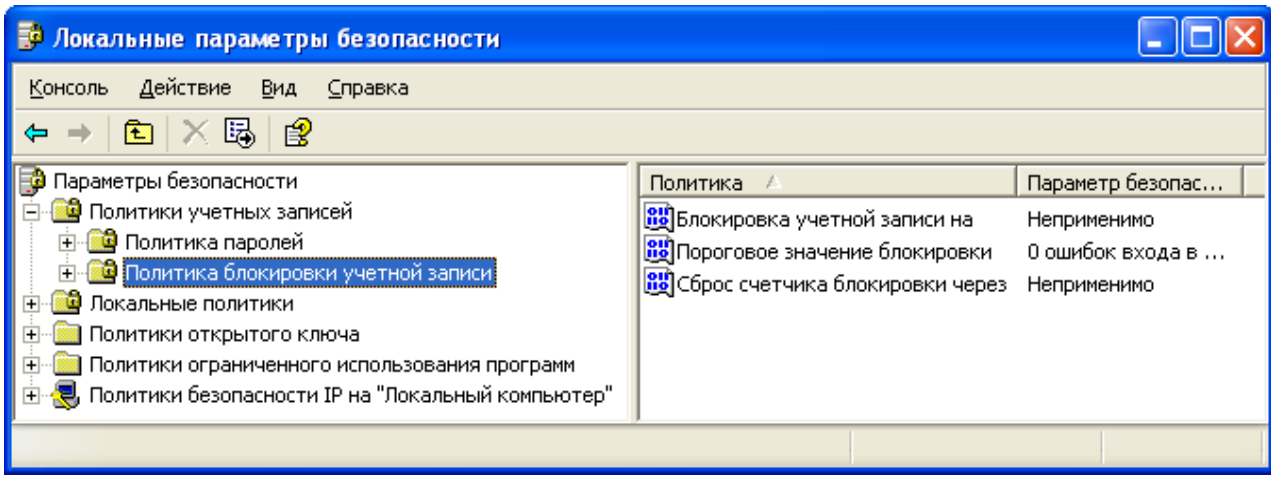


Рисунок 11 – Параметры раздела «Политика блокировки учетной записи».

Настройте параметры следующим образом:

– установить пороговое значение блокировки, равное 3 ошибкам входа в систему (после 3 неудачных попыток входа учётная запись блокируется);

– установить длительность блокировки в параметре «Блокировка учётной записи на» (рис. 12), равную 30 мин (значение 0 означает, что блокировку может снять только администратор);

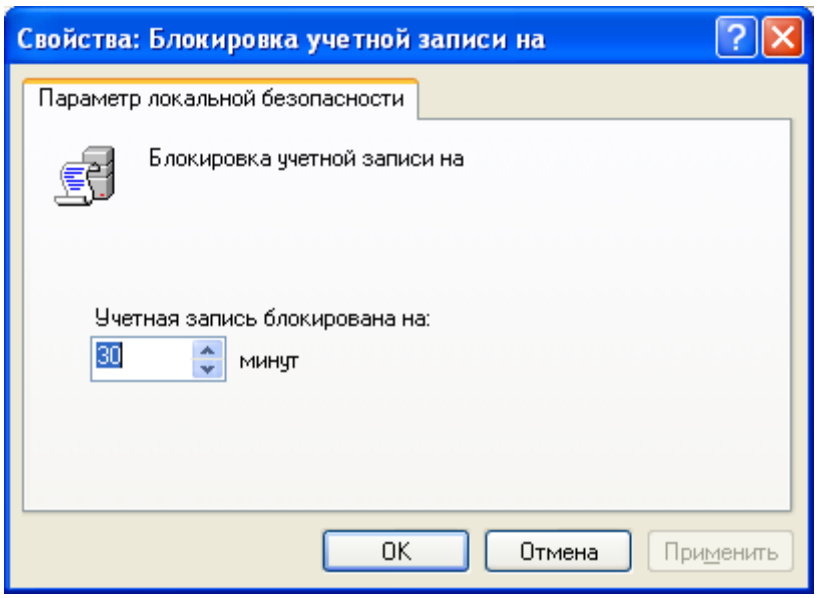


Рисунок 12 – Параметр «Блокировка учетной записи на»

– установите сброс счётчика блокировки через 15 мин. Если в течение установленного времени будет 3 неудачных попытки входа, то учётная запись блокируется. Если неудачных попыток в течении установленного времени будет меньше, то опять допускается 3 неудачных попытки (значение этого параметра не должно превышать длительность блокировки учётной записи).

2.4 Выберите раздел «Назначение прав пользователя». (Параметры безопасности – Локальные политики – Назначение прав пользователя). При входе с систему под учетной записью пользователя 3 раза введите неправильный пароль. Разблокируйте учетную запись. Настройками этого раздела являются права, которыми можно наделять пользователей или группы пользователей (примеры прав: архивирование и восстановление файлов и каталогов, загрузка и выгрузка драйверов устройств, изменение системного времени).

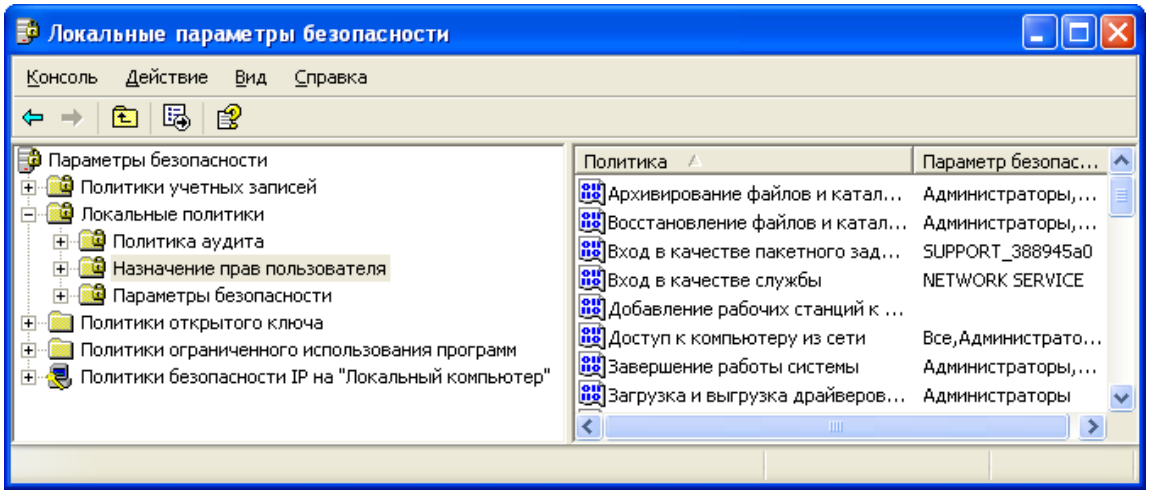


Рисунок 13 – Параметры раздел «Назначение прав пользователя».

Присвоение права «Завершение работы системы»:

– в свойствах выбранного параметра (рис. 14) удалите все группы, кроме группы «Администраторы»;

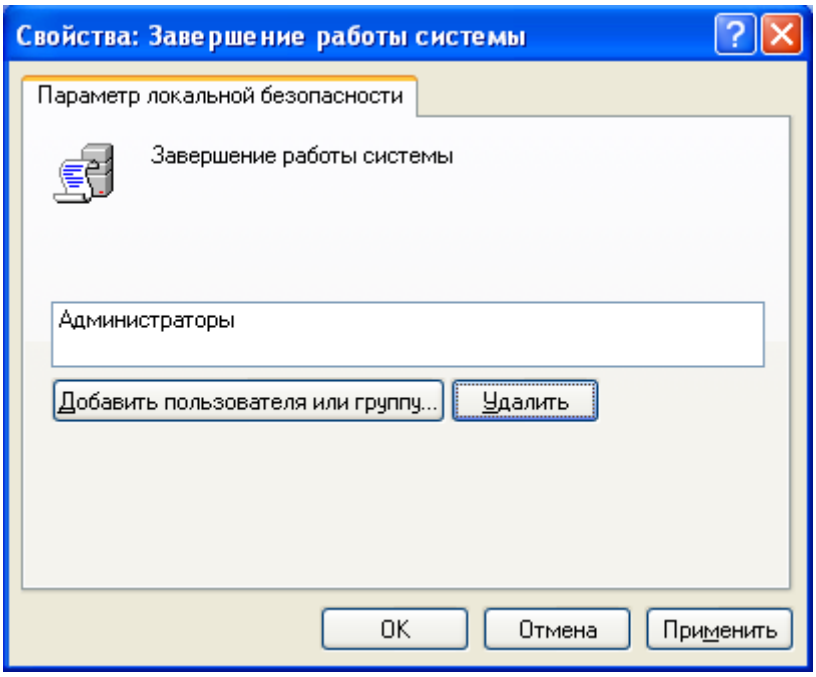


Рисунок 14 – Настройка параметра «Завершение работы системы»

– нажмите «Добавить пользователя или группу»;

– нажмите кнопку «Типы объектов» и добавьте в параметры поиска тип «Группы»;

– выберите искомую группу, рис. 15.

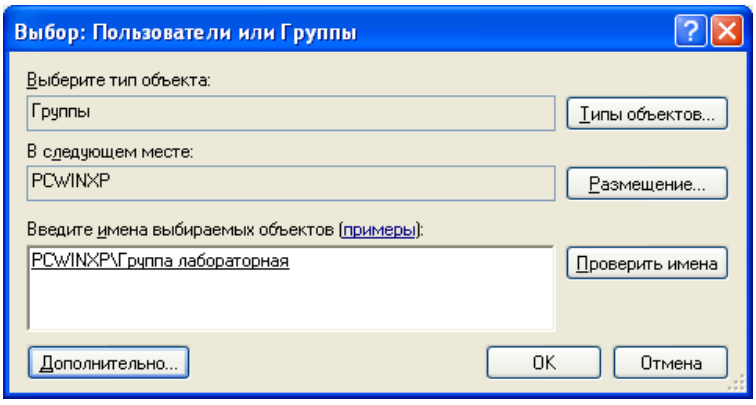


Рисунок 15 – Выбор пользователя или группы пользователей

Таким образом, пользователи, входящие в выбранную группу, в дополнение к правам групп «Пользователи» и «Опытные пользователи» получают право на завершение работы системы.

Проверьте возможность завершения работы системы пользователем созданным в п.1.2. Под учетной записью администратора удалите созданного пользователя из группы, созданной в п. 1.4. Проверьте возможность завершение работы системы созданным пользователем.

Право «загрузка и выгрузка драйверов».

Этот параметр безопасности определяет, какие пользователи могут динамически загружать и выгружать драйверы устройств или другой код в режим ядра. Это право пользователя не применяется для драйверов устройств «Plug and Play».

Право «Закрепление страниц в памяти».

Этот параметр безопасности определяет, какие учетные записи могут использовать процесс для хранения данных в физической памяти, избегая подкачки страниц в виртуальную память на диске. Применение этой привилегии может существенно сказаться на системной производительности, поскольку приводит к уменьшению объема свободной оперативной памяти.

Право «Изменение системного времени».

Это право пользователя определяет, какие пользователи и группы могут изменять время и дату на встроенных часах компьютера. Пользователи, обладающие данным правом, могут изменять представление журналов безопасности. При изменении системного времени события будут заноситься в журнал с указанием измененного, а не реального времени.

Право «Локальный вход в систему».

Это право пользователя определяет пользователей, имеющих возможность интерактивно входить в систему. Данное право необходимо для входа пользователя в систему после одновременного нажатия клавиш CTRL+ALT+DEL на клавиатуре компьютера. Кроме того, это право на вход в систему может понадобиться некоторым службам или административным приложениям, во время работы которых происходит вход пользователей в систему.

Право «Отладка программ».

Это право пользователя определяет, какие пользователи могут запускать режим отладки для любого процесса или ядра. Разработчики, запускающие процесс отладки для собственных приложений, не нуждаются в предоставлении данного права пользователя. Данное право необходимо

предоставить разработчикам, запускающим процесс отладки для новых системных компонент. Эта привилегия обеспечивает широкие возможности доступа к особо важным компонентам операционной системы.

Право «Увеличение приоритета диспетчирования».

Этот параметр безопасности определяет, какие учетные записи могут использовать процесс, обладающий разрешением «Запись свойства» для доступа к другому процессу, с целью повысить назначенный последнему приоритет выполнения. Пользователь, обладающий этой привилегией, может изменять приоритет планирования процесса в окне диспетчера задач.

2.5 Выберите раздел «Параметры безопасности» (Параметры безопасности – Локальные политики – Параметры безопасности). Настройка параметров раздела позволяет изменять настройки операционной системы, каким-либо образом, влияющие на безопасность.

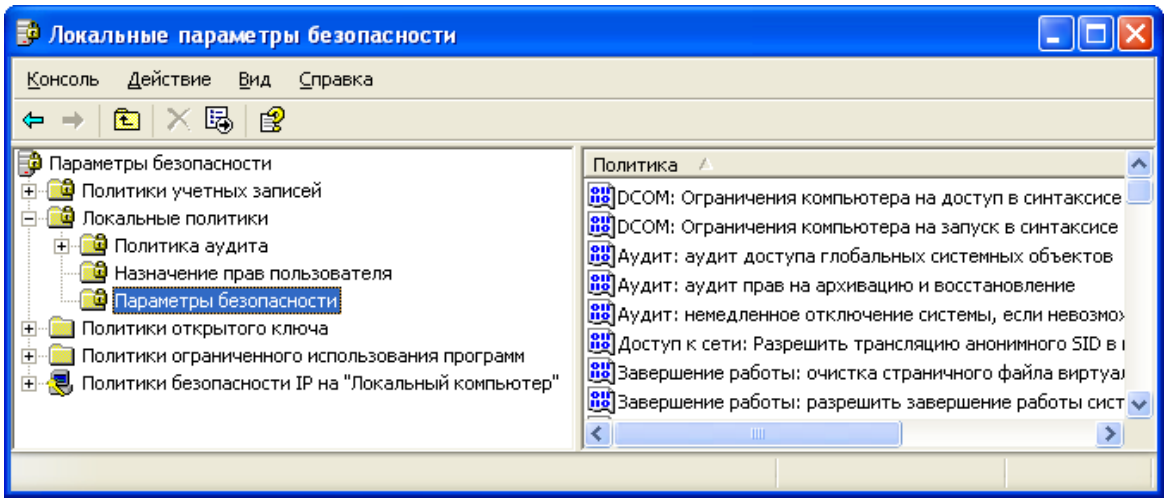


Рисунок 16 – Параметры группы «Параметры безопасности»

Измените следующие настройки.

– Применительно к «Завершению работы», – отключить параметр «разрешить завершение работы системы без выполнения входа в систему», рис. 17;

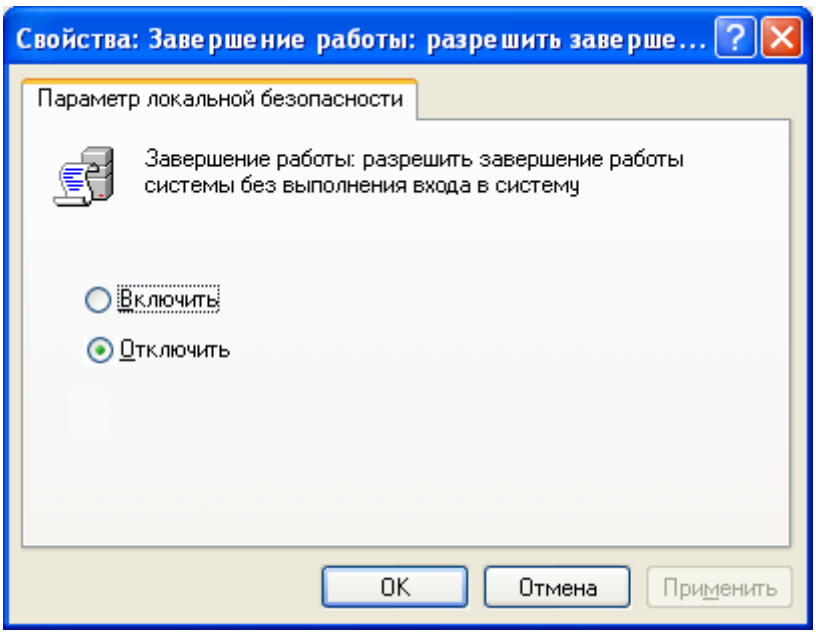


Рисунок 17 – Параметр «Разрешить завершение работы без выполнения входа в систему»

– Применительно к «Интерактивный вход в систему», – включите параметр «не отображать последнего имени пользователя» (рис. 18) и установить значение параметра «напоминать пользователям об истечении срока действия пароля заранее», равным 3 дням.

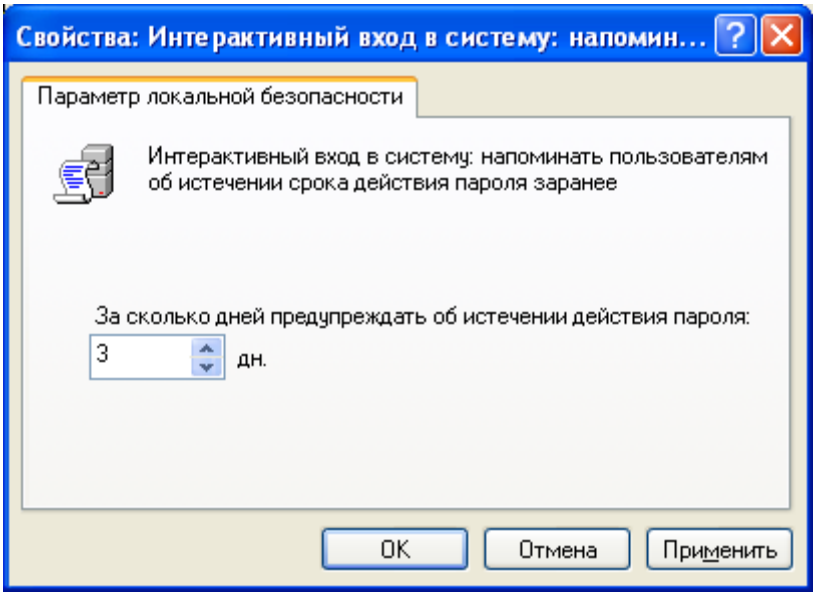


Рисунок 18 – Параметр «Напоминать пользователям об истечении срока действия пароля заранее»

– Применительно к «интерактивный вход в систему», отключите параметр «не требовать нажатия CTRL+ALT+DEL». Этот параметр

безопасности определяет, должен ли пользователь, прежде чем войти в систему, нажать клавиши CTRL+ALT+DEL.

Если эта политика включена на компьютере, пользователь не должен для входа в систему нажимать CTRL+ALT+DEL. В таком случае компьютер становится уязвимым для атак, основанных на перехвате паролей пользователей. Если потребовать нажатия клавиш CTRL+ALT+DEL перед входом в систему, то пользователям будет гарантирован надежно защищенный канал передачи паролей.

Если эта политика отключена, то любой пользователь должен будет перед входом в Windows нажимать CTRL+ALT+DEL (если только он не входит в систему с помощью смарт-карты).

– Применительно к «Устройства», – включите параметр «запретить пользователю установку драйверов принтера».

Чтобы локальный компьютер мог выполнять печать на сетевом принтере, необходимо установить на компьютере драйвер этого принтера. Данный параметр безопасности определяет, кому при добавлении сетевого принтера разрешается устанавливать драйвер принтера. Если параметр включен, то устанавливать драйвер при добавлении сетевого принтера разрешается только группам «Администраторы» и «Опытные пользователи». Если параметр отключен, то устанавливать драйвер при добавлении сетевого принтера может любой пользователь.

– Применительно к «Устройства», – параметр «разрешено форматировать и извлекать съемные носители» (рис. 19) разрешите группам пользователей «Администраторы», «Опытные пользователи».

Этот параметр безопасности определяет каким пользователям разрешается форматировать съемные носители NTFS и извлекать их из устройств.

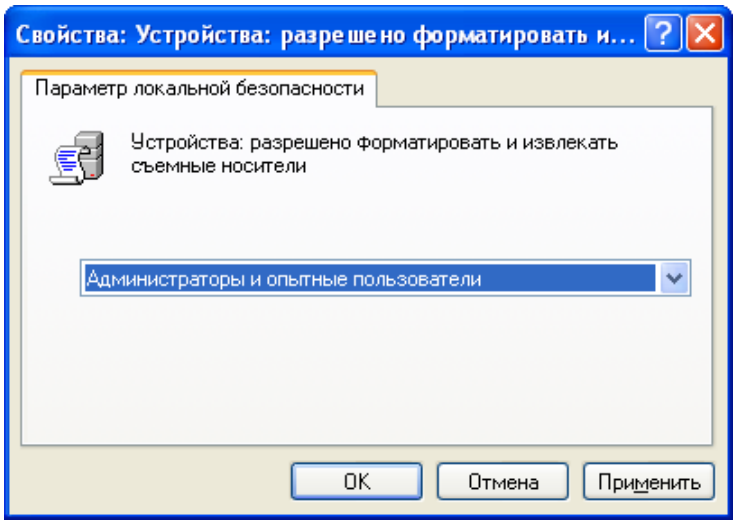


Рисунок 19 – Параметр «Разрешено форматировать и извлекать съемные носители»

– Измените параметр «Переименование учетной записи администратора» (рис. 20), переименование учетной записи усложнит пользователям, не имеющим доступа в систему, процесс угадывания имени пароля пользователя с правами администратора. Этот параметр определяет, следует ли сопоставить идентификатору безопасности (SID) учетной записи Администратор другое имя учетной записи;

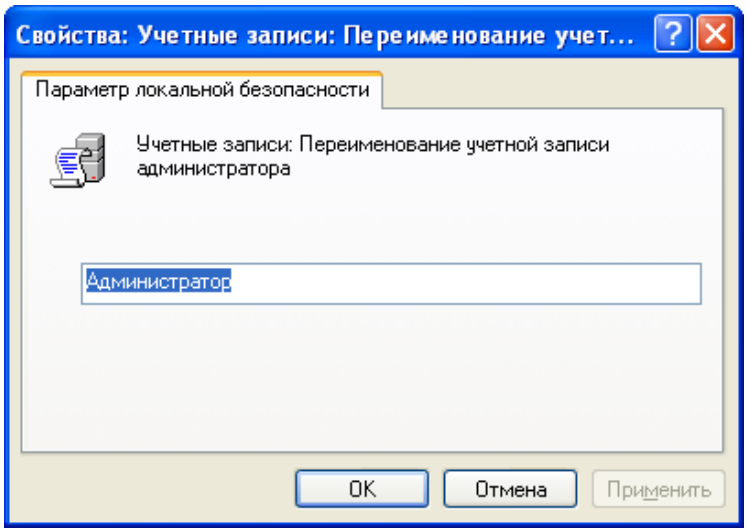


Рисунок 20 – Параметр «Переименование учетной записи администратор»

2.6 Проверьте наличие прав, которыми был наделён пользователь в п.2.4 (проверить возможность завершения работы системы; под учётной записью администратора удалить пользователя из группы, созданной в п. 1.4;

проверить возможность завершения работы системы пользователем с учётной записью, созданной в п. 1.2). Также проверьте следующие настройки: завершение работы без входа в систему, срок действия пароля, не требовать нажатия CTRL+ALT+DEL, переименование учетной записи администратора и состояние учетной записи гость.

Задание:

1. ознакомьтесь с ходом лабораторной работы;
2. создайте пользователя с именем вашей учетной записи в кафедральной сети и в соответствии с вариантом, выполните работу по администрированию. Все параметры и настройки применять к созданному в п.1.2. пользователю и созданной в п.1.4 группе;
3. подготовьтесь к контрольным вопросам.

Таблица 1 – Распределение вариантов

Вариант Параметр										0
максимальный срок действия пароля, дней										
минимальная длина пароля, символов					0				0	
требовать неповторяемости паролей, количество хранимых										
пароль должен отвечать требованиям сложности	кл	кл	кл	кл	кл	кл	кл	кл	кл	кл
пороговое значение блокировки, ошибок										
блокировка учётной записи на…, мин		0								0
сброс счётчика блокировки через…, мин										
разрешить право «Завершение										

работы системы»										
разрешить право «Увеличение приоритета диспетчирования»										
разрешить право «Локальный вход в систему»										
разрешить право «Изменение системного времени»										

Контрольные вопросы:

1. Поясните параметр «Потребовать смену пароля при следующем входе в систему».
2. При помощи какой функции, можно сбросить забытый пароль и кто может воспользоваться этой функцией?
3. Поясните параметр «Требовать неповторяемости паролей»
4. Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если политика включена.
5. Какие параметры входят в политику блокировки учетной записи?
6. Возможно ли, что учетная запись не будет блокирована при количестве ошибок большем, чем установленное пороговое значение?
7. В каком разделе предоставляется возможность назначать пользователям права, связанные с информационной безопасностью?
8. В каком разделе предоставляется возможность устанавливать параметры операционной системы, связанных с информационной безопасностью?

9. Перечислите параметры позволяющие предотвратить разглашение имен учетных записей, пользователей, активных в ОС.

10. Назовите параметр, обязывающий пользователей работать с надежным каналом передачи учетной информации в операционной системе.

Литература:

Нет

3. Лабораторная работа №3 «Защита от компьютерных вирусов».

Цель

Изучение основных принципов работы антивирусных программ и их настроек.

Задание

1. Установка антивирусной программы.
2. Настройка основных параметров.
3. Сканирование жесткого диска.
4. Обновление антивирусной программы.

Описание

1. Зайти на компьютеры с учетной записью 407_fio (инициалы). Например, Иванов Василий Петрович 407_ivp. Пароль 1234567890
2. Сменить пароль указав его 2 раза в графах новый пароль и подтверждение. Новый пароль должен быть не короче 10 символов.
3. Открыть сетевую папку \\cesir\vm\
4. Скопировать папку \\cesir\vm\vmwinxpavir в папку d:\vm\
5. Запустить виртуальную машину нажав на файл Windows XP Professional.vmx. При ответе на вопрос о происхождении машины выбрать вариант I copy it
6. Зарегистрироваться на виртуальной машине, использовав учетную запись Администратор пароль 12345
7. Скачать из папки \\cesir\install\soft\avir\avir установочный файл для антивируса в соответствии с вариантом
8. Произвести установку антивируса. Скриншоты этапов установки вставить в отчет с комментариями.
9. Скриншоты могут быть созданы следующим образом:

а) Скопировать в пямять изображение с экрана нажатием клавиши Print screen (Prt Scrn) для копирования всего экрана и одновременным нажатием клавиш Alt и Print screen (Prt Scrn) для копирования только активного окна.

б) Запустить редактор paint на виртуальной машине (Пуск/Выполнить mspaint).

в) Вставить скопированный образ нажатием одновременным клавиш Ctrl и V.

г)Сохранить полученное изображение на диске виртуальной машины.

10. После установки антивируса провести перезагрузку виртуальной машины (если требуется).

11. В установленном антивирусе рассмотреть параметры настройки сканера, мониторы, обновлений, другие настройки. Соответствующие скриншоты вставить в отчет с комментариями.

12. Попытаться запустить файл c:\1.exe. Рассмотреть реакцию монитора, провести удаление вируса в карантин. Соответствующие скриншоты вставить в отчет с комментариями.

13. Произвести сканирование жесткого диска виртуальной машины. Рассмотреть предлагаемые варианты действий при обнаружении вирусов. Провести очистку виртуальной машины от вирусов. Соответствующие скриншоты вставить в отчет с комментариями.

14. Посмотреть итоговый отчет о сканировании. Соответствующие скриншоты вставить в отчет с комментариями.

15. Провести попытку обновления антивирусных баз. Соответствующие скриншоты вставить в отчет с комментариями.

16. Скопировать папку со скриншотами из виртуальной машины на основную и забрать с собой для написания отчета.

17. Выключить виртуальную машину.

18. Удалить использованную виртуальную машину.

19. Выключить компьютер.

Контрольные вопросы

1. Назовите основные виды вирусов.
2. Назовите основные виды поиска вирусов.
3. Назовите основные виды антивирусных программ.

4. Перечислите основные настройки антивирусных программ.
5. Частота обновления антивирусных программ.

Литература

НЕТ

4. Лабораторная работа №4 «Защита от атак по локальным и глобальным сетям»

Цель

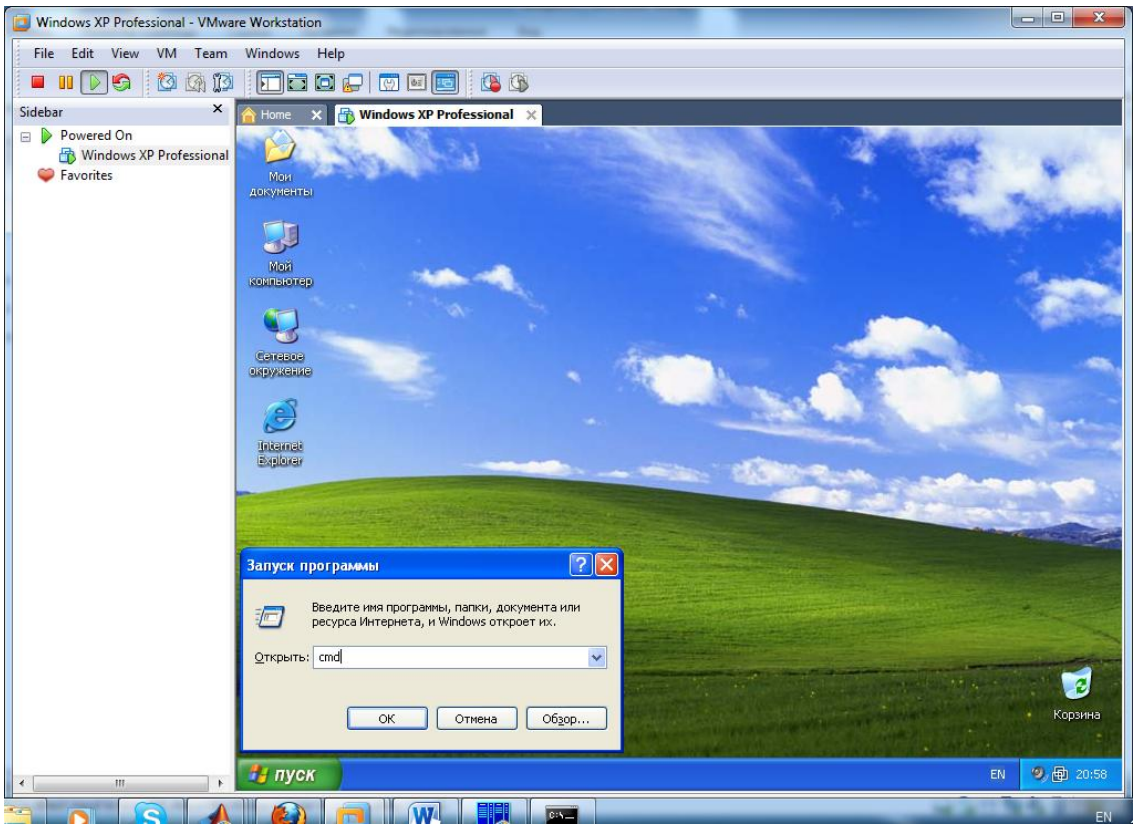
Изучение основных принципов защиты компьютеров в локальных и глобальных сетях.

Задание

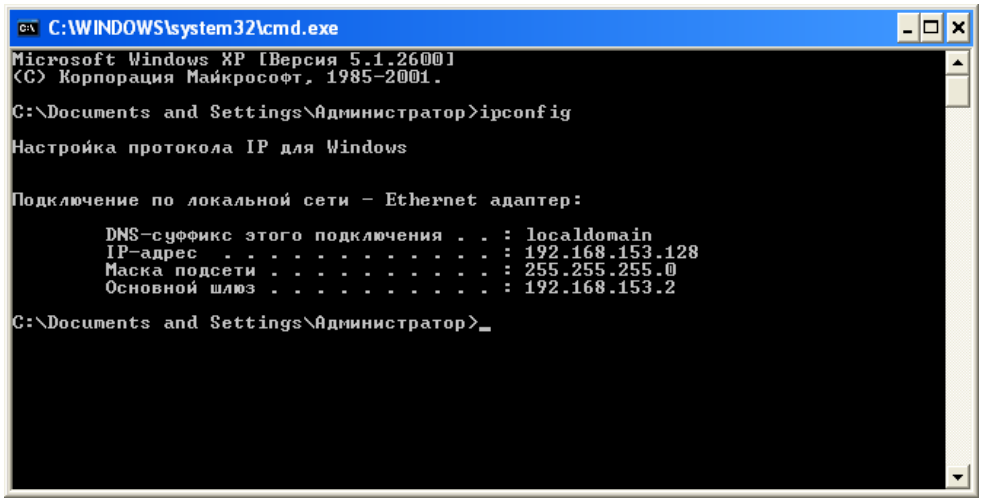
6. Установить файрвол.
7. Настроить параметры файрвола.
8. Создать разграничение доступа к сети.
9. Выполнить разрешенные и запрещенные действия в соответствии с настройками.
10. Просканировать сеть.

Описание

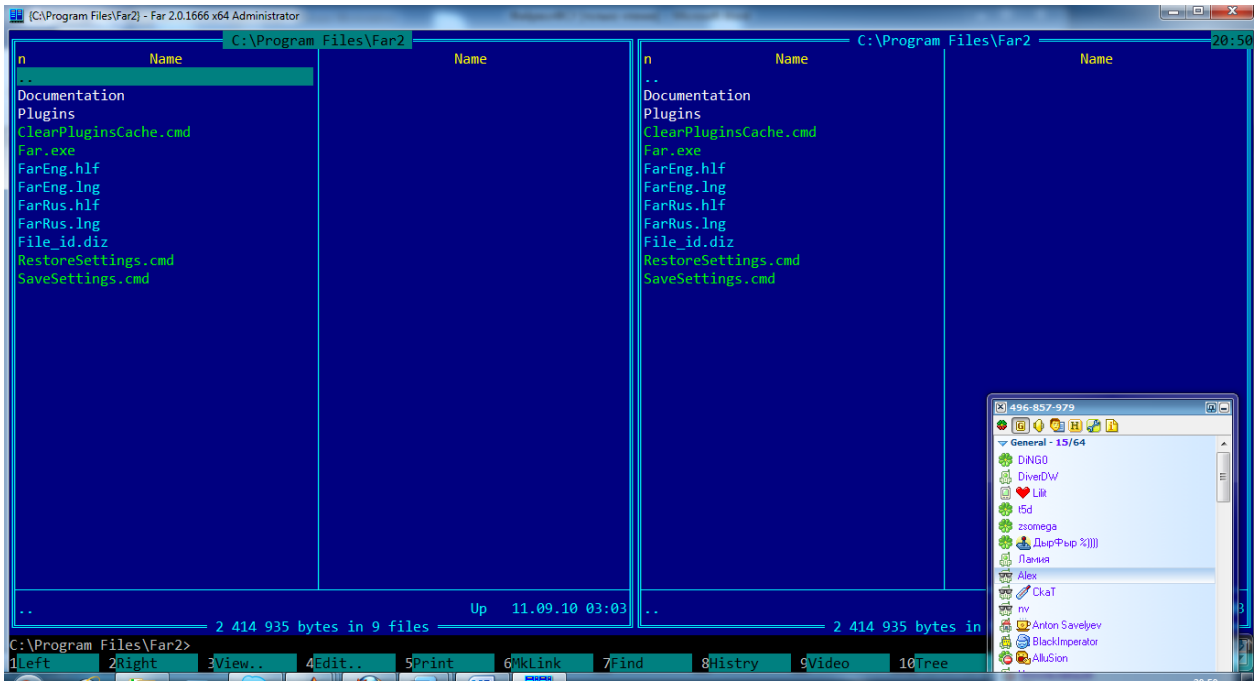
1. Зарегистрироваться на компьютере под своей учетной записью.
2. Запустить виртуальную машину по адресу d:\vm\vmwinxpfire. Логин Администратор, пароль 12345.
3. Определить IP адрес виртуальной машины. Для этого необходимо запустить на виртуальной машине командную строку через меню ПУСК/Выполнить cmd



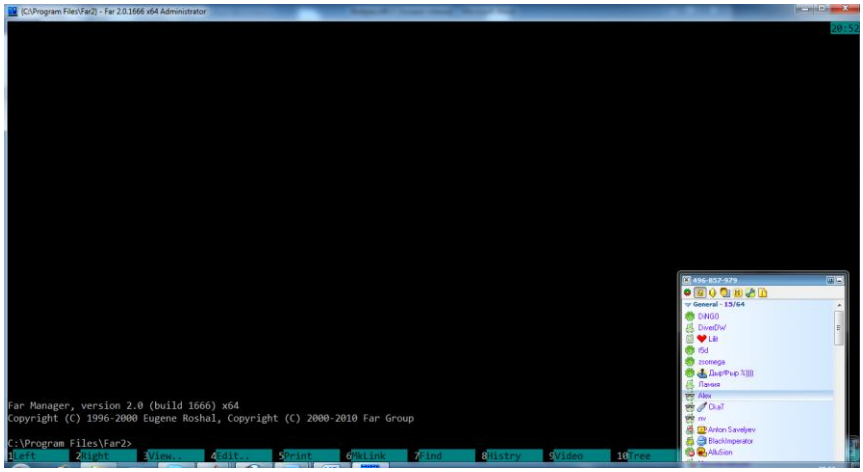
4. Выполнить команду IPCONFIG. Среди настроек сети найти IP адрес и записать его. В дальнейшем этот адрес будет называться IP адрес виртуальной машины (в примере 192.168.153.128). Сделайте скриншот с комментарием.



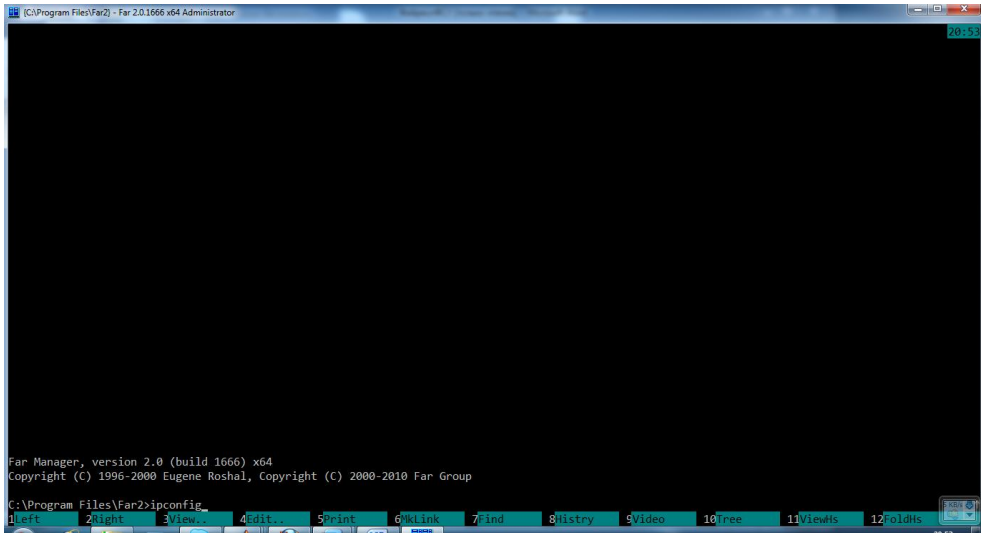
5. Определить IP адрес реального компьютера. Для этого необходимо на реальной машине запустить файловый менеджер FAR (Пуск/Программы/Far)



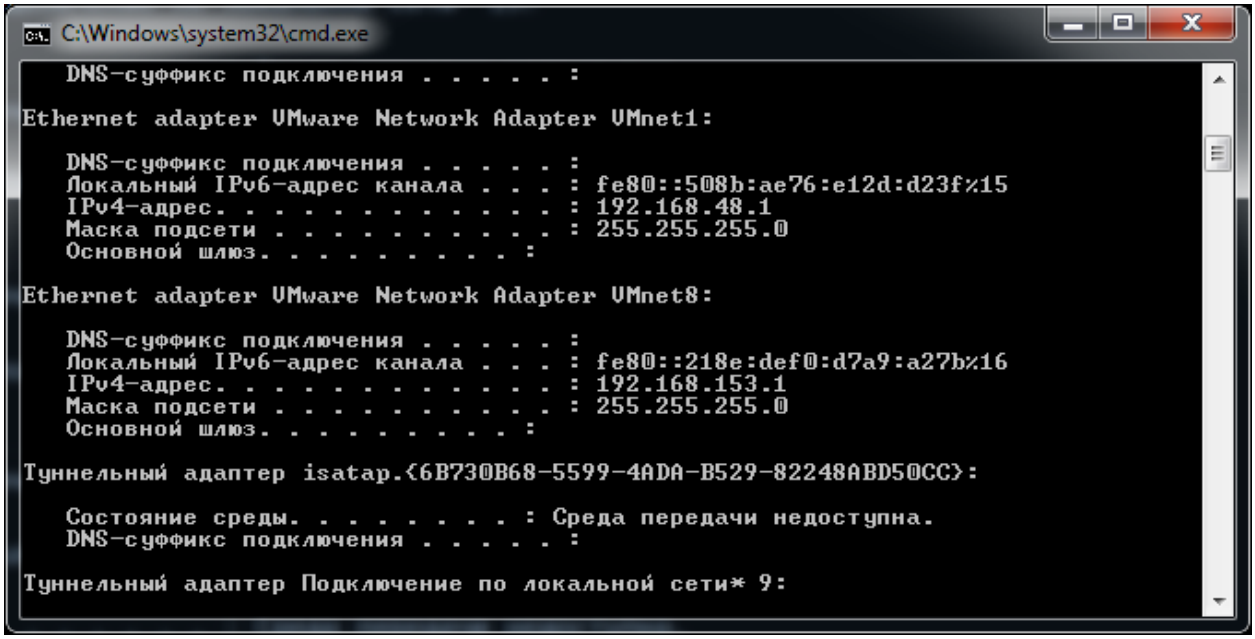
6. Нажать одновременно клавиши Ctrl+O, чтобы скрыть панели.



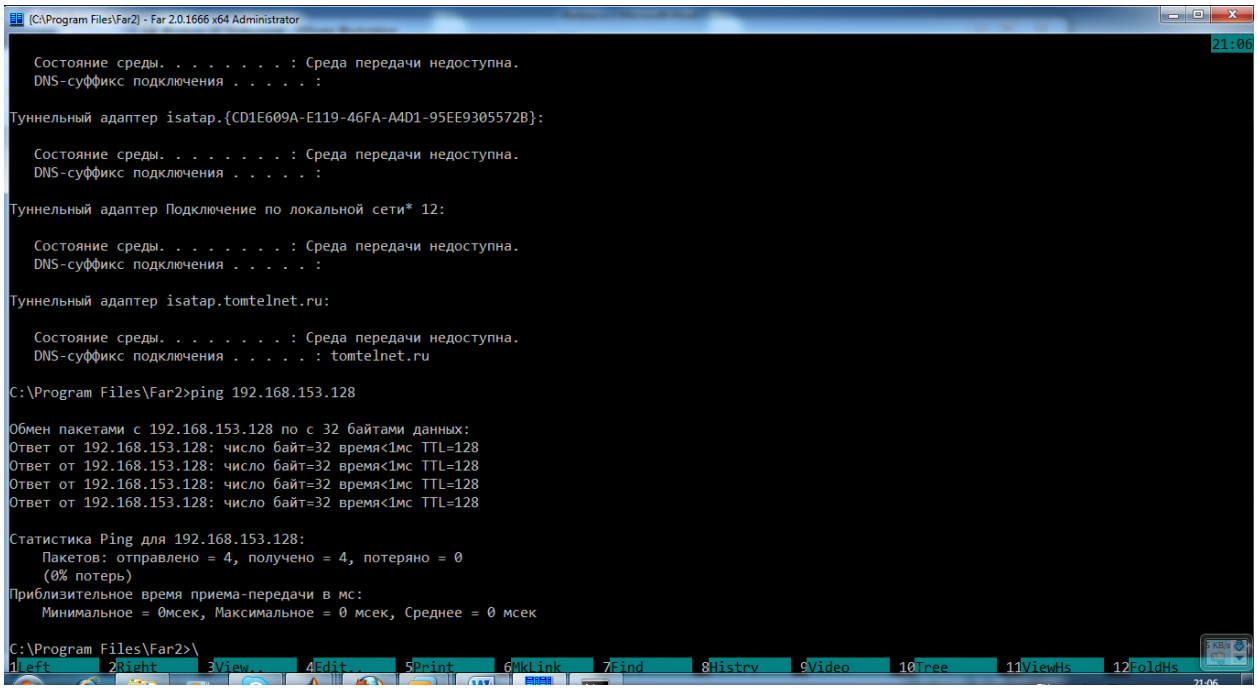
7. Выполнить команду IPCONFIG.



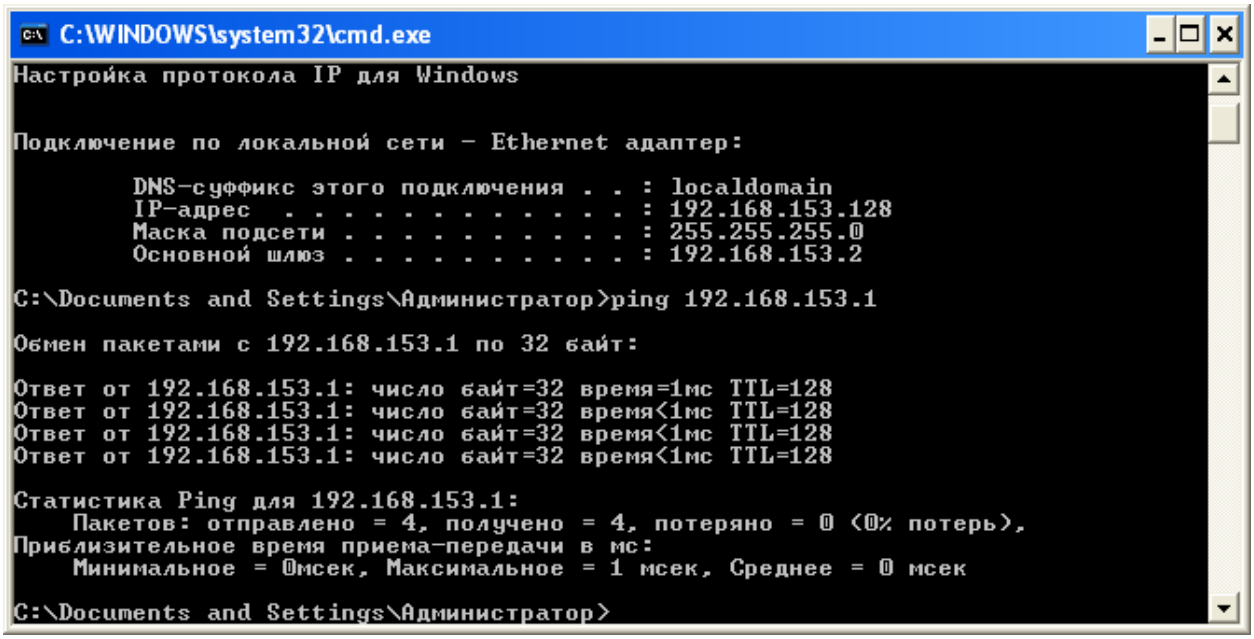
8. Среди настроек сети найти IP адрес, начинающийся на те же 3 числа, что и IP адрес виртуальной машины и записать его. В дальнейшем этот адрес будет называться IP адрес реальной машины. В нашем примере это 192.168.153.1. Сделайте скриншот с комментарием.



9. Проверить доступность виртуальной машины из реального компьютера, выполнив на реальной машине в Far команду PING <IP адрес виртуальной машины>. Сделайте скриншот с комментарием.



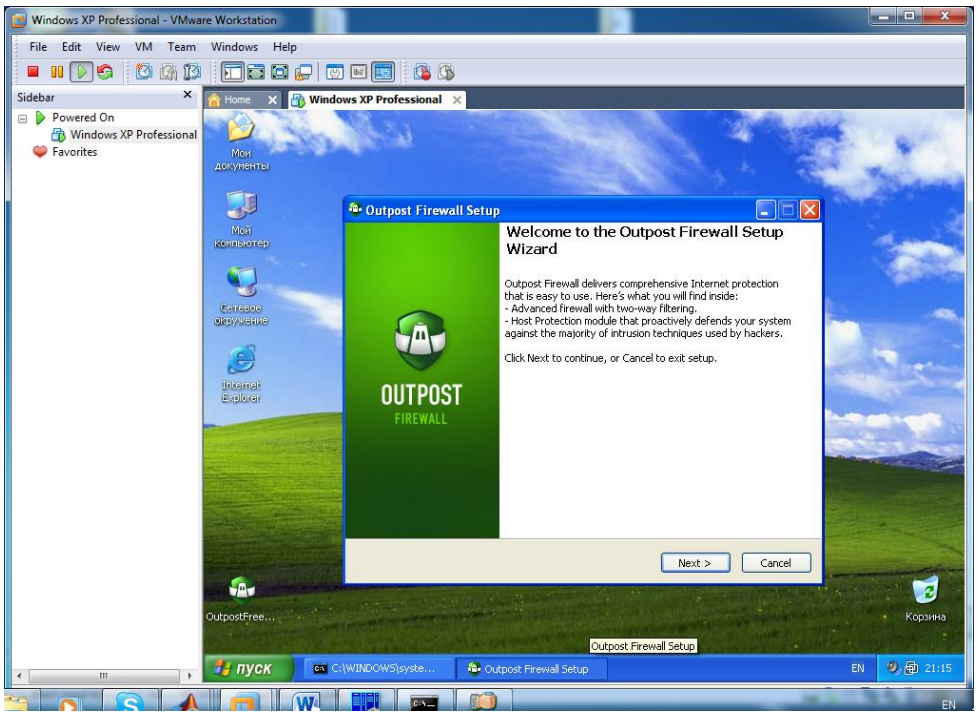
10. Проверить доступность реального компьютера из виртуальной машины, выполнив на виртуальной машине в командной строке команду PING <IP адрес реальной машины>. Сделайте скриншот с комментарием.



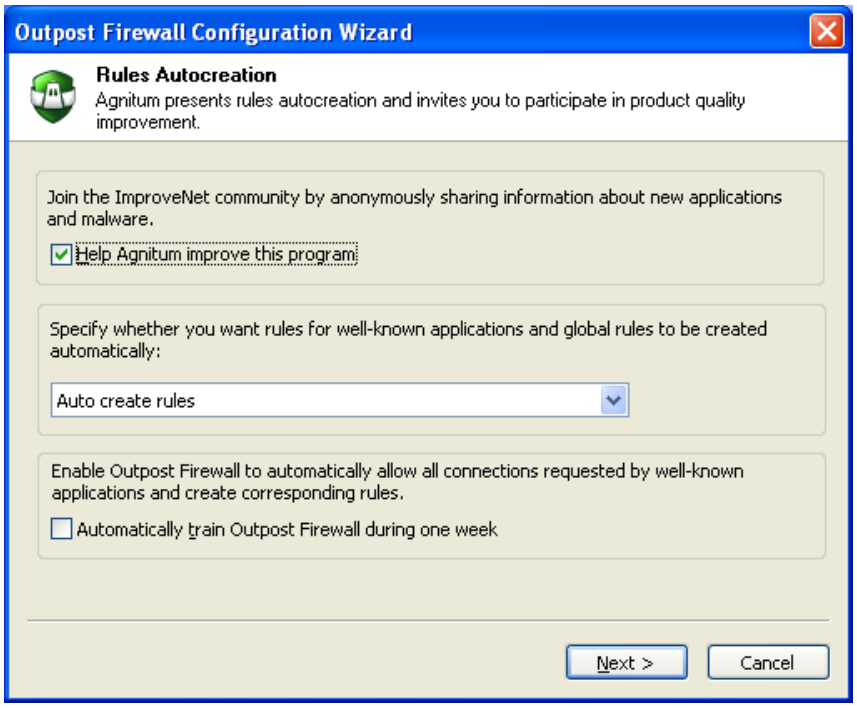
11. Взять файрвол Outpost Firewall Free по адресу \\cesir\install\soft\Firewall\OutpostFreeInstall.exe реальной машины.

12. Скопировать выбранный файрвол на виртуальную машину.

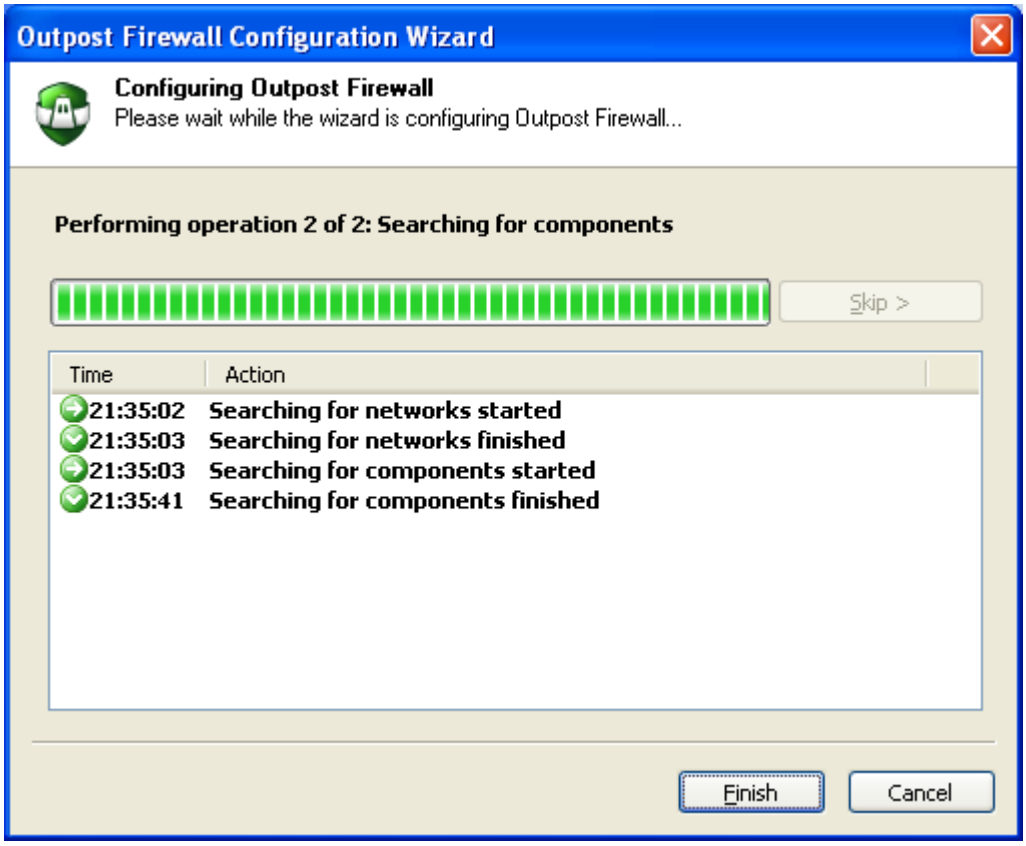
13. Провести установку файрвола. Процесс установки задокументировать скриншотами с комментариями.



14. На запрос о способе формирования правил оставьте настройки по умолчанию – автоматически на усмотрение программы. Сделайте скриншот с комментарием.



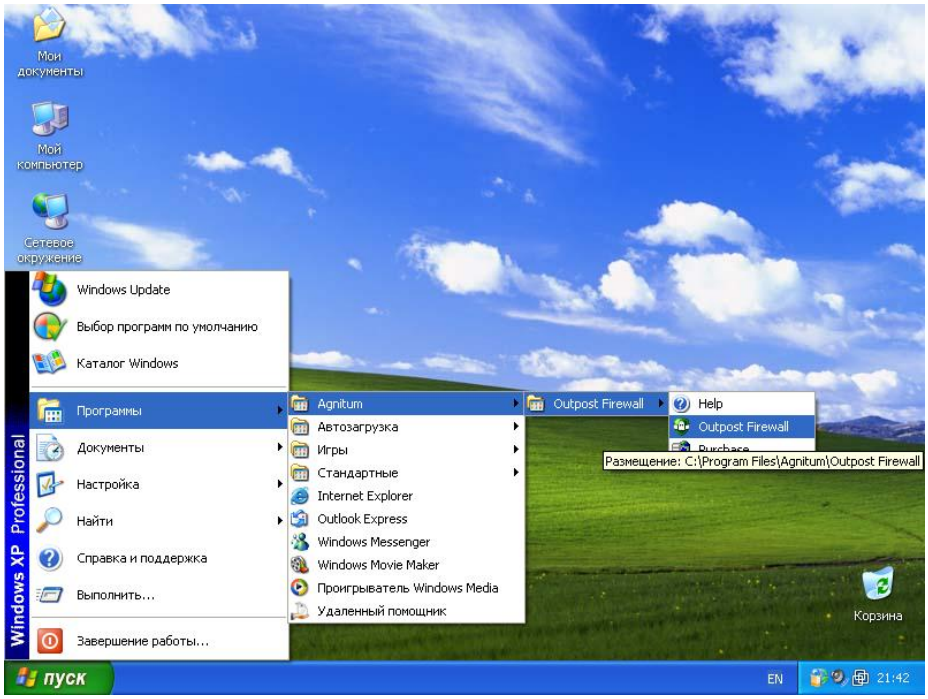
15. Проведите поиск установленных программ и завершите установку.



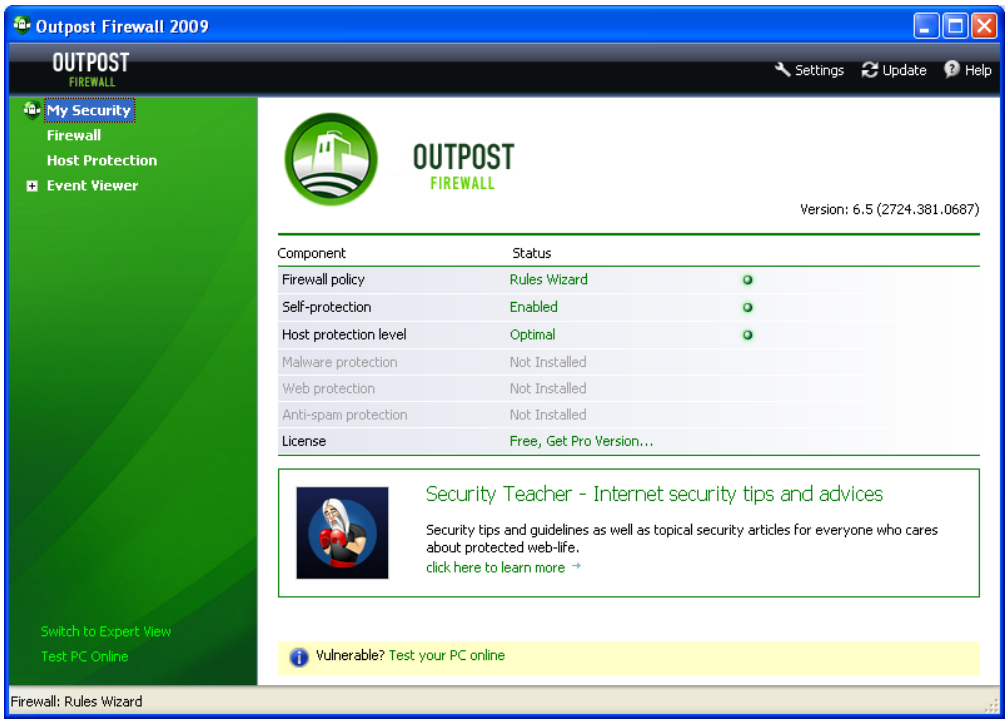
16. По запросу проведите перезагрузку виртуальной машины.

17. После перезагрузки и входа в виртуальную машину проверьте доступность взаимодействия между машинами после установки файвола. Для этого повторите пункты 9 и 10. Обнаружится блокировка входящей активности.

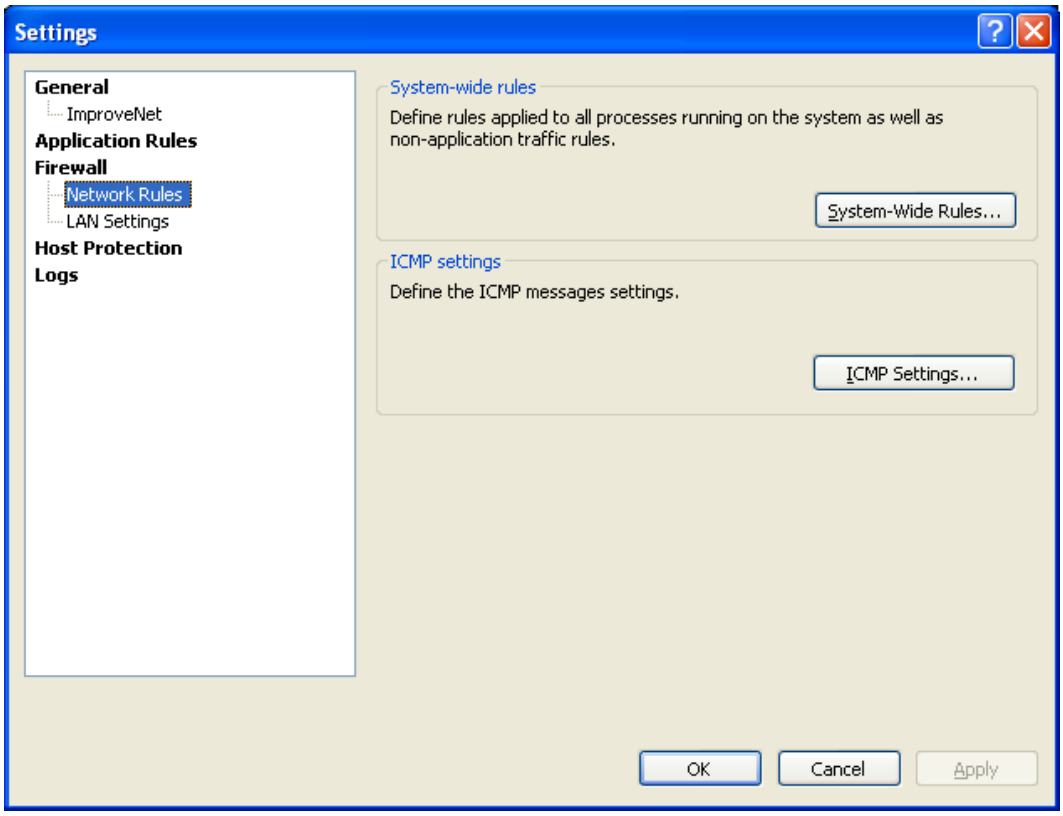
18. Вызовите окно файрвола.



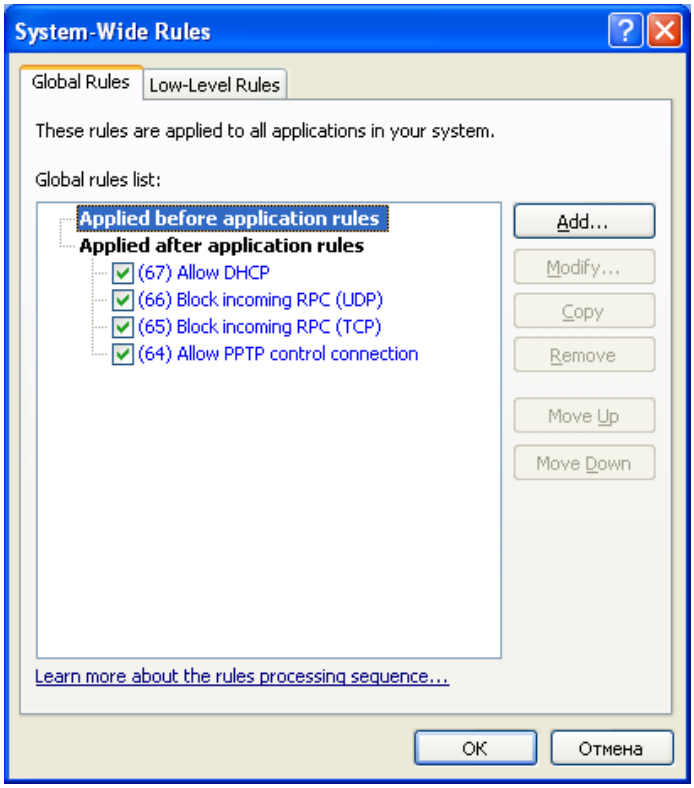
19. Рассмотреть разграничение доступа по IP адресам. Для этого найти раздел настроек, отвечающий за разграничение доступа в сеть по диапазону адресов. Для этого последовательно зайдите в настройки (Settings).



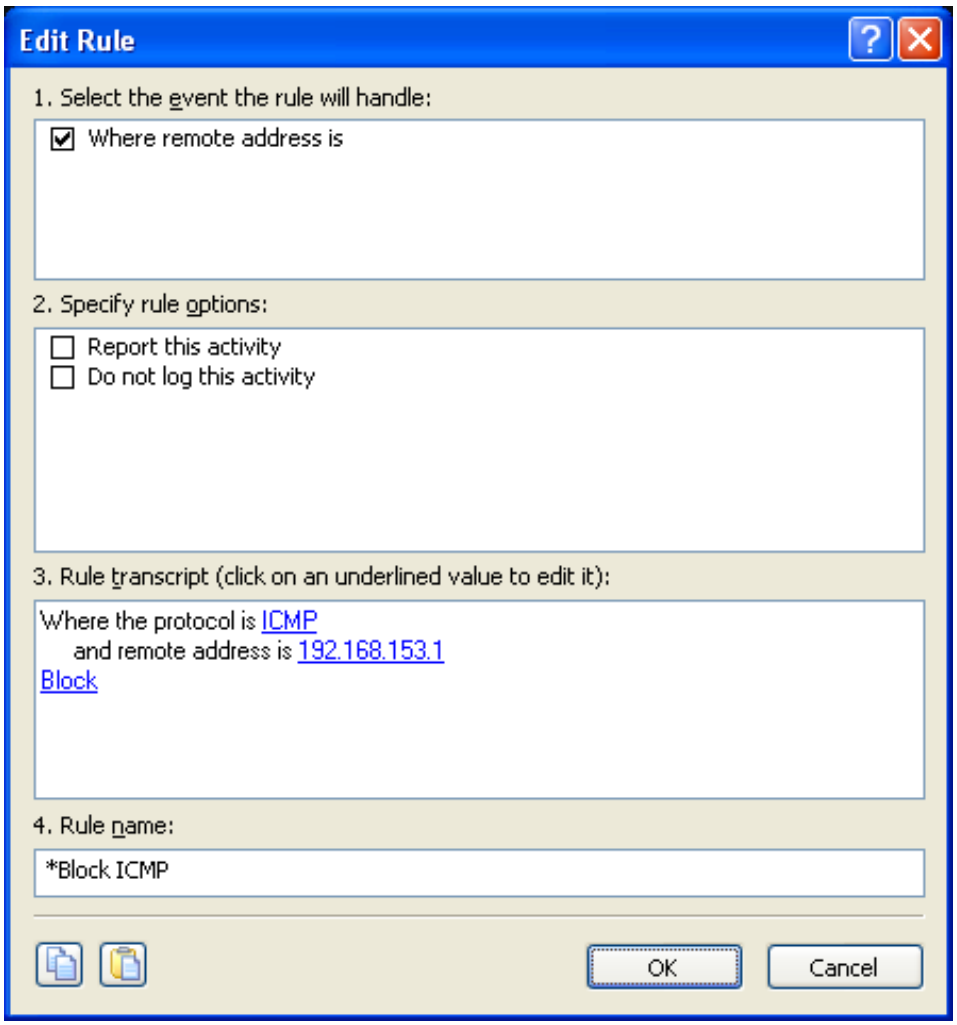
20. Зайдите в раздел настроек сетевых правил (Network Rules кнопка System-Wide Rules…).



21. Добавьте новое глобальное правило, выполняющееся до применения правил, относящихся к приложениям.



22. Полностью заблокируйте сетевую активность по протоколу ICMP (он используется командой ping) с реальной машиной. Для этого выполните действия, представленные на скриншоте и сделайте собственный скриншот настроек.

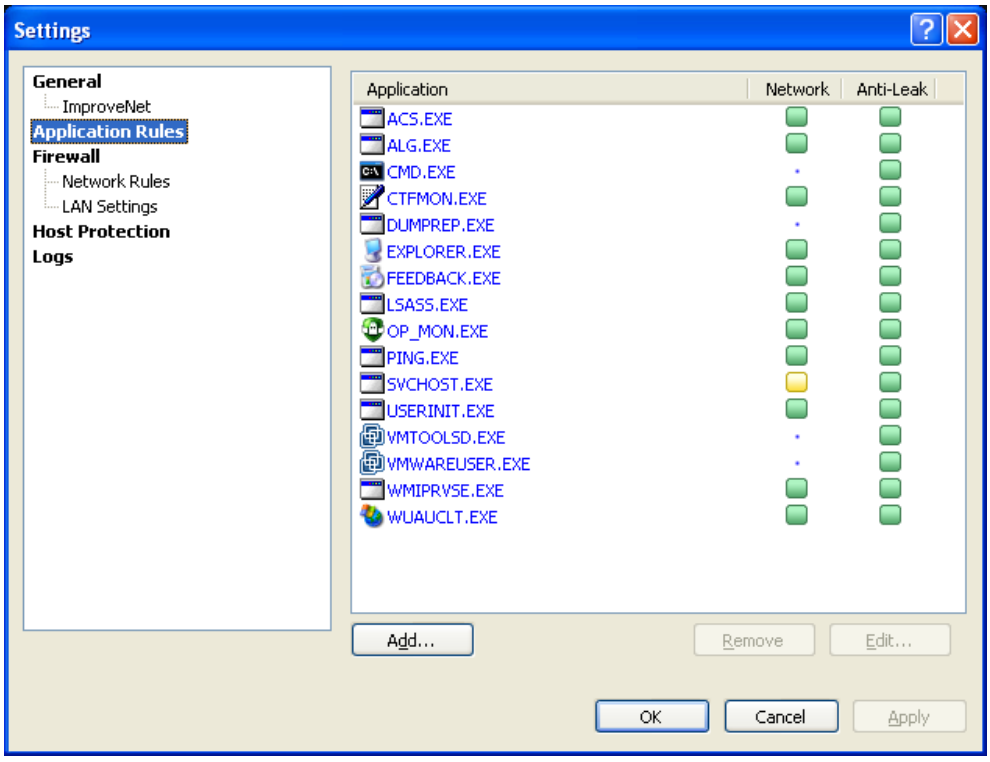


23. Примените сделанные настройки и проверьте доступность реальной машины (пункт 10).

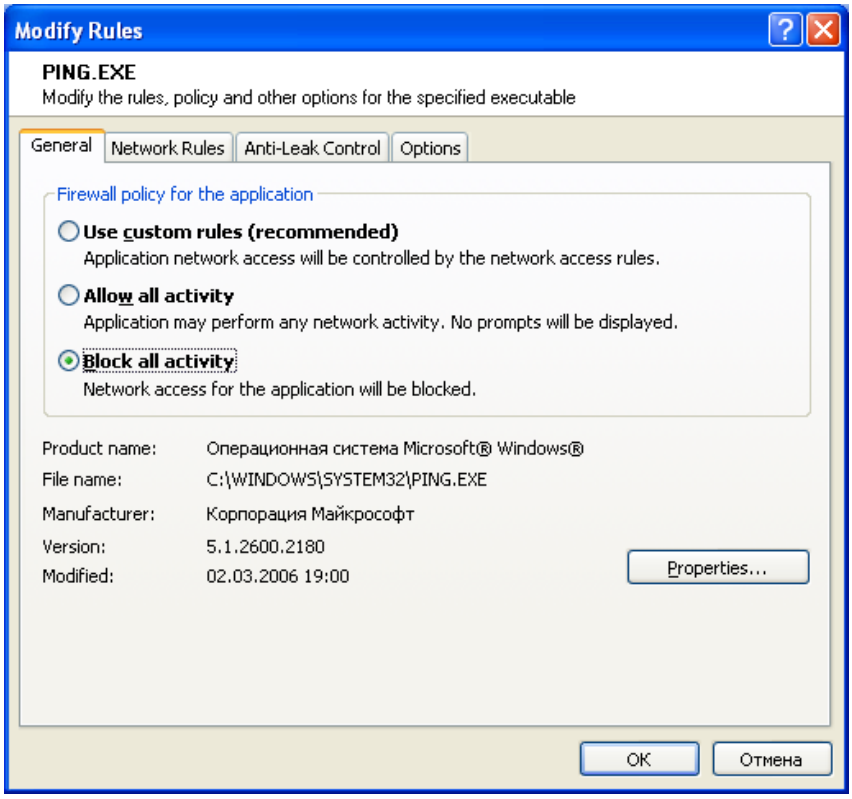
24. Разрешите активность, удалив созданное правило. Сделайте соответствующий скриншот.

25. Найти раздел настроек, отвечающий за разграничение доступа в сеть по программам. Для этого последовательно зайдите в настройки (Settings) (19).

26. Зайдите в раздел настройки правил для приложений.



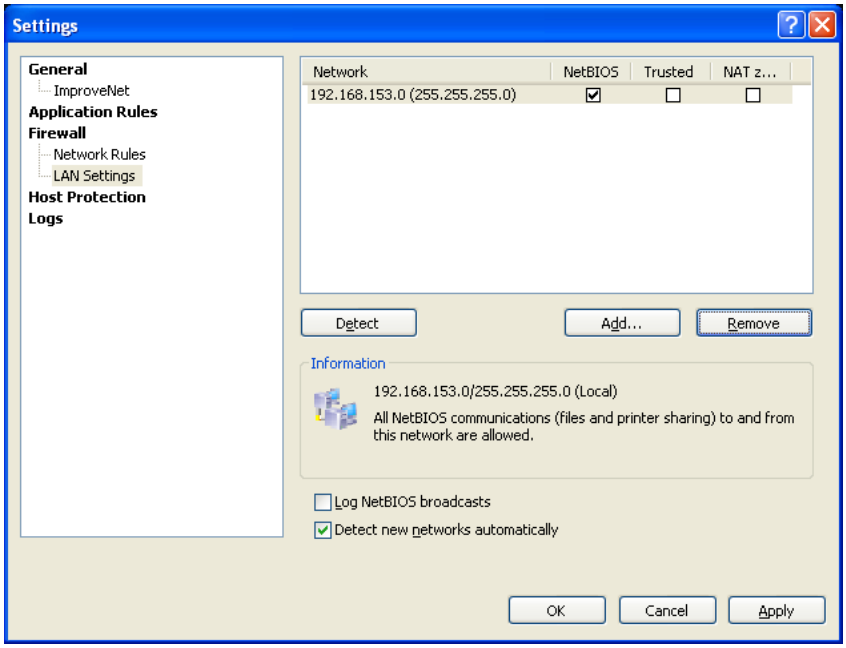
27. Запретите всю деятельность приложению ping. Сделайте соответствующие скриншоты настроек.



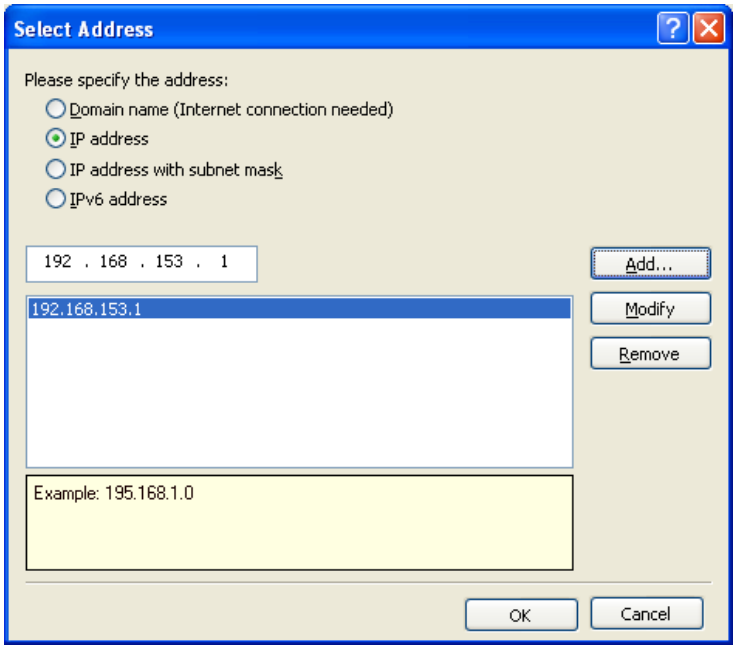
28. Примените сделанные настройки и проверьте недоступность реальной машины из виртуальной (пункт 10).

29. Разрешите любую активность приложению ping.

30. Добавьте реальную машину в доверенную зону, для этого последовательно выполните 19 и откройте настройки локальной сети (LAN settings).



31. Проведите добавление доверенного узла – IP адреса реальной машины. Для добавленной сети установите пометку доверенная (Trusted).



32. Примените сделанные настройки и проверьте, что виртуальная машина из реальной стала доступна (пункт 9).

33. Рассмотреть другие настройки файрвола. Сделать скриншоты и вставить в отчет с пояснениями.

34. Скопировать скриншоты для оформления отчета, завершить работу, провести удаление виртуальной машины.

Контрольные вопросы

1. Основные виды сетевых атак.
2. Основные способы защиты компьютеров в локальных и глобальных сетях.
3. Основные виды файрволов.
4. Основные настройки.
5. Основные режимы работы файрвола.

Литература

Нет

5. Оценка выполнения лабораторной работы

На каждую лабораторную работу студент составляется отчет. Для лабораторных работ №2,3,4 отчет может быть в электронной форме.

Защита лабораторной работы проводиться демонстрацией соответствующих действий по заданию к работе и ответом на контрольные и дополнительные вопросы по теме лабораторной работы.