НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«МЕЖДУНАРОДНЫЙ ИНСТИТУТ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ»

КАФЕДРА «ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА»

ОПЕРАЦИОННЫЕ СИСТЕМЫ

ЛАБОРАТОРНЫЙ ПРАКТИКУМ
для студентов специальности 230101
«Вычислительные машины, комплексы, системы и сети»
всех форм обучения

ЧАСТЬ IV
(Лабораторные работы №7 – 8)

ВОРОНЕЖ 2009

УДК 681.3.06

Рецензент: Заслуженный работник высшей школы Российской Федерации,
профессор кафедры автоматизированных систем управления
Военного авиационного инженерного университета,
канд. техн. наук, профессор Фадин А.Г.

доцент кафедры ядерной физики
Воронежского государственного университета
канд. физ.-мат. наук, доцент Алейников А.Н.

Составитель: канд. техн. наук, доцент кафедры ИВТ Савченко В.А.

Операционные системы: лабораторный практикум для студентов специальности 230101 «Вычислительные машины, комплексы, системы и сети» всех форм обучения. В 4-х ч. Ч.4. / сост. Савченко В.А. – Воронеж: Междунар. ин-т компьютер. технологий, 2009. – 76 с.

Лабораторный практикум содержит методические указания к выполнению лабораторных работ по курсу «Операционные системы». В необходимом объеме приведены теоретический материал и подробные рекомендации для практического выполнения лабораторного практикума.

Лабораторный практикум предназначен для студентов третьего курса очной и четвертого курса заочной формы обучения по технической специальности 230101 «Вычислительные машины, комплексы, системы и сети».

Ответственный за выпуск
зав. кафедрой «Информатики
и вычислительной техники» канд. техн. наук, профессор Юшинин С.Ю.

Печатается по решению Редакционно-издательского совета Международного института компьютерных технологий.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Курс «Операционные системы» является основополагающей дисциплиной при обучении студентов в высшем учебном заведении по специальности «Вычислительные машины, комплексы, системы и сети». Помимо изучения лекционных материалов учащиеся должны приобретать опыт по применению полученных знаний на практике. С этой целью предлагаемый лабораторный практикум ставит своей задачей расширить теоретическую базу в предметной области и привить учащимся практические навыки по работе со специальными возможностями изучаемой операционной системы (ОС), в частности, применительно к сфере ее сетевого администрирования и конфигурирования.

Лабораторный практикум состоит из четырех частей и представляет собой ряд последовательно выполняемых лабораторных работ, тематически разделенных на несколько общих направлений. Предполагается изучение различных инструментов системного администратора – служебных команд и утилит, доступных в алфавитно-цифровом терминале или командной оболочке, оснасток консоли администрирования и их расширений – с применением графического интерфейса пользователя. Отдельно следует отметить изучение мощнейшего программного средства Редактор Реестра ОС, предназначенного, среди прочего, для настройки и оптимизации системы. Рассматриваются основы сетевой безопасности и правила конфигурирования локальных сетей. Дается представление об одной из Unix-подобных ОС и навыках работы в ней.

Каждая лабораторная работа практикума в достаточном объеме содержит теоретические сведения, необходимые для ее выполнения, ряд практических заданий – для закрепления изученного материала, а также тематические контрольные вопросы, предполагающие дополнительное углубленное изучение теоретического материала в рамках решаемых задач. Выполнение последующих заданий лабораторных работ опирается на знания и навыки, полученные при изучении предыдущих. Поэтому важно соблюдать некоторую преемственность в их выполнении, чтобы обеспечить постепенное и логическое усвоение изучаемого материала. При соблюдении этого условия полученные знания обеспечат учащихся надежной практической базой для всестороннего развития в выбранной сфере.

Четвертая часть лабораторного практикума ориентирована на приобретение студентами базовых знаний в области обеспечения сетевой безопасности как на локальном уровне в рамках отдельного компьютера, так и глобальном – при организации доступа в сеть Интернет. С этой целью рассматриваются соответствующие системные инструменты и возможности ОС. Дополнительное внимание уделено организации безопасности файловой системы ОС и ее объектов (файлов и каталогов).

Для расширения знаний сетевого администрирования и закрепления полученных навыков в последней лабораторной работе осуществляется настройка взаимного доступа к общим сетевым ресурсам в консолидированной среде двух альтернативных ОС семейств Windows и Unix.

Лабораторная работа №7

Работа с подсистемой безопасности в ОС Windows XP

Цель работы: Изучить основные возможности подсистемы безопасности и способы защиты данных в среде ОС Windows XP.

7.1. Краткие теоретические сведения

В современных условиях развития сети Интернет как глобального средства коммуникации обеспечение безопасности данных в коммерческой организации становится все более актуальной задачей, возлагаемой, главным образом, на системного администратора. В связи с учащающимися случаями проникновения в незащищенные сети, атаками и просто потенциальными угрозами инструментарий профессионала в области информационной безопасности должен быть максимально широким и включать все возможные аппаратно-программные средства защиты (аппаратные и программные сетевые экраны, брандмауэры, аппаратные и программные средства ограничения локального и удаленного доступа, управления локальной и групповой политикой), а не ограничиваться антивирусными пакетами на защищаемых узлах сети. Большинство программных компонентов для решаемых задач безопасности доступны системному администратору сразу же после установки сетевой операционной системы, в частности, ОС Windows XP. При этом принципиальных отличий в настройке элементов безопасности локального узла или сервера домена не существует, поскольку безопасность в сети подчиняется единому набору правил, называемому политикой безопасности организации.

Таким образом, при создании сети на базе ОС Windows XP безопасность необходимо обеспечивать на двух уровнях: на уровне локального компьютера и на сетевом, уровне домена или рабочей группы. Программные средства профессиональной версии ОС Windows XP позволяют обеспечивать безопасность несколькими способами. Часть из этих средств была унаследована от предыдущих версий операционных систем семейства Windows, другие компоненты, напротив, появились сравнительно недавно и успешно применяются.

С появлением каждой новой сетевой ОС семейства Windows средства безопасности, эволюционируя, претерпевают значительные изменения, позволяющие администратору сети гибко настраивать ее и обеспечивать, тем самым, приемлемый уровень комплексной защиты вычислительной системы. Данное утверждение не является исключением также по отношению к изучаемой ОС Windows XP. В ней имеется ряд программных средств от ОС предыдущего поколения, ОС Windows NT и ОС Windows 2000, но имеются и новые средства обеспечения безопасности, основные из которых представлены ниже.

- *Собственность администратора*. В ранних версиях ОС Windows любые ресурсы (файлы и каталоги), созданные администратором,

становились достоянием всей группы. В профессиональной ОС Windows XP ресурсы теперь принадлежат тому, кто их создал.

- *Ограничения, связанные с использованием пустого пароля.* Теперь пользователи ОС Windows XP могут использовать пустые пароли при регистрации, но с ними они могут регистрироваться локально, только физически присутствуя.
- *Программные ограничения.* Политика безопасности ОС Windows XP может быть присвоена отдельным приложениям на основании пути к исполняемому файлу (порту), Интернет-зоны или сертификата безопасности.
- *Быстрая смена пользователей.* Узлы, работающие в среде ОС Windows XP и при этом не соединенные с доменом, могут быстро переключаться с одного пользователя на другого, не выходя из локальной сети и не закрывая приложений.
- *Мастер сброса пароля.* Если пользователь забыл свой пароль, то он может воспользоваться загрузочным диском для осуществления доступа к своей учетной записи.

Нетрудно заметить, что отмеченные возможности обеспечения безопасности, как локальной, так и глобальной, стали более доступными с точки зрения их сетевого применения и практически ориентированными на гибкое администрирование и конфигурирование ОС. Это позволяет сделать вывод о том, что данная тенденция будет наблюдаться и впредь, позволяя профессионалам постоянно иметь необходимый инструментарий.

В первом приближении некоторые вопросы обеспечения локальной безопасности уже имели место в предыдущих лабораторных работах. В частности, в лабораторной работе №4 было осуществлено знакомство с одним из основных инструментов системного администратора, консолью администрирования MMC и одной из основополагающих оснасток «Групповая политика», являющейся обязательной для целей конфигурирования безопасной операционной среды.

В рамках настоящей лабораторной работы предполагается изучить дополнительные инструменты системного администратора и выполнить ряд мероприятий, направленных на обеспечение сетевой безопасности, а именно осуществить некоторые элементарные действия по управлению локальной политикой безопасности, рассмотреть процедуру безопасного входа в систему, организовать аудит в журналах безопасности Internet Connection Firewall, поговорить о шаблонах безопасности, а также научиться анализировать и конфигурировать подсистему безопасности ОС в целом. Отдельно предполагается рассмотреть вопросы, связанные с обеспечением безопасности файловой системы, ее объектов (файлов и каталогов) как локально, так и при сетевом взаимодействии.

7.2. Подготовка к выполнению лабораторной работы

Возможность управления политикой безопасности (на локальном компьютере или в сети) осуществляется посредством создания консоли администрирования MMC и добавления на нее соответствующих, предназначенных для этих целей средств управления (оснасток и расширений). При этом возможно использование оснасток, изученных ранее и ориентированных на управление правами доступа и разрешениями, имеющимися у пользователя в процессе работы с локальными ресурсам системы. В случае необходимости, применение других системных инструментов и программных модулей сторонних разработчиков (например, ориентированных на аудит и мониторинг ОС) также может быть полезным с целью расширения функционала консоли администрирования. Средства управления политикой безопасности локального узла, подразделения или домена представлены в табл. 7.1.

Таблица 7.1. Средства управления политикой безопасности ОС

№ п/п.	Средство управления политикой безопасности	Описание
1.	Средство «Локальная политика безопасности»	Данное средство используется для прямого изменения политик учетных записей и локальных политик, политик открытого ключа, а также политик безопасности IP локального компьютера.
2.	Шаблоны безопасности	Шаблон безопасности является файлом, представляющим конфигурацию безопасности или политику безопасности. Подобные шаблоны могут применяться к политике локального компьютера или импортироваться в объект **«Групповая политика»**
3.	Средство «Анализ и настройка безопасности»	Данное средство используется для анализа и настройки безопасности локального узла с помощью шаблона безопасности.
4.	Расширение «Параметры безопасности» для групповой политики	Данное средство может использоваться для изменения отдельных параметров безопасности локального узла, подразделения или домена.

Отдельно следует отметить еще одно программное средство **Secedit.exe**, представляющее собой исполняемый файл, запускаемый из командной строки, в рамках пакетного файла или посредством автоматического планировщика заданий. Данное средство используется для автоматизации задач настройки системы безопасности группы компьютеров локальной сети. Для применения данного средства в повседневной практике необходимо иметь навыки использования командного интерпретатора и опыт написания пакетных файлов и сценариев (см. Лабораторные работы №1-3).

В настоящей лабораторной работе предполагается ознакомление с основными принципами организации локальной и сетевой политик безопасности на основе консоли администрирования MMC с применением базовых возможностей указанных выше программных средств и оснасток **«Редактор объекта групповой политики» («Групповая политика»)**, **«Шаблоны безопасности»**, **«Анализ и настройка безопасности»**, а также **«Политики безопасности IP на «Локальный компьютер»** и **«Монитор IP-безопасности»**. При этом для детального изучения принципов создания и настройки консоли администрирования MMC с применением отмеченных средств целесообразно воспользоваться полным руководством, находящимся на Web-узле корпорации Майкрософт (http://www.microsoft.com).

Перед началом выполнения лабораторной работы в среде ОС Windows XP необходимо выполнить следующее:

1) загрузить ОС Windows XP и активировать справочное меню **(Пуск | Справка и поддержка)**;

2) ознакомиться с описанием и возможностями запуска и применения консоли администрирования MMC (см. Лабораторную работу №4);

3) ознакомиться с описанием и возможностями оснасток, предназначенных организации и администрирования локальной и сетевой политиками безопасности в среде ОС Windows XP: **«Редактор объекта групповой политики» («Групповая политика»)**, **«Шаблоны безопасности»**, **«Анализ и настройка безопасности»**, а также **«Политики безопасности IP на «Локальный компьютер»** и **«Монитор IP-безопасности»**.

7.3. Порядок выполнения лабораторной работы

Лабораторная работа выполняется последовательно в соответствии с определенным порядком и включает в себя два учебных задания.

Для выполнения лабораторной работы необходимо у системного администратора получить права полного доступа в текущем домене.

7.3.1. Учебное задание №1. Создание пользовательской консоли администрирования MMC, предназначенной для организации и управления локальными политиками безопасности в среде ОС Windows XP.

Порядок выполнения:

Как было ранее отмечено, локальные политики безопасности применяются на отдельных узлах сети. В состав этих политик входят следующие:

- *Назначение прав пользователя* определяет какие пользователи и группы обладают правами на вход в систему и авторизованы на выполнение соответствующих задач. Некоторые из частных вопросов при организации распределения прав доступа в ОС ранее раскрывались в лабораторной работе №4.
- *Политики аудита* определяют события безопасности, которые, в свою очередь, заносятся в *Журнал безопасности* данного компьютера. При этом в журнал могут заносится успешные, неудачные или те и другие попытки. *Журнал безопасности* является частью оснастки **«Просмотр событий»**, изученной в лабораторной работе №5.
- *Параметры безопасности* определяют действия ОС, направленные на обеспечение безопасности вычислительной системы. Например, к их числу относятся включение или отключение таких параметров безопасности как цифровая подпись данных, доступ оптическим накопителям, установка определенных драйверов или приглашение на вход в систему. Конфигурирование локальной политики посредством изменения некоторых параметров безопасности будет рассмотрено в ходе выполнения текущего учебного задания. При этом необходимо иметь ввиду, что приоритет имеют политики следующих объектов в указанном порядке: подразделение, домен и только затем локальный компьютер. Это обусловлено том, что бесконтрольное применение нескольких политик к одному локальному узлу может породить конфликт между параметрами безопасности.

На основе полученных в предыдущих лабораторных работах знаний и навыков по организации и построению консоли администрирования ММС необходимо выполнить следующее:

1. Создайте новую консоль администрирования в авторском режиме.
2. При необходимости сконфигурируйте параметры созданной консоли должным образом с целью придания ей уникального вида.
3. Добавьте на консоль новую панель вида задач, следуя инструкциям **«Мастера создания вида панели задач»**. В процессе работы **«Мастера»** введите новое имя **«Политика безопасности»** и описание **«Оснастки и расширения»** для данной панели задач; в появившемся окне **«Завершение мастера создания вида панели задач»** уберите флажок **«Добавить новые задачи на эту панель задач после закрытия мастера»** и нажмите кнопку **«Готово»** для подтверждения операции.

4. Добавьте в корень дерева консоли MMC оснастку **«Локальные пользователи и группы»** и одним из ранее изученных способов создайте новую учетную запись с правами группы **«Пользователи».** Имя пользователя, описание и пароль выберите самостоятельно. В процессе создания учетной записи пользователя оставьте флажок **«Потребовать смену пароля при следующем входе в систему»**.

5. Не закрывая консоль, сохраните ее.

Последовательность выполненных действий позволяет создать консоль администрирования MMC, придать ей уникальный вид и удобный интерфейс для дальнейшего использования в рамках настоящей лабораторной работы.

Задание №7.1а. Изучение основных возможностей программного средства **«Локальная политика безопасности»** в среде ОС Windows XP на конкретных примерах.

Прежде, чем интегрировать инструмент **«Локальная политика безопасности»** на созданную заранее консоль администрирования MMC и осуществить его детальное рассмотрение, необходимо отметить, что в ОС Windows XP данный инструмент существует автономно в виде штатного программного средства и может быть использован на локальном компьютере вне рамок оснастки **«Редактор объекта групповой политики»**. В частности, для просмотра локальной политики безопасности им можно воспользоваться, вызвав его из командной строки алфавитно-цифрового терминала с применением командного интерпретатора **Cmd.exe**. Это можно сделать, набрав **secpol.msc** и нажав **Enter** для подтверждения ввода или непосредственно из графической среды ОС посредством команды **Выполнить** в меню **Пуск**. Кроме того, поскольку модуль **«Локальная политика безопасности»** является штатным средством администрирования, он находится в группе соответствующих программных средств, расположенных в меню **«Пуск | Панель управления | Администрирование».**

Несмотря на сказанное выше, дальнейшее изучение локальной политики безопасности будет осуществляться в предположении, что имеется системная необходимость создания собственной консоли MMC с включенным внутрь набором необходимых для администрирования инструментов, в том числе модуля **«Локальная политика безопасности».** Для ознакомления с возможностями локальной политики безопасности в ОС Windows XP с использованием одноименной оснастки прежде всего необходимо выполнить следующие подготовительные действия:

1. Откройте только что созданную консоль администрирования MMC, в которой к этому моменту должна быть уже добавлена оснастка **«Локальные пользователи и группы»**.

2. Воспользовавшись оснасткой **«Редактор объекта групповой политики»**, добавьте политику **«Локальный компьютер»** в корень консоли, как было показано в предыдущих лабораторных работах.

3. С одной стороны, в окне дерева консоли MMC откройте ветвь **«Конфигурация компьютера | Конфигурация Windows | Параметры безопасности»** в **«Политике «Локальный компьютер»**. С другой стороны, в отдельном окне ОС откройте инструмент **«Локальная политика безопасности»** одним из выше описанных способов и, сравнив содержимое открытых окон, обратите внимание на то, что **«Параметры безопасности»** локальной политики абсолютно идентичны тем, которые отображаются в оснастке **«Политика «Локальный компьютер»**.

Таким образом, у системного администратора появляется возможность в случае необходимости интегрировать базовый инструмент локальной безопасности во вновь создаваемую и конфигурируемую консоль MMC.

4. Сохраните и закройте консоль администрирования MMC.

Важно напомнить, что предварительному изучению и конфигурированию некоторых политик, ориентированных на локальный аудит **(«Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Политика аудита»)** была посвящена лабораторная работа №5. Данное обстоятельство позволяет в этот раз не уделять дополнительного внимания вопросам, связанным с политиками аудита. Поэтому с целью обучения и ознакомления с **«Локальной политикой безопасности»** интерес в дальнейшем будут представлять **«Политики учетных записей»**, а также некоторые **«Локальные политики»** при **«Назначении прав пользователя»** и общих **«Параметров безопасности»**.

Секция А. Ознакомление с основными возможностями **«Политики учетных записей»** в ОС Windows XP.

Политики учетных записей **(«Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Политики учетных записей»)** применяются на локальных компьютерах сети и определяют взаимодействие учетных записей с данным компьютером или доменом. Существует три политики учетных записей:

- *Политика паролей* определяет параметры паролей, в частности, соответствие набору обязательных условий и сроку их действия.
- *Политика блокировки учетной записи* определяет условия и период времени блокировки учетной записи.
- *Политика Kerberos* определяет параметры протокола сетевой аутентификации Kerberos, такие как срок жизни сеансового билета и соответствие обязательным условиям. Данный протокол обеспечивает взаимно-секретную аутентификацию компьютеров в сети на основе

клиент-серверной модели. Политика Kerberos не входит в состав политики локального компьютера, она используется только для учетных записей пользователей домена.

Дополнительная информация по данной тематике доступна в справочных разделах **«Локальная политика безопасности»** и **«Параметры безопасности»** оснастки **«Групповая политика»**, а также в разделе **«Методы проверки подлинности»** справки ОС Windows XP **(Пуск | Справка и поддержка)** или на сайте **www.oszone.net**.

Для ознакомления с базовыми возможностями **«Политики учетных записей»** в ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова. В оснастке **«Локальные пользователи и группы»** наведите манипулятором мышь на нового пользователя и задайте ему любой пароль, выбрав команду **«Задать пароль…»** из контекстного меню.
2. Найдите подраздел **«Политика паролей»** в разделе **«Политики учетных записей»** оснастки **«Политика «Локальный компьютер»**.
3. Последовательно просмотрите все политики паролей с целью их дальнейшего применения на практике. Для этого дважды щелкните на каждой из них и на вкладке **«Объяснение параметра»** изучите их сущность.
4. Включите политику **«Пароль должен отвечать требованиям сложности»**, изменив положение соответствующего переключателя на вкладке **«Параметр локальной безопасности»**.
5. Установите минимальную длину пароля в 10 символов, осуществив необходимые действия в соответствующей политике паролей.
6. Перейдите в подраздел **«Политика блокировки учетной записи»** и аналогично изучите сущность расположенных здесь политик безопасности.
7. Установите **«Пороговое значение блокировки»** на три ошибки входа в систему и осуществите блокировку учетной записи на 2 минуты в случае совершенных ошибок ввода.
8. Сохраните и закройте консоль администрирования MMC.

При выполнении заданий секции используйте следующие инструкции:

- перенесите последовательность выполняемых действий по пунктам 5 и 7 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
- перезагрузите компьютер, выберите созданную учетную запись и проверьте влияние новых значений системных параметров политик безопасности на процесс аутентификации,
- сделайте вывод о проделанной работе и запишите его в отчет.

Контрольный вопрос:

Каким образом можно разблокировать компьютер в случае некорректного ввода пароля? Кто в состоянии это сделать?

Секция В. Ознакомление с основными возможностям **«Локальных политик»** при **«Назначении прав пользователя»** в ОС Windows XP.

Локальные политики безопасности, применяемые при назначении прав пользователя **(«Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Назначение прав пользователя»),** позволяют системному администратору определить какие пользователи и группы будут обладать правами на вход в ОС и какие будут при этом авторизованы на выполнение соответствующих задач. Особенностью данных локальных политик является то, что они могут быть применены к любому пользователю или группе в системе простым их (пользователей) добавлением в число тех, на которые рассматриваемая политика распространяется. Это позволяет, тем самым, иметь пользователям возможность влиять на политику безопасности ОС. Для иллюстрации сказанного и ознакомления с базовыми возможностями локальных политик безопасности при **«Назначении прав пользователя»** в ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова. В оснастке **«Политика «Локальный компьютер»** найдите подраздел **«Назначение прав пользователя»** в разделе **«Локальные политики».**
2. Последовательно просмотрите все политики для назначения прав пользователям с целью их дальнейшего применения на практике. Для этого дважды щелкните на каждой из них и на вкладке **«Объяснение параметра»** изучите их сущность.
3. Добавьте созданного ранее пользователя в число тех, которым позволено производить операции архивирования файлов и каталогов в системе. Для этого воспользовавшись одноименной политикой безопасности, **«Добавьте пользователя или группу»** стандартным способом на вкладке **«Параметр локальной безопасности»** и удалите группы, обладающие этим правом по умолчанию.
4. Запретите группам **«Пользователи»** и **«Операторы архива»** доступ к компьютеру из сети. Для этого внимательно изучите политики **«Доступ к компьютеру из сети»** и **«Отказ в доступе к компьютеру из сети».**
5. Добавьте созданного ранее пользователя в число тех, которым позволено осуществлять **«Изменение системного времени».**
6. Добавьте созданного ранее пользователя в число тех, которым позволено осуществлять **«Создание страничного файла».**

7. Добавьте созданного ранее пользователя в число тех, которым позволено осуществлять **«Управление аудитом и журналом безопасности».**

8. Сохраните и закройте консоль администрирования MMC.

При выполнении заданий секции используйте следующие инструкции:

- перенесите последовательность выполняемых действий по пунктам 3-7 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
- перезагрузите компьютер, выберите созданную учетную запись и проверьте влияние новых значений системных параметров политик безопасности на процесс авторизации,
- сделайте вывод о проделанной работе и запишите его в отчет.

Секция С. Ознакомление с основными возможностям **«Локальных политик»** при настройке **«Параметров безопасности»** в ОС Windows XP.

Основные политики, применяемые для обеспечения локальной или сетевой безопасности и представленные в виде набора соответствующих параметров **(«Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Параметры безопасности»),** позволяют системному администратору, наряду с политиками учетных записей и базовыми методами авторизации, организовать первый уровень защиты данных от несанкционированного доступа из сети или же, напротив, позволить уполномоченным пользователям иметь определенные права при обращении к информации.

Для ознакомления с базовыми возможностями рассматриваемого набора политик безопасности в ОС Windows XP выполните следующее.

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова. В оснастке **«Политика «Локальный компьютер»** найдите подраздел **«Параметры безопасности»** в разделе **«Локальные политики».**

2. Последовательно просмотрите все политики безопасности данного подраздела с целью их дальнейшего применения на практике. Для этого дважды щелкните на каждой из них и на вкладке **«Объяснение параметра»** изучите их сущность.

3. Включите возможность очистки страничного файла виртуальной памяти при завершении работы системы, воспользовавшись соответствующей политикой безопасности. Это позволит при определенных условиях избежать перехвата данных из виртуальной памяти.

4. Следующие несколько настроек данного пункта задания реализуют концепцию «безопасного входа в систему», которая может быть практически использована на серверах домена или отдельных узлах локальной сети.

Прежде всего, следует отметить, что некоторым пользователям новый механизм входа в систему с использованием окна приветствия в ОС Windows XP может показаться неудобным или непривычным. Для устранения данного дискомфорта в системе имеется вариант переключения данного механизма в «классический» режим. Для этого необходимо осуществить **«Изменение входа пользователей в систему»** в меню **«Пуск | Панель управления | Учетные записи пользователей»**. В появившемся окне необходимо убрать флажки **«Использовать страницу приветствия»** и **«Использовать быстрое переключение пользователей»** и подтвердить изменения, щелкнув манипулятором мышь по кнопке **«Применение параметров»**.

Данное изменение приводит к тому, что после перезагрузки ОС появляется «классическое» окно входа в систему с двумя полями: **«Пользователь»**, в котором следует набрать имя учетной записи, и **«Пароль»** — для ввода пароля, назначенного этой учетной записи.

Внимание! При переключении механизма входа в «классический» режим утрачивается возможность использования технологии быстрого переключения пользователей. Поэтому, в случае обратного перехода (в положение с использованием окна приветствия) для возврата данной технологии в активное состояние необходимо войти в ОС с правами администратора, перезагрузившись в «безопасном режиме», и установить соответствующий флажок **«Использовать быстрое переключение пользователей»**.

Далее переведите в положение **«Отключено»** параметр безопасности локальной политики **«Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL»**, как это делается на рабочих станциях и серверах домена. Эта настройка обеспечивает пользователей необходимостью одновременно нажимать кнопки **CTRL**, **ALT** и **DEL** каждый раз при входе в ОС, что делает процедуру входа более защищенной.

Отключите возможность отображения имени пользователя (в поле **«Пользователь»**), выполнившего последним вход в систему, воспользовавшись соответствующей политикой безопасности **«Интерактивный вход в систему: не отображать последнего имени пользователя»**. Данная политика исключает возможность несанкционированного манипулирования именем пользователя в сети.

Концепция «безопасного входа в систему» реализована полностью.

5. С целью уведомления пользователей локальной сети включите возможность отображения текста сообщения следующего содержания: **«ВНИМАНИЕ !!! Вы входите в корпоративную сеть компании. Причинение вреда аппаратно-программному обеспечению компании преследуется в административном порядке. Будьте аккуратны, это Ваше имущество !!!»**, воспользовавшись локальными политиками **«Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему»** и **«Интерактивный вход в систему: текст сообщения для пользователей при входе в систему»**.

6. Практический смысл следующего задания заключается в активации так называемой модели «гостевого доступа», позволяющей организовать беспрепятственный общий доступ к объектам (файлам и каталогам) файловой системы из локальной сети. Эта модель является оптимальным выбором для домашнего применения, хотя обладает ослабленной безопасностью в процессе эксплуатации. В этой связи, критически необходимо использовать дополнительные аппаратно-программные средства для защиты клиентских компьютеров от несанкционированного доступа, вирусов и внешних атак.

Кроме модели «гостевого доступа», существует еще одна, классическая модель доступа, называемая «обычной», имеющая место при организации общих сетевых ресурсов. Модель «обычного доступа» обладает повышенным уровнем безопасности и гибкостью при настройке прав. Поэтому применение данной модели целесообразно в корпоративных условиях.

Чтобы активировать модель «гостевого доступа», во-первых, необходимо включить встроенную учетную запись «Гость». Для этого следует найти политику безопасности **«Учетные записи: Состояние учетной записи «Гость»** и перевести соответствующий системный параметр безопасности в положение **«Включено»**.

Во-вторых, в локальной политике **«Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей»** следует изменить значение параметра модели совместного доступа в положение **«Гостевая – локальные пользователи удостоверяются как гости»**.

В-третьих, в локальной политике **«Учетные записи: ограничить использование пустых паролей только для консольного входа»**, регламентирующей использование пустых паролей, необходимо перевести параметр безопасности в состояние **«Отключено»**. Это позволит пользователям с учетной записью «Гость» и пустым паролем иметь возможность беспрепятственного доступа в систему из локальной сети. По умолчанию, во включенном состоянии этого параметра, использование пустых паролей допускается только для консольного входа, то есть для входа в систему с клавиатуры компьютера.

Очевидно, что данная политика в состоянии **«Отключено»** также ослабляет системную безопасность настраиваемой среды при доступе к так называемым «административным» ресурсам, если учетные записи последних надежно не защищены парольной защитой.

Наконец, следует проверить наличие пользователя «Гость» в числе тех, кому в принципе разрешен доступ из локальной сети. Для этого откройте изученную ранее (**секция В** текущего задания) ветвь **«Параметры безопасности | Локальные политики | Назначение прав пользователя»** и в локальной политике **«Отказ в доступе к компьютеру из сети»** убедитесь в отсутствии учетной записи «Гость» среди запрещенных. Если пользователю «Гость» доступ из сети запрещен, то удалите учетную запись.

Таким образом, последние четыре политики позволяют организовать «гостевой доступ» из локальной сети к тому компьютеру, на котором данные настройки были применены. Как следствие, реализованная конфигурация при

использовании на каждом локальном узле в рабочей группе или домене обеспечивает беспрепятственный взаимный доступ к общим локальным ресурсам.

8. Сохраните и закройте консоль администрирования MMC.

При выполнении заданий секции используйте следующие инструкции:

- перенесите последовательность выполняемых действий по пунктам 3-7 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
- перезагрузите компьютер и проверьте влияние новых значений системных параметров политик безопасности,
- сделайте вывод о проделанной работе и запишите его в отчет.

Контрольный вопрос:

Каким альтернативным способом можно включить встроенную учетную запись «Гость» для активации модели «гостевого доступа»?

Задание №7.1б. Изучение основных возможностей программного средства **«Шаблоны безопасности»** в среде ОС Windows XP на конкретных примерах.

В предыдущих заданиях лабораторной работы были рассмотрены отдельные политики безопасности и принадлежащие им системные параметры, изменяемые при конфигурировании безопасности ОС. Однако гораздо эффективней конфигурировать ОС в процессе ее загрузки посредством единовременного применения группы параметров безопасности. Для этих целей в среде ОС Windows XP существует специализированное программное средство **«Шаблоны безопасности»**, представляющее собой оснастку, как и прежде добавляемую к дереву консоли администрирования MMC. В рамках данной оснастки имеется возможность создавать и применять в системе текстовые файлы, содержащие в себе все необходимые настройки безопасности для безопасных областей, поддерживаемых локальной политикой. Именно данные текстовые файлы в ОС принято называть шаблонами безопасности. В ОС Windows XP существует ряд штатных шаблонов безопасности, определяющих конфигурацию безопасности по семи категориям:

1) Политики учетных записей — это набор параметров аутентификации учетных записей. Для учетных записей домена параметры учетной политики должны быть одинаковы по всему домену. Данные политики подразделяются:

- *Политика паролей* — ограничения на пароль, его минимальную длину, хранение старых паролей, минимальный и максимальный срок действия пароля, сложность пароля и, возможно, обратимое шифрование хранимых данных.

- *Политика блокировки учетной записи* отвечает за действие, которое должно выполняться при вводе неверного пароля, включая пороговое число неудачных попыток входа в ОС, при котором происходит блокировка учетной записи или ответные действия, включая частоту сброса счетчиков попыток входа.
- *Политика Kerberos* — набор параметров протокола сетевой аутентификации Kerberos v.5, в частности, включающего время жизни для билетов на их выдачу, билетов службы, максимальное расхождение часов и проверку членства в группе и статуса блокировки учетных записей.

2) Локальные политики — параметры безопасности только для компьютера, на котором применяется шаблон безопасности. Они применяются к базе данных учетной записи локального узла и делятся на три категории.

- *Политика аудита* — набор отслеживаемых событий, которые будут храниться в журнале безопасности локального компьютера.
- *Назначение прав пользователя* определяет участников безопасности, которым будут даны права пользователей на локальном компьютере. Эти права приоритетнее любых разрешений ФС NTFS, назначенных объекту (файлу или каталогу).
- *Параметры безопасности* — спектр параметров, заданных в Реестре ОС. Обычно они указывают, отображать ли имя последнего пользователя, под которым входили в компьютер, или изменять ли имя учетной записи «Администратор».

3) Журнал событий — набор свойств журналов приложений, безопасности и системы, включая максимальный размер журнала, пользователей, которые могут его просматривать, срок хранения событий в журналах и действия, которые надо предпринять, если журналы безопасности достигли заданного максимального размера.

4) Группы с ограниченным доступом позволяют зафиксировать членство в группах безопасности. Допустимые группы безопасности выбирает создатель шаблонов безопасности. Обычно в эту группу включаются «Опытные пользователи», «Администраторы предприятия» и «Администраторы схемы». В результате можно явно указать, какие участники безопасности могут быть членами группы с ограниченным доступом. Данная политика также определяет, членом каких групп может быть сама группа с ограниченным доступом.

5) Системные службы позволяют задать ограничения для служб, установленных на компьютере, в том числе их статус (активизирована или отключена) и какие участники вправе ее запустить или остановить. В частности, например, можно настроить данную политику таким образом, чтобы была отключена служба **«Routing and Remote Access» («Маршрутизация и удаленный дотуп»)** на всех клиентских рабочих станциях. Это обеспечит запрет пользователям настраивать свои персональные компьютеры в качестве серверов удаленного доступа.

6) Реестр определяет безопасность разделов Реестра ОС и их кустов: какие участники безопасности вправе изменять параметры безопасности и аудит каких действий по модификации Реестра следует вести.

7) Файловая система определяет параметры избирательного списка управления доступом (DACL) и системного списка управления доступом (SACL) для любых каталогов, включенных в эту политику. Эти каталоги должны располагаться на носителе с ФС NTFS.

Известно, что компьютеры в сети могут выступать в разных ролях, то есть иметь различное назначение. Это обстоятельство влияет на выработку решения по тому, какие параметры следует применять для формирования политики безопасности для того или иного узла. Это приводит к тому, что перед определением шаблонов безопасности необходимо выявить компьютеры в сети, для которых нужно создать одинаковые параметры безопасности. Обычно для этого достаточно определить роль, которую каждый компьютер выполняет в сети, и уникальные требования безопасности для каждой роли.

Каждая роль, в конечном итоге, будет связана с шаблоном безопасности, определяющим типовую или требуемую безопасность для этого класса компьютеров. Наиболее распространенные роли компьютеров в сети следующие.

Контроллеры хранят базу данных Active Directory, требования безопасности для защиты которой являются самыми строгими.

Серверы приложений содержат клиентские серверные приложения, например, Web-приложения, базы данных SQL или почтовые серверные приложения. В каждой из указанных выше категорий можно определить соответствующие параметры безопасности для серверного приложения.

Файловые серверы или серверы печати хранят данные, совместно используемые в сети. В рамках определения безопасности можно создать специальные списки DACL для определенных хранилищ данных.

Серверы экстрасети — компьютеры с любой сетевой ОС, не являющиеся членами Active Directory. Хотя они могут проводить аутентификацию, но, как правило, располагаются в нейтральной (демилитаризованной DMZ-зоне) и имеют ограниченный доступ к ресурсам внутренней локальной сети.

Рабочие станции — клиентские компьютеры с сетевой ОС, не покидающие территориально офис предприятия. Их можно подразделять в зависимости от отдела или филиала, где они установлены.

Портативные компьютеры — клиентские узлы, имеющие возможность мобильного перемещения. Пользователи этих компьютеров могут обладать особыми привилегиями для выполнения некоторых задач вне корпоративной локальной сети.

Киоски устанавливаются в общественных местах и выполняют одно общедоступное приложение. В шаблоне безопасности киоска можно настроить автоматическую регистрацию на входе с использованием предварительно созданной учетной записи, позволяющей работать со специализированным инсталлированным приложением.

Нетрудно заметить, что такое структурирование узлов по ролям способствует выработке решения по разделению параметров безопасности на группы для их дальнейшей интеграции в соответствующие шаблоны безопасности. Анализ безопасности, выработка решений с подбором соответствующих параметров безопасности, а также примеры реального внедрения принятых решений подробно описываются в практическом курсе MCSE по безопасности сети на основе ОС Windows 2000 от корпорации Microsoft, библиографический источник которого указан в конце данного лабораторного практикума.

В рамках настоящей лабораторной работы для ознакомления с базовыми возможностями рассматриваемого программного средства **«Шаблоны безопасности»** в среде ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова.

2. Добавьте в корень дерева консоли MMC новую оснастку **«Шаблоны безопасности»** способом изученным ранее и разверните ее, чтобы были видны все ее элементы.

3. Создайте новый шаблон безопасности. Для этого выберите манипулятором мышь строку **«C:\WINDOWS\security\templates»**, показывающую локальное место хранения шаблонов безопасности в системе, и далее команду **«Создать шаблон…»** либо из выпадающего контекстного меню, либо из меню **«Действие»** на панели инструментов.

4. Откройте только что созданный шаблон безопасности и обратите внимание на то, что он включает в себя все семь категорий, описанных выше. Кроме того, просмотрите содержащиеся в нем политики безопасности и убедитесь, что все они находятся в состоянии **«Не определено»**.

Таким образом, создается пустой шаблон безопасности, в который можно внести все необходимые параметры, относящиеся к организуемой политике безопасности.

5. Сохраните созданный шаблон, открыв контекстное меню **«Действие»** и выбрав команду **«Сохранить как…»**. Имя шаблону присвойте, например, **MyFirstShablon** или определите его самостоятельно.

Как утверждалось ранее, ОС Windows XP изначально включает в себя ряд шаблонов безопасности, которые могут быть взяты в качестве основы для построения собственной политики безопасности. В частности, в распоряжении администратора может быть готовая политика безопасности, которая, в свою очередь, может быть улучшена и применена позже в системе.

По степени безопасности существуют четыре типа шаблонов:

- основной (Basic),
- безопасный (Secure),
- высокой степени безопасности (High secure),
- смешанный (Miscellaneous).

В качестве примера, среди штатных шаблонов безопасности находятся такие, как **Hisecdc** (сокр. **High secure domain controller**), который устанавливает самый высокий уровень безопасности для контроллера домена, или **Securews** (сокр. **Secure work station**) — устанавливает средний уровень безопасности для рабочих станций. Любой из доступных шаблонов может быть использован для разработки собственной политики безопасности.

Внимание! Перед модификацией штатного шаблона безопасности его следует предварительно сохранить под другим именем, чтобы он не был испорчен перезаписью.

6. Для создания шаблона безопасности, обладающего стандартной функциональностью, возьмите за основу системный шаблон **Setup security**, обеспечивающий уровень безопасности по умолчанию, и сохраните его с другим именем, выбранным самостоятельно или, например, **MySecondShablon**.

7. В только что сохраненном шаблоне выберите самостоятельно и измените несколько политик безопасности. При необходимости воспользуйтесь теми системными политиками, которые уже изменялись в предыдущих заданиях, например, при организации модели «гостевого доступа». Сохраните сконфигурированный таким образом шаблон безопасности.

8. Примените созданный шаблон безопасности в системе. Для этого в оснастке **«Политика «Локальный компьютер»** щелкните дважды на разделе **«Конфигурация компьютера»** и разверните подраздел **«Конфигурация Windows»**. Щелкните правой кнопкой мыши по строке **«Параметры безопасности»**, а затем — по команде **«Импорт политики»**. Выберите созданный шаблон безопасности и импортируйте его в систему, нажав **OK**.

Примечание. Для возврата системных параметров безопасности в состояние «по умолчанию» примените в системе штатный, неизмененный шаблон безопасности **Setup security**. Уровень безопасности ОС Windows XP будет приведен к начальному состоянию.

9. Сохраните и закройте консоль администрирования MMC.

При выполнении задания используйте следующие инструкции:

- перенесите последовательность выполняемых действий по пунктам 3-7 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
- перезагрузите компьютер и проверьте влияние новых значений системных параметров политик безопасности,
- сделайте вывод о проделанной работе и запишите его в отчет.

Контрольный вопрос:

Как Вы полагаете, возможно ли удаленное применение шаблонов безопасности? Если «Да», то какие программные средства для этого необходимы?

Задание №7.1в. Изучение основных возможностей программного средства **«Анализ и настройка безопасности»** в среде ОС Windows XP на конкретных примерах.

Другим, не менее важным, штатным программным средством, предназначенным для анализа настроек некоторого шаблона безопасности и сравнения их с текущими настройками безопасности действующего в системе шаблона, является оснастка **«Анализ и настройка безопасности»**. Учитывая то, что в ОС Windows XP имеется огромное количество политик безопасности, отслеживать каждую из них по отдельности представляется проблематичным. Однако анализ безопасности системы посредством рассматриваемого инструмента позволяет обнаруживать «дыры» в системе, тестировать влияние группового изменения настроек безопасности в ОС без их непосредственного применения, а также выявлять любые отклонения в политике безопасности сети.

Для ознакомления с базовыми возможностями изучаемого инструмента **«Анализ и настройка безопасности»** в среде ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова.

2. Добавьте в корень дерева консоли MMC новую оснастку **«Анализ и настройка безопасности»** способом изученным ранее и выберите ее.

После этого шага инструмент **«Анализ и настройка безопасности»** будет доступен, но нефункционален. Для получения необходимой функциональность его предстоит предварительно сконфигурировать.

3. Поскольку работа данного инструмента основана на использовании базы данных, сначала ее необходимо создать. Инструмент позволяет создать базу данных конфигураций и анализа безопасности, также называемую *локальной базой данных политики* компьютера.

В идеальном случае, база данных должна создаваться сразу же после инсталляции ОС. В этих условиях в ней будут содержаться настройки параметров безопасности в состоянии «по умолчанию». Поэтому при необходимости данная база может быть экспортирована сразу после загрузки системы и быть всегда доступной на случай «отката» к первоначальным настройкам.

Создайте новую базу данных. Для этого в меню **«Действие»** выберите команду **«Открыть базу данных…»**, введите в появившемся диалоговом окне новое имя базы данных (имя выберите самостоятельно) и щелкните на кнопке **«Открыть»**. В следующем окне выберите созданный ранее шаблон безопасности с именем **MyFirstShablon** и импортируйте его в базу данных, подтвердив намерение командой **«Открыть»**.

Если все сделано без ошибок, то при выборе оснастки **«Анализ и настройка безопасности»** в верхней части области сведений консоли администрат-

рирования ММС будет отображаться системный путь, где хранится только что созданная база данных системы безопасности ОС Windows XP.

4. Для анализа сформированной базы данных необходимо выбрать манипулятором мышь оснастку **«Анализ и настройка безопасности»**, а затем — команду **«Анализ компьютера…»** в контекстном меню **«Действие»** (альтернативным способом данную команду можно выбрать из выпадающего контекстного меню, если щелкнуть правой кнопкой мыши по выбранной оснастке). В появившемся диалоговом окне обратите внимание на системный путь и имя файла журнала ошибок, в котором будут сохранятся результаты анализа. При необходимости путь по умолчанию и имя файла могут быть заменены на более подходящие для организации удобного доступа.

Нажмите **ОК** для подтверждения операции анализа безопасности. В процессе проверки безопасности системы в окне состояния будет отображаться ход выполнения задания. По окончании анализа результаты отображаются в области сведений справа и появляется возможность просмотра и изменения необходимых настроек политик безопасности.

Если необходимо, просмотр файла журнала ошибок может быть осуществлен посредством выбора соответствующей команды **«Показать файл журнала»** в меню **«Действие»** на панели инструментов.

5. Последовательно проанализируйте параметры безопасности двух разделов **«Политики паролей»** и **«Локальные политики»**, щелкнув манипулятором мышь по каждому из включенных подразделов. Обратите внимание, что в области сведений справа отображаются теперь три колонки с названиями **«Политика», «Параметр базы данных»** и **«Параметр компьютера»**, то есть имеется возможность сравнения действующих в системе и настраиваемых системных параметров политик безопасности.

6. Измените в базе данных несколько выбранных самостоятельно параметров безопасности анализируемых политик. Для этого щелкните манипулятором мышь на выбранной политике и измените системное значение параметра в появившемся диалоговом окне **«Свойства»**, предварительно установив флажок **«Определить следующую политику в базе данных»**. Описание сущности изменяемого параметра безопасности доступно на соответствующей вкладке **«Объяснение параметра»** окна **«Свойства»**.

Внимание! Имейте ввиду, что изменяемые системные параметры влияют только на базу данных, а не на текущие параметры компьютера.

Таким образом, сравнивая текущие параметры действующей в системе политики безопасности можно настроить необходимые системные параметры с целью их экспортирования в новый шаблон безопасности и дальнейшего использования в ОС Windows XP.

7. Экспортируйте базу данных только что измененных параметров в новый шаблон безопасности с именем **MyThirdShablon**. Сохраните консоль ММС, выгрузите и загрузите ее снова. Проверьте наличие шаблона **MyThirdShablon** в оснастке **«Шаблоны безопасности»** и действительность изменения выбранных параметров политик безопасности внутри шаблона.

Таким образом, созданный шаблон безопасности теперь может быть, при необходимости, применен в системе способом, изученным в предыдущем задании лабораторной работы.

8. Закройте консоль администрирования MMC, сохранив ее.

При выполнении задания используйте следующие инструкции:

- перенесите последовательность выполняемых действий по пунктам 3-7 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
- сделайте вывод о проделанной работе и запишите его в отчет.

Контрольный вопрос:

Какой системный путь и имя файла журнала ошибок задействован по умолчанию в ОС Windows XP при организации анализа и настройки безопасности посредством одноименной оснастки?

С каким системным шаблоном безопасности осуществляется сравнение параметров анализируемого шаблона **MyFirstShablon** в текущем задании?

Для чего применяется команда **«Настроить компьютер…»** в меню **«Действие»** или в контекстном выпадающем меню оснастки **«Анализ и настройка безопасности»**?

Задание №7.1г. Изучение основных возможностей программного средства **«Брандмауэр подключения к Интернету»** в среде ОС Windows XP на конкретных примерах.

Теперь, когда основные действия по предотвращению несанкционированного локального проникновения определены, необходимо обеспечить дополнительный уровень защиты от потенциальных атак извне. Одним самых важных, штатных компонентов защиты ОС Windows XP от внешних угроз является инструмент, ограничивающий обмен информацией между локальной средой и сетью Интернет, **«Брандмауэр подключения к Интернету» (Internet Connection Firewall, ICF)**, коротко брандмауэр или сетевой экран.

ICF представляет собой достаточно мощную систему защиты, которая отслеживает все аспекты работы линий связи и проверяет исходные и конечные адреса информационных пакетов. Для предотвращения попадания нежелательного трафика в локальную сеть из Интернета **ICF** содержит список всех соединений контролируемого компьютера, располагающихся в специальной таблице. Входящий трафик сравнивается с данными из этой таблицы и при несовпадении входящие пакеты блокируются. В частности, это препятствует атакам в виде сканирования портов из сети Интернет. При этом стоит помнить, что **ICF** блокирует любой пакет, неожиданно приходящий в локальную сеть, включая те, которые могут быть полезны пользователю, например, пакеты электронной почты. Поэтому **ICF** необходимо сконфигурировать таким обра-

зом, чтобы исключить подобные коллизии и пропускать сообщения, направляя их соответствующему адресату.

Для ознакомления с базовыми возможностями брандмауэра **ICF** в среде ОС Windows XP выполните следующее:

1. Включите **ICF** в среде ОС Windows XP. Для этого необходимо выбрать сетевое подключение **(«Пуск | Панель управления | Сетевые подключения»)**, предполагаемое к защите посредством **ICF**. Затем, либо из контекстного меню выбрать команду **«Свойства»**, либо щелкнуть по команде **«Изменение настроек подключения»** слева в группе команд **«Сетевые задачи»**. В окне **«Свойства сетевого подключения»** на вкладке **«Дополнительно»** необходимо щелкнуть по кнопке **«Параметры»** брандмауэра Windows и закрыть несанкционированный доступ из сети, выбрав **«Включить (рекомендуется)»** на появившейся вкладке **«Общие»**.

2. Для обеспечения контроля за действиями **ICF** в системе предусмотрен механизм ведения журнала безопасности, который позволяет создавать список действий системы защиты, а именно установку запрета или разрешения на трафик со стороны **ICF**. Это бывает весьма полезно при организации безопасной среды. Включение процесса документирования за действиями **ICF** осуществляется на вкладке **«Дополнительно»** брандмауэра Windows. Для этого необходимо щелкнуть по кнопке **«Параметры»** в разделе **«Ведение журнала безопасности»**, поставить опциональные флажки напротив **«Записывать пропущенные пакеты»** и **«Записывать успешные подключения»**. Подтвердите операцию, нажав **OK**.

Кроме того, имеется возможность регулировать дополнительную функциональность по протоколу управляющих сообщений Интернета **ICPM** (в частности, позволяющего компьютерам в сети обмениваться информацией об ошибках). Список запросов из сети Интернет, на которые будет отвечать конфигурируемый компьютер, представлен в виде набора параметров в разделе **«Протокол ICMP»** на вкладке **«Дополнительно»**.

Включите протоколирование следующих сообщений:

- входящих эхо-запросов;
- входящих меток времени;
- входящих запросов маршрутизатора;
- переадресацию.

Уместно отметить, что по своей сути журнал **ICF** является программным средством, также предназначенным для аудита системы безопасности наряду с теми, что были достаточно подробно изучены в лабораторной работе № 5. К числу подобных средств также следует отнести автономную оснастку **«Просмотр событий»**, расширение **«Политика аудита»** в рамках оснастки **«Политика «Локальный компьютер»**, а также рассмотренную в предыдущем задании оснастку **«Анализ и настройка безопасности»**.

В частности, посредством расширения **«Политика аудита»** можно осуществлять проверку и регистрацию событий в следующих категориях:

- управление учетной записью,
- ввод-вывод данных в сети,
- доступ к конкретному объекту (файлу или каталогу),
- изменение политик сети,
- попытки использования специальных привилегий,
- загрузка пользовательских процессов,
- другие системные действия.

Поскольку аудит в значительной степени расходует системные ресурсы, необходимо заранее определиться с элементами, требующими контроля (иными словами, надо четко представлять себе что необходимо контролировать, чтобы излишне не нагружать систему).

3. Журнал **ICF** имеет свой уникальный формат. В заголовке указываются версия используемого межсетевого экрана **ICF**, имя журнала безопасности, примечание о том, что вход в систему регистрируется по локальному времени, и список доступных полей для регистрационных записей (табл. 7.2).

Польза журнала безопасности **ICF** состоит в том, что после его просмотра можно обнаружить попытки несанкционированного доступа к сети. Изучив поля **action**, **scr-ip** и **dst-ip**, в частности, можно определить, пытается ли кто-то повредить сеть в целом или вывести из строя какое-то определенное устройство.

В любой текстовый редактор загрузите журнал безопасности **ICF**, располагающийся в системном каталоге **C:\Windows\pfirewall.log** и найдите все его отмеченные атрибуты, поля и изучите содержимое журнала в целом, воспользовавшись таблицей 7.2. Вероятно, может оказаться, что осуществленных записей в журнале **ICF** будет не слишком много — это связано с тем, что журнал безопасности был активирован сравнительно недавно.

Дополнительно журнал безопасности **ICF** может быть переименован и сохранен в место, путь к которому системный администратор определяет самостоятельно. Это удобно в том случае, когда имеется необходимость вести несколько отчетов, например, по дням недели или времени дня. Размер файла журнала безопасности **ICF** может быть изменен на вкладке **«Параметры журнала»** с установленного в 4Мб по умолчанию до 32Мб по необходимости.

4. Иногда в процессе работы возникает необходимость не контролировать брандмауэром **ICF** трафик, проходящий в сети через доверенные специализированные приложения, например, приложения контроля информационных пакетов, торрент-клиенты или трафик, проходящий через определенные открытые порты, например, настроенные под так называемый «портфорвардинг». Для этих целей в **ICF** предусмотрена возможность исключений.

Для активации данной возможности по отношению к программам на вкладке **«Исключения»** брандмауэра Windows добавьте, для примера, выбранное приложение, генерируемый трафик которого не будет контролироваться впредь. Закройте окно **«Добавление программы»** и обратите внимание на то, что только что выбранная программа появилась в области исключений **«Программы и службы»** на исследуемой вкладке (напротив неконтролируе-

мого приложения стоит флажок активации, снятие которого обратно приводит к контролю трафика этого приложения).

Таблица 7.2. Поля ввода данных в журнале безопасности **ICF**

№ п/п.	Поле журнала безопас-ности ICF	Описание поля
1.	**Action**	Операция, перехваченная брандмауэром Windows. Входящие данные включают в себя: **OPEN**, **CLOSE**, **DROP**, **INFO-EVENTS-LOST** (указывается количество произошедших событий, не сохраненных в журнале).
2.	**Date**	Дата ввода файла в формате **YY-MM-DD** (год-месяц-день).
3.	**Dst-ip**	**IP**-адрес конечного пункта доставки пакета.
4.	**Dst-port**	Номер порта конечного пункта доставки пакета.
5.	**Icmpcode**	Число, обозначающее поле кода в **ICMP**-сообщении.
6.	**Icmptype**	Число, обозначающее поле ввода текста в **ICMP**-сообщении.
7.	**Info**	Поле для ввода информации о событии, которое зависит от типа действия.
8.	**Protocol**	Протокол связи. Если это не **TCP**, **UDP** или **ICMP**, то здесь указывается цифра.
9.	**Size**	Размер пакета (байт).
10.	**Scr-ip**	**IP**-адрес устройства-отправителя.
11.	**Scr-port**	Номер порта отправителя.
12.	**Tcpack**	**TCP**-номер подтверждения пакета.
13.	**tcp-flags**	**TCP**-флаг, указываемый в начале пакета: **A** – Ack (важность поля подтверждения), **F** – Fin (последний пакет), **P** – Psh (функция «проталкивания» пакета), **S** – Syn (синхронизация последовательности номеров), **U** – Urg (важность поля указателя срочности).
14.	**Tcpsyn**	**TCP**-последовательность номеров пакетов.
15.	**Tcpwin**	**TCP**-размер окна (байт).
16.	**Time**	Время регистрации файла в формате **HH:MM:SS** (часы:минуты:секунды).

5. Аналогичным образом добавьте в исключения порты **TCP** и **UDP** с номером **33474** и наименованием **«µTorrent»**, иногда используемые для организации обмена данными посредством одноименного торрент-клиента.

При выполнении задания используйте следующие инструкции:

- перенесите последовательность выполняемых действий по пунктам 1-5 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
- сделайте вывод о проделанной работе и запишите его в отчет.

Контрольный вопрос:

Какие альтернативные аппаратно-программные средства защиты компьютеров в сети Вам известны?

Изученные в первом задании лабораторной работы инструменты и возможности не являются исчерпывающими для всеобъемлющей организации сетевой безопасности в ОС (спектр специализированных программных средств, предназначенных для локальной и сетевой защиты компьютера, достаточно широк, а его детальное рассмотрение в лабораторном практикуме не представляется возможным), однако в первом приближении они позволяют обезопасить локальную рабочую среду и в некоторой степени защитить ее от сетевого проникновения извне.

Безопасность компьютера не ограничивается только лишь обеспечением сохранности данных, передаваемых по сети. Кроме того, имеется ряд дополнительных возможностей, которые реализуются в ОС при взаимодействии двух подсистем: безопасности и ввода/вывода. Основные возможности, возникающие при таком взаимодействии, главным образом, ориентированы на обеспечение безопасности отдельных объектов (файлов и каталогов) в рамках файловой системы. Рассмотрению этих вопросов будет посвящено следующее учебное задание настоящей лабораторной работы.

7.3.2. Учебное задание №2. Изучение базовых возможностей обеспечения безопасности объектов файловой системы NTFS в среде ОС Windows XP.

Порядок выполнения:

Термины FAT и NTFS являются общими названиями файловых систем (ФС), каждая из которых включает в себя несколько различных модификаций. Например, имеются следующие разновидности ФС FAT: FAT12, FAT16 и FAT32 и, напротив, существует две версии ФС NTFS — v.4.0 и v.5.0.

Если ранее в ОС Windows NT использовалась ФС NTFS v.4.0, то ОС Windows XP предлагает самую последнюю версию ФС NTFS — v.5.0, представленную еще в ОС Windows 2000. Хотя ФС обеих версий приспособлены к

взаимному чтению и записи объектов (файлов и каталогов), в ОС Windows XP имеется ряд преимуществ, которыми ОС Windows NT не наделена. К их числу, например, относятся:

- возможности создания «точек повторной обработки», которыми ОС Windows NT не в состоянии воспользоваться при обращении к жесткому диску с ОС Windows XP;
- также, ОС Windows NT будет игнорировать квоты дискового пространства, установленные под управлением ОС Windows XP;
- кроме того, ОС Windows NT в отличие от ОС Windows XP не сможет ни читать, ни делать запись в шифрованных файлах;
- и наконец, ОС Windows NT будет игнорировать журнал изменений, доступный в ОС Windows XP.

Указанные особенности делают ФС NTFS v.5.0 мощным инструментом безопасности с встроенными возможностями администрирования, который при правильном применении обеспечивает более продуктивную и эффективную организацию системы. Это обстоятельство выгодно отличает данную ФС от ее предыдущей версии и, тем более, от ФС FAT, в сравнении с которой также имеется ряд отличительных особенностей:

- ФС NTFS обеспечивает безопасность на уровне файлов, в отличие от общей безопасности ФС FAT;
- при помощи ФС FAT имеется возможность запретить или разрешить доступ из сети к части дискового пространства, в то время как с помощью ФС NTFS можно установить доступ к конкретным объектам (файлам и каталогам);
- ФС NTFS тесно взаимосвязана с подсистемой безопасности ОС, в целом, и взаимодействует с подсистемой безопасности сети, в частности.

Задание №7.2а. Изучение возможностей квотирования дискового пространства в среде ОС Windows XP на конкретных примерах.

Известно, что «памяти никогда не бывает много!». Это утверждение, в полной мере, относится к внешней памяти жесткого диска. В этой связи, администратору сетевых ресурсов необходимо контролировать расход доступной в его распоряжении внешней памяти. В ФС NTFS имеется штатное программное средство, позволяющее это делать — оно позволяет ограничивать свободное пространство на жестком диске, предполагаемое к выделению пользователям.

Процесс выделения пользователю определенного объема внешней памяти жесткого диска называется квотированием, а сам выделяемый объем — соответственно, квотой на дисковое пространство. Квотирование дискового пространства в организации необходимо с целью его безопасного расходования. Если свободное пространство на жестком диске ограничено, квоты помогут

избежать потери исключительно важных данных, которые просто могут не уместиться на заполненный до отказа диск.

В ОС Windows XP квотирование дискового пространства позволяет выполнять следующие действия.

- Уведомлять пользователя о том, что он превысил порог выдачи предупреждения (но при этом еще не израсходовал свою квоту).
- Не допускать запись на жесткий диск после того, как пользователь исчерпал отведенную ему квоту.

Квотирование диска работает индивидуально в отношении каждого пользователя и каждого тома. При этом квоты «прозрачны» для пользователя. Когда он смотрит на доступное пространство диска, то видит, сколько осталось от выделенной ему части. После исчерпания квоты на диске, дальнейшее сохранение данных невозможно. В этом случае пользователь может удалить объекты (файлы и каталоги) или передать их в собственность другого пользователя, чтобы освободить дисковое пространство, или же попросить сетевого администратора об увеличении котируемого объема.

При установлении пользователям квот необходимо помнить несколько принципиальных моментов. Квотируемый жесткий диск должен быть отформатирован в ФС NTFS. Лицо, выдающее квоты, должно иметь полномочия администратора. Порог выдачи предупреждения должен быть процентов на десять меньше, чем сама квота. Например, квота в 1Гб должна сопровождаться порогом выдачи предупреждения в 900Мб. Когда пользователь израсходует выделенные 900Мб, в регистрационном журнале будет сделана соответствующая запись; когда порог квотирования в 1Гб будет превышен, осуществляется запрет на дальнейшее использование жесткого диска и также делается соответствующая запись в журнале регистрации.

Для ознакомления с возможностями квотирования дискового пространства в среде ОС Windows XP выполните следующее.

Секция А. Активация возможности квотирования локального тома в среде ОС Windows XP.

1. Самостоятельно выберите локальный том, который предполагается квотировать. Например, это может быть тот диск, который не ограничен в применении административными установками.

2. Из контекстного выпадающего меню **«Свойства»** выберите вкладку **«Квота»**, на которой установите флажок рядом с надписью **«Включить управление квотами»**, тем самым, активизировав изучаемую функциональность.

3. Установите квоту в 1Гб и порог предупреждения в 900Мб, выделяемые по умолчанию для каждого нового пользователя квотируемого жесткого диска.

4. Задействуйте протоколирование превышение порога предупреждения и выделенной квоты в журнале регистрации.

5. Нажмите **ОК**, чтобы изменения вступили в силу.

Примечание. Уместно отметить, что выделение квот возможно не только для локальных пользователей, но и для удаленных. При этом обязательным условием, помимо указанных выше, должно быть то, что общим для доступа каталогом должен быть корневой каталог квотируемого тома.

Секция В. Протоколирование и управление квотами локального тома в среде ОС Windows XP.

После того, как дисковые квоты установлены, появляется возможность отслеживать пороги квот, статус предупреждения или реально использованное пространство.

1. Просмотрите выделенные пользователям квоты. Для этого манипулятором мышь щелкните на кнопке **«Записи квот»** и изучите появившийся список существующих в системе пользователей и выделенные им квоты. Обратите внимание на то, что в списке пользователей имеется учетная запись системной группы «Администраторы», у которой предельные значения порога превышения и самой квоты отсутствуют.

Примечание. Если в момент первого запуска диалоговое окно **«Записи квот»** окажется пустым, то необходимо заполнить список пользователей, за которыми предстоит вести наблюдение и протоколирование расхода их дискового пространства.

2. Введите в список нового пользователя, которому необходимо выделить квоту. Для этого в меню **«Квота»** на панели инструментов выберите команду **«Создать запись квоты…»**, а затем в появившемся окне добавьте стандартным способом соответствующего пользователя (в качестве примера можно взять пользователя с именем «Гость»). Обратите внимание на то, что в процессе создания новой записи квоты, имеется возможность установить особые значения предельных параметров порогового значения и самой квоты для данного пользователя.

В меню **«Квота»** также имеется возможность удалить ненужные записи. В случае необходимости удалите ненужного пользователя из сформированного списка. Это делается простым выбором команды **«Удалить запись квоты…»**.

3. Теперь предположим, что некоторому пользователю (например, с именем «Гость») требуется выделить дополнительное пространство на жестком диске. Для изменения его квоты необходимо в окне **«Записи квот»** правой кнопкой манипулятора мышь щелкнуть на его записи, выбрать команду **«Свойства»** и установить новые значения параметров в появившемся окне.

4. Закройте диалоговое окно **«Записи квот»** и нажмите **ОК**, чтобы изменения вступили в силу.

При выполнении заданий секций используйте следующие инструкции:

- перенесите последовательность выполняемых действий по пунктам 2-4 (Секция А) и 1-3 (Секция В) в отчет (возможно приведение гра-

фических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

- сделайте вывод о проделанной работе и запишите его в отчет.

Контрольный вопрос:

Что представляет собой учетная запись **BUILTIN\Администраторы**, отображаемая в списке диалогового окна **«Записи квот»**?

Для чего предназначен процесс сжатия файлов в системе? Можно ли использовать сжатие файлов в системе для предотвращения превышения пользователями заданных квот? Ответьте на вопрос почему?

Какие служебные программы командной строки (или одноименные команды интерпретатора) необходимо использовать для сжатия файлов и распределения квот в среде консоли алфавитно-цифрового терминала ОС Windows XP? Приведите пример использования данных команд при сжатии файлов и распределении квот?

Задание №7.2б. Изучение основных возможностей файловой системы EFS в среде ОС Windows XP на конкретных примерах.

Использование ФС EFS (Encrypting File System — шифрованная файловая система) в ОС Windows XP представляет собой дополнительную возможность защиты данных на жестком диске. При применении ФС EFS сохраняемые на диске файлы шифруются и становятся недоступными, пока к ним не будет обеспечен корректный доступ в рамках NTFS-тома.

При работе с ФС EFS лучше всего зашифровывать целый каталог, а не отдельные файлы. Это ускоряет процесс и делает его более эффективным. Таким образом, появляется возможность создать защиту группы файлов вместо шифрования отдельных из них. При шифровании каталога целиком все запасные копии файлов также шифруются (разумеется, только в том случае, если они хранятся в шифруемом каталоге).

Для ознакомления с возможностями ФС EFS в среде ОС Windows XP выполните следующее.

1. Войдите в систему под любой учетной записью (стандартной или созданной заранее). Наличие прав администратора не обязательно.

2. В служебном программном модуле **«Мой компьютер» (Пуск | Мой компьютер)** создайте самостоятельно каталог и скопируйте в него какой-либо файл, предполагаемый к шифрованию.

3. Щелкните правой кнопкой манипулятора мышь на созданном каталоге и выберите команду **«Свойства»** из контекстного выпадающего меню.

4. На вкладке **«Общие»** появившегося диалогового окна щелкните на кнопке **«Дополнительно»** (или **«Другие»**) и установите флажок рядом с надписью **«Шифровать содержимое для защиты данных»**.

5. Нажмите **«Применить»** и затем **ОК** для подтверждения операции.

Примечание. После шифрования объект будет выделен зеленым цветом.

6. Войдите в систему под другой учетной записью (например, созданной ранее в предыдущих заданиях лабораторной работы) и произведите открытие файла. Обратите внимание на полученный результат.

Примечание. Расшифровывание объектов возможно в обратном порядке и под той учетной записью, в рамках которой происходило шифрование.

При выполнении задания используйте следующие инструкции:

- перенесите последовательность выполняемых действий по пунктам 2-6 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
- сделайте вывод о проделанной работе и запишите его в отчет.

Контрольный вопрос:

Как Вы считаете, по какой причине наличие прав администратора при шифровании не обязательно? Чем обеспечивается защита данных при этом?

Может ли объект (файл или каталог) быть одновременно и зашифрованным, и сжатым? Как Вы считаете, почему?

Какая служебная программа командной строки (или одноименная команда интерпретатора) необходима для шифрования/дешифрования файлов в среде консоли алфавитно-цифрового терминала ОС Windows XP? Приведите пример использования данной команды при шифровании/дешифровании файлов?

Задание №7.2в. Изучение основных возможностей доступа к объектам в среде ОС Windows XP на конкретных примерах.

ОС Windows XP позволяет реализовать совместное использование файлов, папок, принтеров и других сетевых ресурсов. С этими ресурсами могут работать либо другие пользователи локального компьютера, либо пользователи, находящиеся в сети. То, каким образом ресурсы используются совместно, зависит от настройки системы.

Совместное использование на уровне каталога является базовым уровнем, на котором можно осуществлять управление. Совместное использование одного файла невозможно реализовать в ОС Windows XP. Файл должен быть перенесен или создан внутри папки, предназначенной для совместного использования.

Для совместного использования ресурсов в сети сначала необходимо инициировать службу доступа к файлам и принтерам сетей Microsoft **(File and Printer Sharing for Microsoft Networks)**. Если отсутствует вкладка **«Доступ»** в диалоговом окне свойств папки, то указанная служба не подключена.

Поскольку данная служба, как правило, устанавливается в автоматическом режиме в процессе установки ОС, ее ручное инсталлирование не пред-

ставляется к рассмотрению в рамках лабораторной работы (инструкция по процедуре ручного добавления данной службы доступна в центре справки и поддержки ОС, а также на специализированных ресурсах глобальной сети).

ОС Windows XP предлагает пять уровней доступа к объектам (файлам и каталогам) ФС NTFS, которые необходимо знать и разделять, чтобы корректно настраивать параметры безопасности в соответствии с потребностями организации при совместном использовании сетевых ресурсов. Каждый из указанных уровней доступа рассматривается далее в соответствующей секции текущего задания лабораторной работы.

Внимание! Дальнейшее конфигурирование параметров безопасности показано на примере ОС с подключенной опцией **«Простой общий доступ к файлам»** (**«Пуск | Панель управления | Свойства папки»**, вкладка **«Вид»**, окно **«Дополнительные параметры»**), достаточно подробно рассмотренной в лабораторной работе №5.

Секция А. Изучение первого уровня доступа к объектам файловой системы NTFS в среде ОС Windows XP.

Первый уровень (Уровень I) доступа является самым строгим в ФС NTFS: только владелец объекта может читать и модифицировать его. Другие пользователи, включая сетевого администратора, не имеют доступ к таким объектам. Все объекты в каталоге с первым уровнем доступа сохраняют тот же уровень секретности, что и родительский каталог.

Примечание. Возможность создания каталога Уровня I доступна только для учетной записи группы **«Пользователи»** и только в рамках его собственной папки **«Мои документы»**.

Для обеспечения доступа Уровня I необходимо выполнить следующее.

1. Одним из ранее изученных способов создайте новую учетную запись пользователя с правами группы **«Пользователи»** или воспользуйтесь уже готовой учетной записью, полученной в предыдущих заданиях.

2. Войдите в систему с правами группы **«Пользователи»**, воспользовавшись только что созданной учетной записью, и создайте в служебном каталоге **«Мои документы»** (расположен в соответствующем профиле учетной записи) новый подкаталог с именем, выбранным самостоятельно.

3. Установите **«Простой общий доступ к файлам»**, как указано выше.

4. Щелкните правой кнопкой манипулятора мышь на созданном каталоге и выберите команду **«Общий доступ и безопасность»** из выпадающего контекстного меню.

5. В появившемся диалоговом окне на вкладке **«Доступ»** установите флажок рядом с надписью **«Отменить общий доступ к этой папке»** в категории доступа **«Локальный общий доступ и безопасность»**.

6. Нажмите **«Применить»** (в случае необходимости установите новый пароль на текущую учетную запись) и **ОК** для подтверждения операции.

7. Войдите в систему под любой другой учетной записью (в том числе и с правами администратора) и убедитесь, что созданный каталог является недоступным для открытия, тем самым, обеспечивая конфиденциальность сохраненных в нем данных.

Секция B. Изучение второго уровня доступа к объектам файловой системы NTFS в среде ОС Windows XP.

На втором уровне (Уровень II) владелец файла и администратор имеют права на чтение и запись в файле или каталоге. В ОС Windows XP это является настройкой по умолчанию для каждого пользовательского файла в служебном каталоге **«Мои документы»**.

Для обеспечения доступа Уровня II необходимо выполнить следующее.

1. Одним из ранее изученных способов создайте новую учетную запись пользователя с правами группы **«Пользователи»** или воспользуйтесь уже готовой учетной записью, полученной в предыдущих заданиях.

2. Войдите в систему с правами группы **«Пользователи»**, воспользовавшись только что созданной учетной записью, и создайте в служебном каталоге **«Мои документы»** (расположен в соответствующем профиле учетной записи) новый подкаталог с именем, выбранным самостоятельно.

3. Установите **«Простой общий доступ к файлам»**, как указано выше, если он еще не был установлен.

4. Щелкните правой кнопкой манипулятора мышь на созданном каталоге и выберите команду **«Общий доступ и безопасность»** из выпадающего контекстного меню.

5. В появившемся диалоговом окне на вкладке **«Доступ»** удалите флажки рядом с надписью **«Отменить общий доступ к этой папке»** в категории доступа **«Локальный общий доступ и безопасность»** и надписью **«Открыть общий доступ к этой папке»** в категории доступа **«Сетевой общий доступ и безопасность»**, если они находятся в установленных положениях.

6. Нажмите **«Применить»** и **OK** для подтверждения операции.

7. Войдите в систему под любой другой учетной записью, кроме административной (если необходимо, создайте еще одну с правами пользователя) и убедитесь, что созданный каталог является недоступным для удаления и модификация его содержимого невозможна.

Секция C. Изучение третьего уровня доступа к объектам файловой системы NTFS в среде ОС Windows XP.

Третий уровень (Уровень III) позволяет пользователям, входящим в систему из локальной сети, совместно использовать объекты ФС NTFS (файлы и каталоги). В зависимости от типа пользователя ему позволено или запрещено

выполнять определенные действия с файлами Уровня III в каталоге **«Общие документы»**. В частности,

- администраторы локальных компьютеров и опытные пользователи имеют полный доступ,
- ограниченные пользователи имеют доступ «только для чтения»,
- удаленные пользователи не имеют доступа к файлам Уровня III.

Для обеспечения доступа Уровня III необходимо выполнить перемещение желаемого объекта файловой системы в каталог **«Общие документы»**. Выполните следующее:

Воспользовавшись знаниями, полученными в предыдущих заданиях, самостоятельно создайте объект ФС NTFS с доступом Уровня III и занесите последовательность выполняемых действий в отчет.

Секция D. Изучение четвертого уровня доступа к объектам файловой системы NTFS в среде ОС Windows XP.

Один из самых распространенных уровней сетевого доступа является Уровень IV. На этом уровне объекты ФС NTFS доступны для чтения всем удаленным пользователям. Локальные пользователи также имеют право чтения (это касается и учетных записей «Гость»), но не имеют права записи и модификации объектов.

Внимание! Право организации доступа Уровня IV присвоено администратору сети.

Для обеспечения доступа Уровня IV необходимо выполнить следующее:

1. На двух узлах локальной сети создайте новые учетные записи пользователей: на первом узле — с правами группы **«Администраторы»**, на втором — с правами группы **«Пользователи»**. В случае необходимости возможно использование уже готовых учетных записей, созданных в предыдущих заданиях. Если реальная локальная сеть недоступна, воспользуйтесь виртуальной локальной сетью (Лабораторная работа №8 посвящена методике ее построения).

2. На первом узле войдите в систему с правами администратора, воспользовавшись только что созданной учетной записью. Создайте в любом месте локального тома новый каталог с именем, выбранным самостоятельно и запишите в него любой текстовый файл для дальнейших операций.

3. Установите **«Простой общий доступ к файлам»**, как указано выше, если он еще не был установлен.

4. Щелкните правой кнопкой манипулятора мышь на созданном каталоге и выберите команду **«Общий доступ и безопасность»** из выпадающего контекстного меню.

5. В появившемся диалоговом окне на вкладке **«Доступ»** установите флажок рядом с надписью **«Открыть общий доступ к этой папке»** в категории доступа **«Сетевой общий доступ и безопасность»** и удалите флажок ря-

дом с надписью **«Разрешить изменение файлов по сети»**, если он находится в установленном положении.

6. Нажмите **«Применить»** и **OK** для подтверждения операции.

7. На втором узле войдите в систему с правами пользователя, воспользовавшись только что созданной учетной записью. В сетевом окружении домена найдите узел, на котором в предыдущих пунктах задания был открыт общий доступ к каталогу. Откройте созданный администратором предыдущего узла каталог и произведите чтение данных из текстового файла, находящегося внутри.

8. Убедитесь, что созданный каталог является недоступным для удаления и модификация его содержимого по сети невозможна.

Секция E. Изучение пятого уровня доступа к объектам файловой системы NTFS в среде ОС Windows XP.

Второй из распространенных уровней сетевого доступа, который (по мнению автора) достаточно часто встречается при организации локальной сети, в том числе, в домашних условиях, — Уровень V. Этот уровень является наиболее «разрешенным» с точки зрения безопасности объектов файловой системы. Любой пользователь локальной сети может читать, записывать данные по сети, удалять файлы и каталоги, а также модифицировать их содержимое. Из этого следует, что такой уровень безопасности следует вводить только в закрытых и надежно защищенных от внешнего воздействия локальных сетях.

Внимание! Право организации доступа Уровня V присвоено администратору сети.

Для обеспечения доступа Уровня V необходимо выполнить следующее:

1. На двух узлах локальной сети создайте новые учетные записи пользователей: на первом узле — с правами группы **«Администраторы»**, на втором — с правами группы **«Пользователи»**. В случае необходимости возможно использование уже готовых учетных записей, созданных в предыдущих заданиях. Если реальная локальная сеть недоступна, воспользуйтесь виртуальной локальной сетью (Лабораторная работа №8 посвящена методике ее построения).

2. На первом узле войдите в систему с правами администратора, воспользовавшись только что созданной учетной записью. Создайте в любом месте локального тома новый каталог с именем, выбранным самостоятельно и запишите в него любой текстовый файл для дальнейших операций.

3. Установите **«Простой общий доступ к файлам»**, как указано выше, если он еще не был установлен.

4. Щелкните правой кнопкой манипулятора мышь на созданном каталоге и выберите команду **«Общий доступ и безопасность»** из выпадающего контекстного меню.

5. В появившемся диалоговом окне на вкладке **«Доступ»** установите флажок рядом с надписью **«Открыть общий доступ к этой папке»** и флажок

рядом с надписью **«Разрешить изменение файлов по сети»** в категории доступа **«Сетевой общий доступ и безопасность»**.

6. Нажмите **«Применить»** и **OK** для подтверждения операции.

7. На втором узле войдите в систему с правами пользователя, воспользовавшись только что созданной учетной записью. В сетевом окружении домена найдите узел, на котором в предыдущих пунктах задания был открыт общий доступ к каталогу. Откройте созданный администратором предыдущего узла каталог и произведите чтение данных из текстового файла, находящегося внутри.

8. Убедитесь, что созданный каталог является доступным для модификации. Для этой цели модифицируйте по сети содержимое текстового файла в каталоге с общим доступом и сохраните его.

Если модификация файла оказалась невозможной, ответьте на контрольные вопросы в конце задания.

При выполнении заданий секций используйте следующие инструкции:

- перенесите последовательность выполняемых действий по пунктам 3-7 (Секция A), 4-7 (Секция B), 1 (Секция C), 4-8 (Секция D) и 4-8 (Секция E) в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
- сделайте вывод о проделанной работе и запишите его в отчет.

Контрольный вопрос:

Что необходимо сделать применительно к учетной записи пользователя, чтобы осуществить модификацию данных по локальной сети, рассмотренной в примере секции E задания №7.2в?

Приведите пример того, каким образом это возможно сделать в рамках настоящей лабораторной работы?

Полученные в настоящей лабораторной работе знания и изученные возможности снабжают потенциального системного администратора или опытного пользователя базовым инструментарием, ориентированным на обеспечение безопасности компьютера от различного рода сетевых воздействий, атак или угроз как локальных, так и внешних.

Для более детального изучения рассмотренных в лабораторной работе вопросов и других аспектов сетевого администрирования, а также приобретения практических навыков по проектированию безопасности сети в среде ОС семейства Windows целесообразно обратится к учебному курсу MCSE «Безопасность сети на основе Windows 2000» от корпорации Microsoft, который на глубоком профессиональном уровне освещает данную тематику, а также справочнику администратора «Microsoft Windows XP Professional. Администрирование сетей» Роберта Элсенпитера и Тоби Велта для получения дополнительных знаний в рассматриваемых вопросах.

7.4. Содержание отчета по лабораторной работе

Внимание! Прежде чем приступать к оформлению настоящей лабораторной работы, необходимо по окончании ее выполнения аккуратно удалить за собой все рабочие файлы, оснастки и консоли, созданные в процессе.

Отчет по лабораторной работе оформляется в соответствии с требованиями государственного стандарта и должен содержать:

1) титульный лист (**Приложение**);

2) описание и цель работы;

3) краткое описание консоли администрирования MMC, потенциальных возможностей и функций, доступных при ее организации для целей обеспечения локальной и сетевой безопасности в среде ОС Windows XP;

4) краткое описание программных средств и возможностей, ориентированных на обеспечение безопасности ФС NTFS в среде ОС Windows XP;

5) результаты изучения политик безопасности, системных программных средств и настроек ОС, ориентированных на создание безопасной локальной среды ОС Windows XP;

6) письменные ответы на контрольные вопросы, размещенные в соответствующих учебных заданиях лабораторной работы;

7) выводы о проделанной работе.

Лабораторная работа №8

Организация виртуальной локальной сети в ОС Windows XP

Цель работы: Изучить технологию виртуализации альтернативной ОС и рассмотреть возможность организации виртуальной локальной сети на ее основе в среде ОС Windows XP.

8.1. Краткие теоретические сведения

Технология виртуализации предназначена для осуществления возможности одновременного запуска на одном компьютере нескольких (в том числе, различных) ОС. Это позволяет пользователям (и/или системным администраторам) иметь ряд преимуществ при одновременной работе в альтернативных средах без перезапуска самого компьютера. Причем, работая с альтернативной ОС, пользователь не чувствует никаких ограничений в использовании ее возможностей, получая полную иллюзию работы с реальной системой. При этом в такой системе имеется возможность выполнять различные малоизученные или потенциально опасные для нее операции, не беспокоясь о последствиях: поскольку система является виртуальной, ее крах или частичное повреждение не скажется на работе реальной ОС.

Основные преимущества такого подхода состоят в следующем:

- появляется возможность инсталляции на одном компьютере нескольких ОС без необходимости соответствующего конфигурирования физических жестких дисков;
- возможно осуществлять работу с несколькими ОС одновременно с динамическим переключением между ними без перезагрузки реальной системы;
- сокращается время изменения состава и конфигурации установленных виртуальных ОС;
- осуществляется изоляция реального оборудования от нежелательного воздействия программного обеспечения, работающего в среде виртуальной ОС;
- появляется возможность моделирования вычислительной сети на единственном автономном компьютере.

Благодаря этим преимуществам существенно расширяется круг задач, которые можно решать без перезагрузки системы и без опасения нанести ей какой-либо ущерб. Основные из них:

- освоение новой, альтернативной ОС;
- запуск специализированных приложений, предназначенных для работы в среде конкретной ОС;
- тестирование одного приложения под управлением различных ОС;

- установка и удаление оценочных или демонстрационных версий новых приложений;
- тестирование потенциально опасного программного обеспечения, относительно которого имеется подозрение на вирусное заражение;
- управление правами доступа пользователей к данным и программам в пределах виртуальной среды.

Все сказанное выше реализуется посредством применения специализированных инструментов, позволяющих организовывать виртуальную вычислительную среду. Иными словами, этот класс приложений ориентирован на развертывание, так называемых, виртуальных машин.

С точки зрения пользователя, *виртуальная машина* (ВМ) — это конкретный экземпляр некой виртуальной вычислительной среды («виртуального компьютера»), созданный с помощью специального программного инструмента. Обычно такие инструменты позволяют создавать и запускать произвольное число виртуальных машин, ограничиваемое лишь физическими ресурсами реального компьютера.

Собственно инструмент для создания ВМ (его иногда называют *приложением виртуальных машин*) — это обычное приложение, устанавливаемое, как и любое другое, в рамках реальной ОС, именуемую *хостовой* или *ведущей*.

В рамках ВМ пользователь устанавливает, как и на реальном компьютере, нужную ему ОС. Такая ОС, принадлежащая конкретной ВМ, называется *гостевой*. Перечень поддерживаемых гостевых ОС является одной из наиболее важных характеристик ВМ. Наиболее мощные из современных ВМ обеспечивают поддержку более десятка популярных версий ОС семейств Windows, Linux и Mac OS.

Виртуальные машины могут быть построены на базе различных платформ и при помощи разных технологий. Используемая схема виртуализации зависит как от аппаратной платформы, так и от особенностей взаимодействия *хостовой* и поддерживаемых *гостевых* ОС. Некоторые архитектуры обеспечивают возможность виртуализации на аппаратном уровне, другие, напротив, требуют применения дополнительных программных средств.

В настоящее время наибольшее распространение получили три схемы виртуализации:

- эмуляция API гостевой ОС;
- полная эмуляция гостевой ОС;
- квазиэмуляция гостевой ОС

В первом случае, приложение работает в изолированном адресном пространстве и взаимодействует с оборудованием при помощи интерфейса прикладного программирования API, предоставляемого *хостовой* ОС. Если две ОС совместимы по интерфейсу API (например, Windows 98 и Windows ME), то приложение, разработанное для одной из них, будет работать и на другой. Если, напротив, две ОС несовместимы по интерфейсу API (Windows 2000 и Linux), то необходимо обеспечить перехват обращений приложений к API *гостевой* ОС и имитировать ее поведение средствами *хостовой*. При таком

подходе можно установить одну ОС и работать одновременно как с ее приложениями, так и с приложениями альтернативной ОС.

Поскольку весь код приложения исполняется без эмуляции, а эмулируются лишь вызовы API, такая схема виртуализации приводит к незначительной потере в производительности ВМ. Однако, из-за того, что многие приложения используют недокументированные функции API или обращаются к ОС в обход API, даже очень мощные эмуляторы API имеют проблемы совместимости и позволяют запускать не более 70% от общего числа приложений. Кроме того, поддерживать эмуляцию API бурно развивающейся системы, типа Windows, очень нелегко, и большинство эмуляторов API так и остаются эмуляторами какой-то конкретной версии ОС.

Примеры продуктов, выполненных по данной технологии:

- проект Wine, позволяющий запускать DOS-, Win16- и Win32-приложения под управлением ОС Linux и ОС Unix;
- продукт Win4Lin компании Netraverse, позволяющий запускать ОС семейства Windows под управлением ОС Linux:
- проект DOSEMU, позволяющий запускать DOS-приложения под управлением ОС Linux;
- проект UML, позволяющий запускать несколько копий ОС Linux на одном компьютере;
- российский проект Virtuozzo, также позволяющий запускать несколько копий ОС Linux на одном компьютере.

Второй случай — это проекты, поддерживающие технологию полной эмуляции, работают по принципу интерпретации инструкций системы команд *гостевой* ОС. Поскольку при этом полностью эмулируется поведение как центрального процессора, так и всех внешних устройств, то существует возможность эмулировать компьютер с архитектурой Intel x86 на компьютерах с совершенно другой архитектурой, например на рабочих станциях Mac или на серверах Sun, реализуемых на RISC-процессорах.

Главный недостаток полной эмуляции заключается в существенной потере производительности *гостевой* ОС. Поэтому до недавнего времени ВМ с полной эмуляцией чаще всего использовались в качестве низкоуровневых отладчиков для исследования и трассировки ОС. Однако благодаря значительному росту вычислительной мощности в последнее время этот недостаток становится все менее значимым. Наиболее яркий представитель этого вида ВМ — продукт Virtual PC от Microsoft. В качестве других примеров можно привести:

- проект Bochs, позволяющий запускать различные ОС, ориентированные на архитектуру Intel x86, под ОС Linux, Windows и Mac OS;
- продукт Simics, позволяющий запускать различные ОС архитектуры Intel x86 под управлением ОС семейства Windows и других ОС;
- проект Qemu — эмулятор различных архитектур на компьютере.

Технология квазиэмуляции *гостевой* ОС основана на том обстоятельстве, что далеко не все инструкции *гостевой* ОС нуждаются в прямой эмуляции

средствами *хостовой* ОС. Многие из инструкций, необходимых для корректной работы *гостевых* приложений, могут быть непосредственно адресованы *хостовой* ОС. Исключение составляют инструкции для управления, например, такими устройствами, как видеокарта, некоторые контроллеры, таймер.

Таким образом, в процессе работы ВМ с квазиэмуляцией происходит выборочная эмуляция инструкций *гостевой* ОС. Очевидно, что производительность такой ВМ должна быть выше, чем в предыдущем случае.

Примеры проектов, выполненных по технологии квазиэмуляции:

- технология Virtual Platform, на базе которой компания VMware предлагает ряд продуктов, в том числе приложение для рабочих станций VMware Workstation;
- российские продукты Serenity Virtual Station и Parallels Workstation от компании Параллели (англ. Parallels);
- проект Plex86, позволяющий запускать различные ОС архитектуры Intel x86 под управлением ОС Linux.
- проект L4Ka, использующий микроядерную архитектуру ОС;
- проект Xen, позволяющий запускать модифицированные ОС Linux, FreeBSD, NetBSD и Windows XP под управлением ОС Linux, FreeBSD, NetBSD, а также, при соблюдении некоторых условий, обеспечивающий даже прирост производительности.

В рамках настоящей лабораторной работы дальнейшее изучение технологии виртуализации будет реализовано на примере одного из лучших в своем роде программных продуктов — VMware Workstation v.6.5.

Перечень *гостевых* ОС, которые могут быть установлены с применением продуктов семейства VMware, весьма обширен:

- полное семейство ОС Windows — начиная с Windows 3.1x и заканчивая Windows Vista, а также MS-DOS 6.22;
- практически все представители ОС Linux: семейство Mandrake Linux, семейство Red Hat Linux, семейство SuSE Linux, семейство Turbolinux, семейство Ubuntu и другие;
- семейство ОС NetWare от компании Novell;
- семейство ОС Solaris от компании Sun;
- семейство Unix-подобных ОС FreeBSD и NetBSD.

В качестве *хостовой* ОС могут использоваться следующие ОС:

- из семейства ОС Windows: Windows 2000 Professional, Windows 2000 Server и Advanced Server, Windows XP (Home или Professional), семейства Windows Server 2003 и Windows Server 2008;
- из семейства ОС Linux: Mandrake Linux, Red Hat Linux и SuSE Linux.

Следует отметить, что приведенные выше списки *гостевых* и *хостовых* ОС постоянно пополняются другими версиями этих систем, поэтому более подробную и актуальную информацию о поддерживаемых продуктах необходимо искать на официальном сайте компании VMware (www.vmware.com).

Другие яркие представители рассматриваемого типа программного обеспечения, такие как Virtual PC 2004 от компании Microsoft и Parallels Workstation от российской Parallels, очень подробно описаны в книге Гультяева А.К. «Виртуальные машины: несколько компьютеров в одном».

8.2. Подготовка к выполнению лабораторной работы

В настоящей лабораторной работе предполагается получение знаний и навыков по развертыванию виртуальной среды и созданию виртуальной машины с использованием альтернативной ОС в рамках данной среды. Конечным этапом лабораторной работы должен стать процесс настройки виртуальной локальной сети между *хостовой* и *гостевой* ОС с организацией гостевого доступа к общим ресурсам и объектам (файлам и каталогам) обеих ОС.

В качестве альтернативной ОС предполагается использовать Unix-подобную ОС PC-BSD (www.pcbsd.ru) для рабочих станций, ядро которой абсолютно идентично ядру серверной ОС FreeBSD. Разница заключается лишь в том, что ОС PC-BSD наделена дружественным, ориентированным на пользователя графическим интерфейсом, что позволяет использовать ее в домашних условиях и при этом иметь все преимущества и непревзойденную надежность серверной ОС FreeBSD (www.freebsd.org).

Перед началом выполнения лабораторной работы в среде ОС Windows XP необходимо выполнить следующее:

1) загрузить ОС Windows XP;

2) скачать 30-дневную пробную версию программного продукта VMware Workstation v.6.5 с официального сайта www.vmware.com или локально с сайта института.

3) скачать свободно распространяемую ОС PC-BSD для рабочих станций с официального сайта www.pcbsd.ru или локально с сайта института.

Для предварительного изучения возможностей указанных выше программных продуктов, их способов применения и особенностей, целесообразно воспользоваться справочной информацией на официальных сайтах производителей данного программного обеспечения (**примечание:** необходимо знание технического английского языка).

8.3. Порядок выполнения лабораторной работы

Лабораторная работа выполняется последовательно в соответствии с определенным порядком и включает в себя два учебных задания.

Для выполнения лабораторной работы необходимо у системного администратора получить права полного доступа в текущем домене.

8.3.1. Учебное задание №1. Создание виртуальной машины на основе Unix-подобной ОС PCBSD с использованием программного продукта VMware Workstation в среде ОС Windows XP.

Порядок выполнения:

Организация вычислительной среды в рамках виртуальной машины прежде всего подразумевает установку соответствующего программного обеспечения (ПО), ориентированного на реализацию задуманного. 30-дневная оценочная версия программного продукта VMware Workstation доступна на сайте производителя и должна быть скачана при подготовке к данной лабораторной работе. Для полнофункциональной работы оценочной версии продукта необходимо получить у разработчика соответствующий регистрационный ключ.

Создание виртуальной машины на базе альтернативной Unix-подобной ОС PCBSD логично разделить на четыре последовательно выполняемых в среде ОС Windows XP этапа:

A. Установка ПО VMware Workstation;

B. Настройка ПО VMware Workstation;

C. Создание и настройка ВМ на основе ПО VMware Workstation;

D. Установка ОС PCBSD в рамках среды ПО VMware Workstation.

Рассмотрим более подробно каждый из этих этапов.

Этап A. Установка программного обеспечения VMware Workstation в среде ОС Windows XP.

Для установки ПО VMware Workstation необходимо выполнить следующие действия:

1. Запустите на выполнение файл **Setup.exe** скачанного с официального сайта разработчика дистрибутива ПО VMware Workstation.

2. Следуя мастеру установки, примите лицензионное соглашение и определите нужны ли ярлыки для запуска ПО VMware Workstation с рабочего стола, из панели задач или из меню **Пуск.**

3. При необходимости выберите каталог отличный от системного **Program Files** для установки ПО VMware Workstation и нажмите **«Далее»** для подтверждения операции.

4. После этого программа установки выполнит сканирование параметров *хостовой* ОС и возможно попросит скорректировать некоторые из них. Например, если на хост-компьютере разрешена функция автозапуска (**AutoRun**) для дисков CD/DVD, то на экране появится предупреждение, что она может привести к непредсказуемым эффектам при взаимодействии *хостовой* ОС с ВМ, а потому лучше эту функцию отключить, оставив в исходном положении флажок рядом с надписью **«Yes, Disable autorun on the host»**. Определившись с функцией автозапуска, щелкните мышью по кнопке **«Установить».**

5. В процессе установки ПО VMware Workstation на *хостовую* ОС выполняется также установка вспомогательных драйверов (необходимых, в частности, для работы с устройствами USB и SCSI). Если ПО VMware Workstation устанавливается в среде ОС Windows XP SP1 или SP2, то некоторые из таких драйверов могут оказаться непроверенными на совместимость с системой, о чем программа установки предупредит. Поскольку программные продукты от компании VMware работают весьма корректно, можно продолжить установку.

6. Перед завершением своей работы мастер предложит вам ввести регистрационные сведения (имя пользователя, название организации, серийный номер продукта). Процедура установки заканчивается созданием в меню **Пуск** соответствующей программной группы, в которую входят три ярлыка:

- **Virtual Network Editor** (Редактор виртуальной сети) — ярлык для запуска панели конфигурирования базовых параметров виртуальных сетей, создаваемых ПО VMware Workstation;
- **VMware Workstation** (Рабочая станция VMware) — ярлык для запуска панели управления ПО VMware Workstation;
- **VMware Player** (Проигрыватель VMware) — ярлык для запуска приложения, обеспечивающего загрузку виртуальной машины, минуя среду панели управления ПО VMware Workstation.

7. На этом процесс установки ПО VMware Workstation можно считать завершенным и целесообразно перейти к следующему этапу настройки.

Этап В. Настройка программного обеспечения VMware Workstation в среде ОС Windows XP.

Для настройки установленного ПО VMware Workstation необходимо выполнить следующие действия:

1. При первом запуске приложения VMware Workstation на экране появляются дна окна: на переднем плане — окно с «советами на каждый день», а за ним — основное окно продукта VMware Workstation. Перейдем непосредственно к работе и откроем основное окно.

2. Для настройки ПО VMware Workstation откройте диалоговое окно по команде **«Предпочтения» (Preferences)** в меню **«Правка» (Edit)**. Данная команда обеспечивает доступ к основным параметрам работы продукта, которые распределены по девяти вкладкам диалогового окна.

3. Настройте основные опции диалогового окна **«Предпочтения»** в следующем порядке.

На вкладке **«Рабочее пространство» (Workspace)** указать на необходимость хранения списка виртуальных машин, работавших в предыдущем сеансе, установив флажок **«Запоминать открытые виртуальные машины между сессиями» (Remember opened virtual machines between sessions)**; в этом случае при следующем запуске приложения в правой части основного окна будут

представлены вкладки для всех ВМ, остававшихся открытыми при завершении предыдущего сеанса.

Выберите папку, используемую для хранении данных о создаваемых виртуальных машинах (по умолчанию таковой является папка **«Мои документы»** активного пользователя).

Элементы управления, размещенные на вкладках **«Ввод» (Input)**, **«Горячие клавиши» (Hot keys)** и **«Приоритет» (Priority)**, определяют правила использования мыши и клавиатуры ВМ и *хостовой* ОС. Подробнее эти элементы управления будут описаны далее в задании, ориентированном на создание и настройку ВМ на основе изучаемого ПО.

Вкладка **«Отображение» (Display)** позволяет подобрать наиболее подходящий вариант отображения основного диалогового окна приложения VMware Workstation, а также окна ВМ при работе в полноэкранном режиме. Оставьте установленные параметры в состоянии по умолчанию.

Элементы управления, имеющиеся на вкладке **«Память» (Memory)**, определяют режим выделения оперативной памяти хост-компьютера программному продукту VMware Workstation и работающим виртуальным машинам. Ползунок **«Зарезервированная память» (Reserved Memory)** позволяет указать, какой объем физической оперативной памяти (ОП) разрешено использовать приложению для «собственных нужд» и для работы виртуальных машин. Минимальное значение этого параметра соответствует минимальному объему ОП, при котором возможна работа приложения, максимальное значение определяется той оставшейся частью ОП, которая минимально необходима для работы *хостовой* ОС. Перемещение ползунка в ту или иную сторону снижает быстродействие либо ПО VMware Workstation и запущенных ВМ, либо *хостовой* ОС и ее приложений. Однако, следует иметь в виду, что VMware не захватывает сразу все выделенное ей пространство: оно выделяется монитором ВМ по мере необходимости.

Установите ползунок **«Зарезервированная память»** в положение, соответствующее трем-четвертям физически установленного объема ОП, тем самым, гарантированно зарезервировав оставшуюся часть для нужд ОС.

Группа переключателей **«Дополнительная память» (Additional Memory)** на данной вкладке позволяет несколько смягчить ограничения на объем ОП, используемой в интересах ПО VMware:

- **«Привести ОП всех виртуальных машин в соответствие с объемом зарезервированной памяти» (Fit all vitual machine memory into reserved host RAM)** — запускаемые ВМ могут использовать только имеющуюся в распоряжении приложения физическую ОП; если при запуске очередной ВМ (или нового приложения внутри ВМ) окажется, что свободной памяти нет, то запуск не состоится, и на экране появится соответствующее сообщение;
- **«Разрешить подкачку для некоторых ВМ» (Allow some virtual machine memory to be swapped)** — если при запуске очередной ВМ (или нового приложения внутри ВМ) окажется, что свободной памяти

нет, то VMware позволит *хостовой* ОС переместить часть данных из ОП на жесткий диск (в системный файл подкачки); это позволит VMware использовать высвободившуюся часть ОП для запуска очередной ВМ (или нового приложения внутри ВМ), однако, при этом быстродействие всех ВМ при этом снизится из-за затрат времени па подкачку;

- **«Разрешить подкачку для большинства ВМ» (Allow most virtual machine memory to be swapped)** — если при запуске очередной ВМ (или нового приложения внутри ВМ) окажется, что свободной памяти нет, то VMware позволит *хостовой* ОС переместить значительную часть данных из ОП на жесткий диск.

Следует иметь в виду, что для каждой ВМ можно индивидуально задать объем используемой ОП. Однако при этом верхний предел выделяемой памяти зависит от максимального суммарного объема ОП, заданного ползунком **«Зарезервированная память».**

Следующая вкладка диалогового окна настройки VMware называется **«Блокировка» (Lockout)**. Имеющиеся на ней элементы позволяют управлять доступом пользователей к базовым возможностям приложения.

В исходном состоянии параметры безопасности отключены — флажок рядом с надписью **«Разрешить административную блокировку» (Enable administrative lockout)** сброшен. Это означает, что пользователь с любой учетной записью, имеющий право запуска ПО VMware, допущен также и к изменению параметров его работы. Чтобы разрешить доступ к определённым возможностям продукта лишь тем пользователям, которым известен пароль блокировки, выполните следующее.

- Установите флажок **«Разрешить административную блокировку» (Enable administrative lockout).**
- В полях **«Пароль» (Password)** и **«Подтверждение пароля» (Confirm password)** введите слово, используемое в качестве пароля.
- Установите флажки для тех функций, доступ к которым должен блокироваться:
  «Создание новых виртуальных машин» (Create new teams and virtual machines);
  «Редактировать параметры» (Edit settings);
  «Управление виртуальными сетями» (Manage virtual networks).

Оставьте неизменными параметры на вкладке **«Устройства» (Devices),** относящуюся к деактивации функции **Autorun** в *гостевой* ОС, о чем было ранее уже сказано. Убедитесь в том, что данная функция неактивна (для деактивации функции флажок должен быть установлен).

Последняя по порядку рассмотрения, но не последняя по значимости вкладка **«Инструменты» (Tools)**. Чтобы повысить эффективность и удобство работы с программным продуктом VMware, рекомендуется произвести обновление пакета дополнительных инструментов VMware Tools, как только они

будут доступны на сайте производителя. Это делается путем установки соответствующего флажка на данной вкладке.

Необходимо помнить, что устанавливаемые в данном диалоговом окне настройки ПО VMware Workstation применяются ко всем вновь создаваемым ВМ. Некоторые из них могут быть в дальнейшем скорректированы для каждой ВМ индивидуально после ее создания.

Этап С. Создание и настройка виртуальной машины на основе приложения VMware Workstation в среде ОС Windows XP.

В исходном состоянии основное окно изучаемого приложения объединяет в себе и панель управления виртуальными машинами, и «экраны мониторов» ВМ (они добавляются при очередном создании ВМ в виде вкладок с названиями установленных ОС в правой части окна).

После запуска хотя бы одной ВМ в строке состояния окна VMware Workstation появляется ряд значков, обеспечивающих доступ к параметрам внешних устройств виртуальной машины. Кнопки, размещенные в верхней части окна на панели инструментов программного продукта, разделены, в свою очередь, на четыре группы.

Первые четыре (слева) кнопки управляют состоянием активной ВМ, той, которая выбрана на боковой панели слева **(Sidebar)** в разделе **«Избранное» (Favorites)** или вкладка которой открыта в правой части окна. Значение кнопок следующее:

- **«Выключить» (Power off)** — останов ВМ (кнопка доступна, если выбранная ВМ запущена и работает);
- **«Приостановить» (Suspend)** — перевод ВМ в неактивный режим паузы; на время приостановки ВМ прерывается выполнение всех операций, производимых *гостевой* ОС или ее приложениями;
- **«Включить» (Power On)** — запуск ВМ, а также возобновление работы ВМ из режима паузы (кнопка доступна, если выбранная ВМ еще не запущена либо находится в режиме паузы);
- **«Сброс» (Resets)** — «горячий» перезапуск ВМ (действие кнопки аналогично действию одноименной кнопки реального компьютера).

Три следующие кнопки обеспечивают создание снимка состояния ВМ и возвращение к выбранному состоянию в случае необходимости:

- **«Снимок» (Take snapshot)** — создание «снимка» состояния ВМ;
- **«Возврат» (Revert)** — возврат ВМ к состоянию, сохраненному в виде «снимка»;
- **«Управление снимками» (Manage snapshots)** — вызов дополнительного окна для выбора нужного «снимка».

Четыре кнопки и через разделитель дополнительные три управляют соответственно размерами и видом окна ВМ:

- **«Показать или спрятать боковую панель слева» (Show or hide Sidebar)** — название говорит само за себя;

- **«Быстрое переключение» (Quick switch)** — перевод окна ВМ в «промежуточное» состояние (среднее между полноэкранным и оконным режимами) без панелей инструментов и строки состояния;
- **«Полноэкранный режим» (Full Screen)** — другой вид полноэкранного режима, переход в который обеспечивает пользователя специализированной панелью инструментов (кнопка доступна, если выбранная ВМ находится в активном состоянии);
- **«Совместное использование» (Unity)** — режим позволяет отображать приложения *гостевой* ОС прямо на поверхности рабочего стола *хостовой* ОС (кнопка доступна, если выбранная ВМ находится в активном состоянии и установлен пакет инструментов VMware Tools).
- **«Обобщенное представление» (Summary view)** — на вкладке ВМ отображаются сведения о конфигурации ВМ;
- **«В виде приложения» (Appliance view)** — отображение ВМ в качестве Веб-сервера с интерфейсом в виде браузера (кнопка доступна, если выбранная ВМ находится в активном состоянии); данная возможность требует дополнительного конфигурирования и настройки (**«Меню VM | Settings | вкладка Options | опция Appliance View»**)
- **«В виде консоли» (Console view)** — вкладка ВМ используется в качестве монитора *гостевой* ОС

Последние две кнопки управляют записью и воспроизведением работы ВМ; записывается служебная информация, необходимая разработчикам для дальнейшей отладки и устранения ошибок кода программного продукта VMware Workstation.

Ознакомившись с основными инструментами управления виртуальными машинами в рамках ПО VMware Workstation, далее имеет смысл перейти к непосредственному созданию новой ВМ и ее настройке. Для этого предполагается использовать альтернативную *гостевую* ОС PCBSD, ориентированную на домашнее использование, однако имеющую в своем составе полноценное ядро сетевой ОС FreeBSD. Последняя же имеет широкое применение во многих коммерческих организациях в современных условиях. Знание ее основ существенно расширяет профессиональные возможности обучающихся в будущем.

Для создания ВМ с альтернативной *гостевой* ОС PCBSD на базе ПО VMware Workstation необходимо выполнить следующие действия:

1. Создание ВМ с использованием программного продукта VMware Workstation осуществляется с помощью соответствующего мастера. Для его запуска выберите в меню **«Файл» (File)** одноименную команду создания новой ВМ (**«New | Virtual Machine»**).

В появившемся стартовом окне мастера необходимо выбрать один из двух способов создания ВМ:

- в стандартной, типичной (рекомендуемой) конфигурации с параметрами, заданными по умолчанию (переключатель Typical);
- с пользовательским набором параметров (переключатель Custom).

Пользовательский вариант отличается от «типового» тем, что требует детального конфигурирования параметров ВМ. Он обеспечивает наличие у создаваемой ВМ улучшенных характеристик и возможность их подконтрольного изменения пользователем. Дальнейшее конфигурирование ВМ будет осуществляться именно с этой точки зрения.

Установите переключатель в диалоговом окне приветствия в положение **Custom (advanced)** и нажмите **«Далее» (Next)** для подтверждения операции.

2. Появившееся окно иллюстрирует возможности аппаратной совместимости с текущей и предыдущими версиями ПО. В правой части диалогового окна в списке **«Ограничения» (Limitations)** представлены системные ограничения данного продукта. В частности, для ПО VMware Workstation версии 6.5 актуальны ограничения: по отводимой оперативной памяти, числу процессоров и количеству подключаемых сетевых адаптеров или сетевых устройств.

В этом окне оставьте неизмененным выпадающий список **«Оборудование» (Hardware)** в положении **«Workstation 6.5»** и нажмите **«Далее» (Next)** для подтверждения операции.

3. В следующем окне инсталляции *гостевой* ОС необходимо определиться из какого источника (оптический диск или файл образа) будет осуществляться дальнейшая установка системы.

Установите переключатель в положение **«Инсталлировать ОС из файла образа диска .iso» (Installer disc image file .iso)** и, воспользовавшись возможностью выбора **(Browse)**, подключите файл образа с *гостевой* ОС PCBSD, заранее скачанный с официального сайта производителя в процессе подготовки к выполнению лабораторной работы. Нажмите **«Далее» (Next)** для продолжения работы.

Внимание! В процессе установки ОС PCBSD из файла образа (размещенного на жестком диске) автор столкнулся с необъяснимыми (на первый взгляд) ошибками, которые приводили к перезагрузке ВМ и невозможности дойти до конца инсталляции системы. Данная проблема устраняется установкой ОС с оптического носителя DVD. Однако применение DVD-диска требует дополнительных действий по записи файла образа на него. Для этих целей возможно использование любого ПО для записи оптических носителей, например, Nero или Roxio. Процесс записи оптического диска является тривиальным и не подлежит рассмотрению в рамках лабораторной работы.

4. Во вновь появившемся диалоговом окне выбора *гостевой* ОС установите переключатель в положение **«Другая» (Other)** и из расположенного ниже выпадающего списка **«Версия» (Version)** выберите опцию **«FreeBSD»**. Нажмите **«Далее» (Next)** для подтверждения операции и перехода в следующее диалоговое окно мастера.

5. Укажите имя ВМ **(Virtual Machine name)** и путь места-назначения, где предполагается нахождение файлов ВМ *гостевой* ОС в дальнейшем. Целе-

сообразно указать новый каталог места-назначения, отличный от предоставляемого программным продуктом по умолчанию. Нажмите **«Далее» (Next)** для продолжения работы мастера.

6. Укажите количество физических процессоров **(Number of processors)** в появившемся диалоговом окне. При этом необходимо помнить, что, например, двухядерный процессор физически представляет собой одно устройство (в более поздних версиях ПО VMware Workstation появляется дополнительная возможность выбора количества ядер, приходящихся на один процессор).

Установите переключатель в положение **«Один» (One)** и нажмите **«Далее» (Next)** для перехода в новое диалоговое окно.

7. Следующее диалоговое окно позволяет осуществить выбор необходимого объема оперативной памяти, включаемого в конфигурацию ВМ.

Можно либо оставить значение, предложенное мастером, либо установить желаемое значение с помощью ползунка, снабженного дополнительными пояснениями:

- желтый треугольник соответствует минимальным потребностям *гостевой* ОС **(Guest OS recommended minimum)**;
- синий треугольник соответствует максимальному рекомендуемому объему, который обеспечивает наивысшую производительность *гостевой* ОС **(Maximum recommended memory)**;
- зеленым треугольником отмечается рекомендуемый объем оперативной памяти **(Recommended memory)**, оптимальный для выбранной к установке *гостевой* ОС.

Экспериментально отмечено, что для обеспечения нормальной работы ВМ, объем оперативной памяти должен составлять 35-50% физически установленного на системной плате объема. Применительно к рассматриваемому случаю рекомендуется установить не менее 768 Mb оперативной памяти (при котором была отмечена гарантированная стабильность ВМ), несмотря на то, что приложение VMware Workstation для установки *гостевой* ОС рекомендовало нижний предел в 256 Mb.

Выберите ползунком необходимое значение оперативной памяти и нажмите **«Далее» (Next)** для продолжения работы мастера.

8. Следующее окно позволяет указать тип виртуальной сети, под которую требуется сконфигурировать ВМ. Доступно четыре варианта:

- **«Использовать сетевой мост» (Use bridged networking)** — данный способ обычно используется в тех случаях, когда *хостовый* компьютер входит в состав реальной сети, а для нужд ВМ может быть выделен свой IP-адрес (в том числе полученный от DHCP-сервера);
- **«Использовать трансляцию сетевого адреса» (Use network address translation (NAT)** — применяется тогда, когда ВМ не имеет собственного IP-адреса, но ей требуется предоставить выход в Интернет через сетевое подключение *хостового* компьютера;

- **«Использовать сетевое соединение с хостовым компьютером» (Use host-only networking)** — предполагает возможность подключения ВМ к *хостовому* компьютеру через локальную сеть;
- **«Не использовать сетевое соединение» (Do not use a network connection)** — в конфигурацию ВМ не включается сетевой адаптер, и, соответственно, возможность работать в сети отсутствует.

Наиболее предпочтительным вариантом в рассматриваемых условиях является **«Использовать трансляцию сетевого адреса»** (NAT). Установите переключатель диалогового окна в соответствующее положение и нажмите **«Далее» (Next)** для перехода к дальнейшему конфигурированию.

Последующие несколько диалоговых окон мастера позволяют задать параметры виртуального жесткого диска.

9. Сначала необходимо выбрать тип адаптера ввода-вывода. Для этого выберите рекомендуемый параметр **LSI logic (recommended)** в следующем диалоговом окне и нажмите **«Далее» (Next)**.

10. Параметры появившегося окна позволяют указать, нужно ли создавать новый виртуальный диск **(Create a new virtual disk)** или подключить к ВМ один из уже имеющихся. Подключить можно виртуальный диск **(Use an existing virtual disk)** или физический диск *хостового* компьютера **(Use a physical disk)**. В последнем случае речь идет об использовании в составе ВМ так называемого **raw**-диска. Соответственно, выбрав этот вариант, имеется возможность подключить к ВМ раздел физического неразмеченного диска.

Установите переключатель **«Создать новый виртуальный диск» (Create a new virtual disk)** и, щелкнув на кнопке **«Далее» (Next)**, перейдите на следующее диалоговое окно выбора типа диска для создаваемого виртуального пространства.

11. Тип виртуального диска оставьте в рекомендуемом положении **IDE (Recommended)** и перейдите к следующему диалоговому окну, нажав **«Далее» (Next)**.

12. Укажите максимальный размер виртуального диска **(Maximum disk size)** размером в 12 Gb (вместо 8 Gb, предоставляемых по умолчанию). Размер в 12 Gb является необходимым для корректной работы ОС PCBSD.

В этом же окне имеется возможность указать способ выделения пространства под виртуальный диск. Предпочтительным вариантом является разделение виртуального диска на файлы размером по 2 Gb **(Split virtual disk into 2 Gb files)**, поскольку с легкостью позволяют перенести ВМ на другой *хостовый* компьютер в случае необходимости. Однако это вариант требует большего времени для его организации, чем другой имеющийся способ **«Сохранить виртуальный диск как единый файл» (Store virtual disk as a single file)**.

Помимо указанного, имеется возможность улучшения производительности ВМ посредством применения опции **«Распределить все дисковое пространство» (Allocate all disk space now)**. Однако выполнение данной опции при конфигурировании ВМ требует дополнительного дискового пространства

и времени на его распределение. Если Вы располагаете этими дополнительными ресурсами, то данную опцию можно также активировать.

Перейдите на следующий экран, нажав **«Далее» (Next)**.

13. В случае необходимости укажите иное имя файла-дескриптора (с расширением **.wmdk**) виртуального диска. Нажмите **«Далее» (Next)** для подтверждение изменений и перехода к завершающему диалоговому окну.

14. В последнем диалоговом окне демонстрируется сводная информация по осуществленным конфигурационным действиям. Кроме того, имеется возможность внести дополнительные изменения параметров аппаратных средств ВМ. Для этого нажмите кнопку **«Конфигурировать аппаратуру» (Customize hardware)** и, например, удалите 3,5” накопитель на гибких магнитных дисках (если он физически отсутствует в системе или Вы не желаете его использовать в рамках виртуальной среды), нажав одноименную команду (**Remove**) выбранного аппаратного средства **«3,5” дисковод» (Floppy)**.

Параметры ВМ сохраняются в специальном конфигурационном **VMX**-файле текстового формата. Этот файл (как и другие файлы, определяющие работу ВМ), при необходимости может быть перенесен на другой *хостовый* компьютер с целью дальнейшего воспроизведения параметров ВМ в новых условиях.

Кроме того, сделанные настройки могут быть изменены в любое время, в частности, перед запуском уже сконфигурированной ВМ. Для этого, перед тем, как запустить ВМ на выполнение, необходимо выбрать закладку с соответствующей *гостевой* ОС и, дважды щелкнув по необходимому параметру в окне справа, задать ему новое значение.

15. Нажмите **OK** для подтверждения произведенных операций и **«Закончить» (Finish)** для окончания работы мастера в целом.

С этого момента ПО VMware Workstation переходит в автоматический режим установки *гостевой* ОС PCBSD, на что потребуется некоторое время.

16. Следуйте работе мастера установки ОС PCBSD до финальной точки (если при этом понадобится выйти из окна ВМ в среду *хостовой* ОС Windows XP, нажмите одновременно комбинацию «горячих» клавиш **«Ctrl+Alt»**).

Важным обстоятельством является то, что в процессе установки виртуальной ОС PCBSD по возможности необходимо исключить работу других приложений, осуществляющих запись информации на жесткий диск. Это позволит *хостовой* ОС Windows XP не отвлекать системные ресурсы на другие процессы и обеспечит беспрепятственный обмен данными между жестким диском и ПО VMware Workstation.

Автор не видит необходимости описывать полностью работу мастера установки, поскольку процедура инсталляции ОС является штатной и достаточно простой даже для неподготовленного пользователя. Процесс установки виртуальной ОС PCBSD является абсолютно идентичным аналогичному процессу в реальных условиях. Он полностью автоматизирован и сопровождается исчерпывающими комментариями на русском языке (для активации которого необходимо осуществить его выбор в первом диалоговом окне инсталлятора).

Однако в процессе установки *гостевой* ОС PCBSD существует два принципиальных момента, на которые следует обратить особое внимание.

Первый из них заключается в том, что Unix-подобные ОС, обладая повышенной степенью безопасности, всегда требуют от пользователя ввода дополнительного пароля администратора корневой директории (root). Причем данный пароль администратора должен отличаться от пароля, который необходим пользователю для работы с его учетной записью. С этой целью при установке ОС PCBSD необходимо определить оба этих пароля и ввести их по отдельности в появившемся в процессе инсталляции диалоговом окне **«Системные учетные записи»**.

Второй момент связан с выбором виртуального жесткого диска в следующем одноименном диалоговом окне **«Выбор диска»**. Здесь необходимо сначала выбрать виртуальный жесткий диск среди обнаруженных, а затем установить флажок напротив надписи **«Использовать весь диск»** в категории **«Выбор раздела»**, если не предполагается настраивать разделы вручную (для чего ниже имеется соответствующая опция).

Остальные моменты конфигурирования мастера установки не требуют пояснений, необходимо лишь нажимать кнопку **«Далее»** при переходе от одного диалогового окна к другому. На современном оборудовании процесс инсталляции *гостевой* ОС PCBSD может занять достаточно продолжительное время (обычно это около часа, а иногда, и более).

8.3.2. Учебное задание №2. Организация виртуальной локальной сети на основе Unix-подобной ОС PCBSD в среде ОС Windows XP.

Порядок выполнения:

В предыдущем задании настоящей лабораторной работы были предприняты действия по созданию и настройке ВМ на базе альтернативной Unix-подобной *гостевой* ОС PCBSD в среде *хостовой* ОС Windows XP с применением специализированного ПО VMware Workstation.

Результатом корректного конфигурирования ВМ является автоматическое подключение к глобальной сети Интернет при перезагрузке *гостевой* ОС PCBSD. При этом появляется возможность осуществить обновление ОС PCBSD при первом ее запуске (желтый треугольник с вписанным восклицательным знаком в трее ОС свидетельствует о наличии доступных в сети обновлений). Поскольку изучаемая ОС PCBSD является одной из самых безопасных в мире, процесс обновления требует соответствующих санкций — необходимо ввести пароль администратора корневой директории (root).

Дальнейший ход лабораторной работы будет направлен на создание взаимного общего доступа к сетевым ресурсам (в частности, файлам и каталогам) в консолидированной среде двух ОС: *хостовой* ОС Windows XP и *гостевой* ОС PCBSD. Иными словами, предполагается настроить виртуальную локаль-

ную сеть с возможностью взаимной передачи объектов файловой системы из *гостевой* ОС в *хостовую* и обратно.

Взаимный общий доступ к файлам и каталогам предполагается организовать на основе модели «гостевого доступа», которая достаточно широко применяется при организации локальных сетей и уже была упомянута в предыдущей лабораторной работе №7.

Организация виртуальной локальной сети в консолидированной операционной среде двух альтернативных ОС с целью корректного обеспечения доступа к общим сетевым ресурсам и возможностью выхода в глобальную сеть Интернет посредством *гостевой* ОС PCBSD осуществляется в два последовательных этапа.

Этап А. Настройка *хостовой* ОС Windows XP реального компьютера.

Этап В. Настройка *гостевой* ОС PCBSD виртуальной машины.

Прежде чем приступить к непосредственной настройке, необходимо сначала отключить штатные брандмауэры обеих ОС, чтобы полностью исключить их влияние на этом этапе. Кроме того, чтобы исключить влияние стороннего ПО на процесс настройки виртуальной локальной сети, необходимо также отключить сетевые экраны других производителей. Применение сетевых экранов сторонних производителей, как правило, требует их дополнительной настройки, позволяющей разблокировать доступ к локальным сетям, в том числе и к их виртуальным аналогам. В подобных частных случаях необходимо предварительно внимательно изучить документацию к данному ПО. Настройке штатных брандмауэров будет уделено дополнительное внимание в конце настоящей лабораторной работы.

Конфигурированию брандмауэра ОС Windows XP (**«Пуск | Панель управления | Брандмауэр Windows»**), в частности, было посвящено одно из заданий предыдущей лабораторной работы. Поэтому его полное отключение, по мнению автора, не должно вызвать значительных затруднений и повторно рассматривать этот процесс смысла не имеет.

Отключение брандмауэра ОС PCBSD также не вызывает трудностей, но при этом незнакомый графический интерфейс новой ОС требует времени для изучения, которое, однако, в рамках лабораторной работы не предполагается. Принятие решения по его овладению оставляется на самостоятельное усмотрение обучающихся.

Для доступа к брандмауэру ОС PCBSD необходимо:

- манипулятором мышь кликнуть на стилизованном изображении огненного шара (аналога стартового меню **Пуск** в ОС Windows XP) в левой нижней части окна загруженной ОС PCBSD;
- в появившемся меню выбрать подменю **«Компьютер»** (в виде перевернутой, плавно движущейся вкладки), а затем **«Параметры системы»** в разделе **«Приложения»** (название раздела написано мелким шрифтом светло-серого цвета);
- в появившемся окне на вкладке **«Главное»** в разделе **«Сеть и Интернет»** выбрать **«Firewall»** и, дважды щелкнув по названию, загру-

зить системный модуль, отвечающий за настройки брандмауэра ОС PCBSD; при этом потребуется ввести пароль администратора корневой директории (root);

- на вкладке **«Общие»** программного модуля настройки KDE убрать флажок рядом с надписью **«Включать фаервол при загрузке»** (раздел **«Общие настройки»**), нажать кнопку **«Остановить»** (раздел **«Фаервол»**) и подтвердить выполненные операции, нажав **OK** (**«Применить»**); теперь после перезагрузки фаервол не будет загружаться автозапуском.

При настройке любой локальной сети (как проводной, так и виртуальной) необходимо помнить, что все сетевые устройства должны находится в пределах одной подсети. Идентификация каждого устройства осуществляется задаваемым 32-битным **IP**-адресом, например, вида 192.168.1.x и маской подсети наподобие 255.255.255.0 — требование **IP**-протокола **IPv4** (новый **IP**-протокол **IPv6** пока не представляет интереса из-за незначительной его распространенности в мире). Отсюда следует, что пул доступных сетевым устройствам **IP**-адресов, определяемый индексом x и используемый при построении локальной сети, лежит в диапазоне от 192.168.1.1 до 192.168.1.254.

Еще одним, немаловажным моментом, без знания которого осуществить подключение *гостевой* ОС к глобальной сети Интернет (в случае, если имеется подключение *хостовой* ОС) в рамках предлагаемой последовательности будет проблематично, является наличие информации по предпочтительному (первичному) и альтернативному (вторичному) **IP**-адресам **DNS**-серверов интернет-провайдера (**ISP**), предоставляющего доступ в глобальную сеть Интернет. Эту информацию можно получить непосредственно в офисе **ISP** или позвонив в его службу технической поддержки. Если эти данные раздаются провайдером **ISP** автоматически, то их можно увидеть при просмотре сведений соответствующего сетевого подключения.

Этап А. Настройка *хостовой* ОС Windows XP.

Прежде, чем начать процесс конфигурирования *хостовой* ОС, необходимо отметить, что в качестве нее может быть взята не только ОС Windows XP, но, в принципе, любая ОС семейства Windows, а также любая другая, альтернативная ОС (например, Unix-подобная). Принципы настройки локальных сетей (в том числе, виртуальных) остаются неизменными в любом случае. В частности, в статье автора **«Настройка беспроводной сети на базе точки доступа D-link G5402SP/RU в среде ОС Windows Vista Business SP1 и XP Professional SP3»** (раздел **«Публикации»** ресурса www.savchenko.su) рассматриваются вопросы конфигурирования беспроводной локальной сети и обеспечение общего доступа к сетевым ресурсам обеих, рассматриваемых с статье ОС. Опубликованный материал может быть также полезен в контексте освещаемых в настоящей лабораторной работе вопросов, а именно использован

при настройке модели «гостевого доступа» в случае, если *хостовой* ОС будет ОС Windows Vista.

Конфигурирование виртуальной локальной сети со стороны *хостовой* ОС Windows XP на реальном компьютере, прежде всего, подразумевает присвоение ему имени, под которым он будет отображаться в сети, и организацию единой рабочей группы, например, **MSHOME**, в которой будут находится *хостовый* персональный компьютер и *гостевая* виртуальная машина:

1. Полное имя компьютера и рабочей группы в ОС Windows XP могут присвоены на вкладке **«Имя компьютера»** в меню **«Пуск | Панель управления | Система»** (чтобы открыть данную вкладку альтернативным способом, необходимо правой кнопкой манипулятора мышь кликнуть на **«Мой компьютер»** в меню **«Пуск»** и выполнить команду **«Свойства»** из контекстного меню). После перезагрузки, введенные значения параметров должны отобразиться на этой же вкладке в соответствующих полях.

Примечание. При необходимости можно оставить полное имя компьютера и рабочей группы неизменными. Однако имя рабочей группы должно быть при этом запомнено, а еще лучше, где-нибудь записано; оно понадобится для дальнейшей настройки *гостевой* ВМ.

2. Следующее, что необходимо сделать, это настроить «гостевой доступ» из виртуальной локальной сети к общим ресурсам и объектам (файлам и каталогам) *хостовой* ОС Windows XP на реальном ПК. Корректное включение модели «гостевого доступа» обеспечивается конфигурированием **«Локальной политики безопасности»,** что было достаточно подробно описано в **п. 6 Секции С задания №7.1а.** предыдущей лабораторной работы №7.

3. В отношении сетевых настроек *хостовой* ОС Windows XP необходимо выполнить включение протокола **«VMWare Bridge Protocol»**, с помощью которого обеспечивается доступ ВМ к физическим сетям. Данная настройка расположена в свойствах **«Подключения по локальной сети»** на вкладке **«Общие»** (**«Сетевые подключения | Подключения по локальной сети»**). Здесь, в группе **«Компоненты, используемые этим подключением»** необходимо поставить флажок напротив соответствующей настройки.

4. Конфигурирование **TCP/IP** Интернет протокола (принципиально необходимого при настройке любого типа сетей) при организации виртуальной локальной сети, как правило, не требуется. Все настройки виртуального сетевого адаптера **VMware Virtual Ethernet Adapter for VMnet8** (имя адаптера может отличаться цифрой номера или быть иным по написанию, но аналогичным по смыслу) и свойства **TCP/IP** Интернет протокола следует оставить в состоянии по умолчанию, то есть **«Получить IP-адрес автоматически»** и **«Получить адрес DNS-сервера автоматически»** (вкладка **«Общие» | «Свойства: Протокол Интернета (TCP/IP)»**). Это позволит ПО VMware Workstation автоматически присвоить **IP**-адрес виртуального сетевого адаптера реальному ПК посредством встроенного программного **DHCP**-сервера.

Единственное, пожалуй, что будет нелишним сделать при настройке **TCP/IP** протокола, это открыть дополнительные параметры (кнопка **«Допол-**

нительно» на вкладке **«Общие»** диалогового окна **«Свойства: Протокол Интернета (TCP/IP)»**), на вкладке **«WINS»** убрать флажок **«Включить просмотр LMHOSTS»** и выбрать положение **«Включить NetBIOS через TCP/IP»** переключателя **«Параметры NetBIOS»**. Первая опция отключает возможность использования текстового файла **LMHOSTS**, содержащего связи имен ПК с **IP**-адресами. Вторая — включает поддержку службы **NetBIOS через TCP/IP** и разрешения **NetBIOS**-имен в **IP**-адресах (см. Лабораторную работу №2). Завершить настройку протокола на реальном *хостовом* ПК следует, дважды нажав **OK** для подтверждения осуществленных изменений.

Примечание. Если в группе **«Компоненты, используемые этим подключением»** имеется настройка **«Протокол Интернета версии 6»**, то ее необходимо отключить (убрать соответствующий флажок напротив нее). Данная настройка может появиться, если *хостовой* ОС является ОС Windows Vista или Windows 7, а также, если протокол **TCP/IP** версии 6 был установлен вручную.

5. Возможности общего доступа к объектам файловой системы *хостовой* ОС Windows XP желательно организовать следующим образом: в меню **«Пуск | Панель управления | Свойства папки»** на вкладке **«Вид»** рекомендуется поставить флажок «**Использовать простой доступ к файлам и папкам»** в списке **«Дополнительные параметры»**. При этом надо помнить, если этот флажок активен, то организовать **«Новый общий ресурс»** через консоль администрирования (MMC) будет невозможно (см. Лабораторную работу №5).

Создайте в ФС NTFS каталог с произвольным именем, который предполагается сделать общим сетевым ресурсом (см. Лабораторную работу №7), и открыть к нему общий доступ с разрешением изменения содержимого по сети (**«Свойства»** каталога, вкладка **«Доступ»**).

6. В принципе, проведенных настроек *хостовой* ОС Windows XP достаточно, чтобы обеспечить взаимную аутентификацию пользователей в рамках виртуальной локальной сети, но бывают случаи, когда необходимо осуществить дополнительные настройки. Их применение становится необходимым тогда, когда все ранее описанные действия произведены, а требуемый результат не достигнут (общий сетевой ресурс *хостовой* ОС не доступен по какой-либо причине). В этом случае необходимо выполнить нижеследующее.

Во-первых, вызвать редактор Реестра (см. Лабораторную работу №6) и на панели ключей выбрать куст корневого ключа **HKEY_LOCAL_MACHINE (HKLM)**. Щелкнув по нему манипулятором мышь, развернуть ветвь подключа **HKLM\SYSTEM\CurrentControlSet\Control\Lsa** и изменить значения параметров **restrictanonymous** и **restrictanonymoussam** на 0. Эти параметры устраняют некоторые проблемы совместимости «клиентов», программ и служб, которые могут возникать при изменении параметров безопасности и назначении прав пользователей, работающих под управлением различных ОС.

Во-вторых, возможная причина заключается в несоответствии конфигураций **NTLM 2** — механизма сеансовой безопасности (суть которого состоит в том, что при передаче сообщений между ОС по умолчанию предполагается их шифрование, в частности, 56-битным ключом), отвечающего за проверку под-

линности отношений типа «запрос/ответ» *хостовой* и *гостевой* ОС. В этой связи необходимо активировать поддержку **NTLM 2** на том ПК (реальном или виртуальном), к которому пытается подключиться «клиент» с инородной ОС (например, виртуальная машина с *гостевой* ОС PCBSD).

Для активации поддержки механизма **NTLM 2** на реальном ПК с *хостовой* ОС Windows XP в редакторе Реестра необходимо выбрать ветвь подключа **HKLM\System\CurrentControlSet\Control\Lsa** и изменить значение параметра **LMCompatibilityLevel** на 3 (в частности, имеющего идентичное значение в ОС Windows Vista Business SP1). Данный «твик» Реестра позволяет увеличить общий уровень безопасности при передаче данных в локальных сетях.

На этом процесс настройки виртуальной локальной сети со стороны *хостовой* ОС Windows XP можно считать полностью завершенным. Далее имеет смысл перейти к следующему этапу настройки *гостевой* ОС PCBSD.

Этап В. Настройка *гостевой* ОС PCBSD.

Настройка виртуальной локальной сети со стороны *гостевой* ОС PCBSD в целом представляет более сложный процесс, требующий большей усидчивости, поскольку работа в Unix-подобных ОС предполагает знание основ командной консоли (аналогичной, изученной в Лабораторных работах №1 и 2) или «терминала» (часто используемое название в Unix-среде). В этой связи, необходимо отметить, что командная консоль Unix-подобной ОС прошла больший путь развития и эволюционирования, чем ее аналог в ОС Windows XP. Это привело к тому, что сегодня с целью повышения безопасности ОС традиционным считается выполнение всех ориентированных на администрирование задач в рамках командной консоли. Именно по этой причине, изучению командной консоли Unix-подобных ОС следует уделить особое внимание в том случае, если специалистом предполагается администрирование одной из них (например, ОС FreeBSD — в корпоративном секторе или ОС PCBSD, ориентированную на домашнее применение).

В настоящей лабораторной работе не предполагается тщательного изучения всего набора команд «терминала» ОС PCBSD (синтаксис которого существенно отличается от синтаксиса командной консоли ОС Windows XP), тем не менее, в процессе конфигурирования ОС необходимо использование базовых команд, например, таких как **«su»** и **«ifconfig»**, имеющих непосредственное отношение к решению поставленной задачи.

Кроме сказанного, конфигурирование Unix-подобных ОС очень часто предполагает ручное изменение системных параметров, сгруппированных в соответствующих конфигурационных файлах (например, с расширениями **.INI** или **.CONF**). В рамках лабораторной работы предполагается изменение нескольких таких файлов, один из которых, в частности, отвечает за конфигурирование клиент-серверного приложения **Samba**, в свою очередь, обеспечивающего взаимодействие компьютеров в сети и позволяющего организовывать общий доступ к их ресурсам.

Как и в предыдущем случае, конфигурирование *гостевой* ОС PCBSD должно сопровождается соблюдением следующих основных условий: ВМ под управлением *гостевой* ОС должна иметь свое собственное уникальное имя, принадлежать к той же рабочей группе (или домену), что и реальный ПК под управлением *хостовой* ОС, и находится с ним в пределах одной подсети. Дальнейшая последовательность действий призвана обеспечить эти условия:

1. Для назначения нового имени виртуальной машине (в случае, если не устраивает то, которое было присвоено ей по умолчанию при инсталляции *гостевой* ОС PCBSD) в системе имеется возможность изменить его с применением графического пользовательского интерфейса (как это делается в *хостовой* ОС Windows XP). С этой целью необходимо дважды кликнуть на иконке виртуального сетевого адаптера (она расположена в системном трее рядом с часами, где-то между желтым треугольным знаком и иконкой органайзера), выбрать вкладку **«Расширенные настройки сети»**, нажать кнопку **«Изменить настройки»** и, введя пароль администратора (root), изменить значение параметра **«Имя машины»** в верхней строке категории **«Системные настройки»**.

Альтернативным способом изменения имени виртуальной машины является ввод дополнительного параметра непосредственно в конфигурационный файл серверного приложения **Samba**, где находятся базовые сетевые настройки. По умолчанию в Unix-подобных ОС изменение сетевых параметров в конфигурационном файле **Samba** должно осуществляться вручную, хотя, в отдельных случаях, можно установить инструмент **Samba Web Administration Tool (SWAT)**, позволяющий изменять эти параметры, пользуясь веб-интерфейсом. Поскольку процесс установки приложения **SWAT** сопряжен с дополнительными трудностями, в дальнейшем все необходимые сетевые настройки будут осуществляться напрямую в файле **Samba** без использования данного приложения. Установка специализированного инструмента **SWAT** и конфигурирование сети с его помощью оставляется на самостоятельное усмотрение обучающегося.

Местонахождение конфигурационного файла **Samba** с именем **smb.conf** (**smb.conf.sample** — его точная копия) в *гостевой* ОС PCBSD задано абсолютным путем **/usr/PCBSD/local/etc**/ (каталог **PCBSD/** может отсутствовать), в котором первый символ **«/»** указывает на корневую папку (root) или директорию (это основополагающий элемент всех Unix-подобных ОС).

Поскольку ОС PCBSD обеспечивает повышенные требования к безопасности файловой системы, все действия направленные на изменение системных объектов (файлов и каталогов) должны сопровождаться вводом пароля администратора корневой директории (root). В этом контексте, исключение не составляет и файл конфигурационных данных **smb.conf**; действия по его модификации также должны быть авторизированны администратором данной ОС.

Для облегчения процесса администрирования и модификации системных файлов в ОС PCBSD имеется ряд специализированных инструментов. В частности, для навигации по файловой системе предусмотрено мощное приложение — файловый менеджер **«sudolphin»** (приставка **«su»** образована от терми-

на **«sudo»**, что дословно означает **«superuser do»** или «выполнить от имени суперпользователя/администратора (root)»). Его существенное преимущество заключается в том, что он позволяет модифицировать объекты файловой системы, не подтверждая каждый раз осуществляемые изменения и операции.

Для получения полного доступа к объектам файловой системы с возможностью их модифицирования, загрузите файловый менеджер **«sudolphin»**, выполнив следующее:

- манипулятором мышь кликните на стилизованном изображении огненного шара (аналога стартового меню **Пуск** в ОС Windows XP) в левой нижней части окна загруженной ОС PCBSD;
- в появившемся меню выберите подменю **«Приложения»** (в виде перевернутой, плавно движущейся вкладки), а затем **«Система»** в разделе **«Все приложения»** (название раздела написано мелким шрифтом светло-серого цвета);
- в конце появившегося списка приложений найдите файловый менеджер **«sudolphin»** и запустите его на выполнение, введя единожды пароль администратора корневой директории (root).

Пройдите в файловом менеджере **«sudolphin»** по вышеуказанному пути и загрузите конфигурационный файл **smb.conf** в текстовый редактор **KWrite**, который доступен из контекстного меню данного файла (**«Открыть в программе | KWrite»**).

Обратите внимание на структуру конфигурационного файла **smb.conf.** В файле имеются строки, начинающиеся с символов **«#»** и **«;»**, содержащие служебное слово в квадратных скобках **«[»** и **«]»**, а также строки, не имеющие указанных символов. Первые два символа указывают на то, что следующие за ними строки означают комментарий и не являются исполняемыми. Служебное слово в квадратных скобках указывает на область параметров, относящихся к данной категории (например, секция параметров **[global]**). Строки, не содержащие никаких служебных символов, представляют собой собственно параметры (в том числе, глобальные из указанной выше категории) и их значения, обязательные для исполнения *гостевой* ОС PCBSD.

Все параметры в категории **[global]**, расположенные в файле **smb.conf** ниже строки **«Global Settings» («Глобальные установки»)**, являются определяющими при сетевом взаимодействии. К числу этих параметров, прежде всего, относятся те из них, которые определяют имя виртуального компьютера в локальной сети и имя единой рабочей группы. Для изменения имени компьютера в виртуальной локальной сети внесите в файл **smb.conf** новый параметр **netbios name** со значением **VirtualPC** (или другим, выбранным самостоятельно) в категории параметров **[global]**, например, перед параметром **workgroup**, предназначенного для имени рабочей группы. При этом значение самого параметра **workgroup** должно быть изменено на **Mshome** вместо **Mygroup**, присвоенного по умолчанию.

Примечание. Переход на рабочий стол ВМ в среде ПО VMware Workstation осуществляется по щелчку манипулятора мышь на активном окне

приложения (или при нажатии «горячих» клавиш **«Ctrl+G»**); для возврата к рабочему столу реального ПК используется «горячая» комбинация **«Ctrl+Alt»**.

2. Принадлежность *гостевой* ОС PCBSD к той же самой подсети, в которой находится *хостовая* ОС Windows XP, в общем случае, обеспечивается по умолчанию, поскольку (как упоминалось выше) ПО VMware Workstation имеет интегрированный **DHCP**-сервер и осуществляет трансляцию сетевых адресов (NAT). Присвоение реальному компьютеру и виртуальной машине **IP**-адресов из одной подсети происходит автоматически; дополнительных действий по конфигурированию сети в этом направлении, как правило, не требуется.

Убедиться в сказанном можно следующим образом: сначала в *хостовой* ОС Windows XP необходимо обратить внимание на **«Сведения сетевого подключения»** виртуального сетевого адаптера **VMware Virtual Ethernet Adapter for VMnet8** (**IP**-адрес **DHCP**-сервера, **WINS**-сервера и выделенный виртуальному сетевому адаптеру **IP**-адрес реального ПК должны быть в одной подсети, например, 135-й), а затем в *гостевой* ОС PCBSD навести манипулятором мышь на собственный виртуальный сетевой адаптер в системном трее и, в появившейся через пару секунд хинт-подсказке, обратить внимание на то, что ВМ имеет **IP**-адрес, присвоенный в той же подсети.

Перезагрузите ВМ, предварительно сохранив в файле **smb.conf** сделанные конфигурационные изменения. После перезагрузки во вновь образованной рабочей группе **«Mshome»** должны отобразиться реальная и виртуальная машины как со стороны *хостовой* ОС Windows XP, так и со стороны *гостевой* ОС PCBSD (**Стартовое меню ОС | Вкладка «Компьютер» | «Сеть» в разделе «Точка входа» | «Samba shares» | Рабочая группа «Mshome»**).

3. Если после перезагрузки ВМ в рабочей группе **«Mshome»** не отображается ее имя, скорее всего, это связано с некорректной работой программного **DHCP**-сервера ПО VMware Workstation. Для разрешения возникшего вопроса необходимо при получении **IP**-адреса *гостевой* ОС PCBSD отключить **DHCP** и внести все необходимые данные вручную.

Сперва необходимо загрузить **«Утилиту настройки сети»**. Как и раньше, дважды кликните на иконке сетевого адаптера в системном трее ВМ. На вкладке **«Устройства»** появившегося диалогового окна **«Настройка сети»** манипулятором мышь щелкните по кнопке **«Конфигурировать»** и введите пароль администратора (root). В конфигурационном окне сетевого интерфейса **«em0 configuration»** на вкладке **«Общие»** уберите флажок напротив надписи **«Получать IP-адрес автоматически (DHCP)»**, а вместо этого введите ниже **IP**-адрес (в той же подсети) и маску подсети. Нажмите **OK** для подтверждения сделанных изменений.

На вкладке **«Расширенные настройки сети»** диалогового окна **«Настройка сети»** аналогичным образом внесите изменения в системные настройки первичного и вторичного **DNS**-адресов (полученных ранее у Интернет провайдера **ISP**) и **IP**-адреса шлюза (он соответствует **IP**-адресу **WINS**-сервера по протоколу **IPv4**, полученного из сведений о сетевом подключении

хостовой ОС Windows XP). Сохраните настройки, а затем нажмите **OK** для подтверждения осуществленных изменений.

Теперь после перезагрузки *гостевой* ОС PCBSD, в рабочей группе **«Mshome»** реальная и виртуальная машины будут отображаться корректно. Кроме того, если ранее был открыт общий доступ (корректно реализована модель «гостевого доступа» в предыдущем задании) к объектам (файлам и каталогам) *хостовой* ОС, с этого момента имеется возможность входить в общий каталог ОС Windows XP из *гостевой* ОС PCBSD и производить в нем операции чтения/записи объектов ФС NTFS.

4. Продолжим конфигурирование *гостевой* ОС PCBSD в файле **smb.conf** в части настроек параметров безопасности секции **[global]**.

В системе **Samba** имеется два популярных способа управления доступом: на уровне пользователей и на уровне общих ресурсов. Более безопасным является управление доступом на уровне пользователей, задаваемое в файле **smb.conf** параметром безопасности **security**. В изучаемом конфигурационном файле **smb.conf** найдите это параметр и обратите внимание на то, что он имеет значение **user**, то есть управление доступом осуществляется на уровне пользователей по умолчанию. Это самый распространенный вариант организации безопасного доступа в Unix-подобных ОС, поэтому дальнейшие действия в лабораторной работе будут направлены на его настройку.

5. Следующие два параметра **guest account** и **map to guest** отвечают за возможность активации модели «гостевого доступа» в ОС PCBSD.

Первый из них задает имя пользователя-гостя, используемое для доступа к публичным ресурсам из локальной сети. Дело в том, что во всех серверных ОС (ОС FreeBSD и ее потомок ОС PCBSD построены на одном серверном ядре) для каждого из пользователей является обязательным наличие четко организованной учетной записи с соответствующим именем пользователя и паролем. Исключением не является и учетная запись пользователя-гостя, которому в обязательном порядке также должно быть присвоено гостевое имя и соответствующий гостевой пароль для доступа к общим ресурсам серверной ОС.

Найдите данный параметр безопасности в конфигурационном файле **smb.conf** и активируйте штатное имя пользователя-гостя **pcguest**, убрав служебный символ комментирования **«;»** слева от параметра.

Второй из указанных параметров **map to guest** очень важен при использовании безопасности на уровне **user**. Он может принимать три значения: **never** — доступ для пользователей, указавших неверный пароль, будет запрещен; **bad user** — доступ для пользователей, указавших неверный пароль, будет запрещен, если указанное имя пользователя имеется в Unix-подобной ОС; в противном случае пользователь считается «гостем» и получает права гостевой учетной записи; **bad password** — все пользователи, указавшие неверный пароль, считаются «гостями» и получают права гостевой учетной записи.

В рассматриваемом случае приемлемым решением для параметра **map to guest** является значение **bad user**, поскольку, как минимум, обеспечивает необходимость правильного ввода имени пользователя-гостя.

Этот параметр по умолчанию отсутствует в конфигурационном файле **smb.conf**. Внесите его в файл ниже параметра **guest account**.

6. Следующий параметр безопасности, также требующий активации, это **passdb backend**. Как и в предыдущем случае необходимо найти его в конфигурационном файле **smb.conf**, убрать служебный символ комментирования **«;»** слева и присвоить ему новое значение **smbpasswd** вместо присвоенного по умолчанию **tdbsam**.

Данный параметр определяет доступ сервера **Samba** к файлу **smbpasswd**, в котором хранятся имена зарегистрированных в системе пользователей и их пароли (местонахождение данного файла в *гостевой* ОС PCBSD задается путем **/usr/PCBSD/local/etc/samba/smbpasswd**) в зашифрованном виде. При аутентификации пользователя **Samba** ищет учетные данные в этом файле и сравнивает их с теми, которые введены пользователем при регистрации в системе. При совпадении данных пользователя происходит его авторизация.

Следует сказать, что шифрование паролей **Samba** в системе происходит по умолчанию, если не указано иное. Проверьте имеется ли в файле **smb.conf** строка **encrypt passwords = no**, указывающая на то, что пароли **Samba** шифроваться не должны. В зависимости от версии Unix-подобной ОС указанная строка может находится в файле **smb.conf**, но быть при этом закомментированной. Отсутствие этой строки говорит о том, что пароли **Samba** шифруются перед помещением их в файл-хранилище **smbpasswd**.

Кроме того, шифрование паролей является принципиально важным условием, если в локальной сети имеются компьютеры под управлением ОС семейства Windows (например, *хостовая* ОС Windows XP), которые шифруют пароли по умолчанию. Именно поэтому необходимо учесть возможность шифрования паролей **Samba** в *гостевой* ОС PCBSD, иначе доступ для клиентов под управлением ОС Windows XP будет из локальной сети запрещен.

Создание файла-хранилища **smbpasswd** и изменение пароля отдельной учетной записи в нем осуществляется в **«Терминале»** ОС PCBSD посредством одноименного скрипта **smbpasswd** сервера **Samba**. Процедура создания файла-хранилища **smbpasswd**, содержащего хэш-запись пароля к учетной записи **pcguest**, будет рассмотрена позднее.

В конфигурационном файле **smb.conf** дополнительно следует определить местоположение файла-хранилища **smbpasswd** в *гостевой* ОС PCBSD. Для этой цели используется параметр **smb passwd file** со значением абсолютного пути к файлу-хранилищу **smbpasswd** (абсолютный путь записан тремя абзацами выше). Внесите данный параметр в файл **smb.conf** ниже уже активированного **passdb backend = smbpasswd**.

7. Секцию **[global]** можно считать почти сконфигурированной. Последние изменения касаются установок, определяющих корректность отображения кириллических символов общих сетевых ресурсов при доступе к виртуальной локальной сети из *гостевой* ОС PCBSD.

Для конфигурирования данной возможности найдите в файле **smb.conf** строку **«# Charset settings» («Установки таблиц символов»)** и активируйте

все три настройки, убрав комментирующие символы **«;»** слева и присвоив параметрам **unix charset** и **display charset** новое значение кодировки **utf8** вместо **koi8-r**. Сохраните проделанные в файле изменения и сверните текстовый редактор **«KWrite»** на панель задач ОС.

8. Дальнейшие действия предполагается осуществить в направлении организации общего доступа к объектам (файлам и каталогам) ФС UFS *гостевой* ОС PCBSD непосредственно из *хостовой* ОС Windows XP (иными словами, организовать «обратный мост» из ОС Windows XP).

Для этой цели, прежде всего, необходимо создать в рамках ВМ под управлением *гостевой* ОС PCBSD разделяемый сетевой ресурс в виде общего каталога. Пусть именем этого каталога будет **MyShare** (или любое другое на усмотрение обучающегося).

Создание каталога **«MyShare»** осуществим в специально отведенном для этих целей месте, заданном абсолютным путем **/usr/PCBSD/local/share/**. Откройте в файловом менеджере **«sudolphin»** каталог **share/**, пройдя по этому пути до точки назначения, и создайте требуемый каталог обычным образом — по правой кнопки манипулятора мышь вызовите выпадающее контекстное меню и выберите команду **«Создать | Папку»**.

Теперь необходимо присвоить вновь созданному каталогу соответствующий набор разрешений для возможности изменения его содержимого из локальной сети. Для этого наведите манипулятором мышь на каталог **«MyShare»** и в выпадающем контекстном меню выберите команду **«Свойства»**. На вкладке **«Права»** появившегося диалогового окна измените права доступа для категорий **«Группа»** и **«Остальные»** на **«Просмотр и изменение содержимого»** в выпадающем списке. Установите флажок **«Применить изменения ко всем вложенным папкам и их содержимому»** ниже и нажмите **OK** для подтверждения осуществленных действий. Этих изменений должно быть достаточно, чтобы сторонние пользователи локальной сети имели возможность производить операции чтения и записи данных в этом каталоге.

Определение созданного общего каталога в качестве разделяемого ресурса осуществляется в уже знакомом нам конфигурационном файле **smb.conf**, но в другой его чести, расположенной ниже строки **«Share Definitions» («Определители разделяемых ресурсов»)**. Здесь располагаются категории параметров и их значений, относящихся к разделяемым или общим каталогам.

Создайте ниже строки **«Определители разделяемых ресурсов»** новую секцию параметров, например, с именем **[Personal]**, как это, например, сделано для других секций ниже. Под этим именем общий ресурс (каталог) будет отображаться в виртуальной локальной сети. Однако, при этом сам общий каталог должен иметь имя **«MyShare»** (присвоенное ему ранее); абсолютный путь в *гостевой* ОС к этому каталогу фигурирует ниже в виде значения соответствующего параметра **«path»**.

Таким образом, набор параметров, который необходимо ввести в конфигурационный файл **smb.conf** ниже наименования секции **[Personal]** для организации общего каталога в *гостевой* ОС PCBSD, следующий:

```
comment = Common share
path = /usr/PCBSD/local/share/MyShare
guest ok = yes
writable = yes
printable = no
```

Данный набор параметров обеспечивает возможность подключения к каталогу **«MyShare»** посредством сервера **Samba** любого пользователя *хостовой* ОС Windows XP на правах полного доступа (иными словами, это разрешение действия модели «гостевого доступа» по отношению к данному каталогу); за это отвечает ранее установленный параметр **«guest ok»** в значении **«yes»**. При этом запрос аутентификации для такого ресурса выдаваться не будет.

Параметр **writable** со значением **yes** обеспечивает возможность модификации содержимого данного каталога, а **printable = no** — запрещает печать этого содержимого. **«Common share» («Разделяемый ресурс общего пользования»)** это обыкновенный комментарий к общему каталогу.

На этом изменение конфигурационного файла **smb.conf** можно считать завершенным полностью. Сохраните проделанную в файле работу и закройте файловый менеджер **«sudolphin»**.

8. Дальнейший ход лабораторной работы осуществим с использованием **«Терминала»** *гостевой* ОС PCBSD. Загрузите его, выполнив следующее:

- манипулятором мышь кликните на стилизованном изображении огненного шара (аналога стартового меню **Пуск** в ОС Windows XP) в левой нижней части окна загруженной ОС PCBSD;
- в появившемся меню выберите подменю **«Приложения»** (в виде перевернутой, плавно движущейся вкладки), а затем **«Система»** в разделе **«Все приложения»** (название раздела написано мелким шрифтом светло-серого цвета);
- третьим с конца появившегося списка приложений найдите командную консоль ОС **«Терминал»** и запустите ее на выполнение.

Командная консоль **«Терминал»** имеет традиционный вид (она похожа на аналогичную консоль *хостовой* ОС Windows XP). В верхней строке командной консоли введите команду **«Su»**, которая переводит ее в режим администратора корневой директории (root). В появившейся строке приглашения **«password:»** введите соответствующий пароль администратора **(примечание:** при вводе пароль не отображается на экране) и нажмите **«Enter»** для подтверждения операции. Признаком режима администратора (root) является наличие строки **[root@pcbsd]/home/username #** в **«Терминале»**. Системный символ решетка **«#»** указывает на наличие прав администрирования корневой директории (root) у пользователя.

9. Поскольку именем пользователя-гостя является **«pcguest»** необходимо добавить в базу данных **passwd** соответствующую учетную запись. База данных **passwd** предназначена для хранения учетных записей и паролей для доступа непосредственно к *гостевой* ОС PCBSD; эта база данных отличается от

файла **smbpasswd**, который обеспечивает хранение учетных записей для доступа к серверу **Samba** из виртуальной локальной сети.

Для создания в системе нового пользователя, в **«Терминале»** ведите команду **«Adduser» («Добавить пользователя»)**. По этой команде в ОС будет запущен на выполнение консольный «мастер» добавления учетной записи пользователя. Следуйте работе «мастера» и внесите необходимые данные как показано ниже:

Username: pcguest
Full name:
Uid (Leave empty for default): 1002
Login group [pcguest]:
Login group is pcguest. Invite pcguest into other groups? []:
Login class [default]:
Shell (sh csh tcsh bash rbash nologin) [sh]: nologin
Home directory [/home/pcguest]:
Home directory permissions (Leave empty for default):
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]: yes
Lock out the account after creation? [no]: no

Примечание. В процессе заполнения формы базы данных **passwd** учетных записей пользователей некоторые строки целесообразно оставить незаполненными, по умолчанию.

В результате должно получиться следующее:

Username **:** pcguest
Password **:** <blank>
Full Name **:**
Uid **:** 1002
Class **:**
Groups **:** pcguest
Home **:** /home/pcguest
Home Mode **:**
Shell **:** /usr/sbin/nologin
Locked **:** no
OK? (yes/no) **:** yes

При завершении работы «мастера» добавления учетной записи пользователя должно появиться следующее уведомление:

«**Badduser: INFO: Successfully added (pcguest) to the user database.**
Add another user? (yes/no): n
Goodbye!»,

что означает

«**Badduser: Информация: Пользователь pcguest успешно добавлен в базу данных. Добавить другого пользователя? (Да / Нет). До свидания !**».

Из полученных результатов видно, в *гостевой* ОС PCBSD имеется теперь пользователь с именем **«pcguest»** и пустым паролем (**<blank>**). С помощью этой учетной записи появляется возможность иметь гостевой, но локальный (его еще называют «консольный» при вводе с клавиатуры) вход в систему.

Убедиться в наличии этого пользователя в системе можно, открыв в текстовом редакторе **«KWrite»** файл базы данных **passwd**, расположенный по адресу **/etc/passwd**, в последней строке которого будет указано:

pcguest:*:1002:1002:User &:/home/pcguest:/usr/sbin/nologin

Для того, чтобы иметь возможность использовать эти данные для доступа к общим ресурсам *гостевой* ОС из виртуальной локальной сети, необходимо конвертировать базу данных **passwd** учетных записей в файл-хранилище **smbpasswd** и поместить его в папку **/usr/PCBSD/local/etc/samba/**, откуда сервер **Samba** будет считывать данные при аутентификации пользователя-гостя.

10. Конвертирование базы данных **passwd** в файл-хранилище **smbpasswd** осуществляется достаточно просто. Для этого используется команда **cat** следующим образом:

cat /etc/passwd | make_smbpasswd > /usr/PCBSD/local/etc/samba/smbpasswd

Данный конвейерная команда («канал» с перенаправлением вывода в файл) состоит из команды вывода **cat** и скрипта **make_smbpasswd**. Команда **cat** выводит построчно содержимое файла базы данных учетных записей **passwd** на вход скрипта **make_smbpasswd**. Последний, в свою очередь, обеспечивает создание файла-хранилища **smbpasswd**, содержащего хэш-записи всех паролей учетных записей, содержащихся в файле **passwd.**

11. Перегрузите виртуальную машину. После перезагрузки *гостевой* ОС PCBSD становится возможным иметь полный доступ из виртуальной локальной сети (в частности, из *хостовой* ОС Windows XP) к разделяемому ресурсу **[Personal]**.

С точки зрения безопасности доступа имеется необходимость применить в системе еще одну команду, ориентированную на изменение прав доступа к общему ресурсу **[Personal]**.

В Unix-подобных ОС изменение прав доступа к объектам ФС (файлам и каталогам) осуществляется с помощью команды **chmod**. При этом, для использования этой команды иногда используется числовое кодирование режимов. Так, например, код 600 данной команды соответствует режиму: чтение/запись — для владельца, для группы и остальных — доступа нет (иными словами, та-

кой код соответствует правам доступа, характерным для администратора корневой директории (root).

Примените данную команду к файлу-хранилищу **smbpasswd** для того, чтобы никакой пользователь, кроме администратора (root), не смог его изменить или уничтожить. Для этого используйте в командной консоли следующую запись команды:

chmod 600 /usr/PCBSD/local/etc/samba/smbpasswd

13. В дальнейшем, если возникнет необходимость назначить гостевой учетной записи (гостевое имя **«pcguest»**) новый пароль, то это можно сделать с помощью команды **smbpasswd –a pcguest**.

Обратная процедура обнуления пароля гостевого пользователя осуществляется по команде **smbpasswd –an pcguest**.

14. Теперь можно протестировать примененные в *гостевой* ОС PCBSD конфигурационные изменения с помощью команды **testparm** и считать лабораторную работу полностью выполненной.

Заключительные действия в рамках настоящей лабораторной работы целесообразно осуществить в направлении включения и конфигурирования сетевых экранов (брандмауэров) *хостовой* ОС Windows XP и *гостевой* ОС PCBSD. По сути, эти действия трудно назвать конфигурированием, поскольку единственное что необходимо сделать — это позволить сетевым пакетам беспрепятственно проходить в локальной сети от реальной машины к виртуальной.

Запустите штатный брандмауэр *хостовой* ОС Windows XP (см. Лабораторную работу №7) и на вкладке **«Дополнительно»** в списке **«Сетевые подключения»** обратите внимание на то, что подключения виртуального(ых) сетевого(ых) адаптера(ов) контролируются брандмауэром ОС Windows XP. Данные сетевые подключения появляются в настройках брандмауэра ОС Windows XP в процессе инсталляции ПО VMware Workstation. Их наличие в контролируемой брандмауэром области, как правило, не влияет на беспрепятственное прохождение пакетов в локальной сети. Кроме того, процесс аутентификации и авторизации при доступе к ПО VMware Workstation в системе также не контролируется брандмауэром ОС. Об этом говорит тот факт, что на вкладке **«Исключения»** в списке программ или портов присутствует установленный флажок напротив **«VMWare Authd»** — службы, отвечающей за этот процесс. Поэтому эти конфигурационные настройки не оказывают значимого влияния на коммуникацию в локальной виртуальной сети.

Таким образом, со стороны брандмауэра *хостовой* ОС Windows XP значительных препятствий по передаче пакетов данных в виртуальной локальной сети возникать не должно. Однако помимо штатного сетевого экрана ОС Windows XP очень часто в системе имеются другие средства контроля трафика и брандмауэры сторонних производителей, например, бесплатный CoMoDo Firewall или коммерческий Kaspersky Internet Security (KIS) 2009.

Настройка подобных сетевых экранов должна осуществляться согласно документации производителя. В частности, в случае с KIS 2009 для беспрепятственного взаимодействия компьютеров в локальной сети (в том числе, виртуальной) достаточно просто перевести данную сеть в статус доверенной. Для этого необходимо нажать кнопку **«Настройка»** на основном интерфейсном окне брандмауэра KIS 2009, в появившемся диалоговом окне **«Настройки общих параметров защиты»** кликнуть по ссылке **«Защита | Контроль приложений»**, расположенной слева, войти в раздел **«Настройка параметров контроля активности приложений»**, и нажать **«Настройка…»** подраздела **«Сетевой экран»**. На вкладке **«Сети»**, дважды щелкнув мышью по сетевому подключению соответствующего виртуального адаптера, например, **«VMWare Network Adaptor WMnet8»,** выбрать данную локальную сеть. Далее, на вкладке **«Свойства»** появившегося диалогового окна изменить значение параметра **«Статус»** на **«Доверенная сеть»** и подтвердить изменение, нажав **OK**. Изменение тут же должно отобразиться на вкладке **«Сети»** в столбце **«Статус»**. Любая сетевая активность в локальной сети теперь будет санкционирована (на вкладке **«Сетевые пакеты»** сетевой сервис **«Any network activity» («Любая сетевая активность»)** доступен для доверенных сетей).

Со стороны *гостевой* ОС PCBSD включение брандмауэра осуществляется в обратном порядке (см. Лабораторную работу №7):

- манипулятором мышь кликнуть на стилизованном изображении огненного шара (аналога стартового меню **Пуск** в ОС Windows XP) в левой нижней части окна загруженной ОС PCBSD;
- в появившемся меню выбрать подменю **«Компьютер»** (в виде перевернутой, плавно движущейся вкладки), а затем **«Параметры системы»** в разделе **«Приложения»** (название раздела написано мелким шрифтом светло-серого цвета);
- в появившемся окне на вкладке **«Главное»** в разделе **«Сеть и Интернет»** выбрать **«Firewall»** и, дважды щелкнув по названию, загрузить системный модуль, отвечающий за настройки брандмауэра ОС PCBSD; при этом потребуется ввести пароль администратора корневой директории (root);
- на вкладке **«Общие»** программного модуля настройки KDE поставить флажок рядом с надписью **«Включать фаервол при загрузке»** (раздел **«Общие настройки»**), нажать кнопку **«Запустить»** (раздел **«Фаервол»**) и подтвердить выполненные операции, нажав **«OK»** (**«Применить»**); теперь после перезагрузки фаервол будет снова загружаться автозапуском.

Теперь необходимо сконфигурировать брандмауэр на беспрепятственное прохождение пакетов данных и открыть те порты, по которым осуществляется взаимодействие компьютеров по виртуальной локальной сети.

При настройке сетевого экрана KIS 2009 было условлено, что настраиваемая виртуальная локальная сеть находится в статусе **«Доверенная сеть»** и потому в ней возможна любая сетевая активность. Применительно к бранд-

мауэру *гостевой* ОС PCBSD это означает, что по любому порту системы разрешается беспрепятственное прохождение пакетов трафика любого типа.

Настройка брандмауэра *гостевой* ОС PCBSD осуществляется путем создания правила, фильтрующего трафик. Эти правила заносятся в конфигурационные файлы брандмауэра ОС. К числу основных таких файлов брандмауэра, отвечающих за его работу, относятся **pf.conf** и **rc.firewall**.

Согласно принятым касательно трафика установкам необходимо, пользуясь условленным синтаксисом брандмауэра *гостевой* ОС PCBSD, составить подобное правило-фильтр и внести его в конфигурационный файл **/etc/pf.conf**. В наших условиях такое правило имеет вид:

pass in on em0 proto {tcp, udp} all

Данное правило-фильтр обеспечивает беспрепятственное прохождение пакетов запросов, входящих в систему по любому из протоколов **TCP/UDP** из локальной сети для виртуального сетевого интерфейса **em0** (соответствующего в ОС PCBSD виртуальному сетевому адаптеру), по любому сетевому порту.

Впишите данное правило последней строкой в этот конфигурационный файл и закройте его, предварительно сохранив стандартным образом.

После очередной перезагрузки ВМ, настройки будут приняты к исполнению, а виртуальная локальная сеть с общими сетевыми каталогами в консолидированной среде двух альтернативных ОС Windows XP и PCBSD будет функционировать корректно.

Необходимо отметить, что брандмауэр Unix-подобной ОС PCBSD является очень мощным и гибко настраиваемым инструментом безопасности. Он позволяет создавать такие наборы правил-фильтров, которые обеспечивают детализированную фильтрацию трафика определенного типа, будь то входящий трафик по почтовому протоколу **POP3** или же запросы к **DNS**-серверу. Для более полного ознакомления с вопросами настройки ОС PCBSD, в частности, правилами конфигурирования брандмауэра и создания правил-фильтров с целью его корректной работы целесообразно обратиться к книге «FreeBSD. Полное руководство» (2-е издание) признанного специалиста в этой области и активного участника проекта FreeBSD Майкла Лукаса.

В заключение лабораторной работы — несколько слов об организации виртуальной локальной сети двух ОС семейства Windows. Если *гостевая* ОС находится в операционной среде однотипной *хостовой* ОС, то их конфигурирование абсолютно идентично. При этом необходимо настроить одну из них, а для второй — повторить осуществленный алгоритм конфигурирования. Принципы настройки локальных сетей остаются неизменными и соответствуют тем, что были описаны в рассмотренном лабораторном практикуме.

8.4. Содержание отчета по лабораторной работе

Отчет по лабораторной работе оформляется в соответствии с требованиями государственного стандарта и должен содержать:

1) титульный лист (**Приложение**);

2) описание и цель работы;

3) краткое описание ПО VMWare Workstation, его потенциальных возможностей и функций, доступных при организации виртуальной среды в операционных системах семейства Windows;

4) краткое описание последовательности действий при организации виртуальной локальной сети на основе Unix-подобной ОС PCBSD в среде ОС Windows XP;

5) результаты настройки *хостовой* ОС Windows XP реального компьютера с приведением описания последовательности действий и графических фрагментов, сделанных с экрана, в качестве демонстрационного материала;

6) результаты настройки *гостевой* ОС PCBSD виртуальной машины с приведением описания последовательности действий и графических фрагментов, сделанных с экрана, в качестве демонстрационного материала;

7) выводы о проделанной работе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Олифер, В.Г. Сетевые операционные системы : учебник для вузов / В.Г. Олифер, Н.А. Олифер. – СПб. : Изд-во Питер, 2003. – 544 с.

2. Таненбаум, Э. Современные операционные системы / Э. Таненбаум – 2-е изд. – СПб. : Изд-во Питер, 2002. – 1040 с.

3. Станек, У.Р. Коммандная строка Microsoft Windows : справочник администратора / У.Р. Станек – М. : Изд-во ТД «Русская редакция», 2004. – 480 с.

4. Станек, У.Р. Microsoft Windows XP Professional : справочник администратора / У.Р. Станек – М. : Изд-во ТД «Русская редакция», 2003. – 448 с.

5. Элсенпинтер, Р. Microsoft Windows XP Professional. Администрирование сетей. Серия «Справочник администратора» / Р. Элсенпинтер, Т.Дж. Велт. – М. : Изд-во СП ЭКОМ, 2005. – 560 с.

6. Microsoft Corporation. Безопасность сети на основе Windows 2000. Учебный курс MCSE / Microsoft Corporation. – М. : Изд-во ТД «Русская редакция», 2001. – 912 с.

7. Матвеев, М.Д. Самоучитель Microsoft Windows XP : все об использовании и настройках / М.Д. Матвеев, М.В. Юдин, А.В. Куприянова – 2-е изд. : перераб. и доп. – СПб. : Изд-во Наука и Техника, 2006. – 624 с.

8. Руссинович, М. Внутреннее устройство Microsoft Windows : Windows Server 2003, Windows XP и Windows 2000 : мастер-класс / М. Руссинович, Д. Соломон – 4-е изд. – М. : Изд-во ТД «Русская редакция»; – СПб. : Изд-во Питер, 2005. – 992 с.

9. Савилл, Дж. Windows XP/2000 : вопросы и ответы / Дж. Савилл – М. : Издат. дом «Вильямс», 2004. – 1120 с.

10. Хонейкатт, Дж. Реестр Microsoft Windows XP : справочник профессионала : практ. пособ. / Дж. Хонейкатт – М. : Изд-во СП ЭКОМ, 2003. – 656 с.

11. Холмогоров, В. Тонкая настройка Windows XP / В. Холмогоров – СПб. : Изд-во Питер, 2006. – 288 с.

12. Куприянова, А.В. Реестр Windows XP: настройки, трюки, секреты : настольная книга пользователя / А.В. Куприянова ; под ред. М.В. Финкова – СПб. : Изд-во Наука и Техника, 2006. – 192 с.

13. Гультяев, А.К. Виртуальные машины: несколько компьютеров а одном / А.К. Гультяев – СПб. : Изд-во Питер, 2006. – 224 с.

14. Лукас, М. FreeBSD. Подробное руководство, 2-е издание / М. Лукас. – СПб. : Изд-во Символ-Плюс, 2009. – 864 с.

15. http://www.microsoft.com

16. http://www.oszone.net

Приложение. Образец титульного листа

МЕЖДУНАРОДНЫЙ ИНСТИТУТ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ

КАФЕДРА ИНФОРМАТИКИ И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

ЛАБОРАТОРНАЯ РАБОТА № ___

по дисциплине «ОПЕРАЦИОННЫЕ СИСТЕМЫ»

Студента(ки) группы _____

ФИО _____

_____
(подпись)

Проверил:
канд. техн. наук,
доцент каф. ИВТ Савченко В.А. **_____**
(подпись)

Дата « ____ » _____ 2009 г.

ВОРОНЕЖ 2009

Учебное издание

ОПЕРАЦИОННЫЕ СИСТЕМЫ

ЛАБОРАТОРНЫЙ ПРАКТИКУМ
для студентов специальности 230101
«Вычислительные машины, комплексы, системы и сети»
всех форм обучения

ЧАСТЬ IV
(Лабораторные работы №7 и №8)

Составитель:
Савченко Владислав Анатольевич

В авторской редакции

Компьютерный набор Савченко В.А.

Подписано в печать 28.12.2009 г. Формат 60x84/16
Бумага для множительных аппаратов.
Усл. печ. л. 4,81. Тираж 128 экз.
Заказ № 54.

НОУ ВПО «Международный институт компьютерных технологий»
394026, г. Воронеж, Солнечная 29^{б}