

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшее профессиональное образование
«Курганский государственный университет»

Кафедра «Безопасность информационных и автоматизированных систем»

ПРОВЕРКА НАСТРОЕК РАЗРЕШИТЕЛЬНОЙ СИСТЕМЫ ДОСТУПА

Методические указания
к выполнению лабораторной работы
по дисциплине «Программно-аппаратные средства обеспечения
информационной безопасности» для студентов специальности 090105.65

Курган 2013

Кафедра: «Безопасность информационных и автоматизированных систем»

Дисциплина: «Программно-аппаратные средства обеспечения информационной безопасности»
(специальность 090105.65)

Составил: ст. преподаватель В.В. Москвин.

Утверждены на заседании кафедры 23 октября 2013 г.

Рекомендованы методическим советом университета 15 ноября 2013 г.

Цель работы: ознакомиться и получить навыки работы с системами аудита правил разграничения доступа – программами «Ревизор 1 XP», «Ревизор 2 XP».

Приборы и принадлежности:

- 1) персональный компьютер;
- 2) программные комплексы «Ревизор 1 XP», «Ревизор 2 XP»;
- 3) платформа – ОС Windows XP на VirtualBox 4.x.x.

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

1 Работа с программным средством «Ревизор 1 XP»

«Ревизор 1 XP» предназначен для создания и редактирования модели системы разграничения доступа (СРД). В дальнейшем модель СРД будет называться проектом разграничения доступа (ПРД). При этом программой выполняются следующие функции:

1 Автоматическое сканирование локальных логических дисков, а также доступных сетевых папок. Выбор ресурсов для сканирования осуществляется администратором АРМ.

2 Автоматическое считывание установленных прав доступа файловой системы NTFS (для АРМ под управлением ОС семейства Windows NT).

3 Построение по результатам сканирования дерева ресурсов, соответствующего структуре ресурсов АРМ и ЛВС.

4 Автоматическое получение списка локальных и доменных пользователей (для АРМ под управлением ОС семейства Windows NT).

5 Ручная регистрация в ПРД пользователей и установка их уровней допуска.

6 Установка прав доступа пользователей к объектам доступа, а также грифов секретности объектов доступа.

7 Отображение всей информации, содержащейся в ПРД, в удобной форме.

8 Создание отчетов на основе информации о субъектах и объектах доступа.

Программа выполняется администратором АРМ.

Условия применения

Требования к техническим средствам:

Рекомендуемая конфигурация ПЭВМ АРМ:

- процессор Intel Pentium и выше;
- ОЗУ 64 МБ;
- на ЖМД не менее 40 Мбайт дискового пространства;
- видеоадаптер SVGA

При улучшении конфигурации ПЭВМ «Ревизор 1 XP» выполняется быстрее.

Требования к программному обеспечению:

«Ревизор 1 XP» работает под управлением ОС Windows 95, 98, Me, NT 4, 2000, XP и Server 2003. Дополнительных требований к программному обеспечению не предъявляется.

Входные и выходные данные

Входные данные

- Структура ресурсов АРМ и ЛВС. При выполнении сканирования «Ревизор 1 ХР» получает информацию об этой структуре и сохраняет ее в ПРД.
- Установленные права доступа файловой системы NTFS.
- Списки локальных и доменных пользователей системы.
- Информация о разрешительной системе. Вносится администратором при обработке ПРД.

Выходные данные

- ПРД. Физически ПРД сохраняется в виде файла с расширением ARX.
- Отчеты на основе информации, содержащейся в ПРД, в формате HTML.

Функции программы

Сканирование ресурсов. В ходе сканирования «Ревизор 1 ХР» получает информацию о структуре ресурсов АРМ (ЛВС) и сохраняет ее в памяти ПЭВМ.

Считывание прав доступа NTFS. В ходе сканирования дисков с файловой системой NTFS «Ревизор 1 ХР» считывает установленные права доступа и преобразует их в формат, используемый для представления прав доступа в ПРД. Эта функция доступна при запуске программы под управлением ОС семейства Windows NT.

Построение дерева ресурсов. По результатам сканирования «Ревизор 1 ХР» автоматически строит иерархическую структуру, соответствующую структуре ресурсов АРМ.

Получение списка локальных и доменных пользователей. «Ревизор 1 ХР» получает списки учетных записей пользователей, зарегистрированных как непосредственно на АРМ, так и на контроллере домена (в случае, если АРМ входит в состав домена). Эти пользователи регистрируются в ПРД наравне с другими субъектами доступа. Эта функция доступна при запуске программы под управлением ОС семейства Windows NT.

Создание и удаление пользователей. «Ревизор 1 ХР» позволяет вручную добавлять и удалять пользователей ПРД. При создании администратор указывает, какие права доступа получит создаваемый пользователь: либо права доступа по умолчанию, либо права доступа текущего пользователя. При удалении пользователя все установленные для него права доступа теряются.

Моделирование разрешительной системы. При моделировании разрешительной системы администратор устанавливает грифы секретности на объекты доступа, а также настраивает права доступа для созданных пользователей.

Создание отчетов на основе информации о субъектах и объектах доступа. «Ревизор 1 ХР» формирует отчеты в формате HTML на основе информации, содержащейся в ПРД.

Выполнение программы. Для установки «Ревизор 1 ХР» нужно скопировать главный исполняемый файл Revizor1XP.exe в любой каталог на








жестком диске. Никаких дополнительных действий по установке не требуется.

Вызов «Ревизор 1 XP» осуществляется выполнением главного исполняемого файла Revizor1XP.exe. Окно программы (рисунок 1) имеет следующие элементы:

- строка меню.
- панель инструментов.
- дерево каталогов.
- список содержимого каталогов.
- список пользователей.
- строка состояния.

Меню дублирует все функции, доступные с панели инструментов. На панели инструментов расположены следующие кнопки (таблица 1).

Таблица 1 – Кнопки панелей инструментов

	Создание нового проекта
	Открытие проекта
	Сохранение проекта
	Включение / выключение режима наследования разрешений. Если этот режим включен, изменения прав доступа к каталогу будут распространяться на его содержимое
	Создание нового пользователя
	Удаление пользователя
	Создание отчета

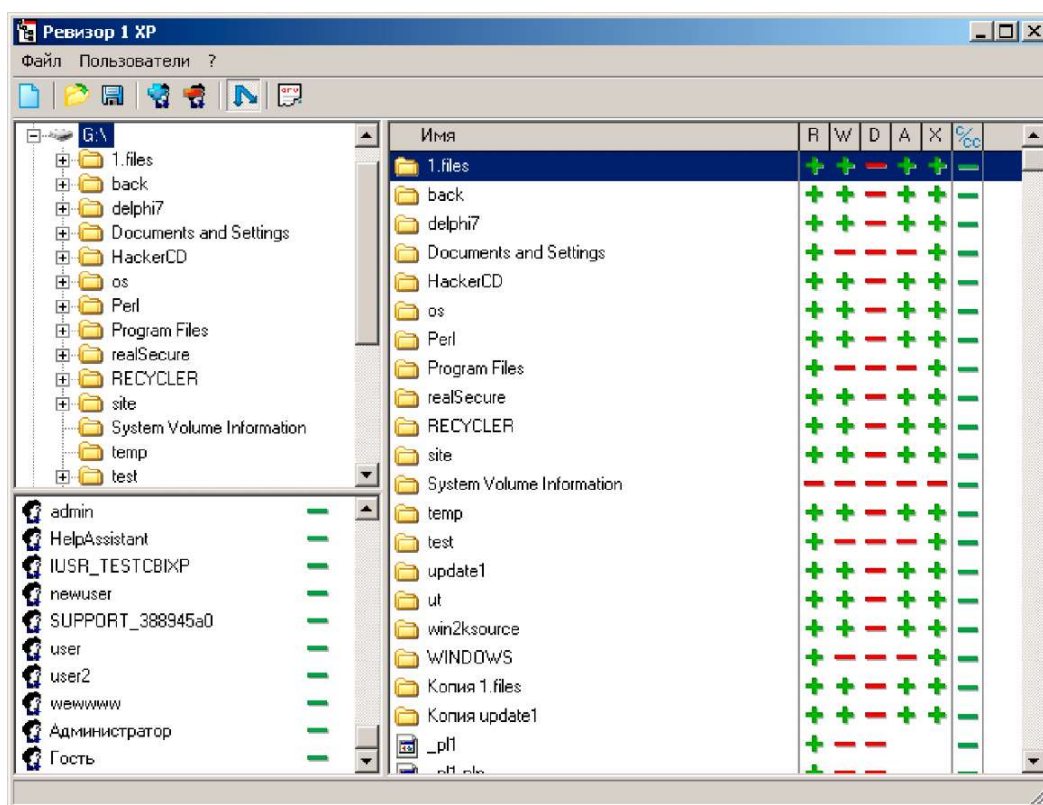


Рисунок 1 – Главное окно программы

Помимо этого из меню могут быть дополнительно вызваны следующие функции:

- «Сохранить как» – сохранить текущий проект под другим именем.
- «Сведения о проекте» – отображение дополнительной информации о проекте, такой как количество пользователей, количество файлов, и прочей.

Кнопки панели инструментов имеют всплывающие подсказки, появляющиеся при задержке курсора мыши над ними.


Если команда, соответствующая кнопке, недоступна, кнопка также недоступна и отображается в сером цвете.

Дерево каталогов отображает структуру каталогов, полученную в результате сканирования. При выборе какого-нибудь каталога его содержимое отображается в правой части окна программы (в списке содержимого каталога).

Список содержимого каталога отображает список объектов, находящихся в выбранном каталоге, а также права доступа («+» означает наличие доступа, «-» – отсутствие) и грифы секретности для них. При двойном щелчке на каталоге (или объекте, который имеет дочерние объекты) осуществляется переход в каталог.

Список пользователей отображает зарегистрированных в проекте пользователей, а также их уровни допуска.

Строка состояния отображает информацию о текущей выполняемой операции.

Создание нового ПРД. Для создания нового ПРД используется кнопка  на панели инструментов или соответствующий пункт меню. После нажатия на эту кнопку на экране появляется окно настройки параметров создаваемого ПРД (рисунок 2).

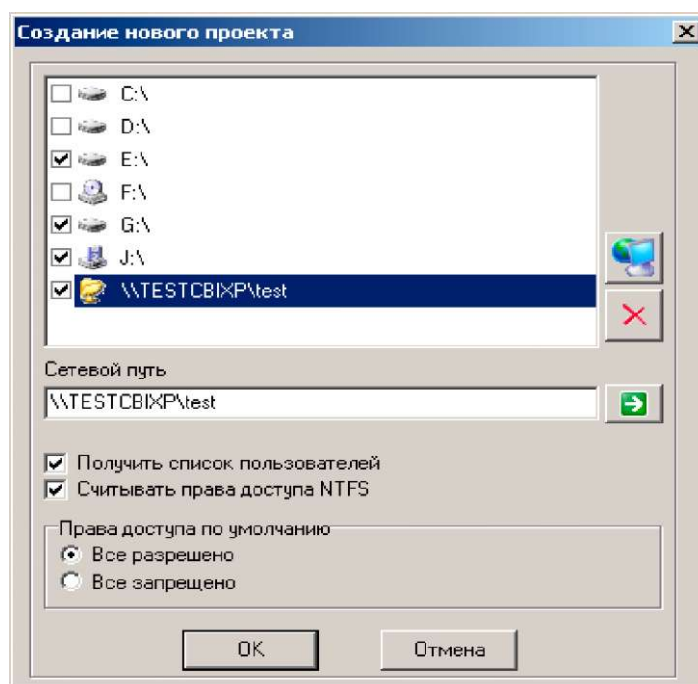



Рисунок 2 – Окно создания нового ПРД

Данное окно содержит список доступных для сканирования ресурсов. В список ресурсов изначально включаются имеющиеся на компьютере

логические диски. Также в него могут быть добавлены общие сетевые папки. Для этого нужно вызвать окно обзора сети с помощью кнопки . При этом программа выполнит сканирование сети и сформирует дерево доступных сетевых ресурсов (рисунок 3).

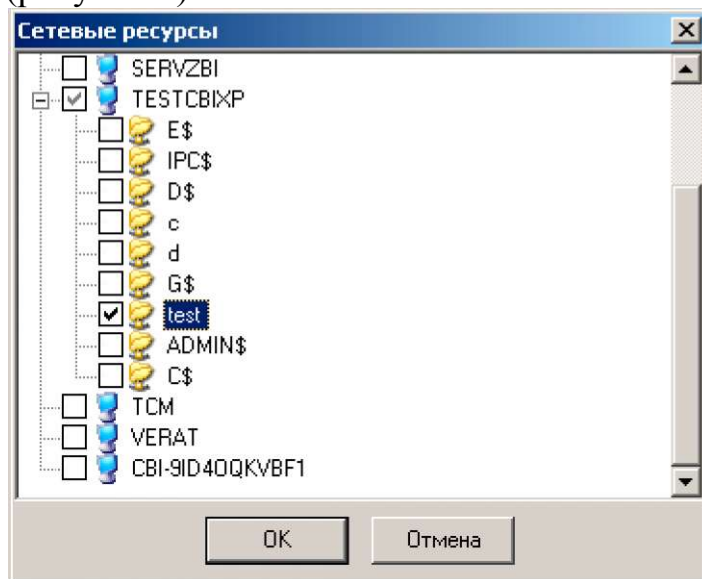




Рисунок 3 – Окно выбора сетевых ресурсов

В появившемся окне нужно отметить требуемые сетевые ресурсы и нажать кнопку «ОК». Отмеченные ресурсы будут добавлены в список выбора ресурсов для сканирования.

Следует обратить внимание, что в некоторых случаях сканирование сети, проводимое программой, может занять достаточно длительное время (например, если в сети много доменов или рабочих групп, членом которых не является данное АРМ). В таких случаях может быть использована возможность ручного добавления сетевых ресурсов в список. Для этого нужно ввести в поле редактирования «Сетевой путь» имя общей папки в формате \\<Имя сервера>\<Имя общей папки> и нажать кнопку . Удалить ненужные сетевые ресурсы из списка можно нажатием кнопки .

В списке ресурсов необходимо отметить те ресурсы, которые должны быть включены в проект.

Помимо выбора ресурсов, необходимо еще задать следующие параметры создаваемого проекта:

«Получить список пользователей» – определяет, будут ли в ходе создания проекта считываться списки пользователей АРМ и домена. При запуске программы под управлением ОС Windows 9x этот параметр недоступен.

«Считывать права доступа NTFS» – определяет, будут ли при сканировании автоматически считываться установленные права доступа NTFS. Для включения данного параметра необходимо, чтобы был включен параметр «Получить список пользователей». В случае если файловая система диска отлична от NTFS, включение данного параметра не окажет никакого эффекта. При запуске программы под управлением ОС Windows 9x этот параметр недоступен.

«Права доступа по умолчанию» - определяет, какие права доступа получат пользователи, если не было произведено считывание установленных прав доступа NTFS. Возможен выбор «Все разрешено» или «Все запрещено».

После установки параметров проекта и нажатия на кнопку «ОК» программа выполняет сканирование ресурсов.

Ход сканирования отображается в окне информации о выполняемой операции. Сканирование может быть прервано нажатием кнопки «Отмена» (рисунок 4).

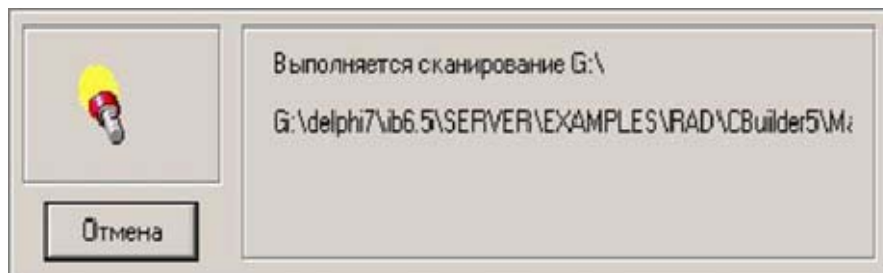


Рисунок 4 – Окно информации о выполняемой операции

При выполнении сканирования следует учитывать, что наличие запущенных антивирусных мониторов или прочих подобных программ может сильно снизить скорость сканирования.

Права доступа к объектам. Список содержимого каталога реализован в виде таблицы, имеющей 7 столбцов.

В первом столбце отображаются имена файлов или каталогов. Столбцы со второго по шестой соответствуют правам доступа к объектам.

Поддерживаются следующие виды доступа:

- Чтение (R) – чтение данных из файла.
- Запись (W) – запись данных в файл.
- Удаление (D) – удаление файла
- Добавление (A) – создание файлов в каталоге.
- Исполнение (X) – запуск исполняемого файла.

Отсутствие или наличие права определяется знаком «+» или «-», отображаемом в соответствующем столбце напротив имени файла.


Седьмой столбец отображает информацию о грифе секретности объекта. Для объекта доступа гриф секретности может принимать следующие значения:

- «-» – несекретный объект;
- «Д» – гриф «Для служебного пользования»;
- «С» – гриф «Секретно»;
- «СС» – гриф «Совершенно секретно».

Права доступа и грифы секретности изменяются одиночным нажатием правой кнопкой мыши на ячейке таблицы, соответствующей требуемому имени объекта и праву доступа. При этом если включен режим наследования разрешений, изменения распространятся и на дочерние объекты.

Работа со списком пользователей. После сканирования ресурсов следующим шагом является формирование списка пользователей. Этот список может уже содержать в себе локальных и доменных пользователей, в случае,

если был включен режим «Получить список пользователей».

Для создания пользователя необходимо нажать кнопку  на панели инструментов, или выбрать соответствующий пункт меню. После нажатия на эту кнопку на экране появляется окно создания нового пользователя (рисунок 5).

В этом окне нужно ввести имя пользователя и указать способ создания пользователя – новый пользователь будет создан с правами доступа по умолчанию или с правами доступа текущего пользователя.

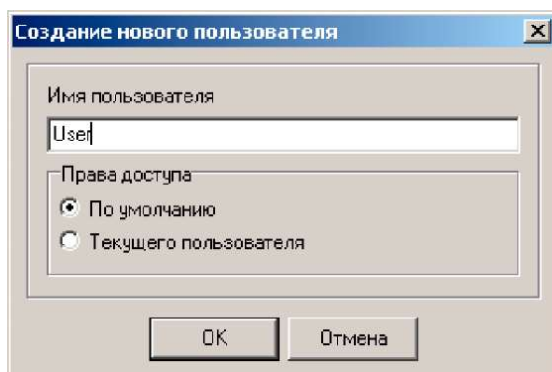






Рисунок 5 – Создание нового пользователя

При создании нового пользователя требуется, чтобы его имя было уникальным в проекте. Если пользователь с введенным именем уже существует, будет выдано сообщение о невозможности создания пользователя.

Для удаления пользователя нужно выделить его имя в списке пользователей и нажать кнопку  на панели инструментов. Пользователь будет удален из проекта, назначенные для него права доступа будут утеряны.

Открытие и сохранение ПРД. Для открытия проекта используется кнопка  панели инструментов. После нажатия на нее на экране появляется диалог открытия файла, в котором нужно выбрать файл проекта.

Для сохранения проекта используется кнопка  панели инструментов. Если проект сохраняется впервые, то на экране появляется диалог сохранения, в котором нужно выбрать файл для сохранения проекта. Дальнейшие сохранения проходят без запроса. Для того чтобы сохранить проект под другим именем используется функция «Сохранить как ...», доступная в меню «Файл».

Создание отчетов. Создание отчета по текущему ПРД осуществляется с помощью кнопки . После нажатия на нее, на экране появляется окно выбора объектов и субъектов доступа (рисунок 6), которые должны быть включены в отчет (ввиду большого объема информации, обычно содержащейся в ПРД, отчеты, как правило, должны иметь выборочный характер).

Следует обратить внимание, что выделение какого-либо узла дерева объектов доступа не приводит к выделению его содержимого. Для выделения содержимого узла необходимо использовать контекстное меню, вызываемое нажатием правой кнопки мыши.

Помимо выбора объектов и субъектов доступа, могут быть изменены следующие параметры:

«Добавлять информацию о грифах секретности» – в отчет будет включена информация о грифах секретности выделенных объектов доступа.

«Добавлять информацию о правах доступа» – в отчет будет включена информация о правах доступа выбранных пользователей по отношению к выбранным объектам доступа.

«Добавить список пользователей» – в отчет будет отдельно включен полный список пользователей проекта.

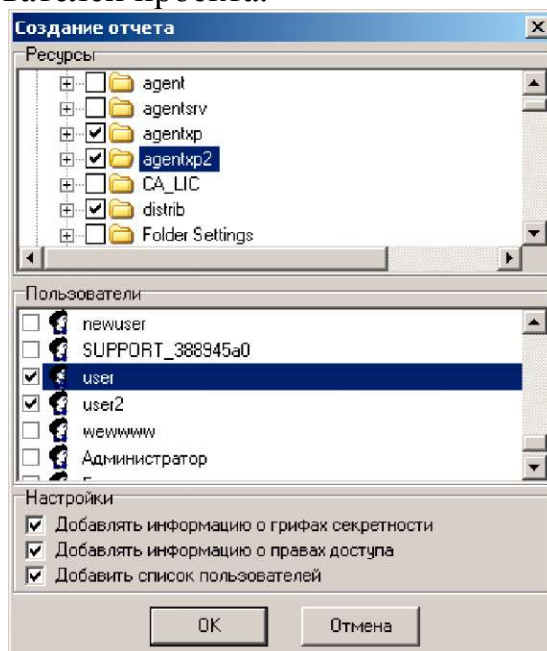


Рисунок 6 – Окно настройки параметров формирования отчета

После задания параметров и нажатия кнопки «ОК» будет запрошено имя файла для сохранения отчета и создан отчет. Программа формирует отчет в формате HTML. Файлы в этом формате могут быть открыты любым веб-браузером (например, Internet Explorer) либо импортированы в офисные приложения, такие как Microsoft Word.

2 Работа с программным средством «Ревизор 2 ХР»

«Ревизор 2 ХР» предназначен для автоматизированной проверки соответствия прав пользователей по доступу к защищаемым информационным ресурсам АРМ, описанным в модели системы разграничения доступа (СРД), реальным правам доступа, предоставляемым установленной на АРМ системой защиты информации, либо соответствующей операционной системой.

Возможности программы. «Ревизор 2 ХР» выполняет следующие функции:

1 Отображение всей информации, содержащейся в ПРД (возможен только просмотр).

2 Сравнение структуры ресурсов АРМ, описанной в ПРД, с реальной структурой ресурсов.

3 Создание отчета по результатам сравнения.

4 Построение плана тестирования объектов АРМ.

5 Проверка реальных прав доступа пользователей к объектам доступа.

6 Создание отчета по результатам тестирования.

Условия применения. «Ревизор 2 XP» применяется на АРМ под управлением операционных систем Windows 95, 98, Me, NT4, 2000, XP и Server 2003. При выполнении программы требуется, чтобы права доступа пользователей были установлены в соответствии с проектной и эксплуатационной документацией АРМ, был обеспечен доступ к ресурсам, присутствующим в ПРД.

Требования к техническим средствам.

Рекомендуемая конфигурация ПЭВМ АРМ:

- процессор Intel Pentium и выше;
- ОЗУ 64 МБ;
- на ЖМД не менее 40 Мбайт дискового пространства;
- Видеоадаптер SVGA.

Требования к программному обеспечению. «Ревизор 2 XP» работает под управлением ОС Windows 95, 98, Me, NT4, 2000, XP и Server 2003. Дополнительных требований к программному обеспечению не предъявляется.

Входные и выходные данные. Входными данными является ПРД, созданный с помощью «Ревизор 2 XP», а также реакция АРМ на попытки доступа к файловым объектам при выполнении тестирования.

Выходными данными «Ревизор 2 XP» являются:

1 Список отличий структуры ресурсов ПРД от реальной структуры ресурсов АРМ. На его основе может быть создан отчет в формате HTML.

2 План тестирования объектов доступа АРМ, с целью определения реальных полномочий пользователей по доступу к файловым объектам. Сохраняется в файле с расширением .pln

3 Протокол тестирования. Сохраняется в файле с расширением .tst

4 Информация о фактических правах доступа, определенных в ходе тестирования. На ее основе может быть создан отчет в формате HTML.

Функции программы.

Просмотр. Для работы с ПРД необходимо его открыть. «Ревизор 2 XP» позволяет просмотреть ПРД в том же виде, в каком он был создан в «Ревизор 1 XP». Если в проекте отсутствуют пользователи, то такой ПРД не будет открыт. «Ревизор 2 XP» позволяет только просматривать ПРД, не внося в них изменений (за исключением сравнения ресурсов).

Сравнение ресурсов. В случае если дерево ресурсов АРМ изменилось со времени создания проекта, «Ревизор 2 XP» позволяет произвести сравнение реального дерева ресурсов с деревом ресурсов ПРД. При сравнении заново выполняется сканирование ресурсов. На основе результатов сравнения может быть создан отчет в формате HTML. После просмотра результатов сравнения можно внести их в дерево ресурсов ПРД и при необходимости скорректировать права доступа к ним с помощью «Ревизор 1 XP».

Тестирование. Тестирование представляет собой моделирование доступа пользователя к объектам АРМ. Моделируются следующие виды доступа:

- Чтение (R) – чтение данных из файла.
- Запись (W) – запись данных в файл

- Удаление (D) – удаление файла.
- Добавление (A) – создание файлов в каталоге.
- Исполнение (X) – запуск программы. В случае успешного запуска файла его выполнение автоматически прерывается.

Выполнение тестирования начинается с построения плана тестирования – списка объектов АРМ с указанием, какие виды доступа к ним должны моделироваться в ходе тестирования. Помимо этого в плане тестирования сохраняется имя пользователя, на основе списка ресурсов которого был создан план.

Для удобства в «Ревизор 2 ХР» существует возможность автоматического построения плана тестирования. Построение плана осуществляется двумя способами: случайная выборка объектов и выбор объектов, чьи разрешения отличаются от родительских. Второй способ позволяет добавить в план тестирования объекты из каждой группы, для которой требуется установка администратором прав доступа, отличных от установленных по умолчанию.

Для тестирования систем с полномочным управлением доступом предусмотрен режим отбора объектов с заданным грифом секретности. Также возможно тестирование разрешительной системы без учета грифов секретности объектов. После автоматического формирования плана администратор добавляет в него объекты, которые не попали в план при автоматическом формировании. Для удобства ручной работы с планом в «Ревизор 2 ХР» есть функции поиска в плане, а также сортировки плана по имени или расширению файлов.

Следующим шагом является удаление из плана тестирования файлов, наличие которых жизненно важно для функционирования операционной системы или установленных средств защиты информации (вместо удаления можно отменить проведение для этих файлов деструктивных тестов, таких как запись и удаление). ***Нарушение целостности этих файлов может привести к полному или частичному разрушению ОС или СЗИ.***

В «Ревизор 2 ХР» есть средство автоматического проведения операций корректировки плана тестирования – фильтрация элементов плана. Существует три вида фильтров:

- фильтр для каталога – удаляет из плана все файлы, находящиеся в указанном каталоге и имя которых соответствует заданной маске (например *.ini в каталоге c:\windows). Применяется также для удаления из плана конкретного файла. В качестве маски имени указывается имя файла (например, boot.ini в каталоге c:\).
- фильтр для каталога и его подкаталогов – удаляет из плана все файлы, находящиеся в указанном каталоге или его подкаталогах и имя которых соответствует заданной маске (например: *.dll в каталоге C:\WINNT\system32).
- глобальный фильтр – удаляет из плана все файлы, имя которых соответствует заданной маске (например, *.vxd).

После завершения формирования плана следующей стадией является тестирование.

Тестирование включает в себя следующие стадии.

Резервное копирование файлов, по отношению к которым будут проведены деструктивные тесты. Для копируемых файлов вычисляются контрольные суммы, по которым проверяется идентичность резервных копий. Резервное копирование осуществляется в указанный администратором каталог. Также может быть включен режим сохранения прав доступа NTFS при резервном копировании (только для АРМ под управлением ОС семейства Windows NT).

Тестирование. На этой стадии выполняется моделирование доступа к объектам, включенным в план тестирования. «Ревизор 2 XP» фиксирует результат попыток доступа к объекту (был ли получен доступ данного вида или нет) и впоследствии сравнивает с матрицей доступа пользователя.

Восстановление файлов, которые были удалены или изменены в ходе тестирования. При восстановлении файлов проводится сравнение их контрольных сумм с вычисленными ранее эталонами, что обеспечивает целостность восстанавливаемых файлов. После восстановления файлов тестирование считается завершенным и возможен просмотр результатов. Также восстанавливаются права доступа NTFS, если был включен соответствующий режим.

Тестирование может проводиться двумя способами: с использованием автоматического (для АРМ под управлением ОС семейства Windows NT) или ручного входа пользователя в систему. При автоматическом способе все тестирование происходит непрерывно, без необходимости выполнять выход и повторный запуск программы. Однако в случае если используемая СЗИ не позволяет выполнять вход систему с использованием стандартных функций Windows (например, требует предъявления аппаратного идентификатора), то тестирование может быть проведено в ручном режиме. При этом выполняется следующая последовательность действий:

1 Для текущего плана запускается процесс резервного копирования. При этом необходимо находиться в системе с правами администратора. После завершения процесса резервного копирования осуществляется выход из программы и вход в систему с правами пользователя, для которого проводится тестирование.

2 Запускается «Ревизор 2 XP», загружается протокол тестирования и запускается процесс тестирования.

3 После завершения процесса тестирования осуществляется выход из программы и вход в систему с правами администратора.

4 Запускается «Ревизор 2 XP», загружается протокол тестирования и запускается восстановления файлов. После его завершения, тестирование считается завершенным.

5 После завершения тестирования становятся доступными его результаты, на основе которых может быть сформирован отчет в формате HTML.

Установка и настройка программы. Для установки «Ревизор 2 XP» нужно скопировать главный исполняемый файл Revizor2XP.exe и Revizor2XP_tester.exe в любой каталог на жестком диске. Никаких дополнительных действий по установке не требуется.

Вызов «Ревизор 2 XP» осуществляется выполнением главного исполняемого файла Revizor2XP.exe

Интерфейс программы. Программа имеет 4 режима работы. При переключении режимов изменяется и внешний вид программы. Существуют общие для всех режимов элементы интерфейса:

Строка меню – содержит пункты, соответствующие режимам работы программы. В соответствующих им подменю продублированы команды с панелей управления, доступных в этих режимах.

- Строка состояния – отображает информацию о текущей выполняемой операции.
- Панель переключения режимов работы.

«Ревизор 2 XP» имеет следующие режимы работы:

- «Просмотр» – режим загрузки и просмотра проекта, выбора текущего пользователя и просмотра его дерева ресурсов.
- «Сравнение» – режим сравнения дерева ресурсов ПРД с реальным.
- «Планирование» – режим построения плана тестирования для текущего пользователя.
- «Тестирование» – режим выполнения тестов разрешительной системы.

Режим просмотра. В окне программы (рисунок 7) имеются следующие элементы:

- список пользователей.
- дерево ресурсов.
- список содержимого папки.
- панель инструментов.

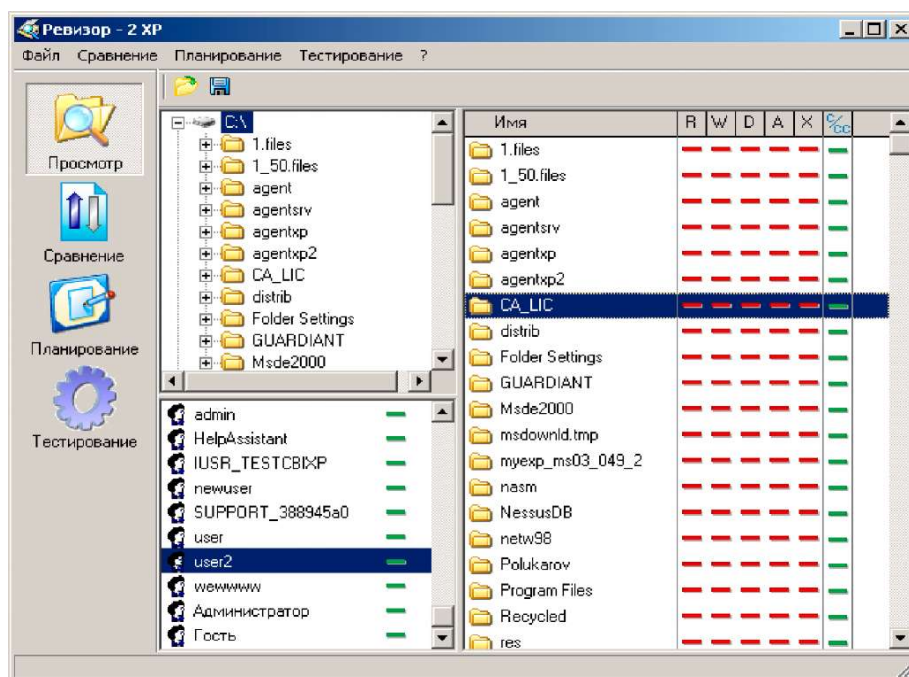







Рисунок 7 – Вид окна программы в режиме построения

В режиме просмотра доступны следующие действия:

- Открытие проекта – нажатием на кнопку  вызывается диалог открытия файла. После выбора файла проекта, в списке пользователей отображаются пользователи проекта. В дереве ресурсов и списке содержимого папки отображаются ресурсы первого пользователя проекта. Если в проекте нет пользователей, то такой проект не открывается, о чем выдается сообщение.

- Сохранение проекта - нажатием на кнопку  выполняется сохранение текущего проекта. Для сохранения проекта под другим именем может быть использована функция «Сохранить как ...», доступная в меню «Файл».

- Выбор пользователя - осуществляется щелчком левой кнопки мыши на имени пользователя в списке пользователей.

Режим сравнения. В этом режиме осуществляется сравнение дерева ресурсов ПРД с реальным (рисунок 8). Сравнение осуществляется нажатием кнопки  на панели инструментов. После окончания сканирования выводится список выявленных отличий. Напротив каждого имени объекта присутствует знак «+» или «-». Плюс означает, что объект отсутствует в дереве ресурсов ПРД, но присутствует в реальном дереве ресурсов (объект был создан после создания проекта), минус – отсутствует в реальном дереве ресурсов, но присутствует в дереве ресурсов ПРД (объект был удален со времени создания проекта). После сравнения и просмотра результатов можно сохранить найденные отличия в дереве ресурсов ПРД нажатием кнопки . Также может быть создан отчет по списку обнаруженных изменений (нажатием кнопки ).

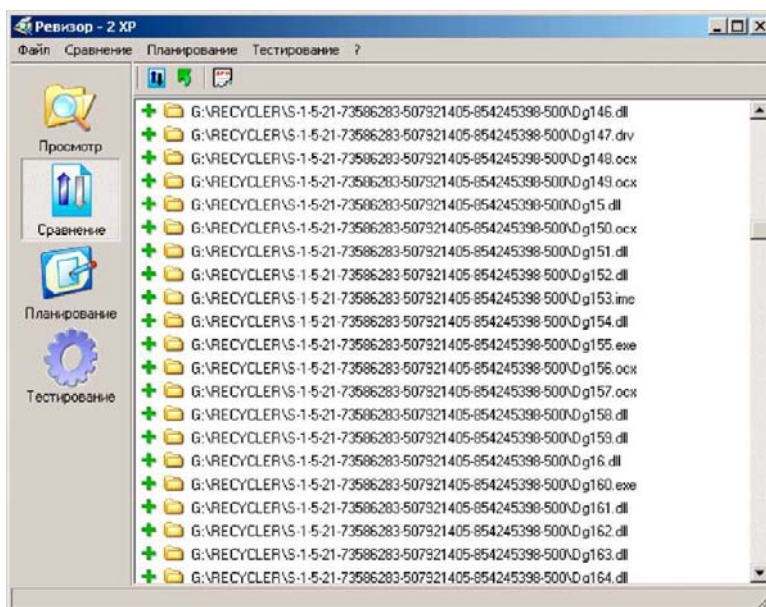


Рисунок 8 – Вид окна программы в режиме построения

Режим построения плана тестирования. В этом режиме создается план тестирования (рисунок 9). Построение плана тестирования осуществляется двумя способами: автоматически или вручную (возможна комбинация этих способов).

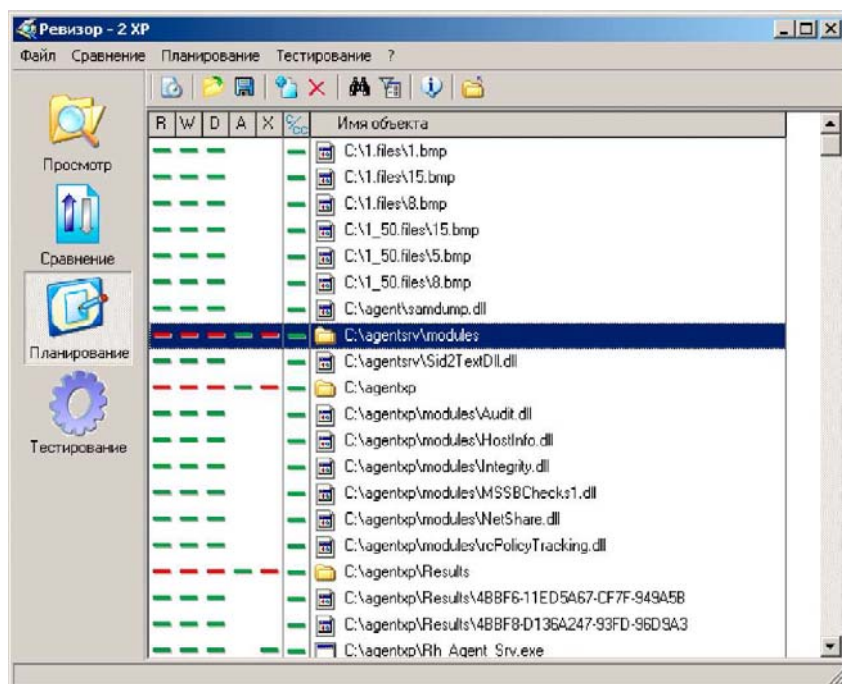











Рисунок 9 – Вид окна программы в режиме построения плана тестирования

Автоматическое построение плана также ведется двумя путями: либо объекты для тестирования выбираются случайным образом, либо для тестирования отбираются те объекты, разрешения или грифы секретности которых отличаются от родительских. После создания плана к нему может быть применен фильтр для удаления из плана файлов, выполнение тестирования которых нежелательно. Панель инструментов имеет следующие кнопки (таблица 2).

Таблица 2 – Кнопки панели инструментов

	Построить план тестирования
	Открыть план тестирования
	Сохранить план тестирования
	Добавить объект для тестирования
	Удалить объект для тестирования
	Поиск в плане
	Вызвать окно фильтра
	Закрывать план тестирования

Также в панели инструментов отображается имя пользователя, для которого создан план.

Создание плана тестирования. Для создания плана тестирования необходимо нажать на кнопку . На экране появится окно настройки параметров формирования плана (рисунок 10).

Доступны для изменения следующие параметры:

«Выбор объектов с разрешениями, отличающимися от родительских» – в создаваемый план тестирования будут автоматически добавлены объекты из каждой группы, для которой требуется установка администратором прав доступа (или грифов секретности), отличных от установленных по умолчанию.

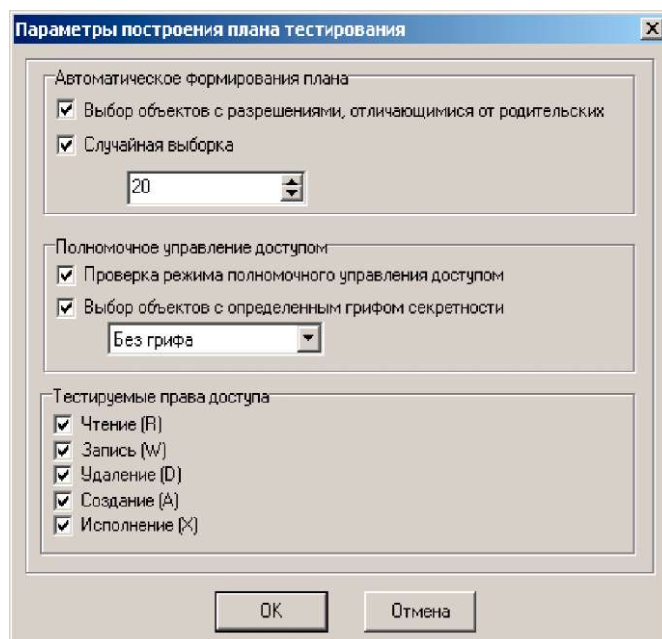


Рисунок 10 – Окно установки параметров формирования плана тестирования


«Случайная выборка» – в план тестирования случайным образом добавляются объекты, в объеме, указанном пользователем (в процентах от общего количества объектов). Если установить объем, равный 100%, то в план тестирования будут добавлены все объекты.

Если оба режима автоматического формирования плана отключены, будет создан пустой план тестирования, в который нужно будет вручную добавить объекты.

«Проверка режима полномочного управления доступом» – определяет, будут ли учитываться грифы секретности при построении плана тестирования.

Также можно указать, объекты с каким грифом секретности отбирать для тестирования и какие права доступа будут тестироваться по умолчанию.

После нажатия на кнопку «ОК» будет сформирован план тестирования в соответствии с заданными параметрами.

В созданный файл тестирования могут быть вручную добавлены объекты, которые не присутствуют в сформированном плане, а тестирование которых должно быть проведено. Для этого нужно нажать кнопку . На экране появится окно выбора объектов (рисунок 11), которые должны быть добавлены в план тестирования.

Следует обратить внимание, что выделение какого-либо узла дерева объектов доступа не приводит к выделению его содержимого. Для выделения содержимого узла необходимо использовать контекстное меню, вызываемое нажатием правой кнопки мыши.

После нажатия кнопки «ОК» выделенные объекты будут добавлены в план тестирования.

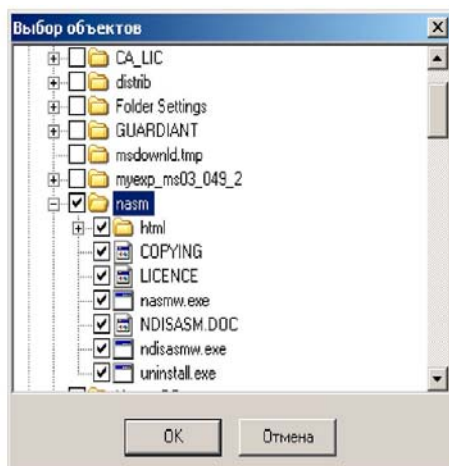


Рисунок 11 – Окно выбора объектов для добавления в план тестирования

Удаление объектов плана тестирования осуществляется с помощью кнопки **✗** на панели инструментов, либо с помощью клавиши «Delete». Нажатие на нее приводит к удалению выделенных объектов.

В «Ревизор 2 XP» есть функция поиска в плане тестирования. Для поиска объекта нужно выполнить команду «Поиск» (кнопка **🔍**), после чего на экране появится окно задания строки для поиска (рисунок 12).

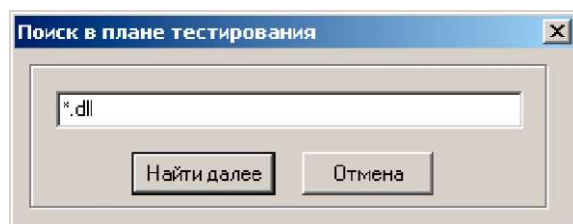


Рисунок 12 – Окно ввода строки поиска.

При задании строки поиска можно использовать символы «?» и «*». После ввода, поиск осуществляется нажатием кнопки «Найти далее». Если подходящий элемент плана найден, курсор устанавливается на него. Чтобы найти следующий элемент плана, нужно нажать на кнопку «Найти далее».

Для удобства просмотра плана тестирования можно использовать функцию сортировки плана по имени, грифу секретности или расширению объектов. Сортировка осуществляется выбором соответствующего пункта контекстного меню, вызываемого нажатием правой кнопки мыши на списке элементов плана.

Отображение плана тестирования. Список выбранных объектов для тестирования отображается в виде таблицы, имеющей 7 столбцов. В столбцах с первого по пятый отображаются права доступа к объекту, в шестом отображается гриф секретности, и в седьмом – имя объекта.

Права доступа пользователя к объекту отображаются следующим образом (см. таблицу 3):


Таблица 3 – Права доступа пользователя к объекту


зеленый плюс	пользователю разрешен данный вид доступа к объекту, и это право будет проверено при тестировании
красный плюс	пользователю разрешен данный вид доступа к объекту, но это право при тестировании проверяться не будет
зеленый минус	пользователю запрещен данный вид доступа к объекту, и это право будет проверено при тестировании
красный минус	пользователю запрещен данный вид доступа к объекту, но это право при тестировании проверяться не будет


Гриффы секретности отображаются зеленым цветом, если режим тестирования полномочного управления доступом включен, и красным – если отключен.

Изменить статус состояние права доступа в плане тестирования можно щелчком левой кнопки мыши по соответствующей ячейке таблицы. Если режим тестирования полномочного управления доступом при построении плана был включен, в плане тестирования используются результирующие права доступа к файлу, которые вычисляются следующим образом:

- Если пользователь имеет уровень допуска не ниже степени секретности файла – он получает доступ, определенный для него разрешительной системой.
- В противном случае у пользователя отсутствует доступ к файлу.

Открытие и сохранение плана. Для открытия плана тестирования используется кнопка  панели инструментов. После нажатия на нее на экране появляется диалог открытия файла, в котором нужно выбрать файл, содержащий план тестирования.

Для сохранения плана тестирования используется кнопка  панели инструментов. Если план сохраняется впервые, то на экране появляется диалог сохранения, в котором нужно выбрать файл для сохранения плана тестирования. Дальнейшие сохранения проходят без запроса. Для того чтобы сохранить план тестирования под другим именем используется функция «Сохранить как ...», доступная в меню «Файл».

Фильтрация элементов плана. Фильтрация позволяет удалять из плана тестирования объекты по маске имени файла. Работа с фильтрами осуществляется через окно (рисунок 13), вызываемое на экран кнопкой .

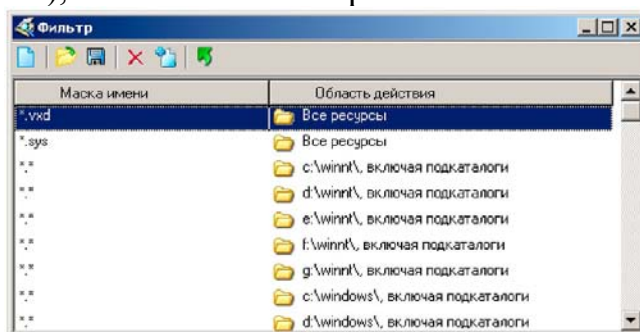











Рисунок 13 – Окно настройки фильтрации элементов плана

Вызываемое окно содержит панель инструментов, на которой есть следующие кнопки:

-  - очистить фильтр
-  - открыть файл фильтра
-  - сохранить файл фильтра
-  - добавить элемент фильтра
-  - удалить элемент фильтра
-  - применить фильтр к плану

Открытие и сохранение фильтра осуществляется нажатием кнопок  и  соответственно. Создание нового фильтра (рисунок 14) осуществляется нажатием кнопки  после чего появляется окно выбора типа создаваемого фильтра: либо создавать пустой фильтр, либо фильтр, предназначенный для удаления из плана основных, важных для функционирования системы, файлов.

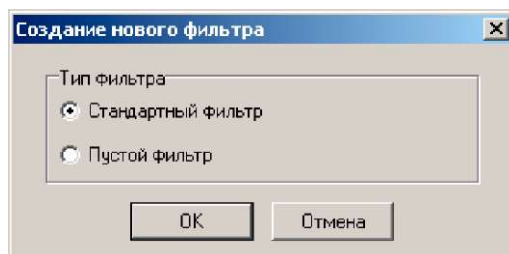




Рисунок 14 – Окно создания нового фильтра

Добавление элемента фильтра. Добавление осуществляется нажатием кнопки  после чего на экране появляется окно создания элемента фильтра (рисунок 15). В нем нужно указать маску имени файла, каталог (не нужно в случае глобального фильтра) и тип фильтра. Каталог и имя файла можно ввести вручную или (если загружен ПРД) выбрать его из дерева ресурсов. Для вызова на экран дерева ресурсов нужно нажать на кнопку , расположенную справа от поля ввода имени каталога.

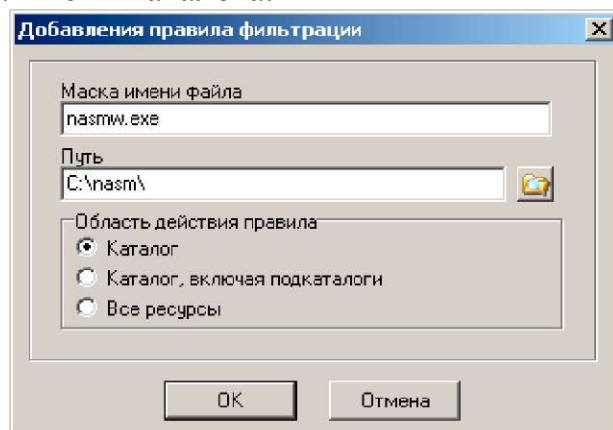




Рисунок 15 – Окно создания нового элемента фильтра


После нажатия на нее на экране появляется дерево ресурсов. Выделив нужный каталог или файл, и нажав на кнопку «ОК» в полях ввода маски имени файла (если был выделен файл) и имени каталога появляются требуемые значения. После ввода данных и выбора типа фильтра следует нажать кнопку «ОК» и элемент фильтра будет добавлен.


Имеются 3 типа фильтров:

- Глобальный фильтр – его действие распространяется на все ресурсы.

Отображается значком  и надписью «все ресурсы» в колонке «область действия».

- Фильтр для каталога – его действие распространяется на содержимое указанного каталога. Отображается значком .

- Фильтр для каталога, включая подкаталоги – его действие распространяется на содержимое указанного каталога и его подкаталогов. Отображается значком .


После того, как фильтр создан, его можно применить к плану тестирования нажатием кнопки . Будут удалены все элементы плана тестирования, удовлетворяющие условиям фильтра.

Режим тестирования. В режиме тестирования выполняется проведение тестов над файлами, включенными в план. Тестирование проходит в 3 этапа:

- Резервное копирование файлов. Выполняется с правами администратора.

- Проведение тестов над файлами, включенными в план. Выполняется с правами пользователя, для которого проводится тестирование.

- Восстановление файлов из резервных копий и удаление временных файлов, созданных в ходе тестирования. Выполняется с правами администратора.

Для начала тестирования необходимо нажать кнопку . На экране появится диалог настройки параметров запускаемого тестирования (рисунок 16).

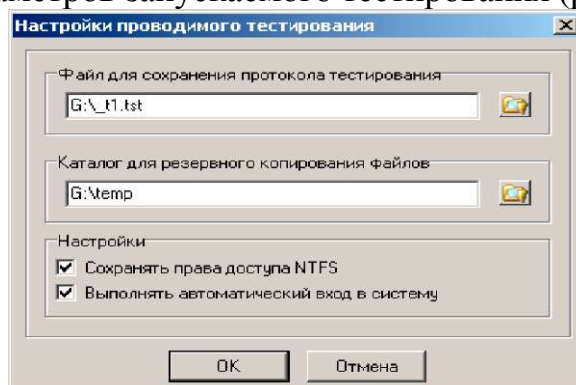


Рисунок 16 – Окно настройки параметров тестирования

В этом окне необходимо указать имя файла для сохранения протокола тестирования (в нем сохраняется информация о выполняемых операциях и их результатах), а также каталог для сохранения резервных копий файлов. Следует обратить внимание, чтобы этот каталог располагался на диске, имеющем достаточно свободного места для размещения резервных копий.

Помимо этого, доступны следующие параметры проводимого тестирования:

«Сохранять права доступа NTFS» – если включить этот режим, то «Ревизор 2 ХР» в ходе резервного копирования сохраняет права доступа в протоколе тестирования и, при последующем восстановлении файлов, восстанавливает их. Этот режим позволяет сохранить установленные права доступа от их повреждения в ходе тестирования. Доступен для АРМ под управлением ОС семейства Windows NT.

«Выполнять автоматический вход в систему» – данный режим позволяет провести тестирование без необходимости выполнять – выход из программы и ручной вход в систему. Однако, использование данного метода невозможно, если установленная СЗИ использует собственную процедуру регистрации в системе (например, с использованием аппаратных идентификаторов), а не стандартную процедуру Windows. Этот режим доступен для АРМ под управлением ОС семейства Windows NT.

Перед началом тестирования нужно убедиться, что в плане тестирования не присутствуют объекты, целостность которых жизненно важна для функционирования ОС и СЗИ. В противном случае возможен выход из строя АРМ после выполнения 2-го этапа.

После нажатия на кнопку «ОК» начинается выполнение резервного копирования. При этом необходимо находиться в системе с правами администратора, чтобы обеспечить программе доступ ко всем ресурсам. При копировании выполняется проверка контрольных сумм исходных файлов и их резервных копий. Значения контрольных сумм исходных файлов сохраняются в протоколе тестирования для проверки восстановления файлов из резервных копий.

После завершения резервного копирования дальнейшие действия зависят от того, был ли включен режим автоматического входа в систему.

В случае если режим был включен, на экране появится окно настройки параметров запуска процесса тестирования (рисунок 17).

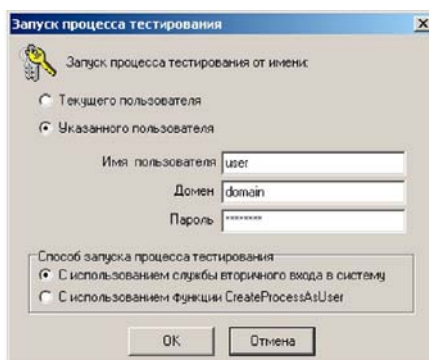


Рисунок 17 – Окно настройки параметров запуска процесса тестирования

В этом окне определяется способ, которым будет запущен процесс тестирования. Доступны следующие варианты:

«От имени текущего пользователя» – процесс запускается от имени того пользователя, под которым в настоящий момент осуществляется работа. Данный способ используется при выполнении ручного входа в систему.

«От имени указанного пользователя» – процесс запускается от имени пользователя, чье имя указывается ниже, в поле «Имя пользователя». Помимо имени, для выполнения программы запуска процесса от имени пользователя необходимо еще указать пароль для входа в систему и домен, к которому принадлежит учетная запись. Если учетная запись расположена на локальном компьютере, то в качестве имени домена может быть введено имя локального компьютера или пустая строка. При запуске программы под управлением ОС Windows 9x этот режим недоступен.

Помимо этого, еще следует указать способ запуска процесса тестирования. «Ревизор 2 XP» предлагает выбор из двух типов запуска:


«С использованием службы вторичного входа в систему» – использование данного способа является предпочтительным. Однако он не поддерживается в Windows NT 4, а также требует, чтобы была запущена служба вторичного входа в систему (она запускается по умолчанию в стандартной конфигурации Windows 2000, XP и Server 2003).

«С использованием функции CreateProcessAsUser» – данный способ следует использовать при проведении тестирования под управлением Windows NT 4. Недостатком данного способа является то, что он требует назначения администратору, проводящему тестирование, дополнительных привилегий, не предусмотренных стандартной конфигурацией. Не рекомендуется использовать этот способ в системах, отличных от Windows NT 4.

Для использования данного способа требуется, чтобы учетной записи администратора, проводящего тестирование, были назначены следующие привилегии (права):

- «Замена маркера уровня процесса».
- «Работа в режиме операционной системы».
- «Увеличение квот».

Привилегии могут быть назначены как непосредственно учетной записи, так и группе, членом которой она является. Для назначения привилегий используется программа «Диспетчер пользователей» (в Windows NT 4) или «Локальная политика безопасности» (в Windows 2000 и более поздних версиях). Эти программы доступны из папки «Администрирование».

После нажатия на кнопку «ОК», запускается процесс тестирования и выполняется последовательность тестов. Если же процесс от имени требуемого пользователя запустить не удалось (например, из-за неправильного пароля или ограничений политики безопасности), то будет выдано сообщение с описанием ошибки. Для повторной попытки запуска процесса тестирования следует нажать кнопку .

В случае если процесс тестирования не удастся запустить после всех попыток, тестирование может быть проведено в ручном режиме.





Если процесс тестирования был запущен, то он выполняет моделирование попыток различных видов доступа к ресурсам, в соответствии с планом тестирования, и сохраняет результаты в протоколе тестирования. После


выполнения всех запланированных тестов, «Ревизор 2 ХР» переходит к стадии восстановления файлов. Восстановление файлов должно выполняться с правами администратора.

При восстановлении файлов из резервных копий осуществляется проверка контрольных сумм восстановленных файлов. В случае если файл не был удачно восстановлен, он не удаляется из каталога для резервных копий. Также, если включен режим сохранения прав доступа NTFS, то выполняется их восстановление.

После завершения восстановления файлов тестирование считается завершенным и становится доступным просмотр результатов.

Если тестирование проводится с использованием ручного режима входа в систему, то порядок его выполнения следующий.


После резервного копирования, выполняется выход из программы и ручной вход в систему с правами пользователя, для которого проводится тестирование. Выполняется запуск «Ревизор 2 ХР» и выполняется команда «Открыть протокол тестирования» (путем нажатия на кнопку ). После открытия протокола, выполняется команда «Приступить к тестированию» (). В окне параметров запуска процесса тестирования следует выбрать «Запуск от имени текущего пользователя» и нажать «ОК». После завершения процесса тестирования выполняется выход из программы и ручной вход в систему с правами администратора. Затем выполняется запуск «Ревизор 2 ХР» и выполняется команда «Открыть протокол тестирования» (путем нажатия на кнопку ). После открытия протокола выполняется команда «Приступить к тестированию» (). Программа выполнит восстановление файлов, после которого тестирование считается завершенным.


Следует отметить, что прерванное вследствие каких-либо проблем тестирование всегда можно продолжить, загрузив протокол тестирования и выполнив команду «Приступить к тестированию» ().


Отображение результатов тестирования. «Ревизор 2 ХР» имеет два режима для отображения результатов тестирования: в виде таблицы и в виде дерева.

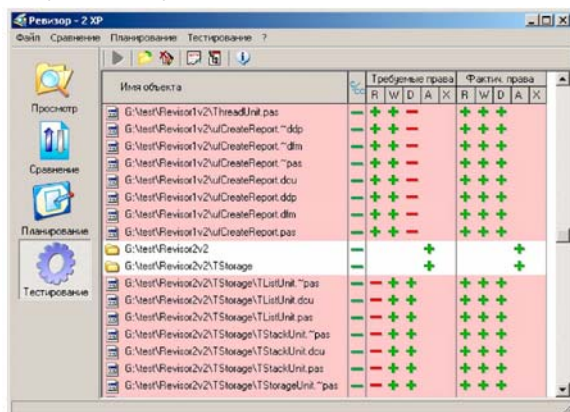
В режиме таблицы результаты отображаются непосредственно в главном окне программы (рисунок 18).

Результаты тестирования отображаются в виде, схожем с отображением плана тестирования, однако, помимо прав, установленных в ПРД, отображаются еще и реальные права доступа, определенные в ходе тестирования. Это позволяет сравнить требуемые права доступа (определяемые требованиями политики безопасности), с фактическими. Для удобства объекты, требуемые права доступа к которым не совпадают с фактическими, выделяются розовым цветом.

Для просмотра результатов в виде дерева, необходимо нажать кнопку . После этого, на экране появится окно, в котором выявленные в ходе тестирования несоответствия разбиваются на две группы: невыполненные запреты – пользователю запрещен доступ в модели разграничения доступа, но на практике он получил доступ к объекту, и невыполненные разрешения –

пользователю разрешен доступ в модели разграничения доступа, но на практике он не получил доступа к объекту. Каждая из этих групп представлена в виде дерева, узлами первого уровня являются права доступа. В случае если выявлены несоответствия, относящиеся к какому-либо праву доступа, узел отображается значком .

В «Ревизор 2 XP» имеется возможность создания отчетов по результатам тестирования. Для создания отчета необходимо нажать кнопку . После этого на экране появится запрос о типе создаваемого отчета. Аналогично двум режимам отображения, существует два типа отчетов:



Имя объекта	Требуемые права					Факт. права				
	R	W	D	A	X	R	W	D	A	X
G:\Test\Revisor\1\2\ThreadUnit.pas	+	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\1\2\CreateReport."ddp	+	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\1\2\CreateReport."dim	+	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\1\2\CreateReport."pas	+	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\1\2\CreateReport.dcu	+	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\1\2\CreateReport.ddp	+	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\1\2\CreateReport.dim	+	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\1\2\CreateReport.pas	+	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\2\2										
G:\Test\Revisor\2\2\TStorage										
G:\Test\Revisor\2\2\TStorage\TListUnit."pas	-	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\2\2\TStorage\TListUnit.dcu	-	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\2\2\TStorage\TListUnit.pas	-	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\2\2\TStorage\TStackUnit."pas	-	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\2\2\TStorage\TStackUnit.dcu	-	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\2\2\TStorage\TStackUnit.pas	-	+	+	+	+	+	+	+	+	+
G:\Test\Revisor\2\2\TStorage\TStorageUnit."pas	-	+	+	+	+	+	+	+	+	+

Рисунок 18 – Окно результата тестирования

Отчет с группировкой информации по имени объекта – данные отображаются аналогично режиму просмотра результатов в виде таблицы. Для этого режима дополнительно можно указать, чтобы в отчет были добавлены только те объекты, по отношению к которым были выявлены несоответствия реальных и требуемых прав доступа.

Отчет с группировкой по правам доступа – данные отображаются аналогично режиму просмотра результатов в виде дерева.

Особенности тестирования систем с полномочным управлением доступом. При тестировании систем с полномочным управлением доступом необходимо учитывать следующие положения:

В случае обращения к файлу, гриф секретности которого выше степени секретности программы, степень секретности программы повышается до грифа секретности файла.

- Программа не может осуществлять запись в файлы, гриф секретности которых ниже, чем степень секретности программы.
- Невозможно копирование файлов в каталоги, гриф секретности которых ниже грифа секретности файлов.
- В некоторых системах защиты информации файл при копировании наследует гриф секретности от каталога, в который он копируется.

Из этого возникают следующие сложности, приводящие к невозможности полноценного тестирования файлов с разными уровнями секретности:

Резервное копирование. Каталог, предназначенный для резервного копирования файлов, должен иметь наибольший из грифов секретности

копируемых файлов. Если файлы наследуют гриф секретности от каталога, в который они копируются, то автоматическое восстановление файлов, чей гриф секретности был ниже, чем у каталога резервного копирования, будет невозможно.

Запись в протокол тестирования. «Ревизор 2 XP» в ходе тестирования осуществляет запись о выполняемых операциях в протокол тестирования. Для того чтобы запись была возможна, необходимо, чтобы файл протокола имел наибольший из грифов секретности тестируемых файлов.

Тестирование. При тестировании, получив некоторый уровень секретности, «Ревизор 2 XP» не сможет осуществить запись данных в файлы с более низким уровнем секретности. Будет зафиксировано отсутствие доступа на запись и добавление данных к этим файлам.

Для разрешения этих проблем в программе есть возможность тестирования объектов с одинаковыми грифами секретности. Отбор таких объектов осуществляется при автоматическом построении плана путем указания требуемого грифа секретности. При выполнении тестирования каталог, предназначенный для резервного копирования файлов и файл протокола тестирования должны иметь тот же гриф секретности, что и тестируемые файлы.

Разграничение доступа к объектам файловой системы APM с установленной ОС Windows XP

Windows XP предоставляет возможность разграничения доступа к объектам файловой системы для каждого пользователя, работающего в ней. Назначение прав доступа к объектам выполняется пользователем «Администратор», или любым другим пользователем наделенным правами администратора.

Создание пользователя. Для создания пользователя необходимо выполнить несколько действий: Перейти в окно оснастки «Локальные Группы и Пользователи». Чтобы открыть оснастку нажмите кнопку «Пуск» и выберите «Панель управления», щелкните дважды значок «Администрирование», а затем «Управление компьютером» (рисунок 19).

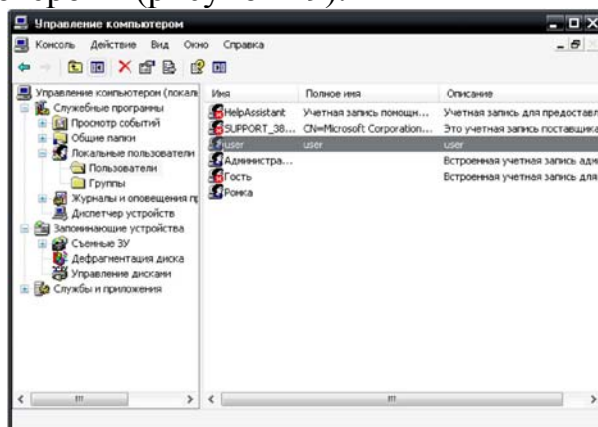


Рисунок 19 – Оснастка Локальные Группы и Пользователи

Далее щелкните правой клавишей мыши, в правой части окна – появится меню, с помощью которого можно создать пользователя. По умолчанию

созданный пользователь будет принадлежать группе пользователей «Пользователи». При необходимости в свойствах пользователя можно установить или изменить некоторые параметры. Во вкладке «Общие»: «Требование к смене пароля при входе в систему», «Запрет на смену пароля», «Срок действия пароля», «Включение, Отключение учетной записи», «Блокировка учетной записи», во вкладке «Членство в группах» можно определить группы, к которым данный пользователь будет принадлежать, во вкладке «Профиль» осуществляется работа с профилем пользователя.

Разграничения доступа. Для того чтобы произвести разграничение доступа для созданного пользователя к какому-либо объекту файловой системы (файл, папка, приложение) щелкните по нему правой кнопкой мыши, появится список возможных действий с этим объектом (рисунок 20).

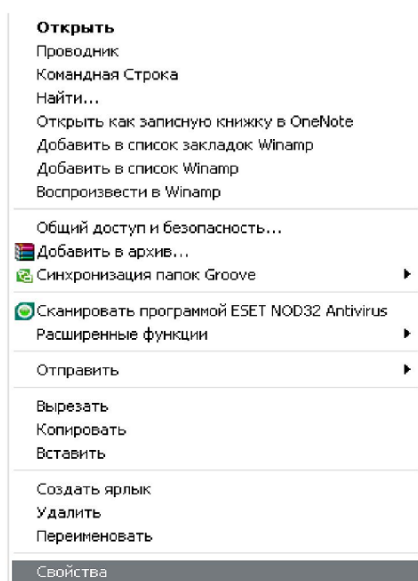


Рисунок 20 – Список возможных действий с объектом

Затем перейти к свойствам объекта. Во вкладке «Безопасность» можно настроить доступ локальных пользователей к объекту (рисунок 21).

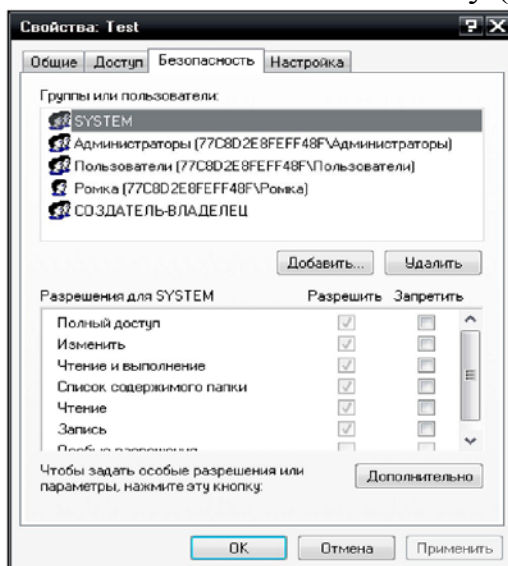


Рисунок 21– Настройка прав доступа.

Внимание! Если вкладка «Безопасность» отсутствует, следует выполнить следующие действия:

1) Нажать кнопку «Пуск», затем «Мой компьютер».

2) В строке меню выбрать вкладку «Сервис», затем «Свойства папки» и вкладку «Вид».

3) Убрать галочку «Использовать простой общий доступ к файлам».

Для того чтобы задать нашему пользователю индивидуальные права, не зависящие от настроек группы к которой он принадлежит, необходимо сделать следующее. Нажать кнопку «Дополнительно» и убрать галочку с пункта «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне» (рисунок 22).

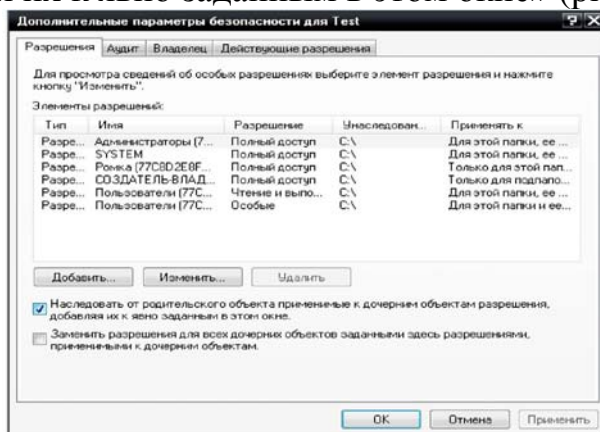


Рисунок 22 – Дополнительные параметры безопасности

Далее появляется окно «Безопасность» (рисунок 23), в котором необходимо нажать кнопку «Копировать». Если выбрать другое – «Удалить», то все объекты в поле разрешений удалятся, и доступ к данному объекту будет разрешен только доступ его владельцу.

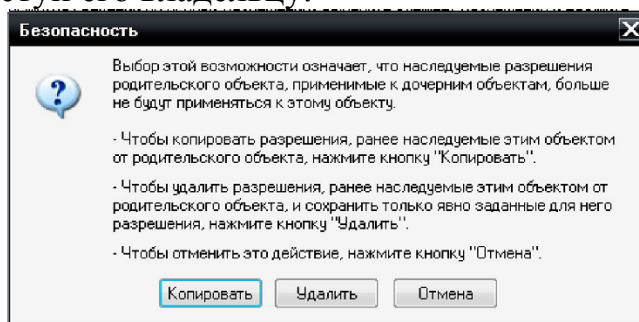


Рисунок 23 – Безопасность

Теперь необходимо перейти во вкладку «Безопасность» и удалить группу «Пользователи» из списка групп.

Внимание! Без выше приведенных действий группу «Пользователи» удалить из списка нельзя. Таким образом, можно удалить любую группу из списка.

Итак, группа «Пользователи» больше не имеет никакого доступа к нашему объекту. Теперь остается только добавить созданного пользователя в список и дать ему соответствующие права для использования этого объекта.

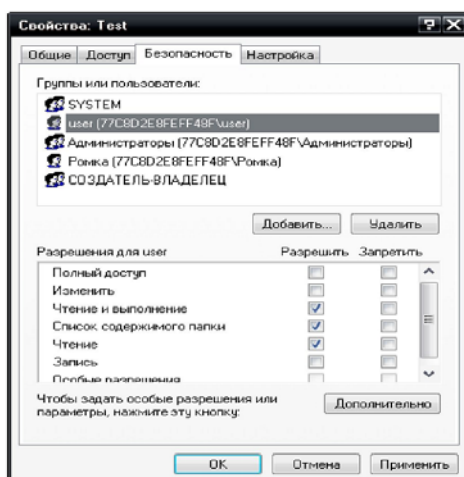


Рисунок 24 – Настройка прав доступа

Во вкладке «Безопасность» нажимаем кнопку «Добавить», далее кнопку «Дополнительно» и «Поиск». Выбираем пользователя, для которого будет проводиться разграничение, и добавляем его в список (рисунок 24).

После чего в поле «Разрешения» можно установить права доступа к этому объекту выбранному пользователю, также можно установить особые права доступа через окно «Дополнительные параметры безопасности».

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1) Создание проекта разграничения доступа (ПРД).

Средствами Windows создать тестируемых пользователей «user» и «user1», наличие пароля обязательно. Создать папки «Test» и «Test 1» на локальном диске С.

Примечание: *Файлы, либо папка, в которой хранятся тестовые файлы, именуется по фамилии студента.*

Добавить в них папки и файлы согласно шаблону (рисунок 25). Типы файлов могут быть произвольными (но соответствующие типам доступов).



Рисунок 25 – Шаблон для подготовки рабочего места к выполнению задания

Варианты заданий разграничения доступа.

Вариант I

Объект/Пользователь	Test	Test 4	Test1.*	Test2.*	Test3.*	Test5.*
User	R	R,A	R,W,D	R,W,D	R	X
User 1	R	-	R	R	R	-
Объект/Пользователь	Test 1	Test 1.4	Test1.1.*	Test1.2.*	Test1.3.*	Test1.5.*
User	R	R,A	-	R	R	X
User 1	R,A	R	R,W,D	R,W,D	R,W,D	X

Вариант II

Объект/Пользователь	Test	Test 4	Test1.*	Test2.*	Test3.*	Test5.*
User	R,A	R,D,A	R	R,W	R	X,D
User 1	R,A	R,A	R	R	R,W,D	X
Объект/Пользователь	Test 1	Test 1.4	Test1.1.*	Test1.2.*	Test1.3.*	Test1.5.*
User	R	R	-	R,W	R,W	X
User 1	R,A	R	R,W	R,D	-	-

Примечание: номер варианта назначается преподавателем

С помощью программы «Ревизор 1 XP» создать ПРД для АРМ согласно одному из шаблонов. При создании проекта выставить галочки **«Считывать права доступа NTFS»** и **«Получить список пользователей»**.

Так как используется системный диск для проверки, то после построения плана тестирования уже при работе с программой «Ревизор 2 XP» рекомендуется применить фильтры, или вручную убрать из плана системные папки и файлы. Сохранить html отчет.

2) Настройка автоматизированного рабочего места (АРМ) в соответствии с созданным проектом при помощи стандартных средств из состава Windows XP.

Произвести разграничение доступа согласно ПРД созданному в пункте **«Создание нового ПРД»**, таким образом, как было описано в пункте **«Разграничение доступа к объектам файловой системы АРМ с установленной ОС Windows XP»**.

Убедиться в правильности разграничения доступа вручную: выполнить вход пользователем «user», а затем «user1» на АРМ и произвести различные действия с объектами такие как чтение, удаление, запись, добавление, и исполнение.

3) Проведение тестирования АРМ на соответствие с ПРД, анализ отчета.

Протестировать АРМ с помощью программы «Ревизор 2 XP». Для этого в «Ревизор 2 XP» необходимо загрузить проект созданный в пункте **«Создание нового ПРД»**. Проводить сравнение не обязательно, так как предполагается, что изменений в АРМ внесено не было.

Создать и сохранить план тестирования, использовать фильтры или удалить вручную системные папки и файлы, если они присутствуют. Перейти в режим тестирования. Нажать кнопку **«Приступить к тестированию»**. В настройках указать каталог для резервного копирования тестируемых файлов, и имя файла для сохранения протокола тестирования. Следует отметить, что не получится произвести резервное копирование файла, занятого каким-либо процессом.

Внимание! *Файл протокола тестирования должен быть доступен для чтения всем пользователям, а программа «Ревизор 2 XP» могла ими выполняться. Так же ни протокол тестирования, ни «Ревизор 2 XP» не должны находиться в папках, доступ к которым для тестируемых пользователей закрыт. Если эти условия не будут выполнены, то при тестировании выскочит ошибка – «Неверные параметры запуска»!*

Поставить галочки **«Сохранять права доступа NTFS»** и **«Выполнять автоматический вход в систему»**. Затем, после того как завершится резервное копирование, необходимо ввести имя тестируемого пользователя, пароль и приступить к тестированию.

Можно не ставить галочку **«Выполнять автоматический вход в систему»**, но тогда придется проводить тестирование вручную. После резервного копирования «Ревизор 2 XP» попросит войти в систему под тестируемым пользователем. Для этого необходимо нажать кнопку «Пуск», затем «Выход из системы» и «Сменить пользователя». После входа в систему нужно будет запустить «Ревизор 2 XP» и в режиме тестирования открыть протокол тестирования, нажать кнопку **«Приступить к тестированию»** и произвести тестирование от текущего пользователя. Затем нужно будет вернуться в систему под администратором, для того чтобы произвести восстановление файлов, посмотреть и сохранить отчет о тестировании.

4) Моделирование несоответствия реальной модели разграничения доступа реализованной на АРМ с ПРД. Повторное тестирование АРМ, анализ отчета.

Смоделировать несоответствие реальной модели АРМ путем нарушения правил доступа для пользователя «user1». Для этого надо изменить параметры доступа к папке «Test» («Test1») таким образом, чтобы права пользователя «user» («user1») на работу с данной папкой и файлами отличались от прав, описанных в ПРД, созданного в пункте **«Создание нового ПРД»**. Протестировать АРМ. Сохранить html отчет.

5) Подготовка отчета для сдачи лабораторной работы.

В отчёте кратко описать выполненные действия с подробными скринами. Привести анализ полученных в работе результатов. В качестве полученных результатов приложить файлы плана и протокола тестирования, а также, html файлы.

6) Сделать вывод по проделанной работе.

ТЕСТОВЫЕ ЗАДАНИЯ К ЛАБОРАТОРНОЙ РАБОТЕ

Входной контроль

1 Безопасность информации – это:

- a) Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз;
- b) Состояние защищенности информации, при котором не происходит нарушение ее целостности;
- c) Нет верного ответа.

2 Что такое НСД (несанкционированный доступ)?

- a) Доступ к информации, с целью получения конфиденциальной информации, при помощи специализированных средств;
- b) Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;
- c) Доступ к информации, несоответствующий правилам разграничения доступа, с целью получения конфиденциальной информации всевозможными способами.

3 «Ревизор 2 ХР» предназначен для:

- a) Автоматизированной проверки соответствия прав пользователей по доступу к защищаемым информационным ресурсам АРМ;
- b) Определения потенциально опасных для АРМ субъектов доступа;
- c) Защиты АРМ, путем разграничения доступа субъектов к объектам и проверки прав доступа данных субъектов к информации.

4 Во сколько этапов «Ревизор 2 ХР» проводит тестирование?

- a) 5;
- b) 1;
- c) Нет верного ответа.

5 Какая модель разграничения доступа используется в данной лабораторной работе?

- a. Мандатная;
- b. Дискреционная;
- c. Смешанная;
- d. Верного ответа нет.

6 Какие существуют типы фильтров?

- a. Глобальный фильтр;
- b. Фильтр для каталога;
- c. Фильтр для каталога, включая подкаталоги;
- d. Фильтр субъектов;
- e. Нет правильного ответа.

7 Какие существуют режимы тестирования?

- a. Пошаговый;
- b. Ручной;
- c. Автоматический;

- d. С использованием дополнительного ПО;
- e. Нет верного ответа.

8 С какой целью необходимо использовать функцию вторичного доступа в систему?

- a. Для того чтобы «Ревизор 2 ХР» мог запустить процесс тестирования от нужного пользователя;
- b. Для того чтобы администратор проводящий тестирование мог произвести его от лица другого пользователя;
- c. Нет верного ответа.

9 В каком виде «Ревизор 2 ХР» предоставляет отчет?

- a. Аналогично режиму просмотра в виде дерева, указывая фактические права и требуемые;
- b. В виде html файла;
- c. В виде режима просмотра, но показывая только несоответствия;
- d. В виде txt файла;
- e. Нет правильного ответа.

10 Можно ли продолжить прерванное по каким-либо причинам тестирование?

- a. Можно, загрузив протокол тестирования;
- b. Нельзя;
- c. В некоторых случаях.

11 «Ревизор 1 ХР» предназначен для:

- a. Создания и редактирования системы разграничения доступа;
- b. Создание правил разграничения доступа, проверка на соответствие этим правилам;
- c. Определение субъектов доступа, не нарушающих правила разграничения.

12 Функции «Ревизор 1 ХР»?

- a. Сканирование ресурсов;
- b. Моделирование разрешительной системы;
- c. Назначение прав доступа пользователей;
- d. Таких функций нет.

13 Что означает режим «Сохранить права доступа NTFS»?

- a. То, что «Ревизор 2 ХР» автоматически меняет права доступа к объекту на «правильные», если реальные права не соответствуют ПРД;
- b. Данный режим сохраняет права в протоколе тестирования и при восстановлении файлов восстанавливает их;
- c. Означает, что при сбое тестирования не будут нарушены права доступа к объектам;
- d. Нет верного ответа.

14 Что означает режим «Права доступа по умолчанию» в «Ревизор 1 ХР»?

- a. Если не было произведено чтение прав доступа NTFS, то пользователям даются права - «Все разрешено» или «Все запрещено» для каждого сканированного объекта;

- b. Сбрасываются все настройки прав доступа до установленных по умолчанию;
- c. Такого режима нет в «Ревизор 1 XP»;
- d. В этом режиме «Ревизор 1 XP» сканирует только те объекты, права доступа к которым не подвергались изменениям.

15 Для чего «Ревизор 2 XP» проводит резервное копирование файлов?

- a. Для сохранения файлов на случай, если произойдет сбой;
- b. На всякий случай;
- c. Для проверки объектов на удаление;
- d. Нет правильного ответа.

Выходной контроль

1 Отображение плана тестирования: каким образом отображаются права доступа к объектам?

- 1 Зеленый плюс - пользователю разрешен данный вид доступа к объекту, и это право будет проверено при тестировании;
- 2 Красный минус - пользователю запрещен данный вид доступа к объекту, но это право при тестировании проверяться не будет;
- 3 Зеленый минус - пользователю разрешен данный вид доступа к объекту, и это право не будет проверено при тестировании;
- 4 Красный плюс - пользователю запрещен данный вид доступа к объекту, и это право будет проверено при тестировании.

2 Что означает «Случайная выборка» с параметром 100?

- 1 Случайным образом выбираются 100 объектов;
- 2 Выбираются все объекты;
- 3 Нет верного ответа.

3 Какие символы можно использовать при поиске в плане тестирования?

- 1 «*», «?»;
- 2 «?», «/»;
- 3 «&», «*», «?»;
- 4 «**», «\$\$».

4 Зачем применять фильтры?

- 1 Для устранения из плана тестирования объектов, при тестировании которых может быть нанесен вред ОС;
- 2 Для того, чтобы исключить системные файлы из плана тестирования;
- 3 Для приведения плана тестирования в более удобный для просмотра вид;
- 4 Для определения объектов, тестировать которые не рекомендуется.

5 Как установить права доступа субъекта таким образом, чтобы ни один другой субъект не смог выполнить никаких действий с данным объектом?

- 1 Свойства:<имя объекта> => Безопасность => Очистить поле «Группы и Пользователи» => Добавить субъекта;
- 2 Свойства:<имя объекта> => Безопасность => Дополнительно => Убрать галочку «Наследовать от родительского объекта...» =>Нажать Удалить => Добавить субъекта;

3 Свойства:<имя объекта> => Безопасность => Дополнительно => Убрать галочку «Наследовать от родительского объекта.» => Нажать Копировать => Добавить субъекта.

6 С какой целью необходимо убирать галочку с «Использовать простой общий доступ к файлам»?

- 1 В свойствах объектов появляется вкладка «Безопасность»;
- 2 Для более детальной настройки прав разграничения доступа субъектов к объектам;
- 3 Не следует убирать эту галочку, так как можно сбить настройки прав доступа для всех субъектов АРМ;
- 4 Для того чтобы можно было настраивать права доступа.

7 От лица кого можно запустить процесс тестирования?

- 1 Текущего пользователя;
- 2 Указанного пользователя;
- 3 Администратора или группы пользователей принадлежащих группе «Администраторы»;
- 4 От любого пользователя АРМ.

8 Для чего нужен «Протокол тестирования»?

- 1 Для сохранения значений контрольных сумм;
- 2 Для сохранения html отчетов по умолчанию;
- 3 Для отображения плана тестирования;
- 4 Для сохранения резервных копий объектов.

9 Можно ли добавлять в ПРД «Общие сетевые» папки?

- 1 Да;
- 2 Нет;
- 3 Да, но не всегда.

10 Выполняет ли «Ревизор 1 XP» сканирование сетевых ресурсов?

- 1 Выполняет;
- 2 Не выполняет;
- 3 Выполняет сканирование общих сетевых папок.

11 Для чего используется способ запуска процесса тестирования с использованием функции CreateProcessAsUser?

- 1 Для корректной работы программы «Ревизор 2 XP» и ОС, установленной на АРМ;
- 2 Для тестирования в системе под управлением Windows NT4;
- 3 Для проведения тестирования в системе с ОС отличной от Windows NT4.

12 Что произойдет, если файл протокола тестирования будет скрыт или недоступен для чтения тестируемым пользователям?

- 1 Ничего не произойдет;
- 2 Появится ошибка «Отсутствует протокол тестирования»;
- 3 Появится ошибка «Неверные параметры запуска»;
- 4 Другое.

13 Что означает параметр «Выполнять автоматический вход в систему»?

- 1 Выбор автоматического режима тестирования АРМ;

2 Выбор режима, в котором администратору не приходится проводить дополнительных действий по настройке ре режима тестирования;

3 Такого параметра не существует.

14За что отвечает параметр «Запуск процесса тестирования от текущего пользователя»?

1 Тестирование выполняется от пользователя, который работает в данный момент в системе;

2 Тестирование пользователей от лица текущего пользователя, работающего в системе;

3 Данный параметр предназначен для ручного проведения тестирования.

15К чему может привести нарушение целостности системных файлов в случае сбоя процесса тестирования?

1 К частичному разрушению ОС и СЗИ;

2 К полному разрушению ОС и СЗИ;

3 Оба выше приведенных варианта;

4 К тому, что придется проводить процесс тестирования АРМ заново.

Список литературы

1 Инструментальный контроль несанкционированного доступа: подробности (Часть 3) // deHack.ru [Официальный сайт]. URL : http://dehack.ru/arts/instrumentalnyj_kontrol_nesanktsionirovannogo_dostupa_podrobno sti_chast_3/ (дата обращения: 11.11.2013)

2 Инструментальный контроль несанкционированного доступа. URL: http://dehack.ru/arts/instrumentalnyj_kontrol_nesanktsionirovannogo_dostupa/ (дата обращения: 11.11.2013)

3 Лабораторная работа № 10: Проверка настроек разрешительной системы доступа к файловым системам с использованием специализированных тестирующих средств и штатных средств из состава ОС. С.189-223 // ФСТЭК. Методическое пособие по аттестации объектов информатизации по требованиям безопасности информации. Контроль защищенности локальных вычислительных сетей от несанкционированного доступа – Сборник типовых лабораторных практикумов.

4 Духан, Е. И. Программно-аппаратные средства защиты компьютерной информации. Практический курс [Текст] : учебное пособие / Е. И. Духан, Н. И. Синадский, Д. А. Хорьков. – Екатеринбург : УрГУ, 2008.

5 Скембрей, Д. Секреты хакеров. Безопасность Windows 2000 – готовые решения [Текст] / Д. Скембрей, С. Мак-Клар ; пер. с англ. – М. : Вильямс, 2002.

6 Кландер, Л. Hacker proof. Полное руководство по безопасности компьютера [Текст] / Л. Кландер ; пер. с англ. Минск : Попурри, 2002.

Москвин Владимир Викторович

ПРОВЕРКА НАСТРОЕК РАЗРЕШИТЕЛЬНОЙ СИСТЕМЫ ДОСТУПА

Методические указания
к выполнению лабораторной работы
по дисциплине «Программно-аппаратные средства обеспечения
информационной безопасности» для студентов специальности 090105.65

Редактор Е.А. Могутова

Подписано к печати 24.12.13	Формат 60×84 1/16	Бумага тип. №1
Печать цифровая	Усл. печ.л. 2,5	Уч.-изд.л. 2,5
Заказ 232	Тираж 22	Не для продажи

РИЦ Курганского государственного университета.
640669, г. Курган, ул. Гоголя, 25.
Курганский государственный университет.