УТВЕРЖДЕН

643.53132931.501252-02 31 01-ЛУ

Программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 XP»

Описание применения

643.53132931.501252-02 31 01

Листов 25

2017

АННОТАЦИЯ

Настоящий документ является описанием «Ревизор 2 XP» - средства автоматизированной проверки соответствия прав пользователей по доступу к защищаемым информационным ресурсам АРМ, описанных в модели системы разграничения доступа (СРД), реальным правам доступа, предоставляемым установленной на АРМ системой защиты информации, либо соответствующей операционной системой.

Документ содержит сведения о возможностях программы, условиях и порядке применения.

«Ревизор 2 XP» разработан в среде Delphi 7, функционирует под управлением операционных систем Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10, Windows Server 2016.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение программы

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

1.2. Возможности программы

«Ревизор 2 XP» выполняет следующие функции:

- Отображение всей информации, содержащейся в ПРД (возможен только просмотр)
- Сравнение структуры ресурсов АРМ, описанной в ПРД, с реальной структурой ресурсов
- Создание отчета по результатам сравнения
- Построение плана тестирования объектов АРМ
- Проверка реальных прав доступа пользователей к объектам доступа
- Создание отчета по результатам тестирования

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Требования к техническим средствам

Рекомендуемая конфигурация ПЭВМ АРМ:

- процессор – Intel Pentium и выше;
- ОЗУ – 2048 МБ;
- на ЖМД не менее 500 Мбайт дискового пространства;
- Видеоадаптер – SVGA.

При улучшении конфигурации ПЭВМ «Ревизор 2 XP» выполняется быстрее.

2.2 Требования к программному обеспечению

«Ревизор 2 XP» работает под управлением ОС Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10, Windows Server 2016. Дополнительных требований к программному обеспечению не предъявляется.

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.

3. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

3.1. Входные данные

Входными данными является ПРД, созданный с помощью «Ревизор 1 XP», а также реакция АРМ на попытки доступа к файловым объектам при выполнении тестирования.

3.2. Выходные данные

Выходными данными «Ревизор 2 XP» являются:

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

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

– Протокол тестирования. Сохраняется в файле с расширением .tst

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

4. СОСТАВ И ФУНКЦИИ

4.1. Состав программы

Revizor2XP.exe – главный исполняемый файл

Revizor2XP_tester.exe – исполняемый модуль, выполняющий имитацию попыток доступа пользователя к ресурсам

4.2. Выполняемые функции

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).

4.2.1. 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».

4.2.2. Тестирование

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

- Чтение (в программе обозначается как 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 XP» 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 XP» 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 файлов 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 XP» 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:

1. 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).

2. 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.

3. 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.
2. После завершения процесса резервного копирования осуществляется выход из программы и вход в систему с правами пользователя, для которого проводится тестирование.
3. Запускается «Ревизор 2 XP», загружается протокол тестирования и запускается процесс тестирования.
4. После завершения процесса тестирования осуществляется выход из программы и вход в систему с правами администратора.
5. Запускается «Ревизор 2 XP», загружается протокол тестирования и запускается восстановление файлов. После его завершения, тестирование считается завершенным.

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

5. ВЫПОЛНЕНИЕ ПРОГРАММЫ

5.1. 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

5.2. 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 соответствующим 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.

5.3. Режим просмотра

В окне программы (рис. 1) имеются следующие элементы:

– Список пользователей
– Дерево ресурсов
– Список содержимого папки
– Панель инструментов

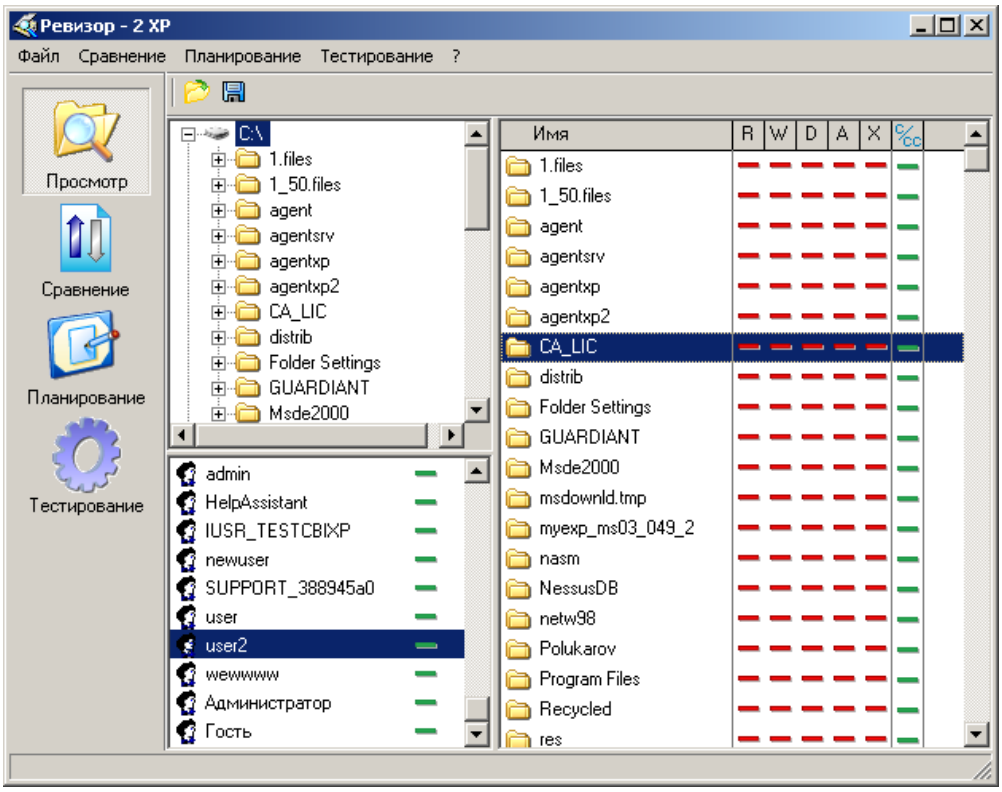

Рис. 1. Вид окна программы в режиме просмотра

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.

– Просмотр дерева ресурсов пользователя – дерево ресурсов доступно только для просмотра. Внесение изменений невозможно, за исключением случая сравнения ресурсов (п. 5.4.).

5.4. Режим сравнения

В этом режиме осуществляется сравнение дерева ресурсов ПРД с реальным. Сравнение осуществляется нажатием кнопки на панели инструментов. После окончания сканирования выводится список выявленных отличий. Напротив каждого имени объекта присутствует знак «+» или «-». Плюс означает, что объекта 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) (рис. 2).

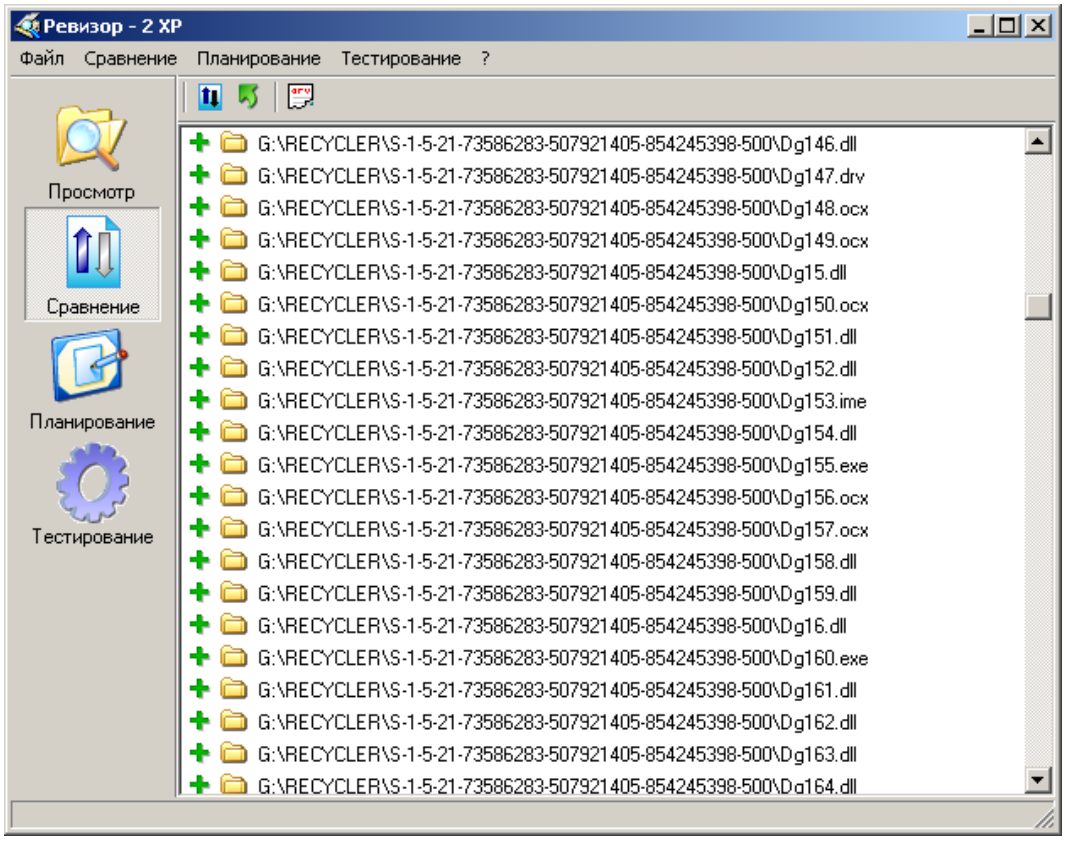

Рис. 2. Вид окна программы в режиме сравнения

5.5. Режим построения плана тестирования

В этом режиме создается план тестирования (рис. 3). Построение плана тестирования осуществляется двумя способами: автоматически или вручную (возможна комбинация этих способов). 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.

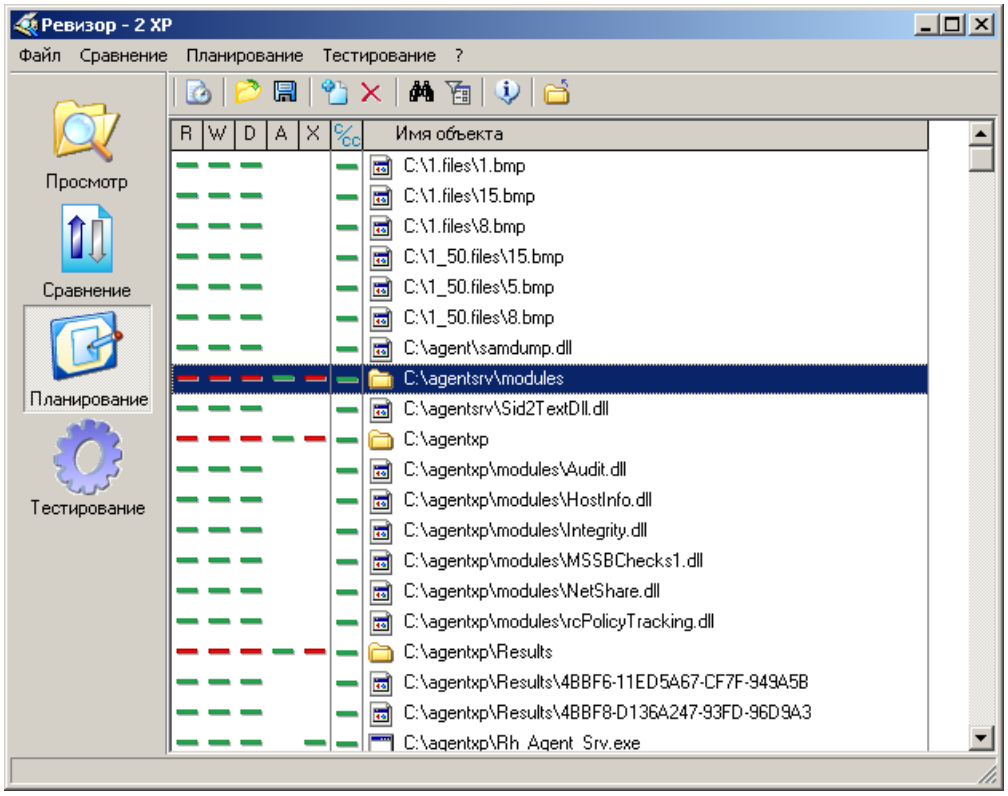

Рис. 3. Вид окна программы в режиме построения плана тестирования

Панель инструментов имеет следующие кнопки:

 Построить план тестирования

 Открыть план тестирования

 Сохранить план тестирования

 Добавить объект для тестирования

 Удалить объект для тестирования

 Поиск в плане

 Вызвать окно фильтра

 Закрыть план тестирования

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

5.6. Создание плана тестирования

Для создания плана тестирования необходимо нажать на кнопку  . На экране появится окно настройки параметров формирования плана (рис. 4).

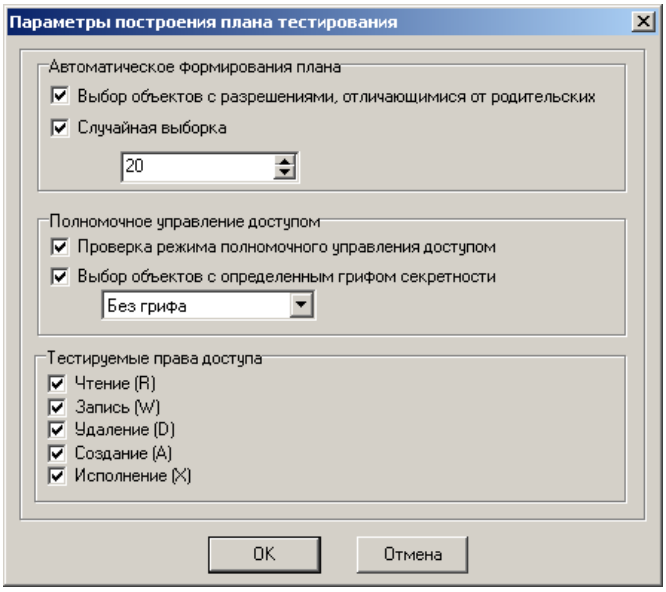

Рис. 4. Окно установки параметров формирования плана тестирования.

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

«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, гриф секретности для объектов (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 план тестирования (рис. 5) могут быть вручную добавлены объекты, которые не присутствуют в сформированном плане, и тестирования которых должно быть проведено. Для этого нужно нажать кнопку . На экране появится окно выбора объектов, которые должны быть добавлены в план тестирования.

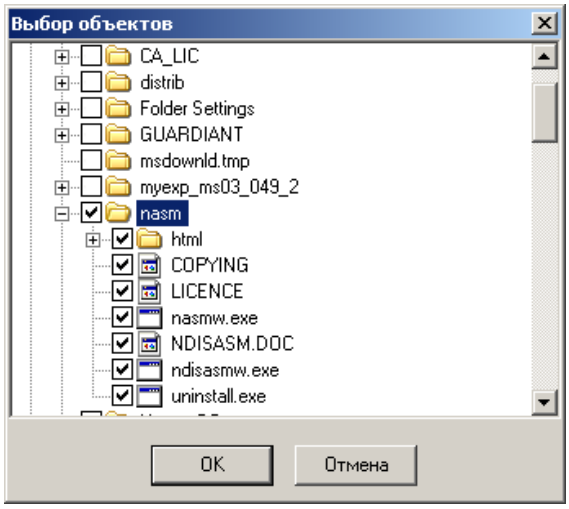

Рис. 5. Окно выбора объектов для добавления в план тестирования.

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.

Удаление объектов плана тестирования осуществляется с помощью кнопки ✕ 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 (рис. 6):

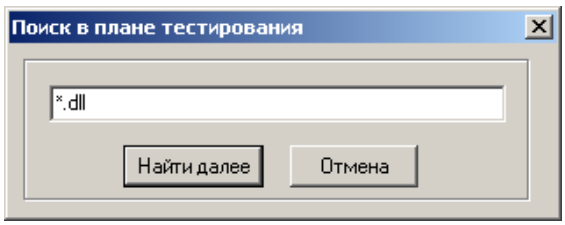

Рис . 6. Окно ввода строки поиска.

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.

5.7. 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:

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

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

Изменить статус состояния 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, то он получает доступ, определенный для него разрешительной системой;

– в противном случае у пользователя отсутствует доступ к файлу.

5.8 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».

5.9 Фильтрация элементов плана

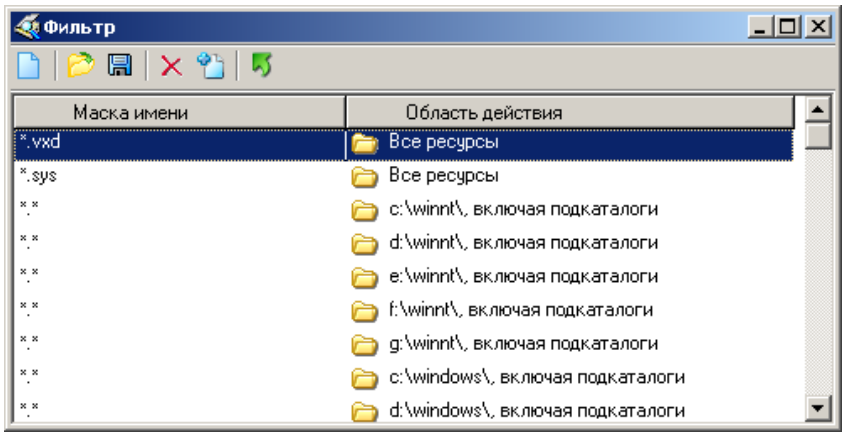

Рис. 7. Окно настройки фильтрации элементов плана.

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

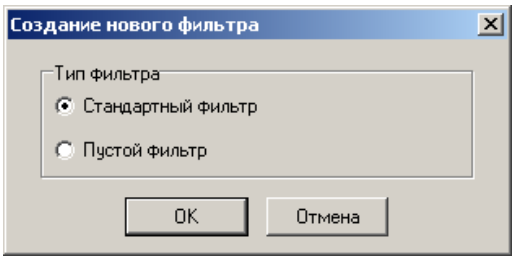

Рис. 8. Окно создания нового фильтра.

Открытие и сохранение фильтра осуществляется нажатием кнопок и соответственно. Создание нового фильтра осуществляется нажатием кнопки , после чего появляется окно выбора типа создаваемого фильтра (см. рис. 8): либо создавать пустой фильтр, либо фильтр, предназначенный для удаления из плана основных, важных для функционирования системы, файлов.

5.10 Добавление элемента фильтра

Осуществляется нажатием кнопки , после чего на экране появляется окно создания элемента фильтра (рис. 9). 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. 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) или имени каталога появляются требуемые значения. После ввода данных и выбора типа фильтра следует нажать кнопку «ОК» и элемент фильтра будет добавлен.

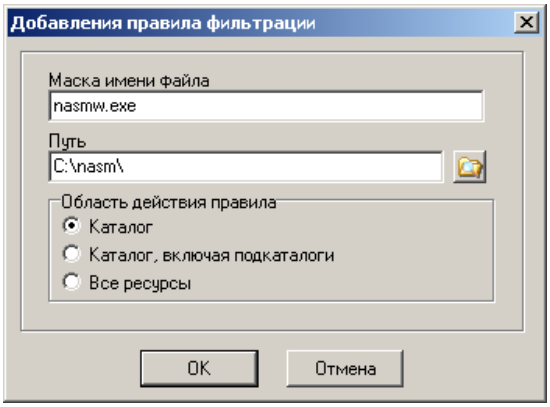

Рис. 9. Окно создания нового элемента фильтра.

5.11 Типы фильтров.

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 .

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

5.12 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 (рис. 10)

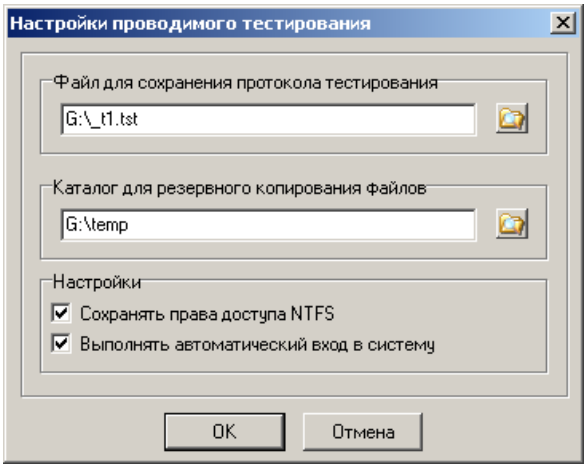

Рис. 10. Окно настройки параметров тестирования

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 это 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 XP» 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 убедится, 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 находится 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 (рис. 11).

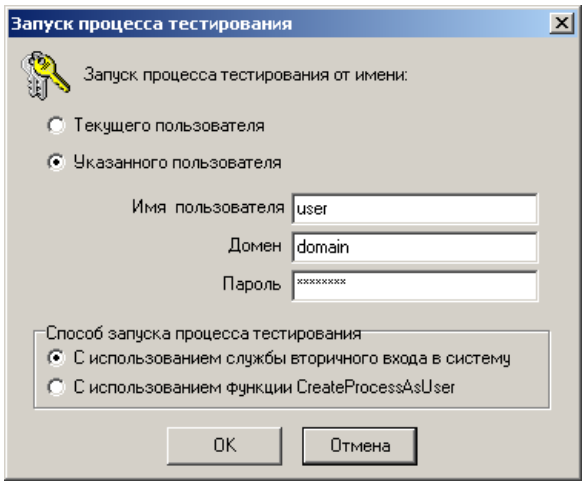

Рис. 11. Окно настройки параметров запуска процесса тестирования

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

«От имени текущего пользователя» - процесс запускается от имени того пользователями, под котором 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 программой 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 требует, чтобы была запущена служба вторичного входа в систему.

«С использованием функции CreateProcessAsUser». Недостатком данного способа является то, что он требует назначения администратору, проводящему тестирование, дополнительных привилегий, не предусмотренных стандартной конфигурацией.

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 (в зависимости от версии ОС Windows) программа «Диспетчер пользователей» или «Локальная политика безопасности». 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 удается 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 XP» 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, выполняется их восстановление.

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

В случае, 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 XP» 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 XP» 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» ().

5.13. Отображение результатов тестирования

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

В режим таблицы результаты отображаются непосредственно в главном окне программы.

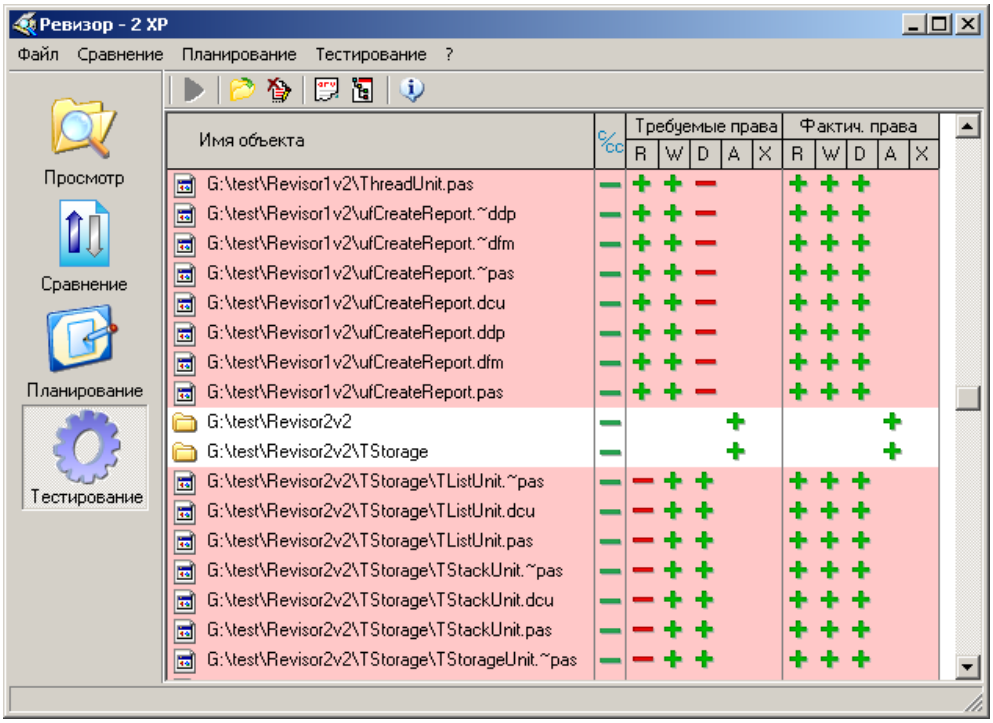

Рис. 12. Окно настройки параметров запуска процесса тестирования

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:

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.

5.14 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 были скопированы, 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.

6. ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место

ЖМД – жесткий магнитный диск

ОЗУ – оперативное запоминающее устройство

ПЭВМ – персональная электронная вычислительная машина

СРД – система разграничения доступа

ПРД – проект разграничения доступа

СЗИ – система защиты информации

ОС – операционная система

7. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подпись	Дата
Изм.	Измененных	Замененных	Новых	Аннулированных					