УТВЕРЖДЕН

643.53132931.501232-02 31 01-ЛУ

Средство создания модели системы разграничения доступа «Ревизор 1 XP»

Описание применения

643.53132931.501232-02 31 01

Листов 16

2017

АННОТАЦИЯ

Настоящий документ является описанием «Ревизор 1 XP» - средства автоматизации процесса создания избирательной модели системы разграничения доступа (СРД) к файловым ресурсам АРМ (логическим дискам, каталогам, файлам) и сетевым ресурсам ЛВС в соответствии с установленными в организации требованиями разрешительной системы.

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

«Ревизор 1 XP» разработан в среде Delphi 7.

«Ревизор 1 XP» 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

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

- Автоматическое сканирование локальных логических дисков, а также доступных сетевых папок. Выбор ресурсов для сканирования осуществляется администратором АРМ.
- Автоматическое считывание установленных прав доступа файловой системы NTFS.
- Построение по результатам сканирования дерева ресурсов, соответствующего структуре ресурсов АРМ и ЛВС.
- Автоматическое получение списка локальных и доменных пользователей.
- Ручная регистрация в ПРД пользователей и установка их уровней допуска.
- Установка прав доступа пользователей к объектам доступа, а также грифов секретности объектов доступа.
- Отображение всей информации, содержащейся в ПРД, в удобной форме.
- Создание отчетов на основе информации о субъектах и объектах доступа.

«Ревизор 1 XP» выполняется администратором АРМ.

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 1 XP» выполняется быстрее.

2.2. Требования к программному обеспечению

«Ревизор 1 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 являются:

- структура ресурсов АРМ и ЛВС. При выполнении сканирования «Ревизор 1 XP» 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.

3.2. Выходные данные

Выходными данными «Ревизор 1 XP» являются

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

4. СОСТАВ И ФУНКЦИИ

4.1. Состав программы

Revizor1XP.exe – главный исполняемый файл.

4.2. Выполняемые функции

4.2.1. Сканирование ресурсов

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

4.2.2. Считывание прав доступа NTFS

В ходе сканирования дисков с файловой системой NTFS «Ревизор 1 XP» 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.

4.2.3.Построение дерева ресурсов

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

4.2.4. Получение списка локальных и доменных пользователей

«Ревизор 1 XP» получает списки учетных записей пользователей, зарегистрированных как непосредственно на АРМ, так и на контролере 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.

4.2.5. Создание и удаление пользователей

«Ревизор 1 XP» 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.

4.3.6. Моделирование разрешительной системы

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

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

«Ревизор 1 XP» формирует отчеты в формате HTML на основе информации, содержащейся в ПРД.

5. ВЫПОЛНЕНИЕ ПРОГРАММЫ

5.1. Установка и настройка программы

Для установки «Ревизор 1 XP» 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.

5.2.Интерфейс программы

Окно программы (рис. 1) имеет следующие элементы:

- Строка меню.
- Панель инструментов.
- Дерево каталогов.
- Список содержимого каталогов.
- Список пользователей.
- Строка состояния.

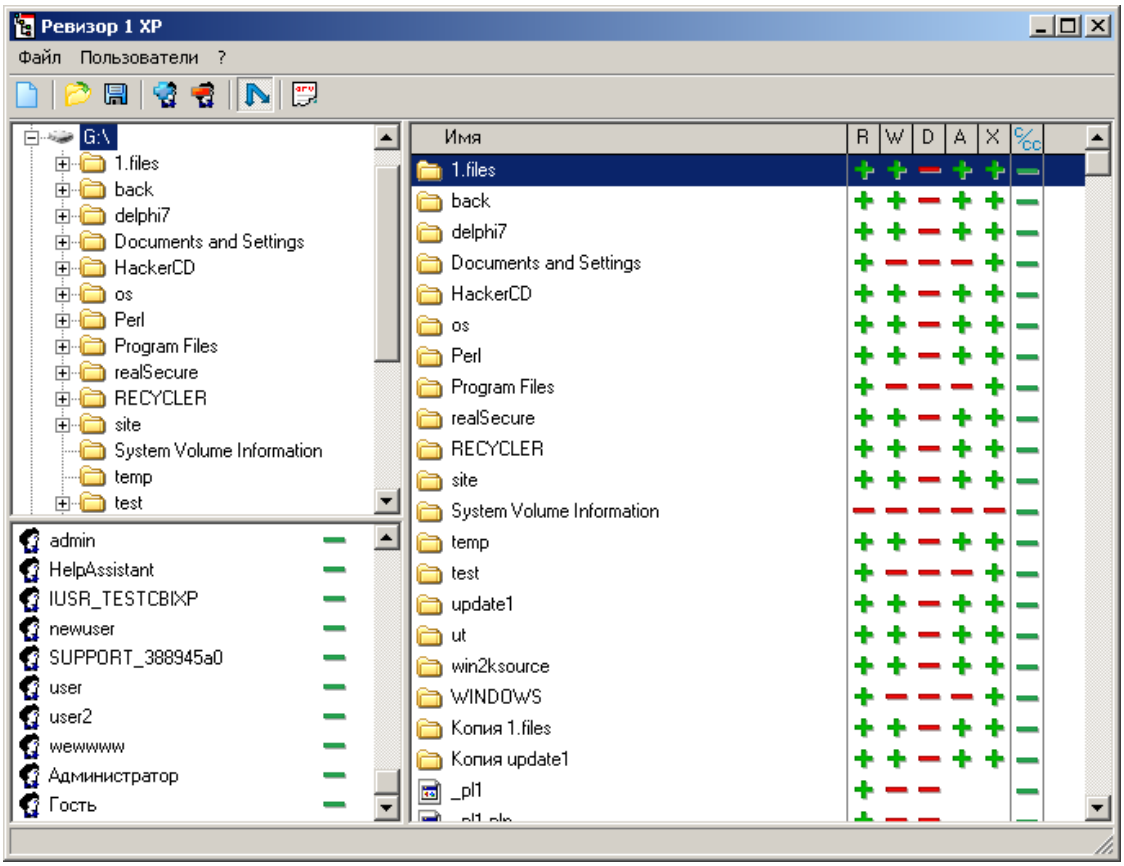

Рис. 1. Главное окно программы

Меню дублирует все функции, доступные с панели инструментов. На панели инструментов расположены следующие кнопки:

 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

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.

5.3. 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 (рис. 2).

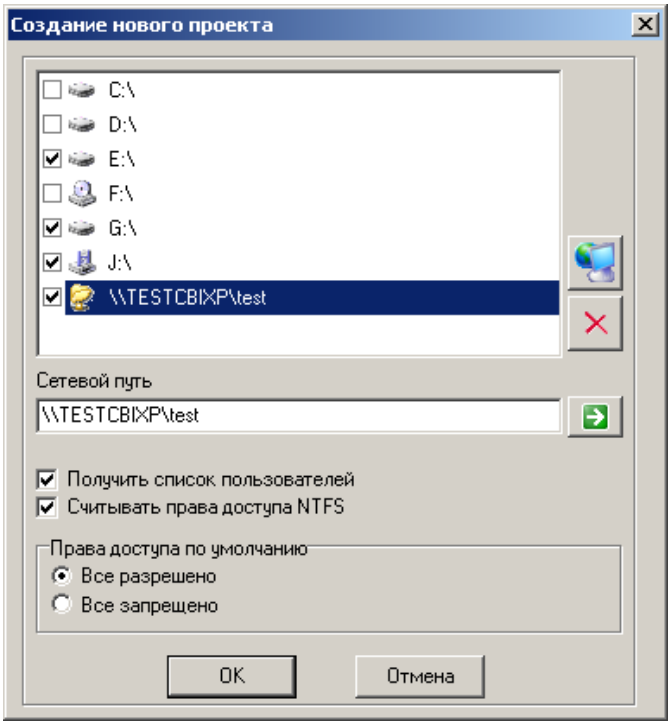

Рис. 2. Окно создания нового ПРД

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.

В появившемся окне (рис. 3) нужно отметить требуемые сетевые ресурсы и нажать кнопку «ОК». Отмеченные ресурсы будут добавлены в список выбора ресурсов для сканирования.

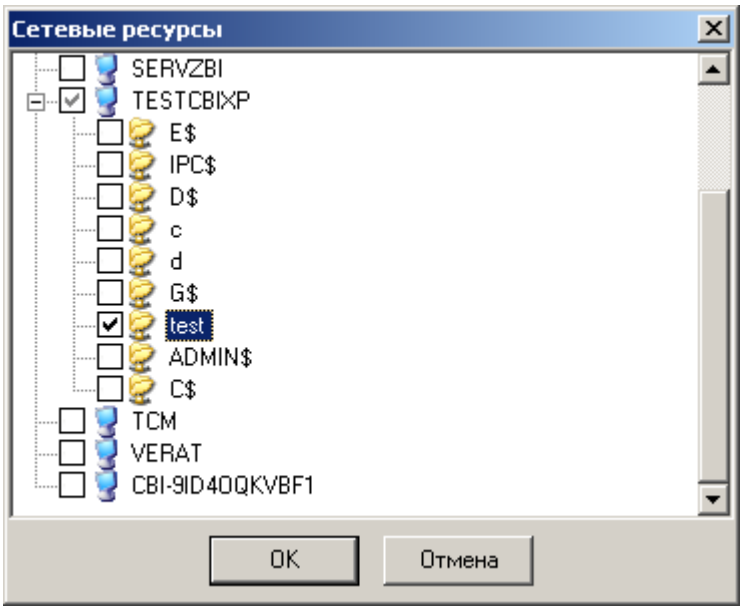

Рис. 3. Окно выбора сетевых ресурсов

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.

«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.

«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 (рис. 4). Сканирование может быть прервано нажатием кнопки «Отмена»

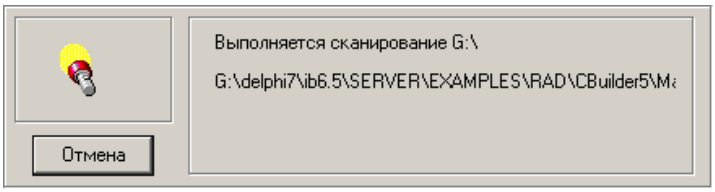

Рис. 4. Окно информации о выполняемой операции

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

5.4. 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 (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 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 «Сов. 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.

5.5. 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 (рис. 5).

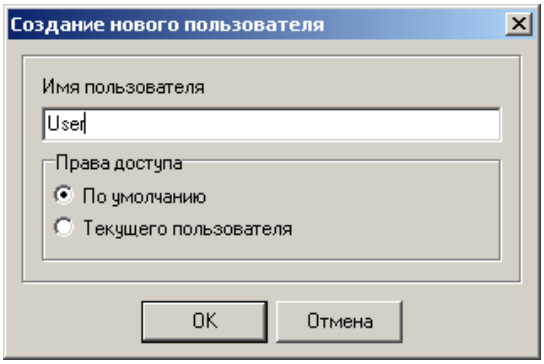

Рис. 5. Создание нового пользователя

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.

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.

5.6. 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».

5.7. Создание отчетов

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

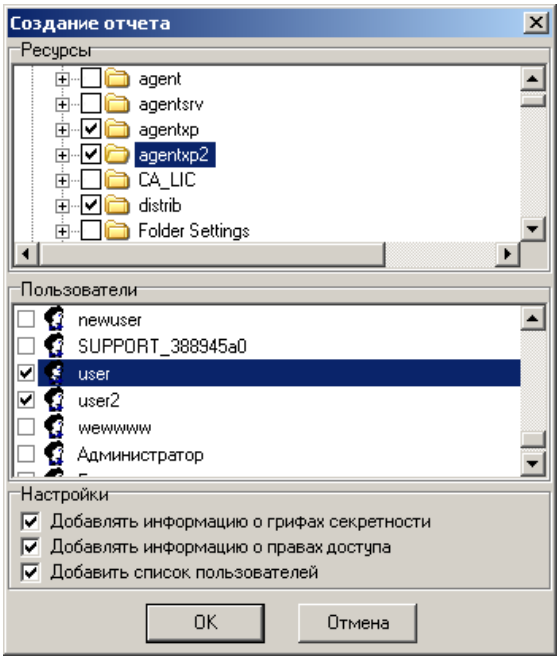

Рис. 6. Окно настройки параметров формирования отчета

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.

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.

6. ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место

ЖМД – жесткий магнитный диск

ЛВС – локальная вычислительная сеть

ОЗУ – оперативное запоминающее устройство

ПЭВМ – персональная электронная вычислительная машина

СРД – система разграничения доступа

ПРД – проект разграничения доступа

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					