МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УДМУРТСКОЙ РЕСПУБЛИКИ

Автономное профессиональное образовательное учреждение Удмуртской Республики «Техникум радиоэлектроники и информационных технологий имени Александра Васильевича Воскресенского»

ПРАКТИЧЕСКИЕ РАБОТЫ

ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

по специальности среднего профессионального образования

11.02.15 Инфокоммуникационные сети и системы связи

Ижевск, 2024

РАССМОТРЕНЫ
методическим объединением
профессионального цикла

Председатель методического
объединения профессионального цикла

Протокол №_____ _____/_____

«____» _____20____г.

Составитель: мастер производственного обучения Масалёв В.Г.

Практическое занятие №1
Тема: «Установка прав доступа с помощью СПО ЗИ»

Цели:

- 1) освоить работу с программой для проектирования моделей разграничения доступа и контроля выполнения разработанных правил;
- 2) получить опыт работы с реализацией механизма разграничения доступа.

Задачи:

- 1) прочитать теоретические сведения;
- 2) прочитать и выполнить инструктивную часть лабораторной работы;
- 3) продемонстрировать преподавателю результаты выполнения лабораторной работы;
- 4) подготовить ответы на вопросы, приведённые в конце лабораторной работы;
- 5) ответить на вопросы преподавателя по лабораторной работе.

Теория

Разграничение доступа — это реализация совокупности правил, разрешающих или запрещающих выполнения тех или иных действий тому или иному пользователю в отношении того или иного ресурса. Это одна из мер обеспечения информационной безопасности, направленная на решение задач обеспечения конфиденциальности и целостности информации.

Ресурсы также называют объектами, а пользователей и программные, аппаратные средства, выступающие от имени пользователя — субъектами.

Модель разграничения доступа — это набор правил, определяющих права доступа к ресурсам. Модели разграничения доступа делятся на 2 вида: модели дискреционного (избирательного) и модели полномочного (мандатного) разграничения доступа.

Модель мандатного разграничения более проста. Её основная идея состоит в следующем: каждый объект имеет свой уровень секретности, каждый субъект имеет свой уровень доступа, субъект может получить доступ к объекту только если уровень доступа субъекта выше либо совпадает с уровнем секретности объекта. Для реализации мандатной модели в системе разграничения доступа достаточно определить уровни секретности ресурсов и уровни доступа пользователей.

Пример: файлу с финансовой стратегией компании может быть присвоен высокий уровень секретности. Если пользователь Бетта, имеющий доступ уровня «Не секретно», попробует просмотреть содержимое этого файла, то система разграничения доступа не позволит ему прочитать файл, так как его уровень доступа недостаточен для выполнения данного действия.

На практике, эта модель реализуется с различными модификациями, призванными повысить обеспечиваемый уровень информационной безопасности. Например, пользователю может быть разрешён доступ только к тем объектам, которые имеют уровень секретности совпадающий с уровнем доступа пользователя. Такая реализация — это один из способов предотвратить несанкционированное понижение уровня секретности информации: ведь пользователь уже не сможет выполнить напрямую перемещение или копирование информации из секретного файла в не секретный, так как просто не будет иметь доступа к не секретным файлам.

Модель дискреционного доступа несколько сложнее и, как правило, требует больше ресурсов на своё поддержание и реализацию. Её основная идея состоит в следующем: для каждого пользователя определён список действий, которые данный пользователь может выполнить с данным объектом. Для реализации дискреционной модели создаётся таблица, включающая все объекты, все субъекты и все разрешения и запреты. Примерный вид такой таблицы иллюстрирует таблица 3.

Таблица 1

Примерный вид таблицы привилегий

	Файлы	**Каталог33**	**Диск115**
Альфа	Разрешено: чтение, запись, выполнение.	Разрешено: чтение, запись, выполнение.	Разрешено: чтение, выполнение.
Бетта	Разрешено: чтение, выполнение.	Разрешено: чтение.	-

Конкретная структура таблицы, состав разрешений и запретов могут различаться и реализовываться по-разному, например, отсутствие записи о правах доступа для пользователя к конкретному объекту может трактоваться системой разграничения доступа и как полное разрешение, и как полный запрет.

Пример: пользователь Бетта не сможет изменить объект «Файлы», но сможет его прочитать (см. таблицу 3); пользователь Альфа может читать и запускать файлы, находящиеся внутри объекта «Диск115», если для них не было установлено отдельных правил, а вот пользователь Бетта к объекту «Диск 115» доступа вообще не имеет. Правда в последнем случае, возможны интересные ситуации. Если пользователю Бетта будет запрещён доступ к «Диск115», но будет разрешён доступ к одному из файлов на нём, то, в зависимости от реализации и настройки системы управления доступом, Бетта сможет работать с файлом, размещённом в закрытом «Диск115».

Важным отличием дискреционной системы разграничения доступа от мандатной является возможность более тонкой и гибкой настройки прав доступа, в том числе, позволяющая пользователям иметь личные файлы и ограничивать к ним доступ других пользователей.

Кроме того, реализации любой модели разграничения доступа, как правило, включает в себя средства группирования и наследования. Например, задавать полностью все права для каждого пользователя системы на каждый объект— очень долгий и трудоёмкий процесс. Для его упрощения и ускорения, пользователей можно разделить на группы, например «Администраторы» и «Пользователи». Затем стоит задать права группы и включить пользователей в эти группы. Теперь разрешения и запреты, заданные для группы или нескольких групп, в которых состоит пользователь, будут наследоваться пользователем, а система управления доступом будет вычислять права пользователя на основе прав групп. К тому же для каждого пользователя всё также можно задать индивидуальные разрешения и запреты.

Аналогичная ситуация происходит с ресурсами. Например, если для группы «Администраторы» разрешён доступ к диску с файлами, то члены этой группы получают полный доступ ко всем файлам на этом диске. Хотя отдельные файлы и каталоги могут иметь свои индивидуальные разрешения, и быть доступными только для отдельных пользователей.

Важно запомнить главный принцип разграничения доступа — принцип минимизации привилегий: «субъект должен иметь только те права и в отношении только тех объектов, которые необходимы ему для выполнения его работы». То есть, пользователь из бухгалтерии не должен иметь прав на изменение настроек системы, а пользователь транспортного отдела не должен иметь доступа к финансовой стратегии компании.

Инструкция

В операционную систему Windows, как и в большинство пользовательских операционных систем, встроена реализация дискреционной модели разграничения доступа на носителях с файловой системой NTFS. Но есть и специальные сторонние

средства защиты информации, позволяющие добавить в ОС мандатное разграничение доступа.

Программный набор «Ревизор XP» предназначен для создание проектов разграничения прав доступа и уровней допуска пользователей в операционных системах семейства Windows в файловой системе NTFS. Данный набор состоит из 2 частей: «Ревизор XP 1» предназначен для создания проекта модели разграничения прав доступа и необходимых уровней допуска к объектам файловой системы для каждого пользователя; а «Ревизор XP 2» предназначен для проверки соответствия реально действующих настроек значениям, указанным в проекте.

Создание проекта с помощью «Ревизор XP 1»

Подключите к своей виртуальной машине новый жёсткий диск. Создайте собственный каталог в корневом разделе диска этого диска и разместите в нём несколько файлов. В дальнейшем на этом каталоге и его содержимом будет удобно экспериментировать с настройками прав доступа.

Запустите «Ревизор XP 1» и создайте новый проект. Окно создания нового проекта представлено на рисунке 1.

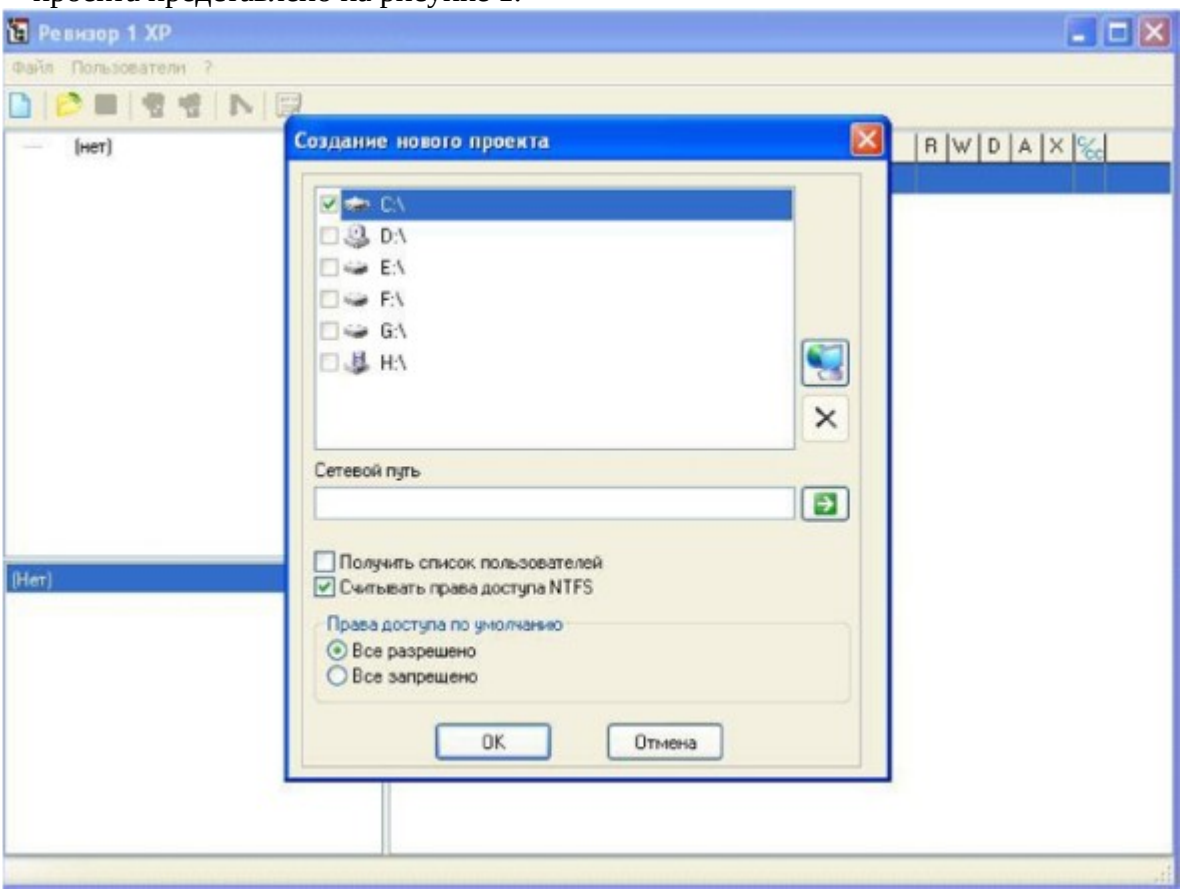


Рис. 1. **Окно «Создание нового проекта» программы «Ревизор XP 1»**

В открывшемся окне нужно указать, какие диски и сетевые папки нужно включить в проект. Включите в проект только созданный вами жёсткий диск. После нажатия кнопки «OK», произойдёт сканирование указанных путей, а затем отображение их структуры и содержимого в главном окне программы. Главное окно программы примет вид, представленный на рисунке 2.

Теперь можно редактировать гриф секретности и права доступа каждого объекта файловой системы для каждого пользователя. Сначала отредактируем список пользователей: программа позволяет создавать и удалять из проекта пользователей. Соответствующие кнопки находятся на панели инструментов. Также можно воспользоваться меню «Пользователи».

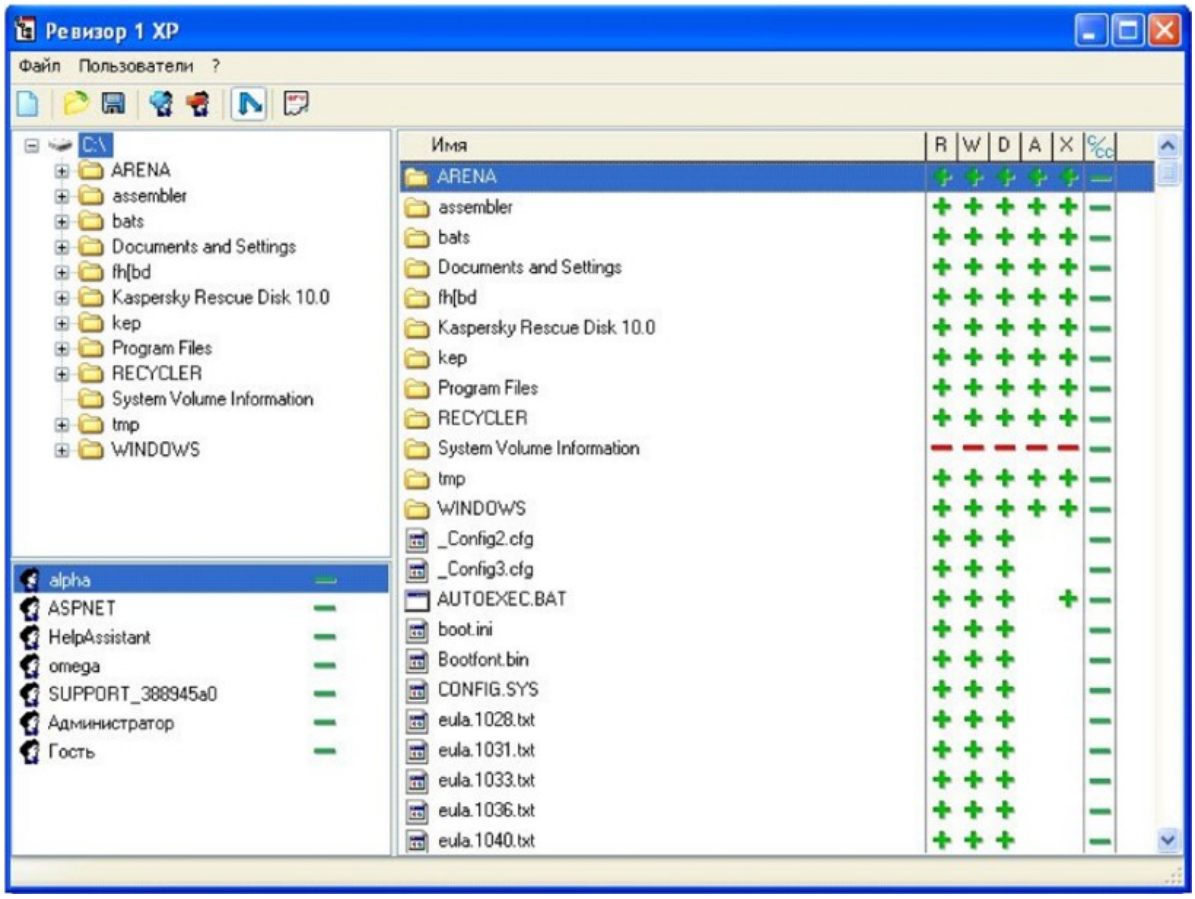


Рис. 2. **Главное окно программы «Ревизор XP 1» с загруженным деревом файловой системы**

Обратите внимание, что все действия, производимые в проекте, в проекте и остаются! Т.е. они не влияют на систему: созданные в проекте пользователи не появляются автоматически в системе, а заданные права доступа и грифы секретности — не присваиваются файлам в файловой системе. Все настройки придётся выполнять вручную в соответствии с созданным проектом.

Создайте 2 пользователей и назовите их по своему желанию. Не забудьте создать таких же пользователей в ОС и обязательно задайте им непустые пароли.

Когда список пользователей приведён к необходимому виду, можно задать уровень секретности для каждого из пользователей. Уровень секретности, доступный пользователю можно изменить кликом по знаку текущего уровня рядом с именем пользователя. По умолчанию у вех пользователей задан уровень секретности «Не секретно» (обозначен зелёным минусом в списке пользователей).

Уровни допуска пользователей и, соответственно, уровни (грифы) секретности объектов файловой системы могут иметь следующие значения:

- 1. «-» — «Не секретно».
- 2. «Д» — «Для служебного пользования».
- 3. «С» — «Секретно».
- 4. «СС» — «Совершенно секретно».

Задайте пользователям разные уровни допуска. Пример перечня пользователей с разными уровнями допуска и разными привилегиями в отношении объектов файловой системы представлен на рисунке 3.

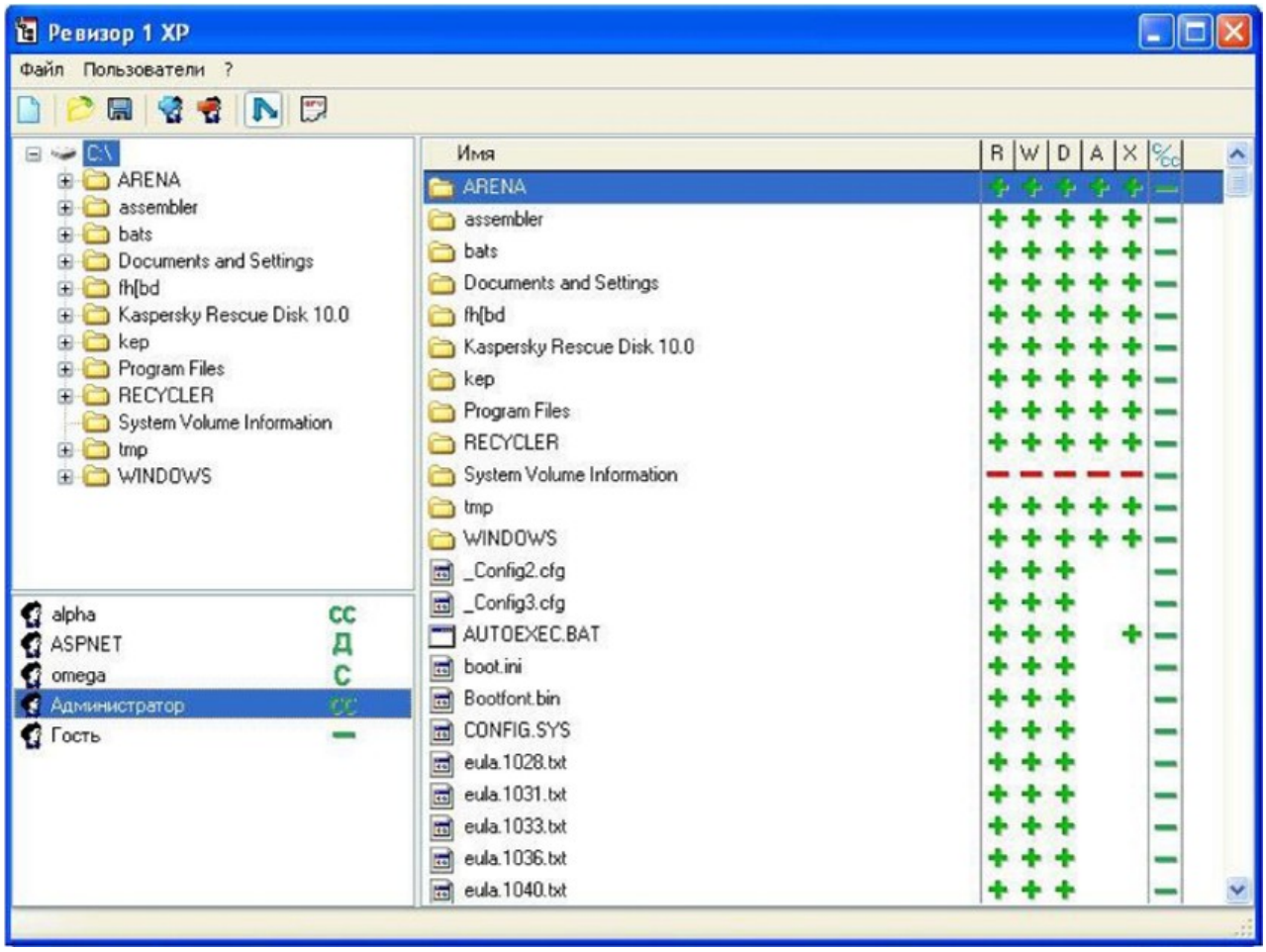


Рис. 3. **Главное окно программы «Ревизор XP 1»: пользователи с разными правами**

Теперь можно приступать к определению правил доступа к объектам файловой системы. По умолчанию, включён режим наследования: соответствующая кнопка на панели инструментов нажата. Этот режим означает, что правила доступа родительского объекта наследуются всеми его потомками (т.е. «все файлы и подкаталоги»). Задайте права доступа и уровни секретности созданному вами каталогу и его содержимому для каждого из пользователей. Пусть у каждого пользователя будет свой набор привилегий.

Сохраните проект, воспользовавшись кнопкой на панели инструментов или меню «Файл».

С помощью специальной кнопки на панели инструментов начните формирование отчёта. Вы увидите окно «Создание отчёта». В нём нужно указать, какую информацию включить в отчёт: выбрать объекты файловой системы, пользователей и ряд дополнительных параметров, влияющих на содержимое документа. Обратите внимание, что выбор родительского объекта в данном случае не означает включение в отчёт информации о его потомках (см. рис. 4). То есть, если вы включили в отчёт каталог, то в отчёте будет содержаться информация только о самом каталоге, но не о файлах и подкаталогах, которые в нём содержатся. Для включения информации о правах доступа к объекту и всем вложенным в него объектам нужно воспользоваться командой из контекстного меню «Выделить содержимое».

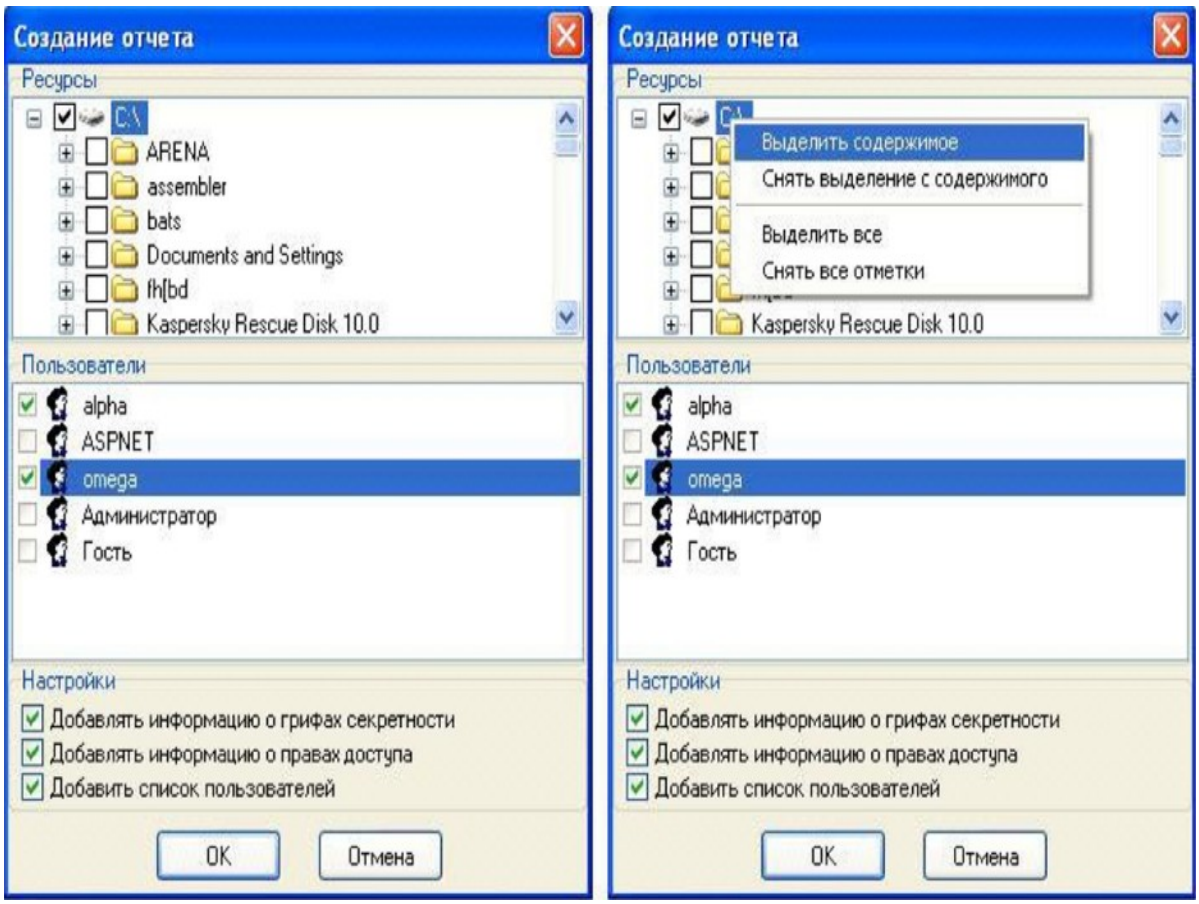


Рис. 4. **Окно выбора объектов для формирования отчёта**

Проверка настроек системы разграничения доступа

«Ревизор XP 2» предназначен для проверки выполнения настроек разграничения доступа, оформленных в виде проекта программы «Ревизор XP 1». Для выполнения проверки запустите «Ревизор XP 2» и загрузите проект разграничения прав доступа, созданный в «Ревизоре XP 1». Теперь в главном окне программы «Ревизор XP2» вы можете просмотреть проект модели разграничения прав, но внесение изменений в него ограничено.

Нажмите кнопку «Сравнение» на панели инструментов слева — вы перейдёте в режим сравнения структуры и содержимого объектов реальной файловой системы с информацией о них же, включённой в проект.

Нажмите на кнопку «Сравнить» на появившейся вверху панели инструментов — начнётся сравнение.

Скорее всего, особенно, если вы включили в проект системные каталоги, будут найдены новые объекты, которые появились в файловой системе после формирования проекта (помечены «+»-ом), и отсутствующие объекты, которые были удалены после формирования проекта (помечены «-»-ом).

Если перечень отличий остался пуст, то информация об объектах файловой системы, включённая в проект, полностью соответствует нынешнему состоянию этих объектов файловой системы.

Если изменения найдены, сформируйте отчёт по найденным изменениям (соответствующая кнопка на верхней панели инструментов) и сохраните его. Отчёт будет выглядеть примерно так (см. рисунок 5)

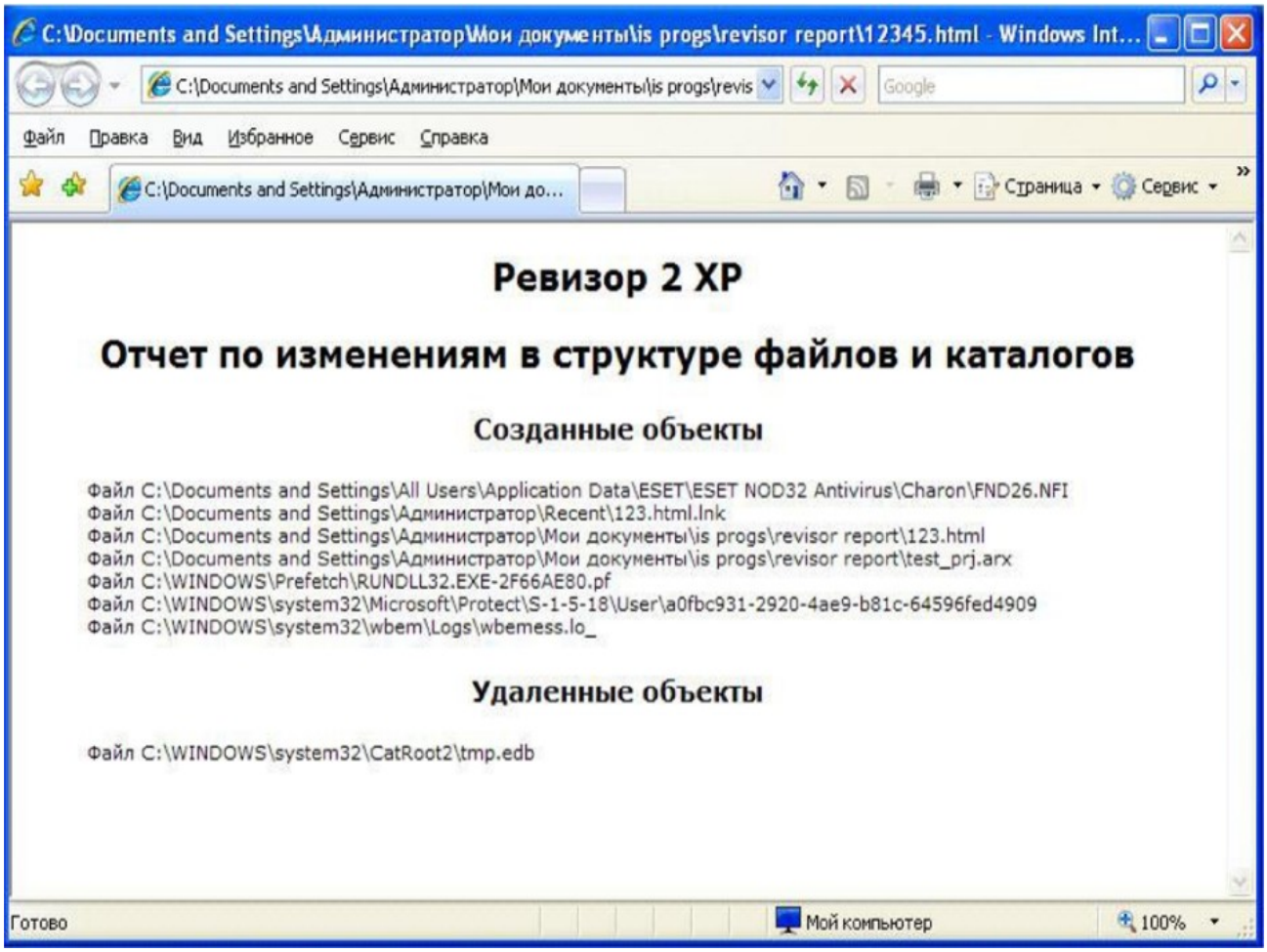


Рис. 5. **Отчёт по выявленным различиям между проектом и файловой системой**

Если изменения были найдены, нужно скорректировать проект в соответствии с ними. Чтобы сделать это автоматически, нажмите кнопку «Внести изменения» на верхней панели инструментов.

Сохраните изменённый проект, воспользовавшись меню «Файл» или кнопкой «Сохранить проект» в режиме «Просмотр».

Теперь можно переходить к тестированию — проверке правильности настроек правил доступа на данный момент. Для этого нужно сформировать план тестирования, то есть выбрать объекты файловой системы, к которым программа попытается получить доступ от лица выбранного пользователя.

Вернитесь в режим просмотра проекта и выберите пользователя, права которого хотите тестировать. Затем нажмите кнопку «Планирование» на панели слева — вы перейдёте в режим подготовки тестирования. Нажмите кнопку «Создать план тестирования» — появится окно параметров плана, представленное на рисунке 6.

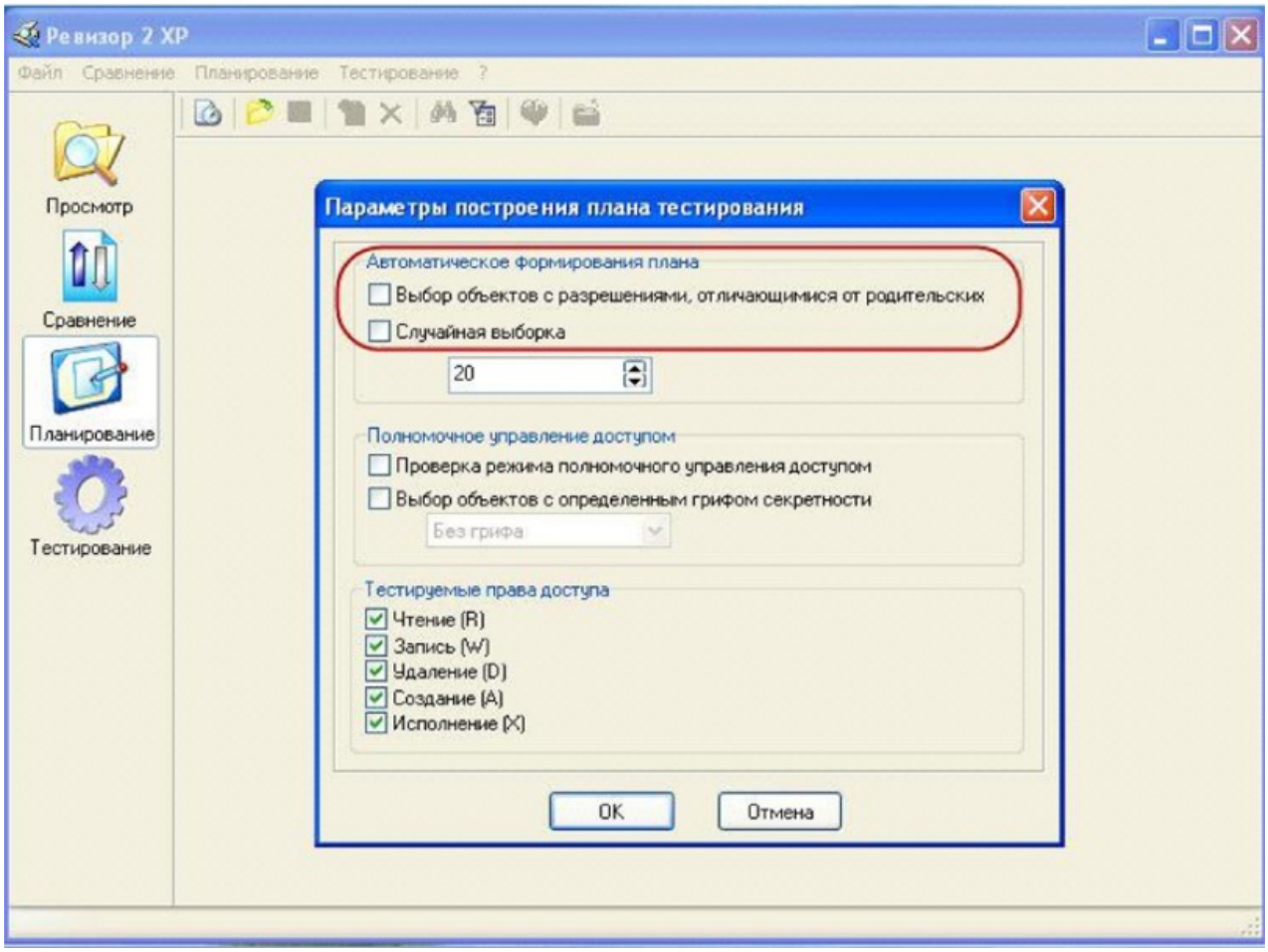


Рис. 6. **Окно параметров построения плана тестирования**

Первый блок, «Автоматическое формирование плана», позволяет включить в план объекты из проекта, выбранные программой в соответствии с заданными условиями. Если оба флажка в этом блоке сняты, то будет сформирован пустой план, и добавлять объекты в него придётся вручную.

Следующий блок, «Полномочное управление доступом», позволяет указать, будут ли при тестировании проверяться настройки уровней секретности. И нужно ли автоматически добавлять в план объекты с выбранным грифом (если автоматическое формирование плана включено).

Последний блок, «Тестируемые права доступа», предлагает указать, какие права будут тестироваться «по умолчанию» для выбранных объектов файловой системы.

Чтобы включить в список проверки все необходимые вам объекты файловой системы, **сбросьте все флажки в группе «Автоматика»** (см. рис. 6) и добавьте в план все объекты вручную. **Обратите внимание, что добавление объекта НЕ добавляет его содержимое!** После чего окно программы «Ревизор XP 2» примет вид, представленный на рисунке 7.

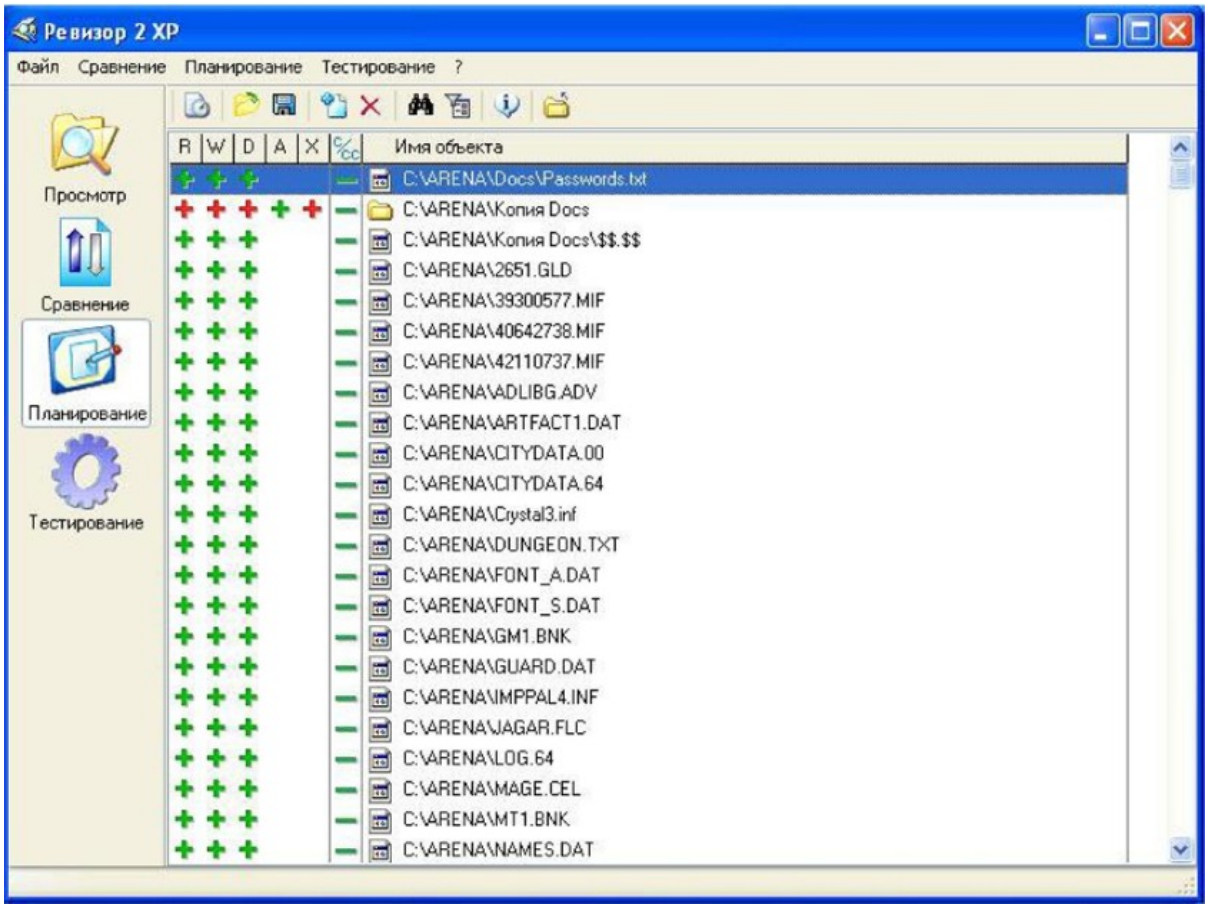


Рис. 7. **Окно плана проекта**

На рисунке 17 слева от имени объекта указано, какие права будут тестироваться по отношению к этому объекту. В таблице 2 представлены значения прав.

Таблица 2

Обозначения прав доступа в плане тестирования

Условный знак	**Смысл**
Зелёный плюс	Пользователю разрешён данный вид доступа к объекгу, и это право будет проверено при тестировании
Красный плюс	Пользователю разрешён данный вид доступа к объекту, но это право при тестировании проверяться не будет
Зелёный минус	Пользователю запрещён данный вид доступа к объекту, и это право будет проверено при тестировании
Красный минус	Пользователю запрещён данный вид доступа к объекту, но это право при тестировании проверяться не будет

Для удаления объектов из плана можно воспользоваться кнопкой «Удалить элемент плана тестирования» панели инструментов или соответствующим пунктом меню «Планирование».

Элементы плана можно сортировать, при помощи контекстного меню. Также, есть возможность поиска элементов плана с использованием масок имён файлов.

Просмотрите информацию о плане тестирования (соответствующая кнопка на верхней панели). Проверьте, совпадает ли имя пользователя, для которого составлен план проверки, с пользователем выбранным вами в режиме «Просмотр». Сохраните ваш план тестирования.

Перейдите в режим выполнения тестирования нажатием кнопки «Тестирование» на панели переключения режимов. Далее будет запущен процесс проверки по открытому плану тестирования.

Обратите внимание: пользователь, права доступа которого будут проверяться, должен существовать в системе на момент начала тестирования!

Нажмите кнопку «Приступить к тестированию» — появится окно настроек параметров тестирования, представленное на рисунке 8. Укажите файл, для ведения протокола тестирования (файл должен быть доступен для всех пользователей системы, поэтому лучше всего будет разместить его в корне системного диска) и каталог для сохранения резервных копий файлов (этот каталог не должен в ходить в список объектов, подлежащих тестированию). Также, рекомендуется поставить флажок «Сохранять права доступа NTFS»: в этом случае, при выполнении резервного копирования и восстановления из резервной копии после завершения тестирования, будет восстановлен не только сам файл, но и права доступа к нему.

Флажок «Выполнять автоматический вход в систему» означает, что при тестировании не нужно будет «вручную» заходить в систему с учётными данными пользователя, права которого проверяются. Но этот режим работы невозможен, если на машине установлены дополнительные средства ограничения входа в систему, например проверка аппаратных ключей или ввод дополнительных паролей.

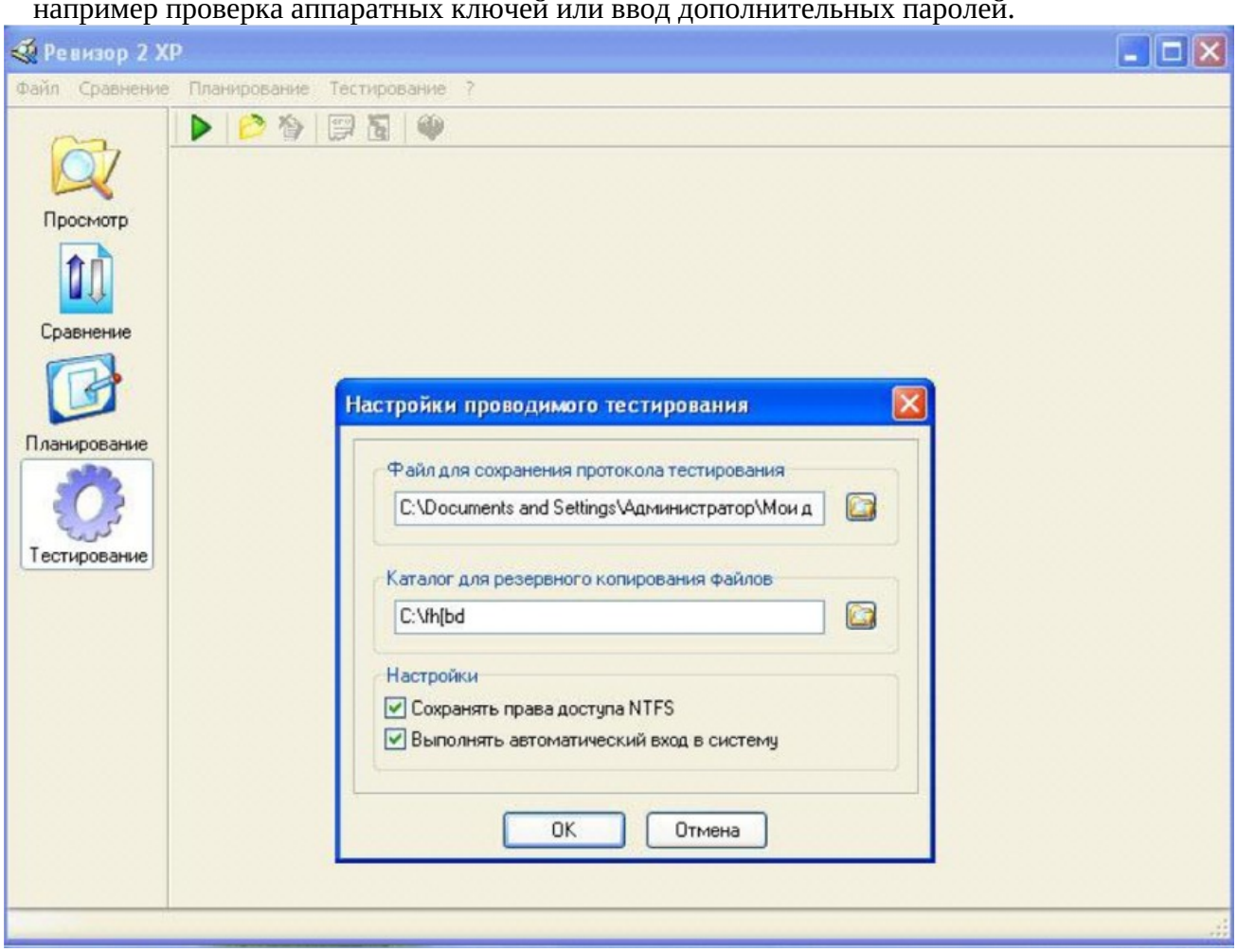


Рис. 8. **Окно настроек тестирования**

После сообщения о том, что для выполнения резервного копирования вы должны находиться под учётной записью администратора, выполнится резервное

копирование. Затем появится окно ввода учётных данных тестируемого пользователя, представленное на рисунке 9.

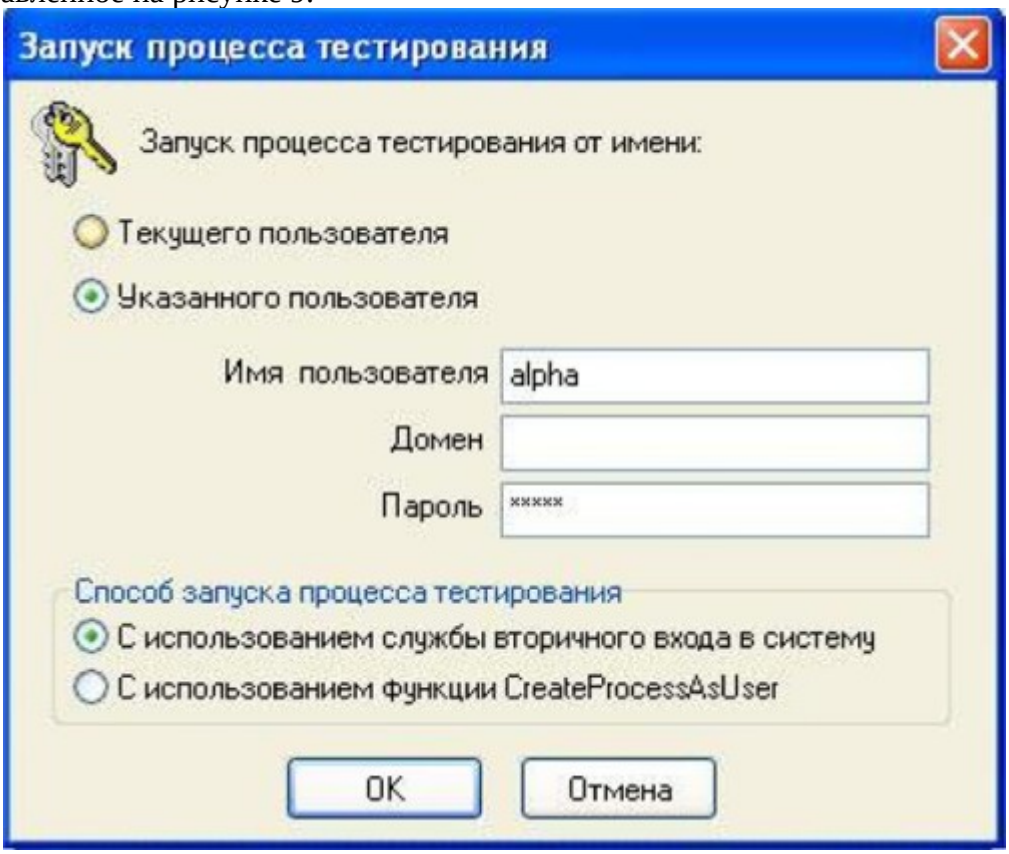


Рис. 9. **Окно ввода учётных данных тестируемого пользователя**

Введите учётные данные вашего пользователя (пользователь должен реально существовать в системе, если это нс так, самое время создать его). Реко-мендуется переключатели оставить по умолчанию. Нажмите «Ок» и начните тестирование. Ход выполнения процесса тестирования отображается в окне, представленном на рисунке 10.

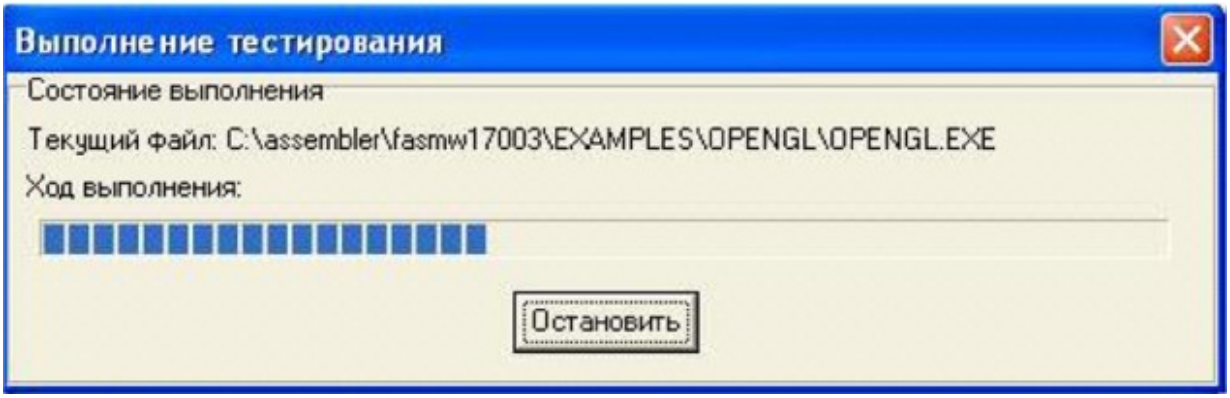


Рис. 10. **Ход выполнения тестирования**

После завершения тестирования и выполните восстановление файлов из резервных копий, на экран будет выведен результат тестирования. Окно с результатом тестирования имеет вид, представленный на рисунке 11. Розовым выделены строки, в которых обнаружены расхождения между правами доступа по проекту и по факту.

Также, результаты тестирования могут быть представлены в виде дерева. Посмотрите результаты тестирования, представленные в виде дерева, воспользовавшись соответствующей кнопкой в верхней панели инструментов (см. рис. 12).

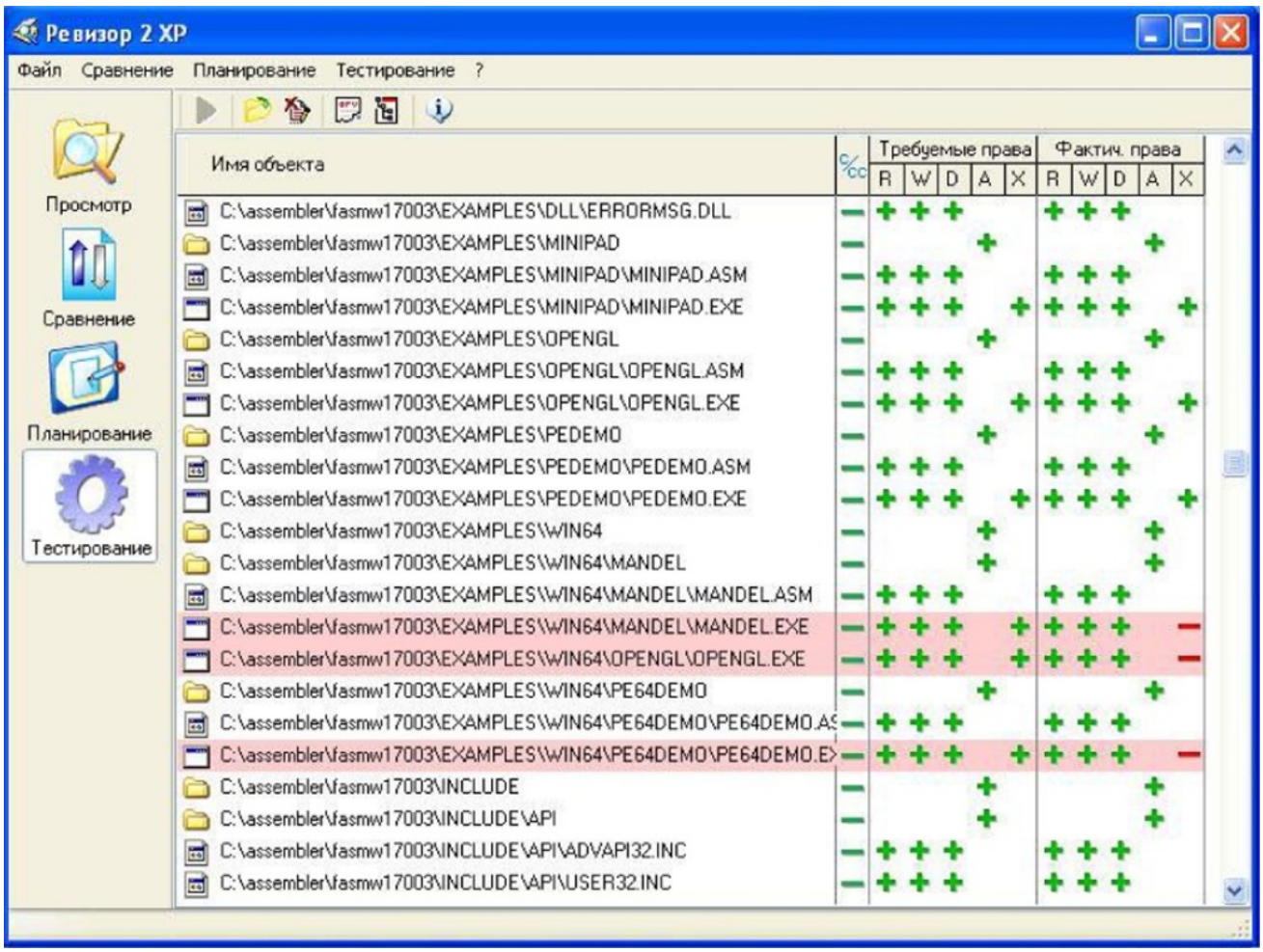


Рис. 11. **Окно результатов тестирования**

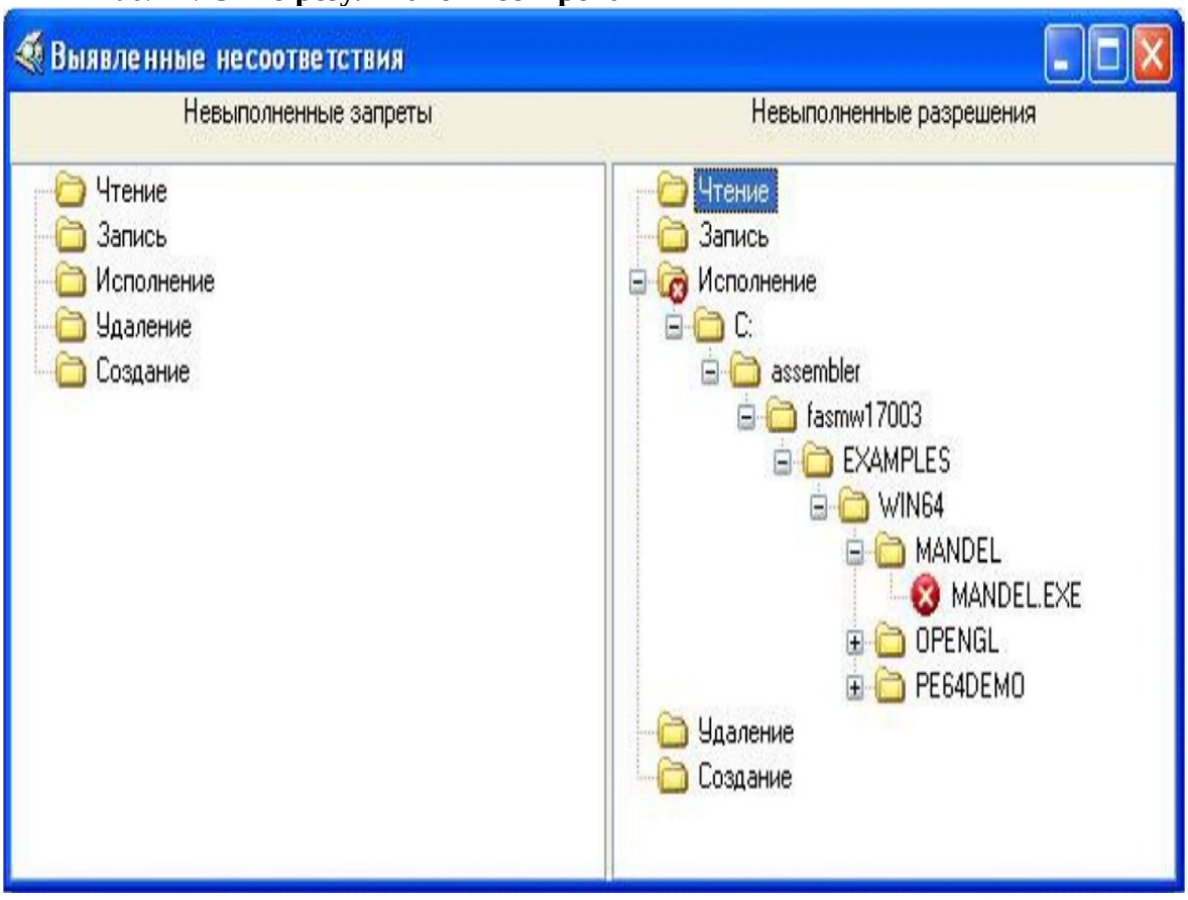


Рис. **12. Просмотр результатов тестирования в виде дерева объектов**

Сформируйте и сохраните отчёт (см. рис. 13). Исправьте несовпадающие права доступа в соответствии с проектом и повторите тестирование. Найдены ли те же различия?

Настройка прав доступа пользователей или групп пользователей к конкретным объектам может отличаться в разных ОС. Часто для решения таких задач применяются отдельные программные продукты, делающие настройку полномочий более удобной за счёт лучшего интерфейса, а иногда и дополнительных функций, отсутствующих в самой ОС.

Ревизор 2 XP

Отчет по результатам тестирования

Пользователь: alpha

Время проведения тестирования: 14.01.2014 6:10:19

Имя файла	**Требуемые права**				**Фактические права**				
	н	**W**	и	**A X**	**R**	**W**	**O**	A	**X**
C:ARENADocsPasswords.txt	+	**4-**	**4-**		+	+	+		
C:ARENAKonnn Docs				**4-**				+	
C:ARENAKo пи я Docs$$.$$			**4-**	**Г**	**4-**	+	+		
C:ARENA2651.GLD					+	+	+		
C:ARENA393Q0577.MIF	+		**4-**		+	**4-**	+		
C:ARENA40642738.MIF	+	**4-**	**4-**		+	+	+		
C:ARENA42110737.MIF	**4-**	**4-**	**4-**		+	+	+		
C:ARENAADLIBG.ADV	+	+	**4-**		+	+	+		
C: ARENAARTFACT1 .DAT	**4-**	+	**4-**		**4-**	+	+		
C:ARENACITYDATA.00	**4-**	**4-**	**4-**		-	**4-**	**4-**		
C:ARENACITYDATA.64	**4-**	**4-**	**4-**		**4-**	**4-**	**4-**		
C:ARENACrystal3.inf		+	+		-	+			

Рис. 13. **Фрагмент отчёта по результатам тестирования**

В среде Windows XP для более удобной настройки прав доступа к конкретным объектам необходимо включить соответствующее отображение вкладок в окне свойств объекта файловой системы. Для этого нужно из меню «Сервис» открыть окно «Свойства папки» в окне проводника Windows, как это показано на рисунке 14.

На вкладке «Вид» нужно снять флажок «Использовать простой общий доступ к файлам (рекомендуется)». Тогда вкладки «Доступ» и «Безопасность» в свойствах объектов файловой системы примут нужный нам вид (см. рис. 15).

Теперь для пользователей и групп пользователей можно задать права на каждый конкретный файл и каталог, используя пункт «Свойства» из контекстного меню объекта файловой системы.

Добейтесь полного соответствия реально действующих правил доступа правилам, заданным в проекте, и повторите проверку действующих прав доступа.

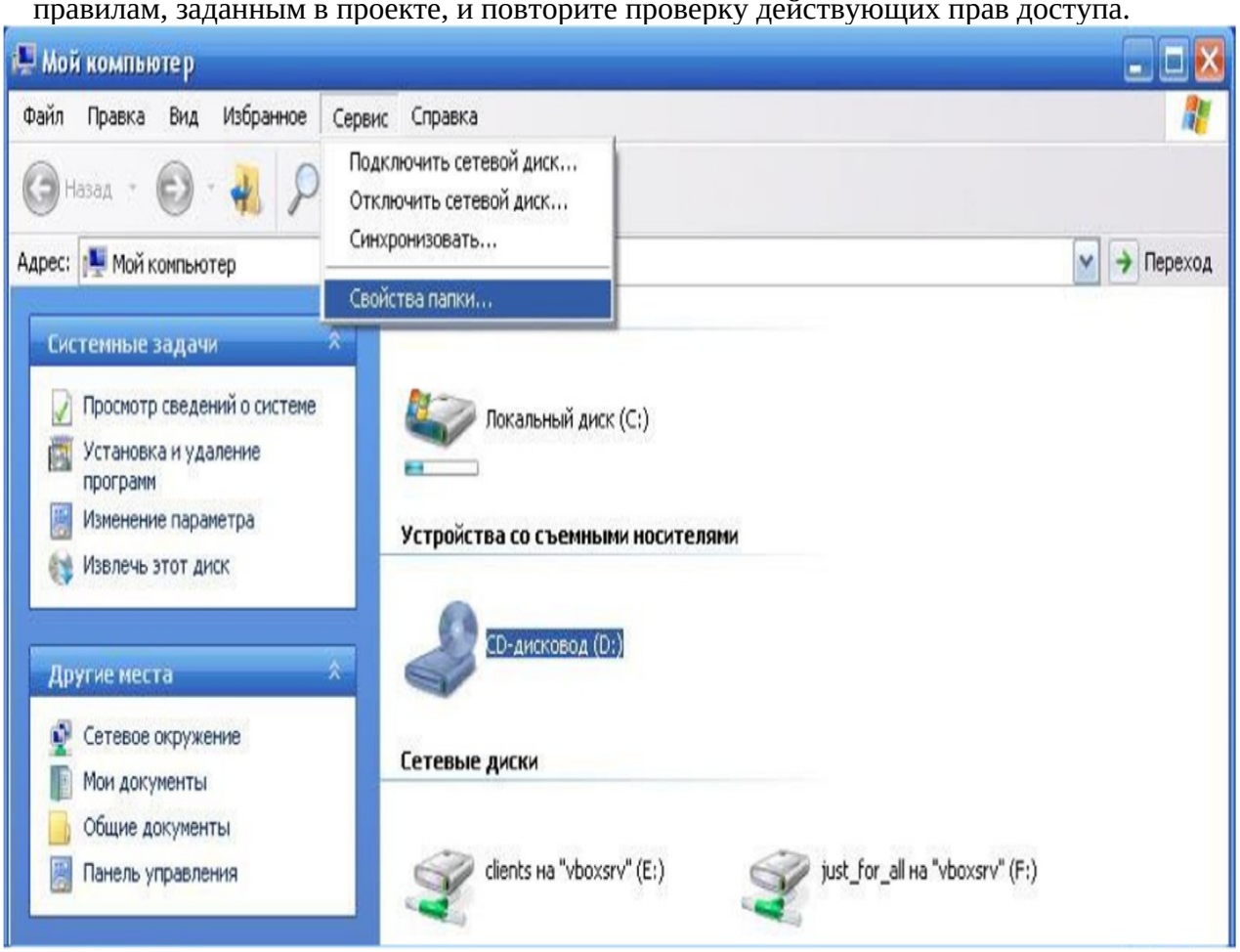


Рис. 14. **Пункт «Свойства папки...» в меню «Сервис»**

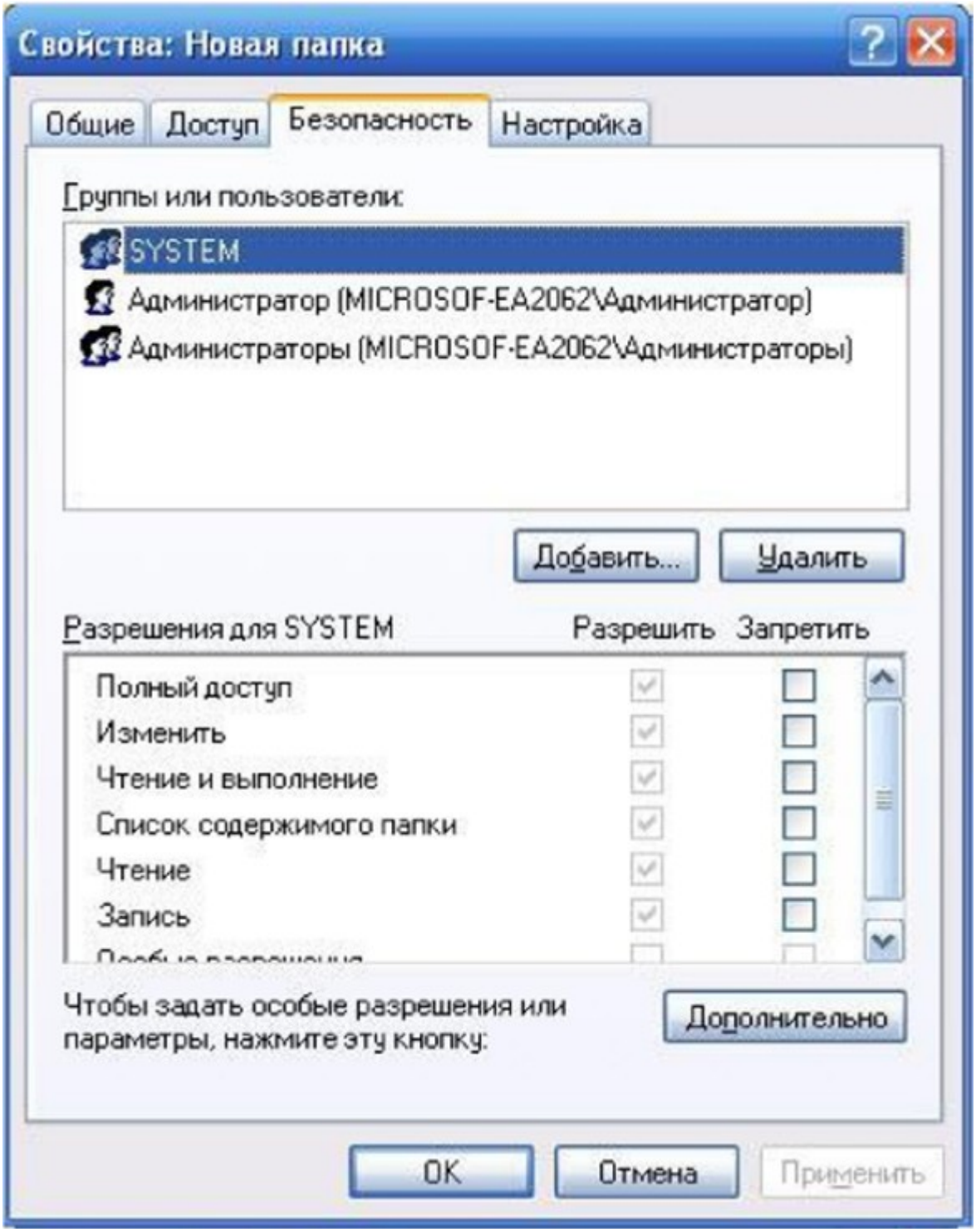


Рис. 15. **Свойства файла**

Вопросы

- 1. Что такое разграничение доступа?
- 2. Зачем нужна система разграничения доступа?
- 3. Какие типы моделей разграничения доступа выделяют?
- 4. Каков главный принцип разграничения доступа?
- 5. Какой тип модели разграничения доступа реализован в ОС Windows?
- 6. Какие средства настройки системы разграничения доступа включены в ОС Windows?
- 7. Каковы сильные и слабые стороны систем разграничения доступа?
- 8. Для чего предназначен пакет программ «Ревизор XP»?
- 9. Каково назначение и основные функции программы «Ревизор XP1»?

- 10. Каково назначение и основные функции программы «Ревизор XP2»?
- 11. Кратко опишите алгоритм работы с пакетом программ «Ревизор XP».

Практическое занятие №2
Тема «Законодательство в сфере защиты информации»

Цель занятия – закрепление теоретических знаний в области правового обеспечения информационной безопасности.

1. Учебные вопросы

1. Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации.
2. Федеральные законы в области информации и информационной безопасности.
3. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.
4. Правовые режимы защиты информации.
5. Правовые вопросы защиты информации с использованием технических средств.

2. Методические указания студентам по подготовке и проведению практического занятия

2.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы «Российское законодательство в области информационной безопасности», используя литературу, а также конспект лекций. При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

2.2. Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию. Затем студенты последовательно усваивают учебные вопросы, касающиеся положений Конституции РФ, Доктрины информационной безопасности РФ и федеральных законов в области информационной безопасности, правовых режимов защиты информации, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

3. Контрольные вопросы

1. Охарактеризуйте информацию и ее основные показатели.
2. Какие существуют подходы к определению понятия «информация».
3. В чем заключается двуединство документированной информации с правовой точки зрения.
4. Дайте характеристику следующих видов информации: документированная, конфиденциальная, массовая.
5. К какому виду информации относится записанный на бумаге текст программы для ЭВМ?
6. Назовите основные виды конфиденциальной информации.
7. Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?
8. Какие свойства информации являются наиболее важными с точки зрения обеспечения ее безопасности?

9. Охарактеризуйте место правовых мер в системе комплексной защиты информации.

10.Назовите основные цели государства в области обеспечения информационной безопасности.

11.Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.

12.Какой закон определяет понятие «официальный документ»?

13.Какой закон определяет понятие «электронный документ»?

14.В тексте какого закона приведена классификация средств защиты информации?

15.Какие государственные органы занимаются вопросами обеспечения безопасности информации и какие задачи они решают?

16.Назовите основные положения Доктрины информационной безопасности РФ.

17.Назовите составляющие правового института государственной тайны.

18.В каких случаях нельзя относить информацию к государственной тайне?

19.Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?

20.Назовите группу видов ущерба, возникающего при утечке сведений, составляющих государственную тайну.

21.Дайте определение системы защиты государственной тайны и укажите ее составляющие.

22.Что в соответствии с законодательством РФ представляет собой засекречивание информации.

23.Перечислите основные принципы засекречивания информации.

24.Что понимается под профессиональной тайной?

25.Какие виды профессиональных тайн вам известны?

26.В чем заключается разница между понятием «конфиденциальная информация» и «тайна»?

27.В чем состоит сложность служебной тайны с точки зрения определения ее правового режима?

28. Что представляет собой электронная цифровая подпись?

29.Каковы основные особенности правового режима электронного документа?

30.Назовите основные ограничения на использование электронных документов?

Практическое занятие №3
Тема «Разработка политики безопасности объекта»

Цель: разработать политику безопасности объекта.

Задание: Гейм клуб «Pro.comP» хочет организовать областной турнир по Dota2. Однако состояние информационной безопасности в компании настораживает. Необходимо разработать политику безопасности гейм клуба, ориентируясь в разработке на модель системы с полным перекрытием. Сформировать отчет по проделанной работе

Список оборудования: система для демонстрации отчета

Программное обеспечение: программа для демонстрации отчета

Теоретические сведения:

Политика безопасности организации – это важный документ, который разрабатывают в любой информационной системе. В ней указывают уязвимости систем, возможные угрозы, нарушителей и рекомендации по противостоянию им. Учитываются процедуры управления, сбора, обработки, защиты и распределения

информации. Регламентируется процедура разработки политики безопасности специальными нормативно-правовыми документами, такими как, например, стандарт ГОСТ Р ИСО/МЭК 15408-1-2013.

Порядок выполнения работы:

• Описать модель объекта (составляющие его компоненты, каналы обмена данными между ними

и внешними объектами, свойства информации, которые нуждаются в защите в каждой

рассматриваемой ситуации);

• Описать модели угроз;

• Описать модели потенциальных нарушителей (как внешних, так и внутренних);

• Провести анализ рисков и отсеять наименее вероятные и менее фатальные по наносимому

ущербу угрозы;

• Сформировать рекомендации по внедрению средств защиты информации в клубе, рекомендации

по сотрудникам.

Содержанием отчета:

1. Цель работы.
2. Описание модели объекта.
3. Описание модели угроз.
4. Описание модели потенциальных нарушителей.
5. Анализ рисков.
6. Рекомендации по внедрению средств защиты информации.
7. Выводы.

Практическое занятие №4
Тема «Установка и снятие СЗИ с помощью программы СЗИ НСД»

Цель работы: Ознакомление с установкой и снятием СЗИ НСД **Страж NT 3.0** и их использования, закрепить знания по теме «Обеспечение безопасности информационных технологий**».**

Способствовать формированию соответствующих общих и профессиональных компетенций: ОК 01, ОК 02, ОК 03, ОК 04, ПК 3.1, ПК 3.2, ПК 3.3.

Средства для выполнения работы:

– аппаратные: ПК;

I. Теоретическая часть Назначение программы

Система защиты информации от несанкционированного доступа «Страж NT» (версия 3.0) представляет собой комплекс средств защиты информации в автоматизированных системах на базе персональных компьютеров.

СЗИ «Страж NT» предназначена для комплексной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах на базе персональных ЭВМ. СЗИ «Страж NT» может использоваться при разработке систем защиты информации для автоматизированных систем до классов защищенности 3А, 2А и 1Б включительно в соответствии с требованиями Руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», а также для создания информационных систем обработки персональных данных до 1 класса включительно.

Условия применения

СЗИ «Страж NT» может устанавливаться на автономных рабочих станциях, рабочих станциях в составе рабочей группы или домена, серверах, в том числе в составе кластера. СЗИ
«Страж NT» может функционировать на одно- и многопроцессорных компьютерных системах под управлением операционных систем Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 и Windows Server 2008 R2. Компьютер, на котором устанавливается СЗИ «Страж NT», должен удовлетворять требованиям, необходимым для загрузки операционной системы.

В силу особенностей реализации защитных механизмов СЗИ «Страж NT» существуют дополнительные требования к аппаратному обеспечению компьютера:

– загрузочный жесткий диск должен иметь не менее 63 секторов перед началом первого раздела (32 256 байтов);

– при использовании USB-клавиатуры и USB-идентификаторов пользователей в некоторых случаях требуется наличие не менее 2 контроллеров USB;

– в случае применения в качестве идентификаторов пользователей USB флэш-накопителей в BIOS компьютера должна быть включена поддержка таких устройств.

Тип файловой системы на жестких дисках компьютера не имеет значения, это может быть FAT 16, FAT 32 или NTFS. Жесткий диск компьютера, на котором установлена операционная система, должен иметь свободное пространство объемом не менее 30 Мб.

Перед началом установки СЗИ «Страж NT» рекомендуется установить все системное и прикладное программное обеспечение, предусмотренное на данном рабочем месте. Установка дополнительного программного обеспечения в процессе функционирования СЗИ «Страж NT» является нежелательной.

Для установки, настройки и управления функционированием СЗИ «Страж NT» должен быть назначен администратор системы защиты. Пользователь, выполняющий функции администратора системы защиты, должен быть создан перед началом установки системы защиты стандартными средствами операционной системы. При установке системы защиты на локальный компьютер администратор системы защиты должен быть включен в группу локальных администраторов. В случае установки системы защиты на компьютер, входящий в домен, администратор системы защиты должен входить в группу локальных администраторов компьютера, а также в группу администраторов домена. Администратор системы защиты должен иметь одинаковое имя и пароль для входа на всех компьютерах, на которых планируется установка СЗИ «Страж NT».

Администратор системы защиты должен быть подготовленным пользователем, знающим принципы функционирования и имеющим навыки работы с операционной системой и СЗИ
«Страж NT».

Механизмы системы защиты

В СЗИ «Страж NT» реализована смешанная разрешительно-запретительная модель защиты информации с жестким администрированием. Система защиты представляет собой совокупность следующих основных подсистем:

– идентификации и аутентификации;

– разграничения доступа;

– контроля потоков информации;

– управление запуском программ;

– управления защитой;

– регистрации событий;

– маркировки документов;

– контроля целостности;

– стирания памяти;

– учета носителей информации;
– преобразования информации на отчуждаемых носителях;
– контроля устройств;
– тестирования системы защиты.

Подсистема идентификации и аутентификации обеспечивает опознание пользователей при входе в компьютер по персональному идентификатору и подтверждение подлинности путем запроса с клавиатуры личного пароля. Данная подсистема также обеспечивает блокировку экрана компьютера и идентификацию пользователя после такой блокировки.

Подсистема разграничения доступа реализует дискреционный и мандатный принципы контроля доступа пользователей к защищаемым ресурсам. Функционирование данной подсистемы основано на присвоении защищаемым объектам атрибутов защиты.

К атрибутам защиты ресурса, имеющим отношение к разграничению доступа, относятся:
– идентификатор безопасности владельца ресурса;
– список контроля доступа;
– режим запуска (для исполняемых файлов);
– метка конфиденциальности (гриф для неисполняемого файла или допуск для исполняемого файла).

Дискреционный принцип основан на сопоставлении полномочий пользователей и списков контроля доступа ресурсов (логических дисков, папок, файлов, принтеров).

Мандатный принцип контроля доступа реализован путем сопоставления при запросе на доступ к ресурсу меток конфиденциальности пользователя, прикладной программы и защищаемого ресурса.

Подсистема контроля потоков информации предназначена для управления операциями над ресурсами, имеющими различные метки конфиденциальности.

Подсистема запуска программ предназначена для обеспечения целостности и замкнутости программной среды и реализована путем разрешения для исполняемых файлов режима запуска. Если режим запуска программы не разрешен, то файл не является исполняемым и не может быть запущен пользователем ни при каких условиях.

Подсистема управления защитой включает в себя следующие программы администрирования системы защиты:

Программа	Назначение
Установка и снятие системы защиты	Загрузка всех компонентов системы защиты информации, выполнение необходимых настроек в операционной системе, удаление всех компонентов при снятии системы защиты.
Настройка системы защиты	Установка параметров системы защиты информации, а также создание замкнутой программной среды, применение шаблонов настроек и другие сервисные функции.
Учет носителей	Настройка параметров работы системы защиты с носителями информации.
Менеджер пользователей	Управление пользователями системы защиты информации, их свойствами и персональными идентификаторами.
Менеджер файлов	Управление ресурсами, а также их защитными атрибутами.
Контроль устройств	Настройка правил работы системы защиты с устройствами компьютера.
Журнал событий	Работа с журналом событий системы защиты.
Редактор шаблонов настроек	Автоматизированное создание шаблонов настроек системы защиты.
Монитор системы защиты	Отображение состояния системы защиты, а также быстрый вызов функций управления системой защиты.

Подсистема регистрации обеспечивает регистрацию запросов на доступ к ресурсам компьютера и возможность выборочного ознакомления с регистрационной информацией и ее распечатки.

Подсистема маркировки документов обеспечивает автоматическое проставление учетных признаков в документах, выдаваемых на печать, а также регистрации фактов печати документов.

Подсистема контроля целостности предназначена для настройки и периодической проверки параметров целостности системы защиты, программного обеспечения и постоянных информационных массивов.

Подсистема стирания памяти реализует механизм заполнения нулями выделяемых программам областей оперативной памяти и стирания файлов на диске по команде удаления. В рамках данной подсистемы также реализовано стирание файла подкачки страниц по завершении сеанса работы.

Подсистема учета носителей информации позволяет управлять доступом к носителям информации в соответствии с разрешениями и параметрами, прописанными в журнале учета носителей.

Подсистема преобразования информации на отчуждаемых носителях позволяет включить дополнительную защиту для съемных носителей с помощью режима прозрачного преобразования всей информации на носителе.

Подсистема контроля устройств позволяет формировать необходимую конфигурацию устройств для пользователей в соответствии с установленными разрешениями.

Подсистема тестирования системы защиты предназначена для комплексного тестирования основных механизмов системы защиты, как на локальном компьютере, так и на удаленном, с использованием локальной вычислительной сети.

Подготовка к установке системы защиты

Перед установкой СЗИ «Страж NT» на компьютер следует провести ряд обязательных процедур:

1) проверить оперативную память компьютера, а также его жесткий диск на отсутствие вирусов;

2) убедиться в наличии на жестком диске свободного места, достаточного для установки и функционирования системы защиты;

3) убедиться, что на компьютере в данный момент не запущены какие-либо программы, препятствующие работе с системным реестром, выполняющие функции защиты от шпионского программного обеспечения и так далее.

4) убедиться в наличии исправного персонального идентификатора (в случае использования ГМД он должен быть отформатирован) и в возможности его чтения подсистемой идентификации (см. раздел Тестирование подсистемы идентификации);

5) убедиться, что пароль пользователя, устанавливающего систему защиты, не содержит символов кириллицы и специальных знаков, а его длина не превышает 15 символов.

Тестирование подсистемы идентификации

Тестирование подсистемы идентификации предназначено для определения возможности чтения персональных идентификаторов в подсистеме идентификации до загрузки операционной системы. Тестирование подсистемы идентификации проводится до установки системы защиты информации.

Для запуска тестирования необходимо в BIOS Setup компьютера установить принудительную загрузку с носителя информации, на котором поставляется установочный комплект системы защиты. После появления диалога, приведенного на Рис. 1, необходимо предъявить необходимый персональный идентификатор.

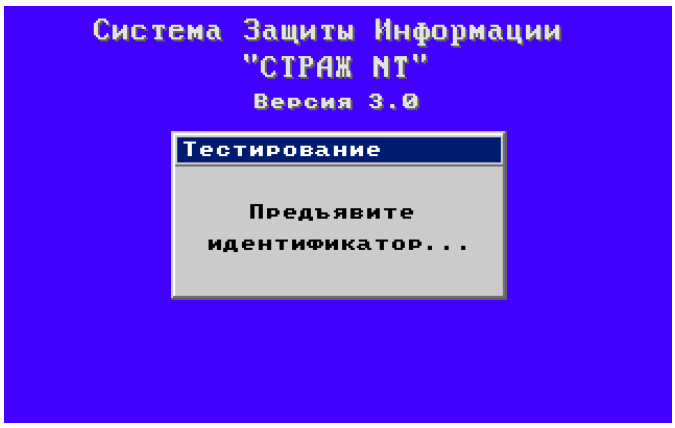


Рисунок 1 – Тестирование подсистемы идентификации

Тестирование считается успешным, если на экране появится сообщение, как на Рисунке 2.

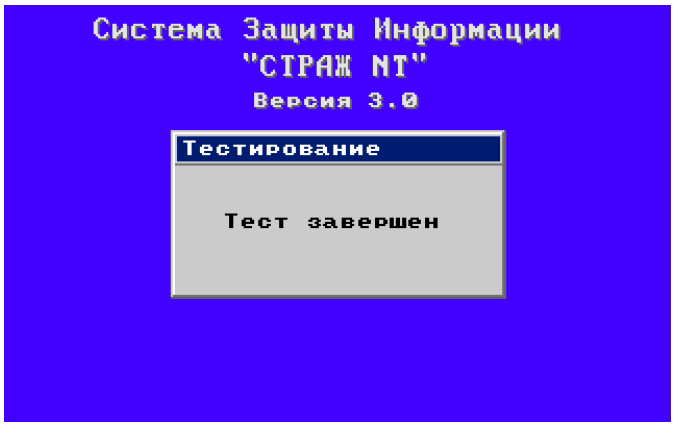


Рисунок 2 – Результат тестирования подсистемы идентификации

После появления сообщения о результатах тестирования следует перезагрузить компьютер.

Установка системы защиты

Для начала процесса установки СЗИ «Страж NT» необходимо установить компакт-диск в привод CD-ROM. При этом операционная система самостоятельно запустит **Мастер установки**. Если окно **Мастера установки** не появляется, необходимо запустить его самостоятельно, открыв в программе **Проводник** содержимое компакт-диска и запустив программу **GInstall.exe**. Если компьютер работает под управлением ОС старше MS Windows XP, и включен контроль учетных записей пользователей (UAC), при запуске программы на экране появится окно, как показано на Рис. 3. Для продолжения необходимо нажать кнопку Да .

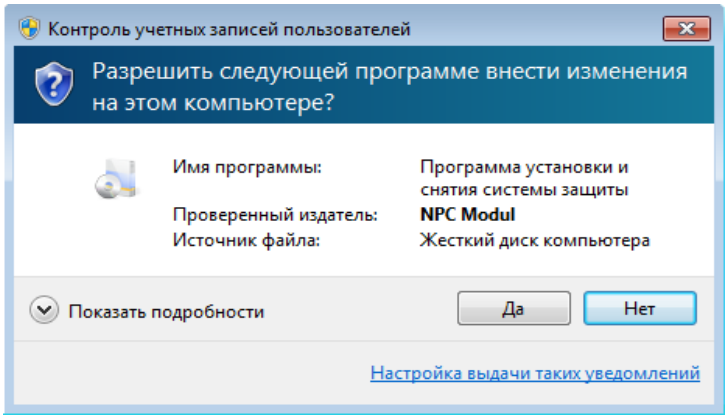


Рисунок 3 – Сообщение подсистемы контроля учетных записей пользователей

Если система защиты уже установлена на данном компьютере, **Мастер установки** проинформирует об этом и предложит снять систему защиты, иначе на экране появится окно, как показано на Рис. 4.

Из **Мастера установки** можно выйти, нажав 

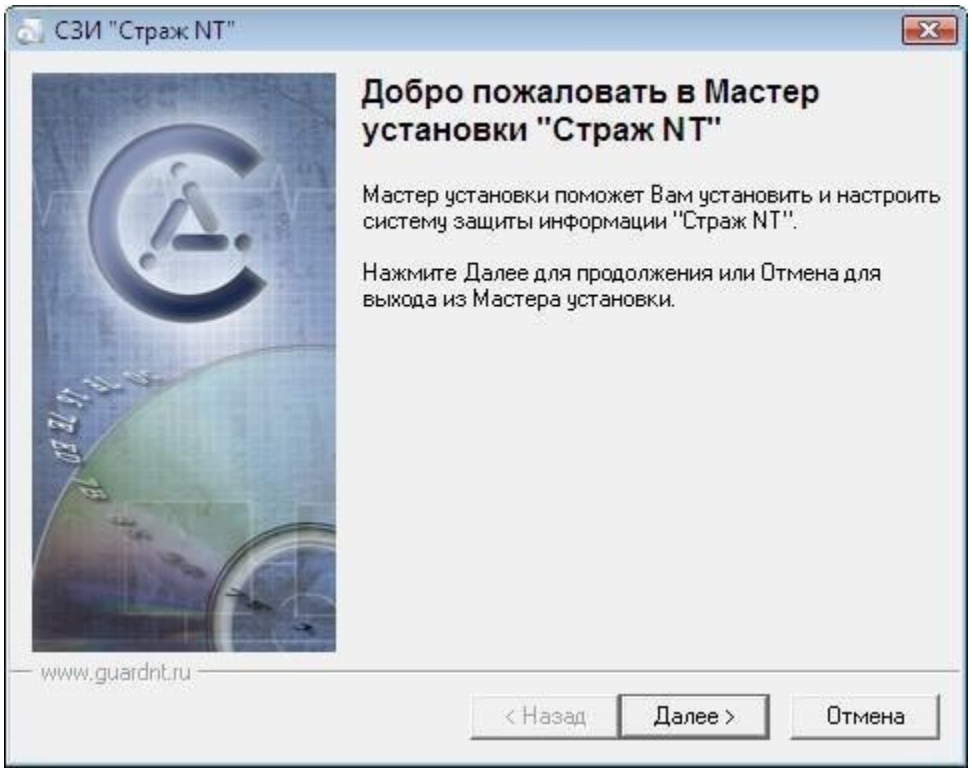


Рисунок 4 – Начальная страница Мастера установки

После нажатия кнопки 

на экране появится окно с текстом лицензионного соглашения (см. Рис. 5). Внимательно прочитайте его. Для продолжения установки системы защиты необходимо нажать кнопку **Я принимаю условия лицензионного соглашения**.

Задание

1. Изучить программное обеспечение Страж NT 3.0:
2. Видеоурок №1. Установка и снятие СЗИ

Практическое занятие №5
Тема «Исследование возможностей управления пользователями с помощью СЗИ НСД.

Задание 1. Изучите возможности системы защиты информации от несанкционированного доступа «Страж NT»:

— назначение;
— запуск и регистрация системы защиты;
— создание пользователей;
— реализация мандатной модели разграничения доступа;
— реализация дискреционной модели разграничения доступа;
— обеспечение замкнутости программной среды;
— контроль целостности;
— организация учета съемных носителей информации;
— регистрация событий;

— гарантированное удаление данных.

Задание 2. Установка автономной версии СЗИ от НСД Dallas Lock 8.0. Инсталлировать автономную версию системы защиты Dallas Lock 8.0 на компьютер может только пользователь, обладающий правами администратора на данном компьютере. Это может быть локальный или доменный пользователь.

Если пользователь доменный, то важно, чтобы он был добавлен в группу «Администраторы» или «Администраторы домена».

Пользователь, установивший систему защиты, автоматически становится суперадминистратором, на которого не распространяются ограничительные действия Dallas Lock 8.0.

Необходимо запомнить имя и пароль этого пользователя, так как некоторые операции можно выполнить только из под его учетной записи. Изменять имя (переименовывать) суперадминистратора средствами Windows нельзя. Имя и пароль пользователя для входа в операционную систему, выполнившего установку, автоматически становятся именем и паролем для первого входа на компьютер с установленной системой защиты Dallas Lock 8.0 пользователем в качестве суперадминистратора.

Для установки автономно работающего СЗИ от НСД Dallas Lock 8.0 необходимо запустить приложение «Dallas Lock 8.0.msi». После запуска программы установки следует выполнять действия, указанные в подсказках инсталлятора.

На каждом шаге установки предоставляется возможность полной отмены инсталляции с возвратом всех сделанныхизменений. Для этого служит кнопка «Отмена». Переход на следующий этап установки выполняется с помощью кнопки «Далее».

Во время установки клиента Dallas Lock 8.0 выполняется автоматическая настройка Брандмауэра Windows. При запуске инсталлятора Dallas Lock 8.0 на компьютере с установленной операционной системой Windows 7, если включен механизм контроля учетных записей, после запуска приложения «Dallas Lock 8.0.msi» на экране будет выведено диалоговое окно для подтверждения операции.

Контроль учетных записей пользователей

Разрешить следующей программе установить программное обеспечение на этом компьютере? Имя программы: Dallas Lock 8.0 Проверенный издатель: Confident Источник файла: Жесткий диск компьютера Показать подробности Да/Нет Для продолжения установки следует ответить «Да», после чего запустится инсталлятор системы Dallas Lock 8.0. Dalias Lock 8.0 СЗИ НСД Dallas Lock 8.0 Данная программа выполнит установку системы защиты информации от несанкционированного доступа Dallas Lock 8.0-K на вашем компьютере.

Для установки необходимо:

Обладать правами администратора

Отключить антивирусную защиту в BIOS компьютера и программные антивирусные средства.

Наличие не менее 30 Мб свободного дискового пространства на системном разделе жёсткого диска

Операционная система должна быть установлена на диск C.

Путь установки: C:DLLOCK80 Начать установку/ Отмена Для установки необходимо нажать кнопку «Начать установку», после чего программа приступит к инсталляции продукта. На данном этапе программа попросит осуществить ввод определенных параметров. Для защиты от нелегального использования продукта необходимо ввести серийный номер лицензии Dallas Lock 8.0, который указан на компактдиске с дистрибутивом в поле «Код» и в формуляре комплекта поставки. Если требуется ввести компьютер в Домен безопасности в процессе установки системы, то в соответствующие поля необходимо ввести имя Сервера безопасности и

его ключ доступа. Для установки автономно работающей версии никаких данных в полях «Сервер безопасности» и «Ключ досту па к СБ» вводить не надо.

Добавить компьютер в Домен безопасности можно и позже, в процессе работы автономной версии Dallas Lock 8.0. После нажатия кнопки «Далее» процесс установки системы будет завершен. Dallas Lock 8.0 Установка… Проверка прав текущего пользователя. Текущий пользователь является Администратор-Копирование Файлов… Копирование Файлов успешно завершено. Создание ярлыков. Ярлыки успешно созданы. Установка драйвера системы защиты. Драйвер безопасности успешно установлен. Регистрация компонентови настройка системы. Настройка системы успешно завершена Администратором системы безопасности HasnaMet otzi. Далее система потребует перезагрузки компьютера. Первый вход на защищенный компьютер сможет осуществить пользователь, под учетной записью которого выполнялась инсталляция системы защиты Dallas Lock 8.0, либо доменный пользовать, если компьютер является клиентом контроллера домена. После установки системы защиты и перезагрузки компьютера на рабочем столе пользователя и в меню «Пуск» появятся иконки оболочки администратора системы защиты Dallas Lock 8.0.

Практическое занятие №6
Тема «Исследование настройки маркировки документов с помощью СЗИ НСД»

Задание 1. Маркировка распечатываемых документов

1. Запустить Dallas Lock и на вкладке «Параметры безопасности» зайти в категорию «Аудит». В окне программы выбрать пункт «Печать/редактировать штамп». 18

2. В новом окне нажать кнопку «да», а затем «редактировать» и в редакторе штампа создать свой штамп путем нажатия на кнопку «добавить элемент». Новый штамп должен содержать следующие параметры: дата и время, компьютер, имя пользователя и метку мандатного доступа. Редактирование содержания штампа происходит через элемент «Изменить текст».

3. Сохранить новый штамп на рабочий стол, нажав на кнопку программы в левом верхнем углу и последующим нажатием кнопки «сохранить как» и выбрать соответствующий путь. После этого выйти из редактора штампа. Если появится уведомление о том, что изменения не были применены – нажать на кнопку «Да».

4. Создать на рабочем столе новый документ формата .docx.

5. Перейти в параметр «Печать», в качестве принтера выбрать «Microsoft XPS Document Writer» и нажать кнопку «Да». В появившемся окне выбора пути сохранения файла указать «Рабочий стол».

6. Открыть созданный документ расширением .xps и убедиться, что штамп был успешно добавлен в документ.

Задание 2. Настройка маркировки и теневого копирования

1. Откройте консоль BM StartSNS и в окне программы ЦУ выберете «Контроль печати».

2. Настройте список принтеров. Для этого выберите вкладку «Настройки» и раскройте раздел Политики → Контроль печати. 44 Включите политику для принтера «Настройки по умолчанию». Убедитесь, что в графе «Категории конфиденциальности» по умолчанию указано «Любой категории». Обратите внимание, что при необходимости в ячейке колонки «Разрешения» могут устанавливаться права пользователей для печати документов для конкретных принтеров или для элемента «Настройки по умолчанию». Нажмите кнопку «Применить».

3. Настройте для принтеров функцию теневого копирования. Для этого: – в

разделе политик «Политики → Контроль печати» найдите пункт «Теневое копирование» и с помощью кнопки внимательно ознакомьтесь с ее описанием; – измените установленное по умолчанию значение на «Определяется настройками принтера»; – нажмите кнопку «Применить».

4. Настройте для принтеров функцию маркировки документов. Для этого: – в разделе политик «Политики → Контроль печати» найдите пункт «Маркировка документов» и с помощью кнопки внимательно ознакомьтесь с описанием ее параметров; – измените установленное по умолчанию значение на «Стандартная обработка» – этот режим может использоваться во всех поддерживаемых приложениях. В данном режиме предпочтительнее печатать документы целиком. При печати фрагмента документа маркер будет содержать сведения только о распечатанных страницах без учета общего количества страниц документа (так как распечатанный фрагмент воспринимается как отдельный документ); – используя кнопку «Редактировать» , ознакомьтесь с возможностью редактирования заданных грифов маркировки. Выберите краткий гриф для шаблона «Гриф №1», затем откройте вкладку 45 «Категории конфиденциальности» и проверьте галочки для необходимых типов документов; – обратите внимание, что если в политике «Маркировка документов» выбран параметр «Расширенная обработка», то с помощью кнопки-ссылки «Приложения, включенные в расширенную обработку» можно управлять перечнем приложений, которые будут поддерживать маркировку печатаемых документов; – нажмите кнопку «Применить».

5. Проверьте работу механизмов теневого копирования и маркировки документов при печати. Для этого на ВМ компьютера StartSNS под учетной записью «adminsns» создайте любой из документов, добавьте произвольное содержимое.

6. Выполните печать документа на установленном по умолчанию виртуальном принтере. В промежуточном диалоговом окне «Атрибуты документа» системы Secret Net Studio введите произвольный учетный номер, а затем сохраните с любым именем файл печати .xps.

7. Проверьте результат.

Практическое занятие №7

Тема «Разработка инструкции по организации защиты данных пользователя»

Цель работы — разработать набор электронных инструкций по курсу «Информационная безопасность и защита информации»

Задачи:

1. разработать набор электронных инструкций для обучения пользователей основам информационной безопасности.

Практическое занятие №8

Тема «Организация процедуры экстренной модификации»

Задание 1. Составить акт о причинах модификации

Задание 2. Разработать инструкцию по организации экстренной модификации.

Практическое занятие №9

Тема «Разработка плана защиты и обеспечения непрерывной работы автоматизированной системы»

Задание 1. Разработайте план обеспечения непрерывной работы и восстановления работоспособности подсистемы защиты информации автоматизированной системы

Практическое занятие №10

Тема «Разработка концепции информационной безопасности организации»

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р

ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов **– Концепции и Политики информационной безопасности.** Если Концепция ИБ в общих чертах определяет, **ЧТО** необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит, **КАК**, какими средствами и способами они должны быть реализованы. Концепция информационной безопасности используется, для: принятия обоснованных управленческих решений по разработке мер защиты информации;

- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности**.**

3. Задание. Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

Общие положения

Назначение Концепции по обеспечению информационной безопасности. Цели системы информационной безопасности

1. Задачи системы информационной безопасности.

Проблемная ситуация в сфере информационной безопасности

1. Объекты информационной безопасности.
2. Определение вероятного нарушителя.
3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.
4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

5. Общестатистическая информация по искусственным нарушениям информационной безопасности.
6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

Механизмы обеспечения информационной безопасности Предприятия

Принципы, условия и требования к организации и функционированию системы информационной безопасности.

1. Основные направления политики в сфере информационной безопасности.
2. Планирование мероприятий по обеспечению информационной безопасности Предприятия.
3. Критерии и показатели информационной безопасности Предприятия.

Мероприятия по реализации мер информационной безопасности предприятия

Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

Техническое обеспечение информационной безопасности Предприятия.

Общие положения.

- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

Правовое обеспечение информационной безопасности Предприятия. Правовое обеспечение юридических отношений с работниками Предприятия.

- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

Оценивание эффективности системы информационной безопасности Предприятия.

Программа создания системы информационной безопасности Предприятия

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Концепция ИБ заданного предприятия по плану, приведенному в задании

5. Варианты

Вариант – номер по списку в журнале.

Номер варианта	**Организация**	**Метод оценки риска**
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Колледж	3
4	Офис страховой компании	4
5	Рекрутинговое агентство	1
6	Интернет-магазин	2
7	Центр оказания государственных услуг	3
8	Отделение полиции	4
9	Аудиторская компания	1
10	Дизайнерская фирма	2
11	Офис интернет-провайдера	3
12	Офис адвоката	4
13	Компания по разработке ПО для сторонних организаций	1
14	Агентство недвижимости	2
15	Туристическое агентство	3
16	Офис благотворительного фонда	4
17	Издательство	1
18	Консалтинговая фирма	2
19	Рекламное агентство	3
20	Отделение налоговой службы	4
21	Офис нотариуса	1
22	Бюро перевода (документов)	2
23	Научно проектное предприятие	3
24	Брачное агентство	4
25	Редакция газеты	1
26	Гостиница	2
27	Праздничное агентство	3

28	Городской архив	4
29	Диспетчерская служба такси	1
30	Железнодорожная касса	2

Практическое занятие №11

Тема «Ввод информации в САПР СЗИ. Расчет радиуса контролируемой зоны с помощью САПР СЗИ»

Задание1. Разработать модель объекта информатизации -автоматизированное рабочее место в защищаемом помещении предприятия и выполнены измерения ПЭМИН (побочные электромагнитные излучения и наводки) с целью определения возможности утечки информации за пределы моделируемой контролируемой зоны.

Практическое занятие №12

Тема «Исследование механизма доступа в систему с использованием СПО ЗИ и УП»

Цели: изучить механизмы управления доступом.

Теоретические вопросы:

1. Модели управления доступом.
2. Выбор модели управления доступом.
3. Дискреционное управление доступом.
4. Мандатное управление доступом.
5. Списки управления доступом.
6. Ролевое управление доступом.

Задание 1. Поясните фрагмент матрицы доступа:

	Файл	Программа	Линия связяи	Реляционная таблица
Пользователь 1	orw с системой консоли	e	Rw	с 8.00 до 18.00
Пользователь 2				

Задание 2. Заполните таблицу:

Разрешения доступа к общим папкам

Разрешение	Позволяет
Изменение	
(Чтение)	
(Полный доступ)	

Задание 3. Пусть пользователю User101 назначены разрешения для получения доступа к ресурсам как отдельному пользователю и как члену 43 группы. Определите, какие результирующие разрешения будут у User101 в следующих ситуациях:

1. User101 — член групп Group1, Group2 и Group3. Для папки ПапкаА у Group1 есть разрешение Read (Чтение), у Group3 — Full Control (Полный доступ), а для Group2 разрешений не назначено. Какими результирующими разрешениями будет обладать User101для ПапкиА?

2. User101 также является членом группы Sales, которой назначено разрешение Read для ПапкаВ. Для User101 как отдельного пользователя, отменено разрешение Full Control для ПапкаВ. Какие результирующие разрешения будет иметь User101 для ПапкаВ?

Задание 4. Определите результирующие разрешения пользователей, спланируйте совместное использование папок и разрешений доступа к ним, назначьте разрешения доступа к папке, подключитесь к ней, закройте к ней доступ и проверьте эффекты от сочетания разрешений доступа к общей папке и разрешений NTFS:

3. Открыт доступ к папке Data. Группа Sales имеет для нее разрешение read (Чтение), а для вложенной в нее папки ^ Sales — NTFS-разрешение Full Control

(Полный доступ). Каким будет результирующее разрешение группы Sales для доступа к папке Sales при подключении по сети к папке Data?

4. Папка Users (Пользователи) содержит личные папки пользователей. Каждая личная папка содержит данные, доступные только пользователю, именем которого она названа. Папка Users доступна группе Users с разрешением Full Control (Полный доступ). Userl и User2 имеют разрешения NTFS Full Control только для своих личных папок: никаких разрешений NTFS для остальных. Эти пользователи — члены группы Users. ^ Какими разрешениями доступа к папке Userl будет обладать Userl при подключении к общей папке Users? Какими будут его разрешения для папки User2?

Задание 5. Закройте доступ к заданной папке.

Практическое занятие №13

Тема «Сравнение средств защиты информации от НСД»

Задание 1. Заполнить таблицу

Характеристика				
Дистрибуция и установка				
Доступность дистрибутивов				
Простота установки				
Ограничения при установке				
Простота удаления				
Документация				
Наличие документации				
Полнота документации				
Доступность документации				
Общие характеристики				
Наивысший уровень секретности				
Допустимые ИС				
Собственная безопасность				
Сертификация				
Простота интерфейса				
Ценовые характеристики				
Возможности				
Дискреционный контроль				
Мандатный контроль				
Контроль запуска				

процессов				
Механизм замкнутой программной среды				
Контроль целостности				
Контроль внешних устройств				
Использование электронных идентификаторов				
Контроль печати				
Журналирование				

Практическое занятие №14

Тема «Разработка алгоритма генерации одноразовых паролей»

Теоретические сведения.

Аутентификация с одноразовым паролем обладает устойчивостью к атаке анализа сетевых пакетов, что дает ей значительное преимущество перед запоминаемыми паролями.

Технологии использования одноразовых паролей можно разделить на следующие:

1. Использование генератора псевдослучайных чисел, единого для субъекта и системы. В данном случае используется генератор псевдослучайных чисел с одинаковым значением для субъекта и для системы.
2. Использование временных меток вместе с системой единого времени. Аутентификация основана на генерации случайных чисел через определенные временные интервалы.
3. Использование базы случайных паролей, единой для субъекта и для системы. Основан на единой базе паролей для субъекта и системы и высокоточной синхронизации между ними, при этом каждый пароль из набора может быть использован только один раз.

Одноразовые пароли предназначены для усиления аутентификации в клиент-серверных системах: кроме обычного долговременного (статического) пароля клиент предъявляет серверу дополнительный пароль, срок действия которого ограничен определенным сеансом аутентификации или промежутком времени. Даже если противник узнает пароль текущего сеанса или промежутка, он не сможет использовать его в следующем. Аутентификация может быть двусторонней: после успешной аутентификации клиента сервер генерирует новый одноразовый пароль и предъявляет его клиенту. Стороны генерируют одноразовый пароль R , комбинируя общий секретный ключ K с уникальной синхропосылкой. Ключ K должен вырабатываться без возможности предсказания, распространяться с соблюдением мер конфиденциальности и храниться в секрете. Ключом является двоичное слово фиксированной или произвольной длины.

Задание 1. Используя любой известный метод, разработать алгоритм генерации одноразовых паролей.

Практическое занятие №15

Тема «Организация разграничения доступа к ресурсам системы»

Цели: Изучить способы разграничения доступа. Научиться распределять права доступа сотрудникам предприятия в зависимости от их должностных обязанностей.

Теоретические вопросы:

1. Технические средства разграничения доступа к устройствам.
2. Механизмы разграничения доступа к устройствам.

Ход работы:

1.Запустите виртуальную машину «Secret Net Client». Для настройки конфигурации виртуальной машины VMware задаст вопрос о том была ли она скопирована или перемещена (рис. 1), выберите вариант «I Moved It» (виртуальная машина перемещена). После загрузки операционной системы войдите под локальной учетной записью «Администратор» (рис. 2). Будет необходимо выбрать параметр «Вход в: XP-MSDN (этот компьютер)». После этого будет выведено сообщение об изменении аппаратной конфигурации. Снимите блокировку рабочей станции (Да) и выполните следующее:

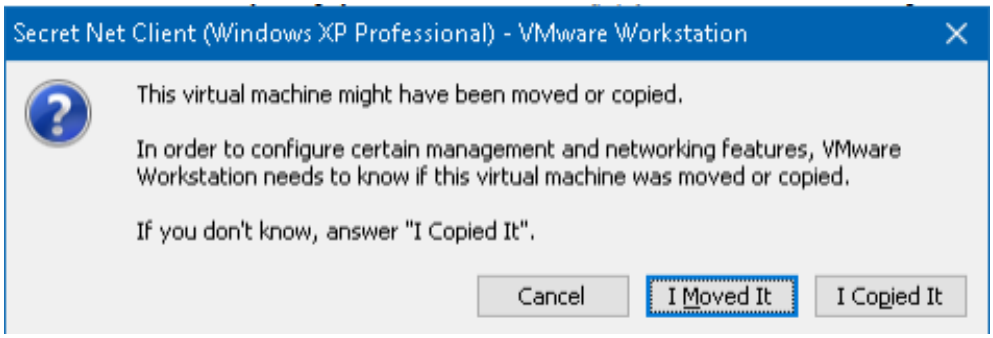


Рисунок 1 – Запрос конфигурации при запуске виртуальной машины

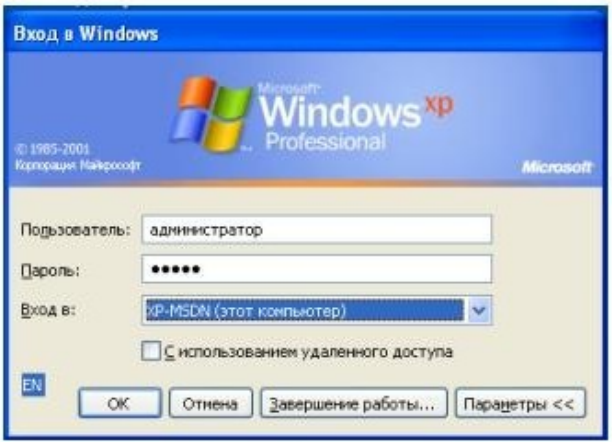


Рисунок 2 – Вход в систему под локальной учетной записью Откройте свойства учетной записи Администратор (Мой компьютер-

Управление - Локальные пользователи- Пользователи - Администратор). Измените уровень допуска на строго конфиденциально (Вкладка Secret Net

7 - Доступ), разрешите управление категориями конфиденциальности, вы- вод и печать конфиденциальных документов (рис. 3). Создайте учетные за- писи user и conf. Настройте пользователю conf категорию доступа конфиденциально и добавьте возможность печати конфиденциальных документов (рис. 4). Для пользователя user по умолчанию задан уровень допуска «Не- конфиденциально».

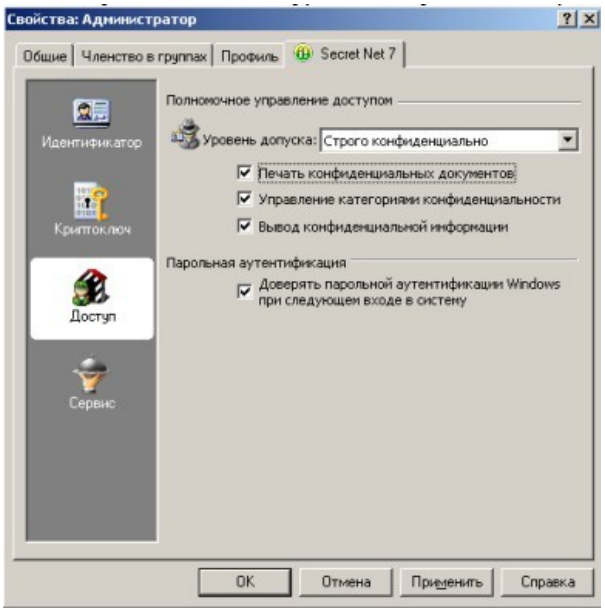


Рисунок 3– Параметры управления полномочным доступом для пользователя Администратор

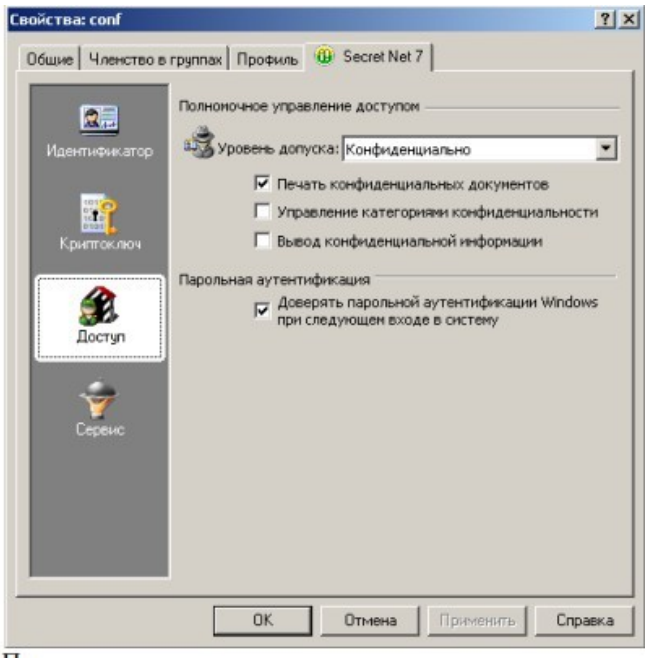


Рисунок 4– Параметры управления полномочным доступом для пользователя conf

2.Вызовите оснастку для управления параметрами объектов групповой политики (Пуск-Программы-Код безопасности- Secret Net – Локальная политика безопасности) и перейдите к разделу «Параметры безопасности |

Параметры Secret Net» - выберите папку «Устройства». Утвердите изменения. В правой части окна появится общий список устройств. - выберите в списке оптический диск «VMWare IDE CDR» (или другой CD дисковод, который будет предоставлен средством виртуализации VMware), вызовите контекстное меню и выберите команду «Свойства». В группе настройки вы- берите «Подключение устройства разрешено» (рис. 5). В группе «полномочный доступ» выберете параметр доступа «Для устройств задана категория конфиденциальности» и выберете категорию конфиденциальности «Строго конфиденциально» (рис. 6).

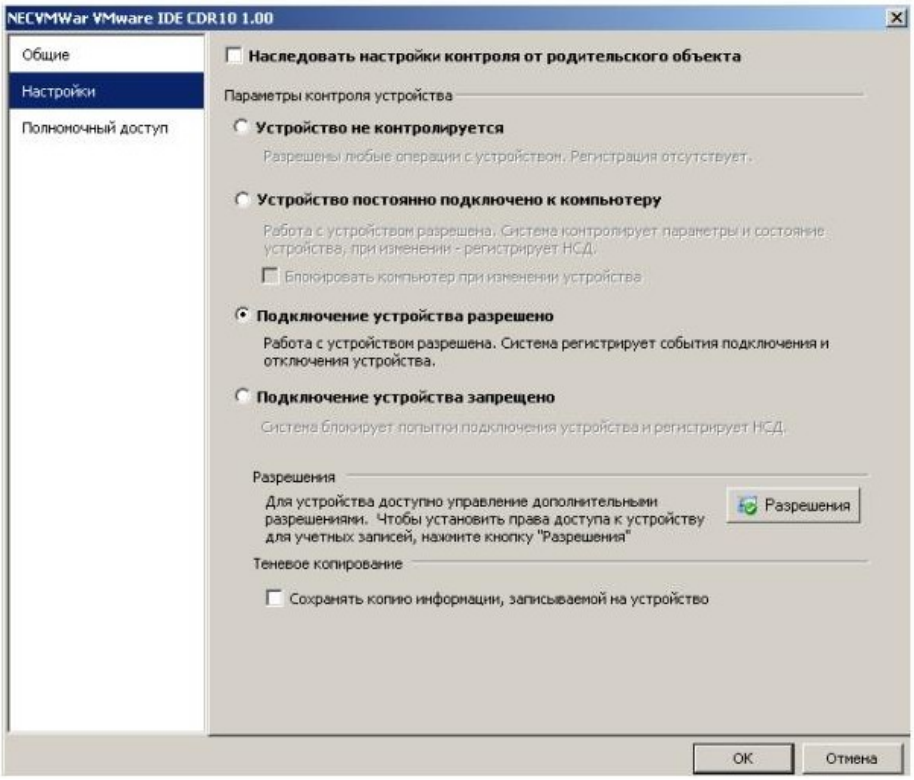


Рисунок 5- Настройки виртуального CD- привода в групповых политиках Secret Net

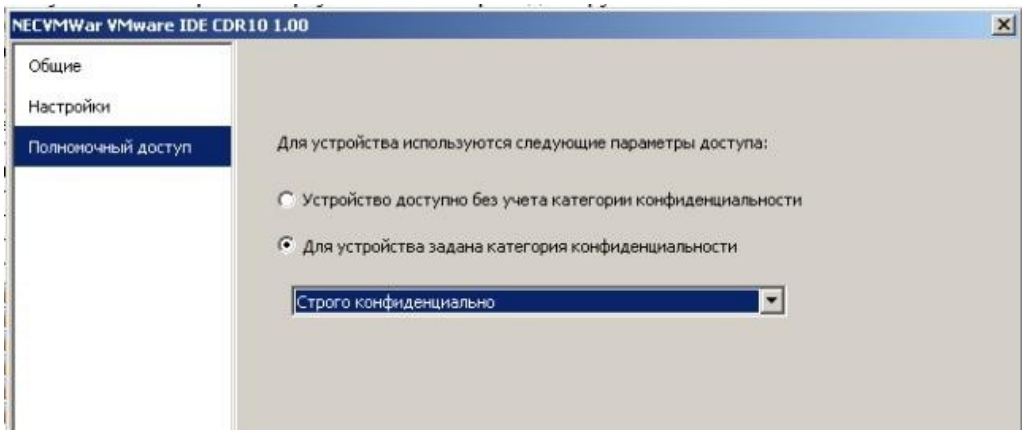


Рисунок 6 – Настройки конфиденциальности виртуального CD-привода в групповых политиках Secret Net

- войдите под учетной записью «user» и убедитесь, что вход в систему, при наличии устройства с категорией конфиденциальности выше, чем у пользователя, недоступен. Приведите результат в отчете.

3.Войдите под учетной записью «Администратор», измените назад параметры конфиденциальности оптического диска на «Устройство доступно без учета категории конфиденциальности», запретите использование оптических дисков для пользователя 8 «user» следующим образом: откройте раз- решения в свойствах CD-дисковода (Настройки Разрешения), добавьте пользователя user и запретите всех разрешения к данному CD приводу (рис. 7) - галочки «запретить».

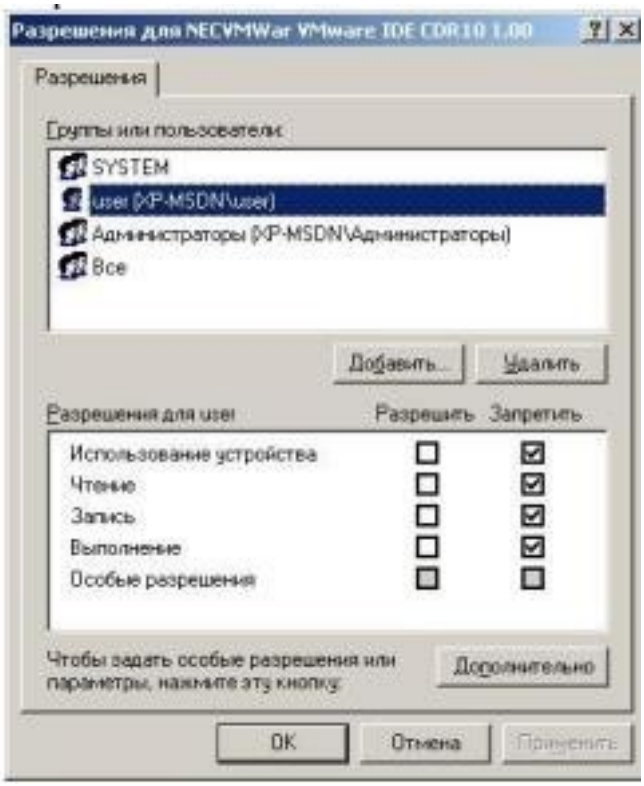


Рисунок 7 – Изменение прав доступа к CD-приводу для пользователя user.

- Войдите под учетной записью user и убедитесь в запрете доступа, по- пытавшись открыть CD-привод в проводнике.

4.Настройку политик контроля устройств можно выполнить индивидуально для каждого устройства (отдельной модели), класса или группы устройств с использованием принципа наследования параметров. Для настройки политики контроля устройств выполнить следующее:

- Войдите под учетной записью Администратор. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу «Параметры безопасности | Параметры Secret Net»
- выберите папку «Устройства». В правой части окна появится общий список устройств. - выберите в списке объект «Устройства USB», вызовите контекстное меню и выберите команду «Свойства».

На экране появится диалог для настройки параметров объекта. По умолчанию в диалоге отображаются параметры группы «Общие» (рис. 8), представляющие основные сведения об объекте.

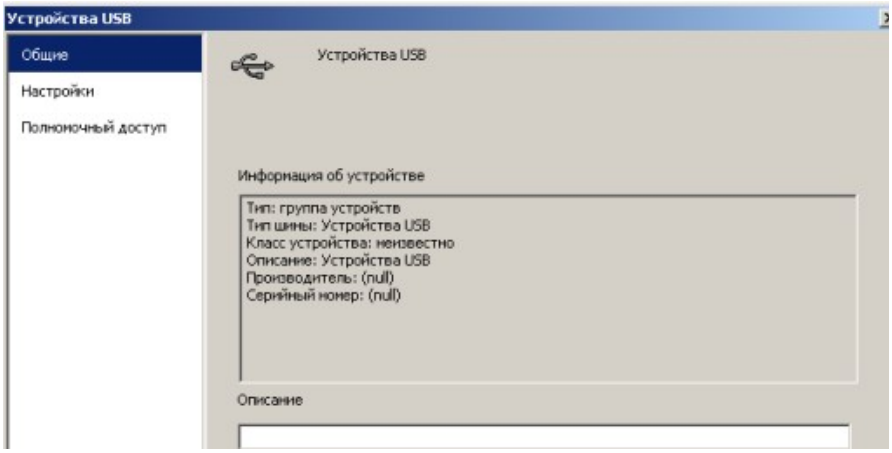


Рисунок 8 – Вкладка общие для группы устройства USB 9

- перейдите к группе параметров «настройки» и поставьте значения параметров в соответствии с рис. 9. Примените настройки ко всем дочерним объектам.

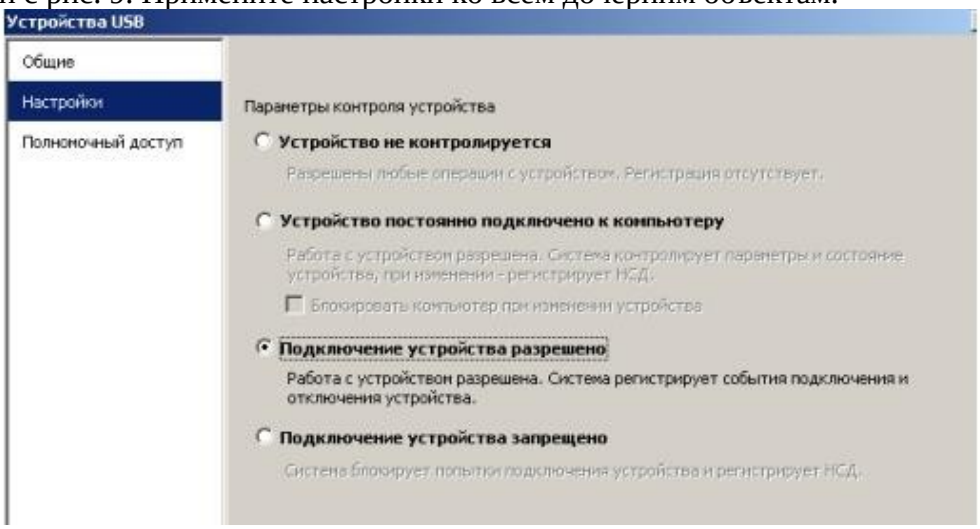


Рисунок 9 – Вкладка «Настройки» для группы устройства USB

При этом для подключенных устройств можно задать следующие пара- метры:

– Поле «Устройство не контролируется». Если в поле установлена от- метка — для объекта отключен режим контроля.

– Поле «Устройство постоянно подключено к компьютеру». Если в поле установлена отметка — для объекта включен режим контроля, при ко- тором устройство должно быть постоянно подключено к компьютеру. В случае изменения состояния устройства в журнале регистрируются события несанкционированного доступа (НСД), и система ожидает утверждение изменений аппаратной конфигурации администратором безопасности. Для усиления защиты можно дополнительно включить режим автоматического блокирования компьютера при изменении состояния устройства: для этого установите отметку в поле «Блокировать компьютер при изменении устройства». Возможность разблокировки компьютера будет иметь только администратор безопасности.

– Поле «Подключение устройства разрешено». Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать. В случае изменения состояния устройства в журнале регистрируются соответствующие события. Утверждение изменений аппаратной конфигурации при этом не требуется. Параметр присутствует только для тех устройств, для которых от- слеживается процесс подключения и можно запретить использование.

– Поле «Подключение устройства запрещено». Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство запрещается подключать к компьютеру. Попытки подключения устройства регистрируются в журнале как события НСД. Параметр присутствует только для тех устройств, для которых отслеживается процесс подключения и можно запретить использование.

Практическое занятие №16
Тема «Исследование механизма контроля и регистрации с использованием СПО ЗИ и УП»

Для настройки механизма регистрации событий необходимо:

1. настроить параметры журнала безопасности;

2. составить общий перечень событий, регистрируемых в системе до идентификации пользователя;

3. составить персональный перечень регистрируемых событий для каждого пользователя.

Для настройки параметров журнала безопасности:

1. Вызовите окно настройки общих параметров и перейдите к диалогу "Журнал":

2. Установите значение максимального размера журнала и укажите механизм очистки журнала при его переполнении (при превышении максимального значения).

3. Нажмите кнопку "OK" или "Применить".

Для настройки перечня регистрируемых событий:

1. В окне настройки общих параметров выберите диалог "Регистрация событий":

2. Отметьте категории событий Windows 2000 и события Secret Net 2000, которые должны регистрироваться в журнала безопасности.

3. Нажмите кнопку "OK" или "Применить".

Для настройки персонального перечня регистрируемых событий:

1. В программе "Проводник" выберите интересующего вас пользователя, вызовите на экран окно настройки свойств и перейдите к диалогу "Регистрация событий":

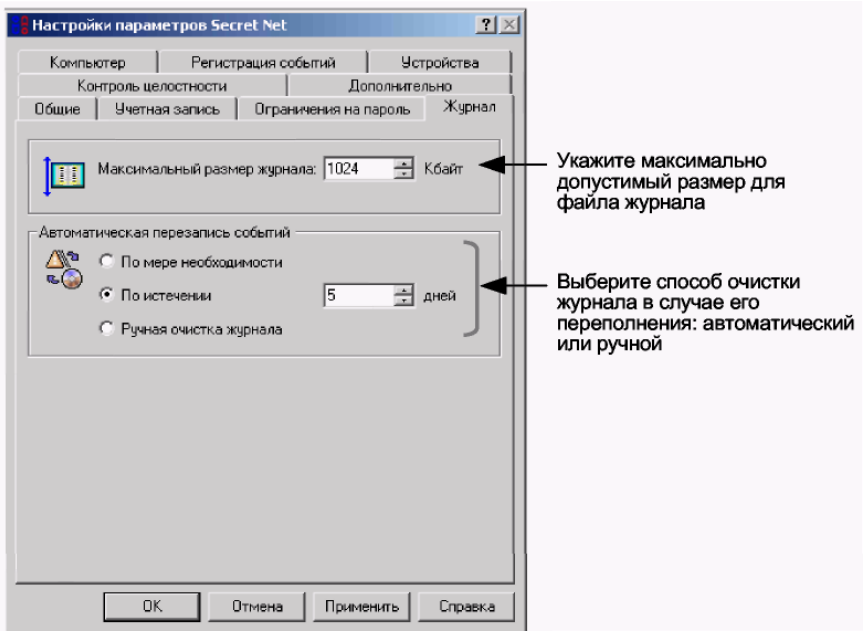


Рис. 1. Настройка параметров журнала безопасности.

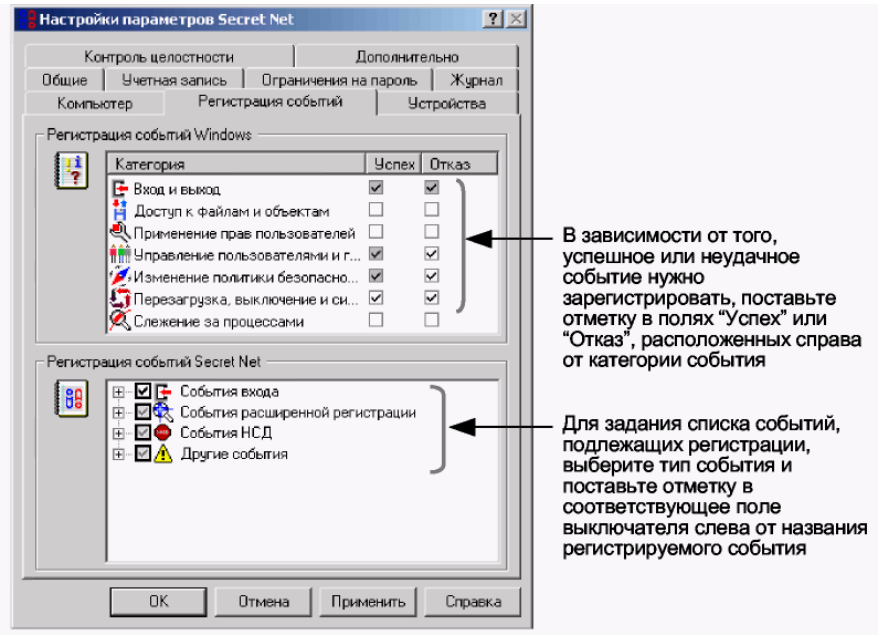


Рис. 2. Диалог "Регистрация событий"

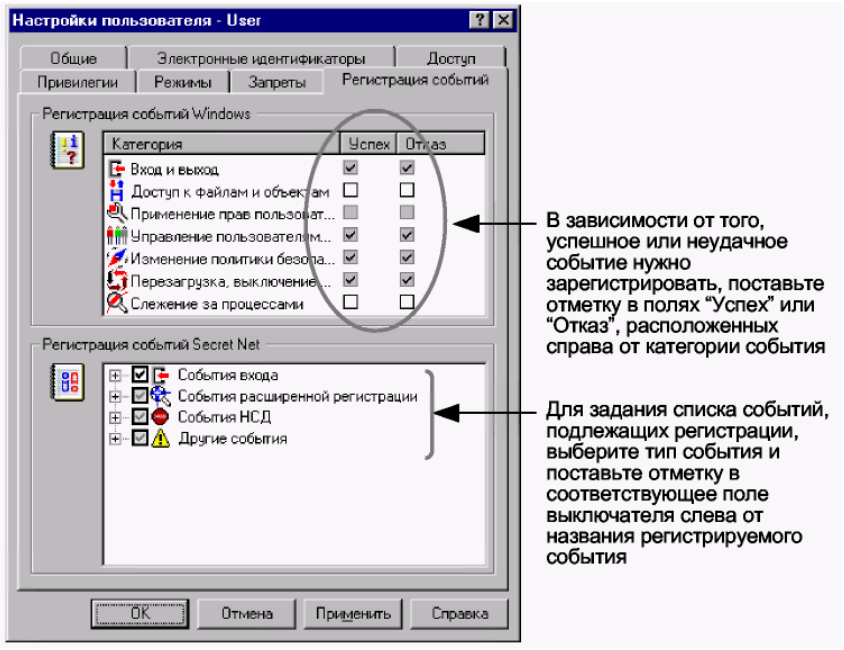


Рис. 3. Диалог "Регистрация событий"

2. Отметьте категории событий Windows 2000 и события Secret Net 2000, которые необходимо регистрировать в журнале безопасности.

3. Нажмите кнопку "OK" или "Применить".

Задание:

1. настроить параметры журнала безопасности;

2. составить общий перечень событий, регистрируемых в системе до идентификации пользователя;

3. составить персональный перечень регистрируемых событий для каждого пользователя.

Практическое занятие №17
Тема «Исследование проблемных ситуаций с использованием СПО ЗИ и УП»

Задание.

1. Составить презентацию на тему «Исследование проблемных ситуаций с использованием СПО ЗИ и УП»

Практическое занятие №18
Тема «Сравнение типов межсетевых экранов»

Задание:

Заполните таблицу

Характеристика	Виды межсетевых экранов				

Практическое занятие №19
Тема «Проведение анализа трафика сайта»

Цель: Проверить умение использовать снифферы для анализа сетевого трафика и понимание структуры HTTP-запросов и ответов.

Задание:

1. Установить и настроить сниффер (Wireshark, Fiddler или Charles Proxy).
2. Перехватить HTTP/HTTPS-трафик сайта (например, https://example.com).
3. Провести анализ HTTP-запросов и ответов, изучить заголовки и тело ответа.
4. Задокументировать результаты с примерами запросов и ответов.

Практическое занятие №20
Тема «Сравнение средств анализа защищенности»

Задание:

Заполните таблицу

Характеристика	Средства анализа защищенности				

Практическое занятие №21
Тема «Исследование возможностей многофункционального поискового прибора»

Цель работы: исследовать обеспечение защищенности информации с помощью системы виброакустической и акустической защиты "Соната-АВ" модель 1М и многофункционального поискового прибора “Пиранья”, научиться использовать вышеприведенные приборы**.**

Объект исследования: вибрационные, акустические, оптикоэлектронный (лазерный), акустоэлектрические электромагнитные, электрические, параметрические каналы ТКУИ, передаваемой по кабельным линиям связи, ИК ТКУИ.

Предмет исследования: степень защищенности по рассматриваемым ТКУИ, и возможность контроля с помощью системы виброакустической и акустической защиты "Соната-АВ 1М" и многофункционального поискового прибора “Пиранья”.

Результат выполнения работы оформить в виде отчета.

Практическое занятие №22
Тема «Исследование возможностей комплекса обнаружения радиоизлучающих средств и радиомониторинга»

Цель работы: изучить возможности комплекса обнаружения радиоизлучающих средств и радиомониторинга

Задание: разработать инструкцию пользователя комплекса обнаружения радиоизлучающих средств и радиомониторинга

Практическое занятие №23
Тема «Исследование возможностей работы фильтров сетевых помехоподавляющих»

Цель работы: изучить возможности фильтров сетевых помехоподавляющих

Задание: разработать инструкцию пользователя по установке и эксплуатации фильтров сетевых помехоподавляющих

Практическое занятие №24
Тема «Исследование уязвимостей и построение модели угроз объекта защиты»

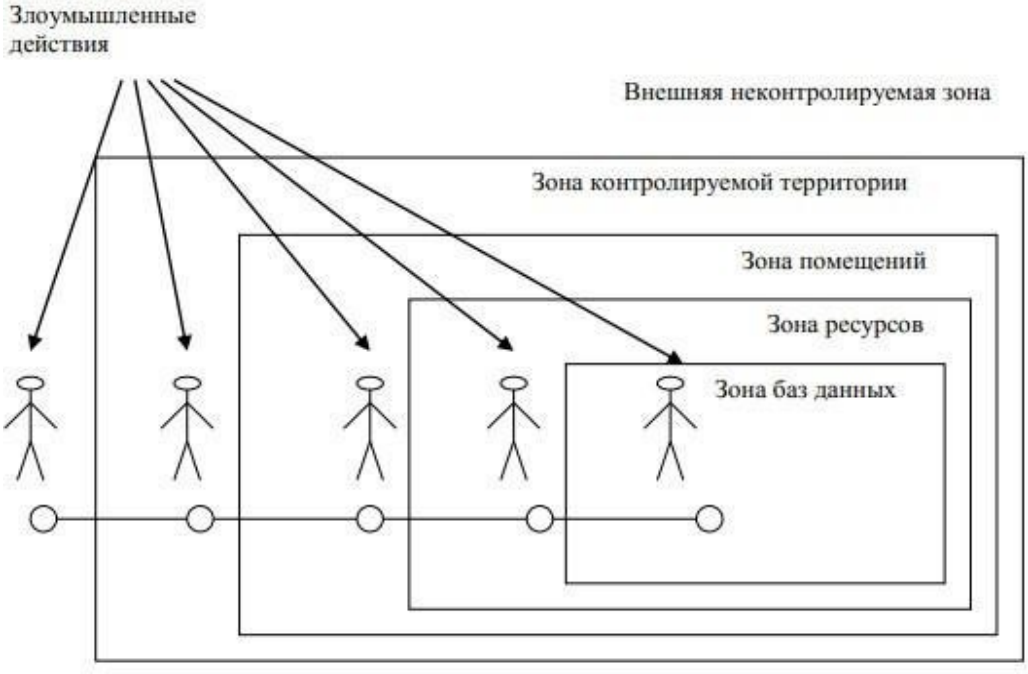
Цель: анализ и построение модели информационной безопасности.

Теоретические вопросы:

1. Классы каналов несанкционированного получения информации.
2. Моделирование угроз безопасности информации.
3. Модель нарушителя информационной безопасности.

Задание 1. Приведите примеры каналов несанкционированного полу- чения информации.

Задание 2. Структурированная схема потенциально возможных зло- умышленных действий в автоматизированных системах обработки данных:



Определите выделенные зоны для заданного объекта.

Задание 3. Проведите анализ потенциальных каналов утечки на указан- ном объекте. Составьте перечень каналов утечки информации на защищае- мом объекте с указанием места расположения по образцу:

Каналы утечки информации с объекта защиты			Место расположения
1			2
1.	Оптический канал	Окно со стороны проспекта	Каб. №1
		Окно со стороны проспекта	Каб. №2
		Окно со стороны проспекта	Каб. №3
2.	Радиоэлектронный канал	Стоянка автотранспорта на просп.	указать
		Система часофикации	указать
		телефон	указать
		Розетки	указать
		ПЭВМ	указать
		Воздушная линия электропередачи	указать
		Система оповещения	указать
		Система пожарной сигнализации	указать
3.	Акустический канал	Теплопровод подземный	указать
		Водопровод подземный	указать
		Стены помещения	указать
		Батареи	указать
		Окна контролируемого помещения	указать
4.	Материально-вещественный канал	Документы на бумажных носителях	указать
		Персонал предприятия	указать
		Производственные отходы	указать

Задание 4. Постройте модель угроз защищаемого объекта:

№ элемента	Цена информации	Путь проникновения	Оценка реальности	Величина угрозы	Ранг угрозы

Практическое занятие №25
Тема «Исследование возможностей устройства для защиты объектов информатизации»

Цель работы: изучить возможности устройства для защиты объектов информатизации

Задание: разработать инструкцию пользователя устройства для защиты объектов информатизации

Практическое занятие №26
Тема «Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств»

Цель работы: изучить возможности устройства защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок

Задание: разработать инструкцию пользователя устройства защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок

Практическое занятие №27
Тема «Организация мер по комплексному обследованию защищенности информационной системы»

Цель работы: изучить содержание и последовательность работ выполняемых при построении комплексной системы защиты информации. Закрепить знания полученные на лекции.

Теоретическая часть

При создании комплексной системы защиты конфиденциальной информации необходимо защищать информацию во всех фазах ее существования - документальной (бумажные документы, микрофильмы и т.п.), электронной, содержащейся и обрабатываемой в информационных системах и отдельных средствах вычислительной техники, включая персонал, который ее обрабатывает - всю информационную инфраструктуру. При этом защищать информацию необходимо не только от несанкционированного доступа к ней, но и от неправомерного вмешательства в процесс ее обработки, хранения и передачи на всех фазах, нарушения работоспособности информационной системы, воздействия на персонал и т.п.

Целью работы должно являться построение комплексной системы защиты конфиденциальной информации (далее по тексту КСЗИ). Это предполагает необходимость использования, создания и разработки совокупности организационных и технических элементов КСЗИ, взаимообусловленных и взаимоувязанных, и базируется на использовании методологии построения комплексной системы защиты конфиденциальной информации.

Методология есть совокупность способов и приемов рассмотрения вопросов информационной безопасности и методов их решения в целях построения комплексной системы информационной безопасности. Она дает возможность в рамках единого подхода использовать согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Организационные и технические меры защиты информации, реализуемые в рамках КСЗИ, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

− неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

− неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

− неправомерного блокирования информации (обеспечение доступности информации).

Процесс построения КСЗИ включает следующие этапы:

1. Формирование требований к защите информации, содержащейся в информационной системе.
2. Разработка КСЗИ информационной системы.
3. Внедрение КСЗИ информационной системы.
4. Аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие.
5. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы.
6. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

1. Формирование требований к защите информации, содержащейся в информационной системе

Формирование требований к защите информации, содержащейся в информационной системе, осуществляется обладателем информации с учетом ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (далее - ГОСТ Р 51583) и ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении.

Общие требования» (далее - ГОСТ Р 51624) и в том числе включает:

− принятие решения о необходимости защиты информации, содержащейся в информационной системе;

− классификацию информационной системы по требованиям защиты информации (далее - классификация информационной системы);

− определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации;

− определение требований к системе защиты информации информационной системы.

1.1. При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется:

1. Анализ целей создания информационной системы и задач, решаемых этой информационной системой.
2. Определение информации, подлежащей обработке в информационной системе.
3. Анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система.
4. Принятие решения о необходимости создания КСЗИ информационной системы, а также определение целей и задач защиты информации в информационной системе, основных этапов создания КСЗИ информационной системы и функций по обеспечению защиты информации, содержащейся в информационной системе, обладателя информации.

1.2. Классификация информационной системы может проводиться в зависимости от значимости обрабатываемой в ней информации, способов её обработки и масштаба информационной системы.

Требование к уровню (классу) защищенности включается в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание КСЗИ информационной системы, разрабатываемые с учетом ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (далее - ГОСТ 34.602), ГОСТ Р 51583 и ГОСТ Р 51624.

Результаты классификации информационной системы оформляются актом классификации.

1.3. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно- функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации содержит описание информационной

системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

1.4. Требования к системе защиты информации информационной системы определяются в зависимости от уровня (класса) защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации.

Требования к системе защиты информации информационной системы включаются в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание КСЗИ информационной системы, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и должны в том числе содержать:

- цель и задачи обеспечения защиты информации в информационной системе;
- класс защищенности информационной системы;
- перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;
- перечень объектов защиты информационной системы;
- требования к мерам и средствам защиты информации, применяемым в информационной системе;
- требования к защите информации при информационном взаимодействии с иными информационными системами и информационно- телекоммуникационными сетями.

При определении требований к системе защиты информации информационной системы учитываются положения политик обеспечения информационной безопасности обладателя информации в случае их разработки по ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

2. Разработка КСЗИ информационной системы

Разработка КСЗИ информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание КСЗИ информационной системы с учетом ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (далее - ГОСТ 34.601), ГОСТ Р 51583 и ГОСТ Р 51624 и в том числе включает:

1. Проектирование КСЗИ информационной системы.
2. Разработку эксплуатационной документации на систему защиты информации информационной системы.
3. Макетирование и тестирование КСЗИ информационной системы (при необходимости).

КСЗИ информационной системы не должна препятствовать достижению целей создания информационной системы и ее функционированию.

При разработке КСЗИ информационной системы учитывается ее информационное взаимодействие с иными информационными системами и информационно-телекоммуникационными сетями.

2.1. При проектировании КСЗИ информационной системы:

- определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);

− определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в информационной системе;

− выбираются меры защиты информации, подлежащие реализации в КСЗИ информационной системы;

− определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

− определяется структура КСЗИ информационной системы, включая состав (количество) и места размещения ее элементов;

− осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы;

− определяются параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации;

− определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно- телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

Результаты проектирования КСЗИ информационной системы отражаются в проектной документации (эскизном (техническом) проекте и (или) в рабочей документации) на информационную систему (систему защиты информации информационной системы), разрабатываемых с учетом ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (далее - ГОСТ 34.201).

При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации и их сертификация в соответствии с законодательством Российской Федерации или производится корректировка проектных решений по информационной системе и (или) ее системе защиты информации с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.

2.2. Разработка эксплуатационной документации на систему защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание КСЗИ информационной системы.

Эксплуатационная документация на КСЗИ информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна в том числе содержать описание:

− структуры КСЗИ информационной системы;

− состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;

− правил эксплуатации КСЗИ информационной системы.

2.3. При макетировании и тестировании КСЗИ информационной системы в том числе осуществляются:

− проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

− проверка выполнения выбранными средствами защиты информации требований к системе защиты информации информационной системы;

− корректировка проектных решений, разработанных при создании информационной системы и (или) КСЗИ информационной системы;

− корректировка проектной и эксплуатационной документации на систему защиты информации информационной системы.

3. Внедрение КСЗИ информационной системы

Внедрение КСЗИ информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

1. Установку и настройку средств защиты информации в информационной системе.
2. Разработку документов, определяющих правила и процедуры, реализуемые обладателем защищаемой информации для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (далее - организационно-распорядительные документы по защите информации).
3. Внедрение организационных мер защиты информации.
4. Предварительные испытания КСЗИ информационной системы.
5. Опытную эксплуатацию КСЗИ информационной системы.
6. Анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению.
7. Приемочные испытания КСЗИ информационной системы.

3.1. Установка и настройка средств защиты информации в информационной системе проводится в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и документацией на средства защиты информации.

3.2. Разрабатываемые организационно-распорядительные документы по защите информации определяют правила и процедуры:

− управления (администрирования) системой защиты информации информационной системы;

− выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;

− управления конфигурацией аттестованной информационной системы и КСЗИ информационной системы;

− контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

− защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

3.3. При внедрении организационных мер защиты информации осуществляются:

− реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;

− проверка полноты и детальности описания в организационно- распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер защиты информации;

− отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

3.4. Предварительные испытания КСЗИ информационной системы проводятся с учетом ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем» (далее - ГОСТ 34.603) и включают проверку работоспособности КСЗИ информационной системы, а также принятие решения о возможности опытной эксплуатации КСЗИ информационной системы.

3.5. Опытная эксплуатация КСЗИ информационной системы проводится с учетом ГОСТ 34.603 и включает проверку функционирования КСЗИ информационной системы, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации КСЗИ информационной системы.

3.6. Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем КСЗИ информационной системы и предотвращения реализации угроз безопасности информации и включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы.

При анализе уязвимостей информационной системы проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением.

В случае выявления уязвимостей информационной системы, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей.

3.7. Приемочные испытания КСЗИ информационной системы проводятся с учетом ГОСТ 34.603 и включают проверку выполнения требований к системе защиты информации информационной системы в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание КСЗИ информационной системы.

4. Аттестация информационной системы и ввод ее в действие

В качестве исходных данных, необходимых для аттестации информационной системы, используются модель угроз безопасности информации, акт классификации информационной системы, техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание КСЗИ информационной системы, проектная и эксплуатационная документация на систему защиты информации информационной системы, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационной системы, материалы предварительных и приемочных испытаний КСЗИ информационной системы.

Аттестация информационной системы проводится в соответствии с программой и методиками аттестационных испытаний до начала обработки информации, подлежащей защите в информационной системе. Для проведения аттестации информационной системы применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям о защите информации и аттестат соответствия в случае положительных

результатов аттестационных испытаний.

Повторная аттестация информационной системы осуществляется в случае окончания срока действия аттестата соответствия или повышения класса защищенности информационной системы. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании КСЗИ информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

Ввод в действие информационной системы осуществляется в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации и с учетом ГОСТ 34.601 и при наличии аттестата соответствия.

5. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется обладателем защищаемой информации в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает:

- управление (администрирование) системой защиты информации информационной системы;
- выявление инцидентов и реагирование на них;
- управление конфигурацией аттестованной информационной системы и ее КСЗИ;
- контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

5.1. В ходе управления (администрирования) системой защиты информации информационной системы осуществляются:

- заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе;
- управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;
- установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;
- централизованное управление системой защиты информации информационной системы (при необходимости);
- регистрация и анализ событий в информационной системе, связанных с защитой информации (далее - события безопасности);
- информирование пользователей об угрозах безопасности информации, о правилах эксплуатации КСЗИ информационной системы и отдельных средств защиты информации, а также их обучение;
- сопровождение функционирования КСЗИ информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации;

5.2. В ходе выявления инцидентов и реагирования на них осуществляются:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств

защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

− своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

− анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

− планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

− планирование и принятие мер по предотвращению повторного возникновения инцидентов.

5.3. В ходе управления конфигурацией аттестованной информационной системы и ее КСЗИ осуществляются:

− поддержание конфигурации информационной системы и ее КСЗИ (структуры КСЗИ информационной системы, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации информационной системы и ее КСЗИ);

− определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее КСЗИ;

− управление изменениями базовой конфигурации информационной системы и ее КСЗИ, в том числе определение типов возможных изменений базовой конфигурации информационной системы и ее КСЗИ, санкционирование внесения изменений в базовую конфигурацию информационной системы и ее КСЗИ, документирование действий по внесению изменений в базовую конфигурацию информационной системы и ее КСЗИ, сохранение данных об изменениях базовой конфигурации информационной системы и ее КСЗИ, контроль действий по внесению изменений в базовую конфигурацию информационной системы и ее КСЗИ;

− анализ потенциального воздействия планируемых изменений в базовой конфигурации информационной системы и ее КСЗИ на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность информационной системы;

− определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию информационной системы и ее КСЗИ;

− внесение информации (данных) об изменениях в базовой конфигурации информационной системы и ее КСЗИ в эксплуатационную документацию на систему защиты информации информационной системы;

− принятие решения по результатам управления конфигурацией о повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

5.4. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

− контроль за событиями безопасности и действиями пользователей в информационной системе;

− контроль (анализ) защищенности информации, содержащейся в информационной

системе;

− анализ и оценка функционирования КСЗИ информационной системы, включая выявление, анализ и устранение недостатков в функционировании КСЗИ информационной системы;

− периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

− документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

− принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) КСЗИ информационной системы, повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

6. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации

Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется обладателем защищаемой информации в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно- распорядительными документами по защите информации и в том числе включает:

1. Архивирование информации, содержащейся в информационной системе.
2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

6.1. Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности обладателя защищаемой информации.

6.2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

Оборудование и материалы

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор с тактовой частотой 3000МГц и выше, оперативная память − не менее 4 Гб и более, свободное дисковое пространство − не менее 1000 Мб, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов − 65535).

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система XP Professional и выше, библиотека Microsoft

.NET Framework версии 1.1 или выше, антивирусное ПО.

Указания по технике безопасности

При выполнении лабораторной работы **запрещается**:

− самостоятельно производить ремонт персонального компьютера, а также установку и удаление имеющегося программного обеспечения;

− нарушать общепринятые правила техники безопасности при работе с электрооборудованием, в частности, касаться электрических розеток металлическими предметами и т.д.;

− принимать пищу, напитки и сорить на рабочем месте пользователя персонального компьютера.

В случае неисправности персонального компьютера необходимо **немедленно** сообщить об этом обслуживающему персоналу лаборатории (системному администратору, оператору).

Содержание отчета

1. Титульная страница отчета.
2. Цель лабораторной работы.
3. Ответы на контрольные вопросы.
4. Описание выполненной работы.
5. Вывод.

Контрольные вопросы

1. Перечислите основные этапы построения КСЗИ.
2. Назовите ГОСТ с учётом которых должны быть разработаны требования к системе защиты информации.
3. Перечислите основные понятия которые будут определены при проектировании КСЗИ.
4. Перечислите основное содержание эксплутационной документации КСЗИ.
5. Перечислите этапы внедрения системы защиты информации.
6. Перечислите процессы выполняемые при обеспечении защиты информации в ходе эксплуатации аттестованной информационной системы.

Список индивидуальных тем

1. Банк
2. Больница
3. Юридическая фирма
4. Фирма, занимающаяся маркетинговыми исследованиями
5. Психологическая клиника
6. ЗАГС
7. УФМС
8. Казначейство
9. Радиозавод
10. Контора по ремонту и обслуживанию ПК
11. Налоговая инспекция
12. ВУЗ
13. УКЦ
14. Страховая компания
15. Дата-центр (ЦОД)
16. Интернет-провайдер
17. Сотовый оператор
18. Магазин бытовой техники
19. Аэропорт
20. Фирма по разработке ПО
21. Аптека
22. Склад, лучшее наверное система складских помещений
23. Железнодорожный вокзал
24. Электростанция

25. Управление дорожного хозяйства

Практическое занятие №28

Тема «Исследование возможностей системы оценки защищенности оптических линий связи»

Цель работы: изучить возможности системы оценки защищенности оптических линий связи

Задание: подготовить презентационный материал на тему «Методы оценки защищенности оптических линий связи»

Практическое занятие №29

Тема «Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН. (»

Цель работы: изучить возможности системы защищенности технических средств от утечки информации по каналу ПЭМИН

Задание: подготовить презентационный материал на тему «Методы оценки защищенности технических средств от утечки информации по каналу ПЭМИН»

Практическое занятие №30

Тема «Исследование возможностей системы оценки защищенности выделенных помещений»

Цель работы: изучить возможности системы оценки защищенности выделенных помещений

Задание: подготовить презентационный материал на тему «Методы оценки защищенности выделенных помещений»

Практическое занятие №31

Тема «Исследование возможностей индикаторов поля»

Цель работы.

Изучить работу и схему индикатора поля.

Теоретические сведения.

Характеристики индикатора поля.

Рабочая частота от 20 МГц до 1300 МГц.

Чувствительность 1 мВ.

Пределы локализации от 0,05 м до 7 м.

Напряжение питания от 4,5 В до 9 В.

Ток потребления 8 мА.

Тип антенны - телескопическая.

Схема индикатора поля (поискового прибора) показана на рисунке 108.

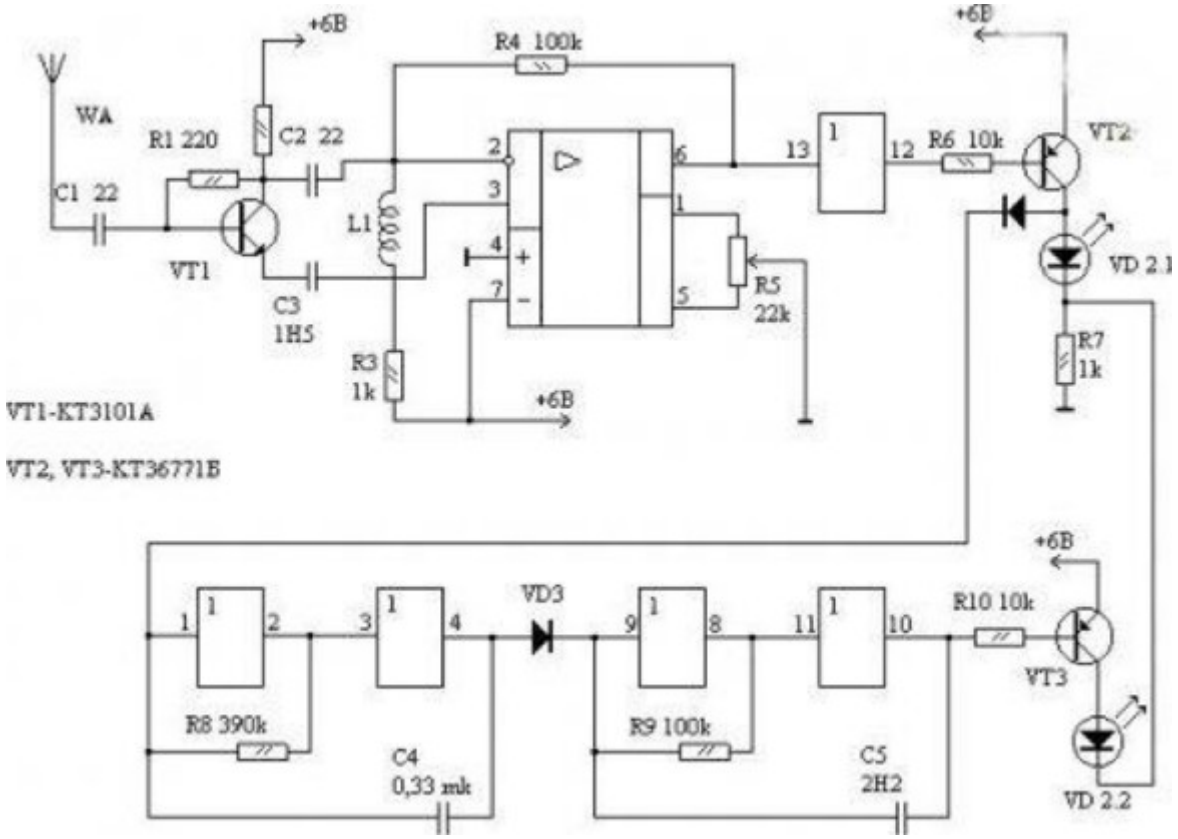


Рисунок 108 - Схема индикатора поля

Прибор удобно использовать для контроля за работой и настройки маломощных передающих устройств, работающих в широком диапазоне частот.

Это устройство предназначено для локального поиска радиозакладок. Его отличительными особенностями являются простота повторения, надежность, малые габариты. Недостаток - немного реагирует на посторонние излучения радиоэфира от телерадиопередающих станций, радиотелефонов.

Входной сигнал, наведенный телескопической антенной, поступает на входной усилитель ВЧ, построенный на транзисторе VT1, и далее, через фильтр С/, ***L/,*** Сз на детектор-компаратор DA1. Порог включения компаратора устанавливается резистором R_5. Сигнал компаратора с выхода 6 через инвертор DD1.3 и ключ VT2 управляет генератором прямоугольных импульсов на элементах DD1.4, DD1.5 с частотой 1 Гц, который, в свою очередь, включает генератор звуковой частоты на DD1.EDD1.2.

Светодиод VD1-двухцветный. VD1.1 сигнализирует о включении питания зеленым светом, VD2.2 - об обнаружении источника радиоизлучений красным.

Настройка прибора заключается в выборе ОУ DA1 с возможно большим коэффициентом усиления. Расстояние на котором индикатор должен устойчиво реагировать имея антенну длиной 30 см, на радиопередатчик мощностью 1 мВт, должно быть не менее 50 см.

Транзистор КТ3101 можно заменить на КТ371, КТ368 с коэффициентом усиления не менее 150. Операционный усилитель - К140УД608. К140УД708. Светодиод АЛС331 можно заменить обычными, типа АЛ307, включив их вместо VD1.1 и VD1.2. Катушка индуктивности имеет 19 витков, намотанных в ряд на любом резисторе МЛТ 0,125, проводом ПЭЛ-0,1.

Содержание отчета.

- 1. Цель работы.
- 2. Исследуемые схемы.
- 3. Принцип работы индикатора поля.
- 4. Выводы.

Практическое занятие №32

Тема «Поиск и локализация скрытых видеокамер»

Цель работы: изучить возможности устройства для поиска и локализация скрытых видеокамер

Задание: разработать инструкцию пользователя устройства для поиска и локализация скрытых видеокамер

Практическое занятие 33

Тема «Исследование методов защиты сотовых телефонов от несанкционированного прослушивания»

Цель работы: изучить методы и возможности устройств защиты сотовых телефонов от несанкционированного прослушивания

Задание: подготовить презентационный материал на тему «Методы защиты сотовых телефонов от несанкционированного прослушивания»

Практическое занятие №34

Тема «Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов »

Цель работы: изучить методы и возможности устройств блокирования средств несанкционированного прослушивания и передачи данных различных стандартов

Задание: подготовить презентационный материал на тему «Методы блокирования средств несанкционированного прослушивания и передачи данных различных стандартов»

Практическое занятие №35

Тема «Оценка защищенности помещения с помощью многофункционального поискового прибора»

Цель работы: изучить методы оценки защищенности помещения с помощью многофункционального поискового прибора

Задание: подготовить презентационный материал на тему «Оценка защищенности помещения с помощью многофункционального поискового прибора»

Практическое занятие №36

Тема «Исследование методов криптографической защиты информации»

Цель работы: Изучить различные методы криптографической защиты информации

Задание: Описать работу и привести примеры следующих методов криптографической защиты информации:

- шифрование данных методами подстановки, перестановки и полиалфавитными шифрами;
- шифр гаммирования;
- сеть Фейштеля;
- алгоритм RSA;
- создание электронной подписи в документе;
- защита графического файла с помощью цифрового водяного знака;
- реализация протокола ДиффиХеллмана на эллиптических кривых.

Содержание отчета:

- описание используемого метода,
- описание исходных данных,
- алгоритм работы программы,

- текст программы,
- результаты работы программы,

Практическое занятие №37

Тема «Исследование работы генератора шума по сети электропитания и линиям заземления»

Цель работы: изучить возможности генератора шума по сети электропитания и линиям заземления

Задание: разработать инструкцию пользователя генератора шума по сети электропитания и линиям заземления

Практическое занятие №38

Тема «Поиск и обнаружение радиоизлучающих средств»

Цель работы: изучить методы и возможности устройств поиска и обнаружения радиоизлучающих средств

Задание: подготовить презентационный материал на тему «Поиск и обнаружение радиоизлучающих средств»

Практическое занятие №39

Тема «Разработка инструкции по аттестации объектов информатизации»

Цель работы: закрепление теоретических знаний по вопросам аттестации помещений по требованиям безопасности информации.

Учебные вопросы:

1. Система объектов информатизации по требованиям безопасности информации.
2. Виды аттестации помещений по требованиям безопасности информации.
3. Особенности проведения аттестации помещений по требованиям безопасности информации.

Задание: разработать инструкцию по аттестации объектов информатизации.

Объект информатизации: АПОУ УР «ТРИТ им. А.В. Воскресенского»