Лабораторная работа №6 "Настройка механизма дискреционного управления доступом"

Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в ИС, а столбцами — объекты (ресурсы) ИС. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

Данный метод предоставляет более унифицированный и удобный подход, так как вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и неоптимальность (большинство клеток — пустые). Фрагмент матрицы установления полномочий показан в табл. 1.

Таблица 1.

Фрагмент матрицы установления полномочий

Субъект	Каталог d:\Heap	Программа prty	Принтер
Пользователь 1	cdrw	x	w
Пользователь 2	r		w с 9:00 до 17:00

Где: c – создание, d – удаление, r – чтение, w – запись, x – выполнение.

ЗАДАНИЕ

Установите права дискреционного доступа для пользователей "user1", "user2" и "user3" в соответствии с матрицей разграничения доступа (Табл. 2).

Таблица 2.

Матрица разграничения дискреционного доступа

Субъект	**Объект**		
	text.txt	***text1.txt***	***text2.txt***
user1	rx	r	Полный доступ
user2	-	rwx	-
user3	Полный доступ	-	rwx

ХОД РАБОТЫ

1. Перезагрузите компьютер и загрузите ОС под учетной записью администратора .

2. Создайте защищаемые ресурсы: C:\SNДУД\text.txt; C:\SNДУД\text1.txt; C:\SNДУД\ text2.txt (Рис. 1).

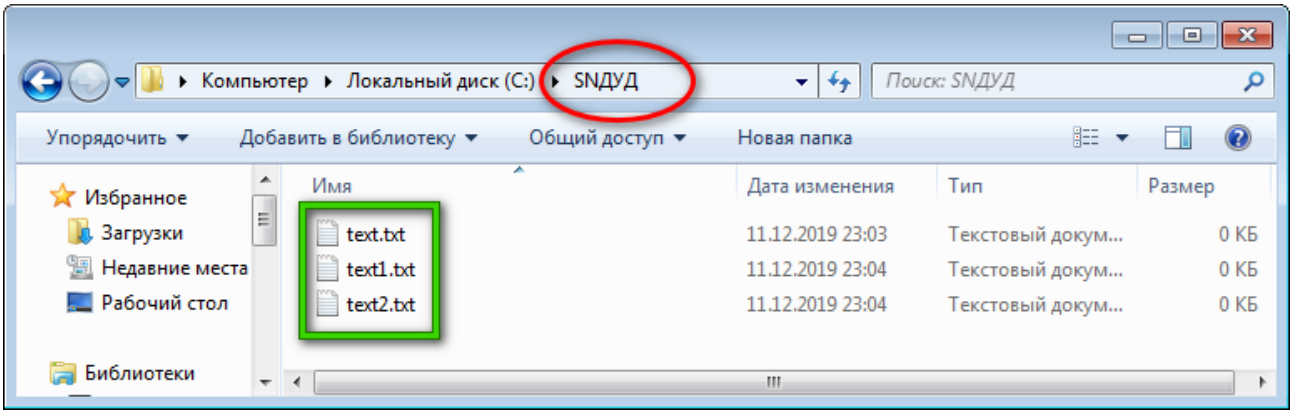

Рис. 1. Защищаемые ресурсы.

3. Для параметров, для которых не задано явное разрешение, установите явный запрет в соответствии с заданием. Для этого откройте "Свойства" файла (например, C:\SNДУД\text.txt) и откройте вкладку Secret Net. Снимите, если есть, галочку "Наследовать настройки доступа от родительского объекта" и нажмите кнопку "Разрешения" (Рис. 2).

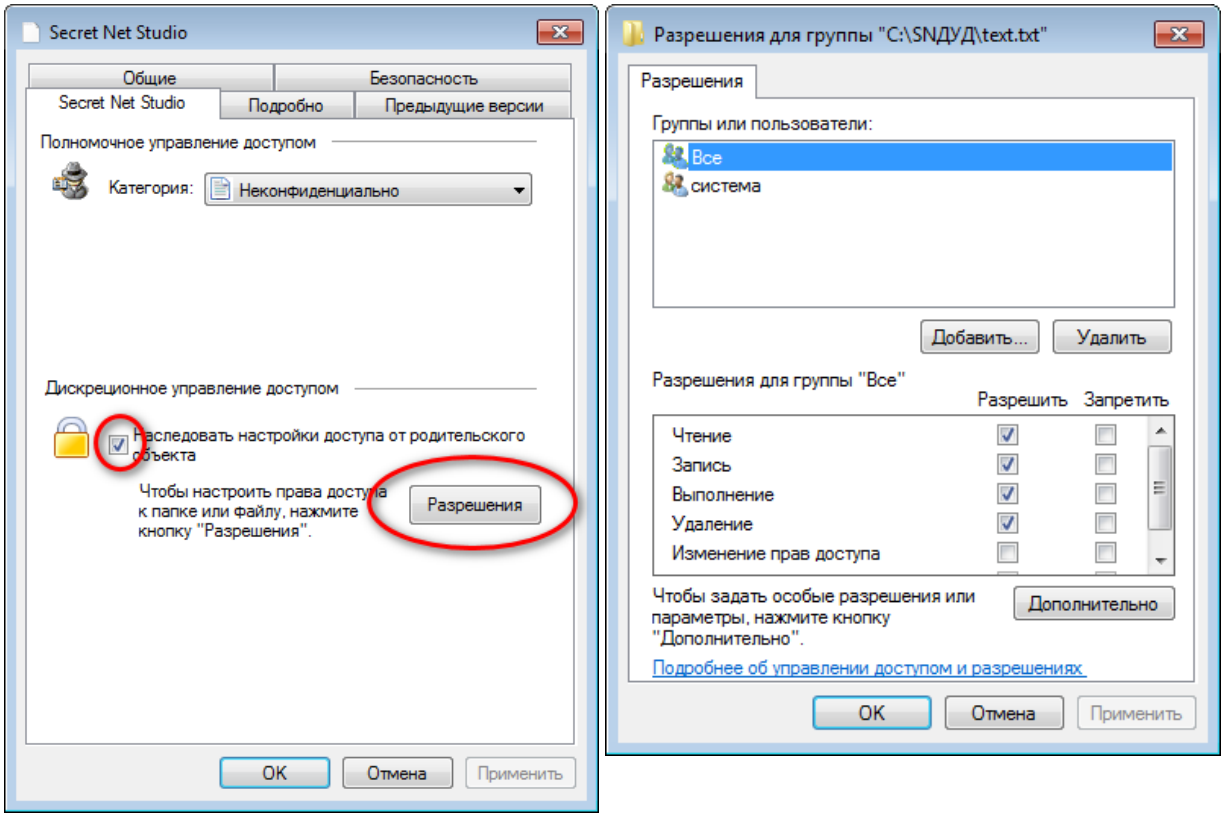

Рис. 2. Настройка разрешений.

4. Удалите группы "Все", «Система» и добавьте пользователя "user1". Для этого нажмите кнопку «Добавить», затем кнопку «Дополнительно» и выполните поиск. Выберите пользователя и нажмите кнопку «OK» (Рис. 3).

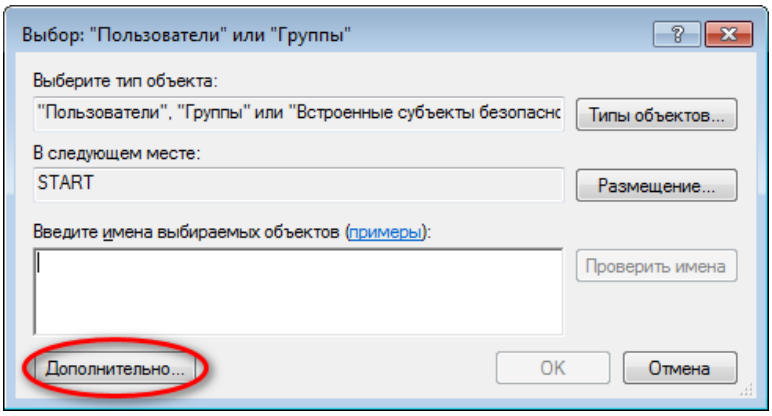

Рис. 3. Добавление пользователя.

5. Установите пользователю "user1" права в соответствии с заданием и нажмите кнопку "Применить" (Рис. 4).

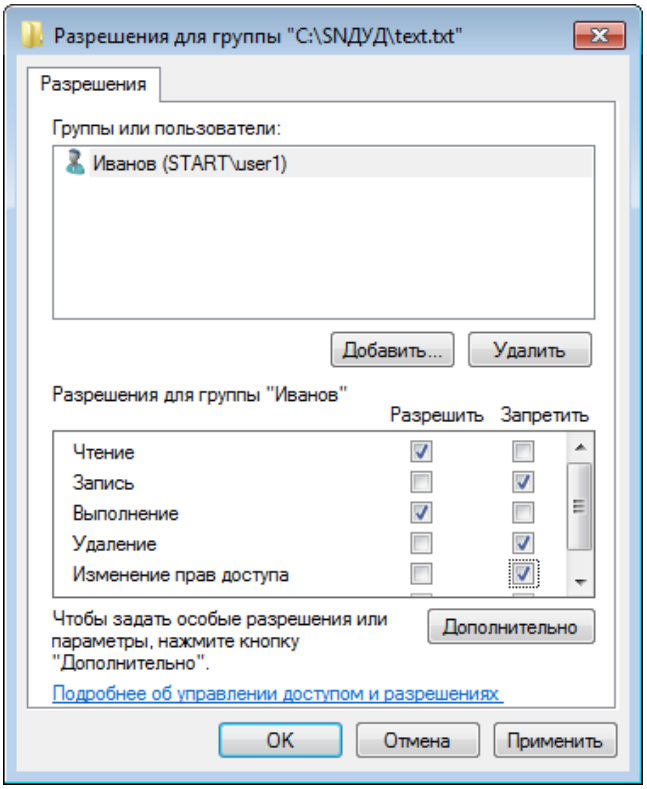

Рис. 4. Настройка прав.

Поскольку "user1" является членом группы пользователей компьютера, топоявится сообщение Windows, предупреждающее, что заданная в Secret Net политика запрета приоритетная и "user1", несмотря на то что группе "Пользователи" разрешена запись файла и удаление, не будет иметь разрешения на данные действия (Рис. 5).

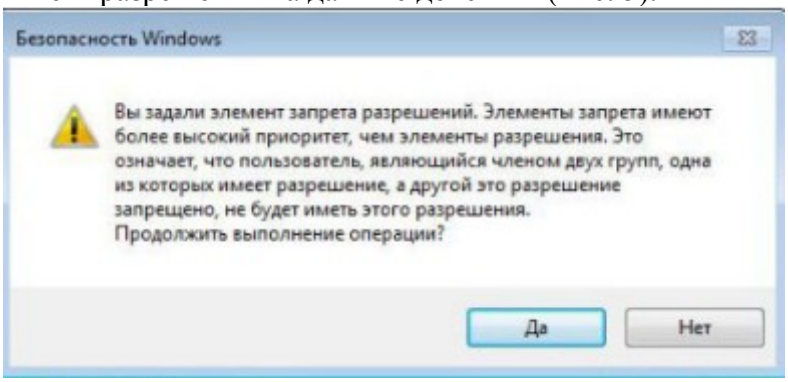

Рис. 5. Окно предупреждения.

6. Настройте аудит для файла "text.txt". Для этого нажмите кнопку "Дополнительно". В появившемся окне откройте вкладку "Аудит" (Рис. 6).

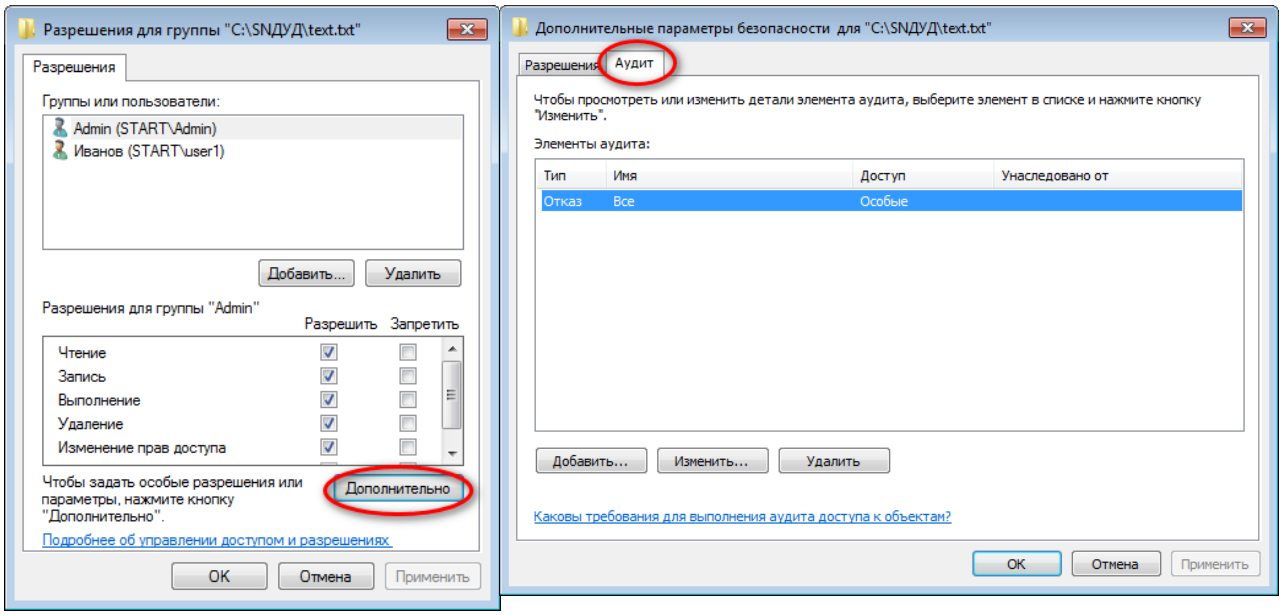

Рис. 6. Настройка «Аудита».

7. Удалите аудит успеха для всех и добавьте аудит отказа для пользователей. Для добавления нажмите кнопку "Добавить → ДополнительноРис. 1. Защищаемые ресурсы. → Поиск". В появившемся перечне пользователей и групп выберите группу "Пользователи", затем нажмите кнопку "ОК". Выставьте необходимый аудит отказа и нажмите кнопку "ОК".

8. Завершите работу программы.

9. Проделайте аналогичные действия для установки дискреционного доступа по данным матрицы к остальным ресурсам и для остальных пользователей.

10. Перезагрузите компьютер. Выполните идентификацию пользователем "user1". Убедитесь, что пользователю "user1" доступны только разрешенные действия с ресурсами.

11. Выполните идентификацию пользователем "user2". Убедитесь, что пользователю "user1" доступны только разрешенные действия с ресурсами.

12. Выполните идентификацию пользователем "user3". Убедитесь, что пользователю "user1" доступны только разрешенные действия с ресурсами.

Если у пользователя нет разрешения на действия с файлом, то появится сообщение об отказе в доступе (Рис. 7).

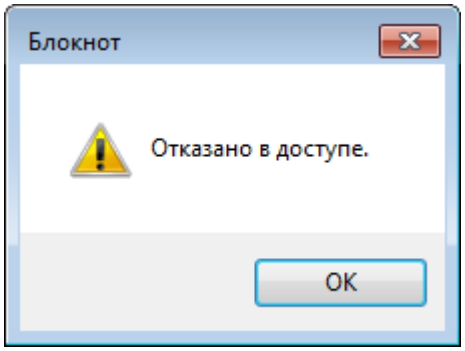

Рис. 7. Сообщение об отказе в доступе.

13. Откройте журнал Secret Net и ознакомьтесь с записями журнала.