**Министерство науки и высшего образования Российской Федерации**

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий Дисциплина:**

«Программно-аппаратные средства защиты информации»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 4**

**“Системы обеспечения информационной безопасности от НСД. Secret Net”**

**Выполнил:**

Ахраров Али, студент группы N3350



(подпись)

**Проверил:**

Калабишка Михаил Михайлович

(подпись)

**Санкт-Петербург 2024**

Оглавление

[1 Введение 3](#_Toc182593485)

[1.1 Цель и задачи 3](#_Toc182593486)

[2 Ход работы 4](#_Toc182593487)

[2.1 Вход в систему в качестве администратора и изучения параметров системы 4](#_Toc182593488)

[2.2 Предварительная настройка параметров полномочного управления доступом 6](#_Toc182593489)

[2.3 Установка категорий конфиденциальности для Folder1 7](#_Toc182593490)

[2.4 Настройка параметров избирательного разграничения доступом 12](#_Toc182593491)

[2.5 Попытка изменения доступа на Системный диск С 15](#_Toc182593492)

[2.6 Предварительная настройка механизма замкнутой програмной сре- ды 16](#_Toc182593493)

[3 Заключение 19](#_Toc182593494)

[Список литературы 20](#_Toc182593495)

# Введение

## Цель и задачи

Для организации эффективной совместной работы пользователей и обеспечения на- дежной защиты ресурсов компьютера от несанкционированного доступа в системе Secret Net 5.1 используются следующие механизмы управления доступом пользователей к ресур- сам компьютера:

* + - механизм избирательного управления доступом;
    - механизм полномочного управления доступом;
    - механизм замкнутой программной среды (ЗПС).

# Ход работы

## Вход в систему в качестве администратора и изучения параметров системы

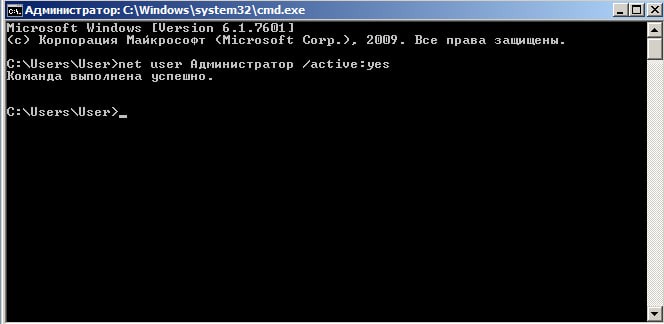


Рис. 1: Активация учетной записи администратора

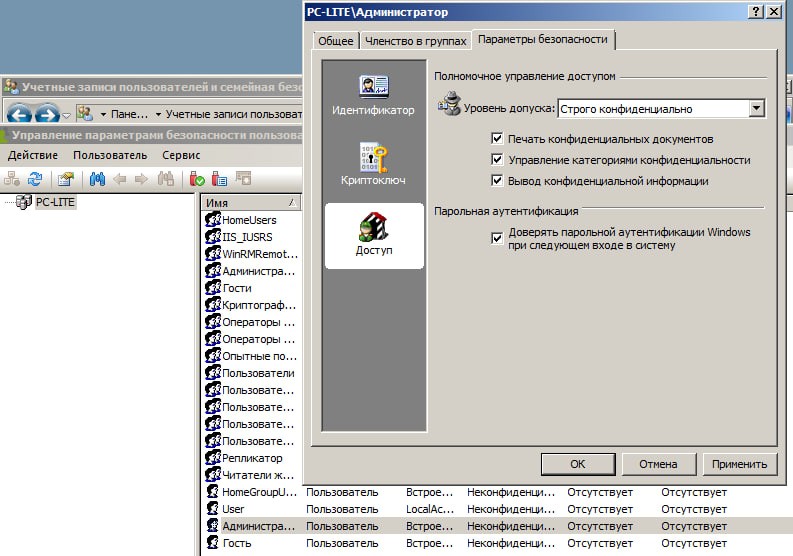


Рис. 2: Назначения максимальных прав администратору

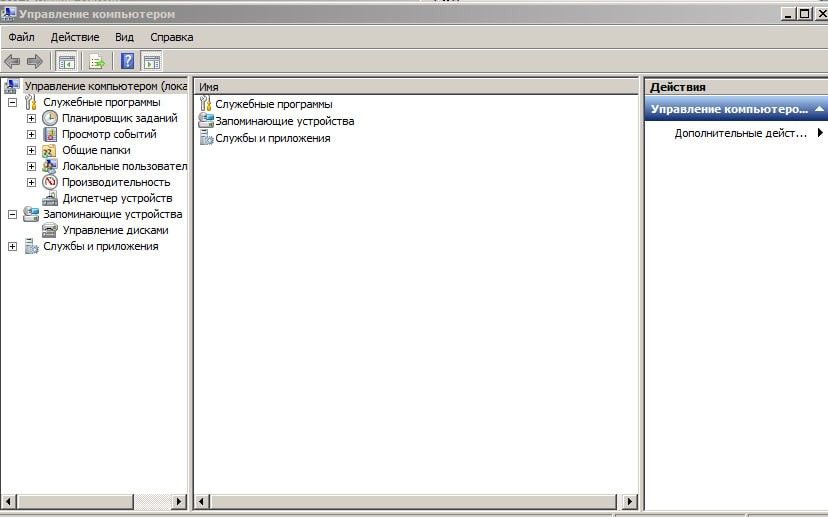


Рис. 3: Оснастка для управления параметрами компьютера

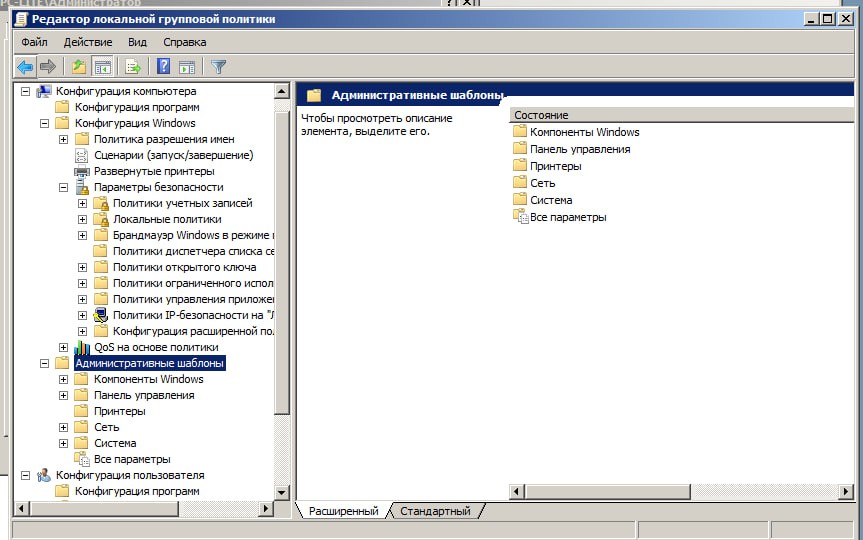


Рис. 4: Групповые политики

Основываясь на анализе инструментов для настройки параметров объектов групповой политики и компьютера, можно заключить, что на рабочей станции уже зада- ны базовые настройки системы по умолчанию, которые обеспечивают общую безопасность системы.

## Предварительная настройка параметров полномочного управления доступом

На диске C создадим иерархию каталогов: Folder1, Folder2, Folder3, Folder4.

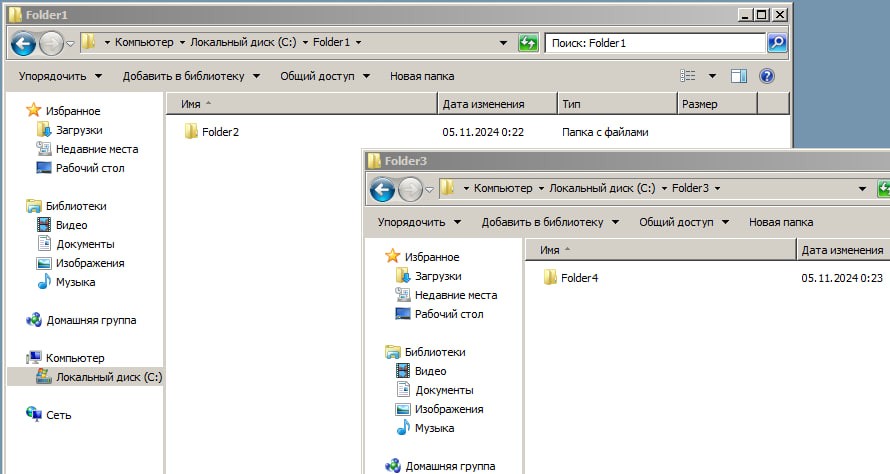


Рис. 5: Создание иерархий каталогов

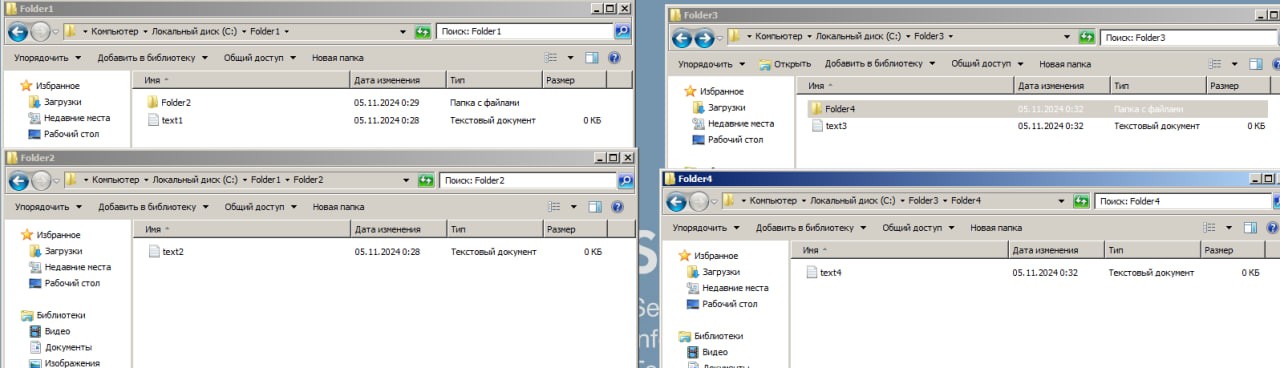


Рис. 6: Создание файлов в каталогах

Чтобы управлять конфиденциальной информацией, изменим уровень допуска

пользователя.

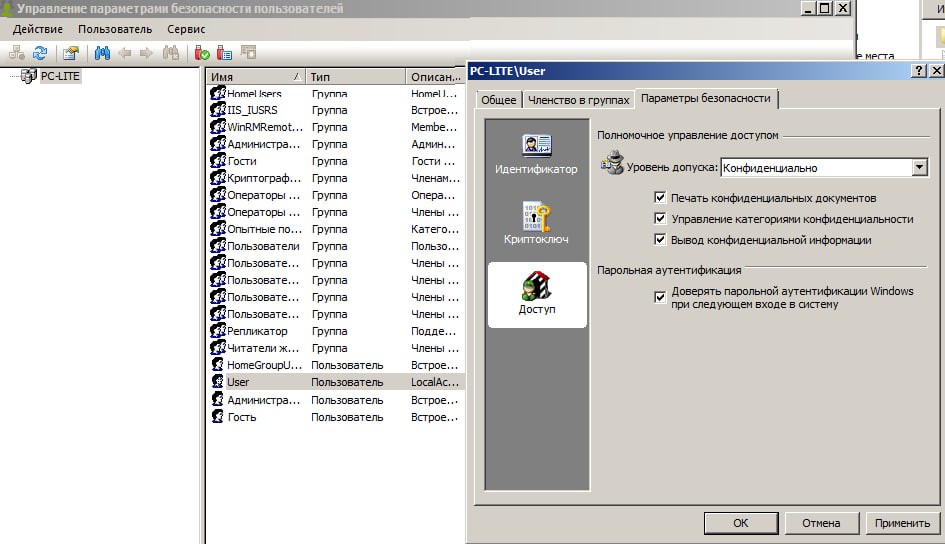


Рис. 7: Установка уровня допуска для пользователя

## Установка категорий конфиденциальности для Folder1

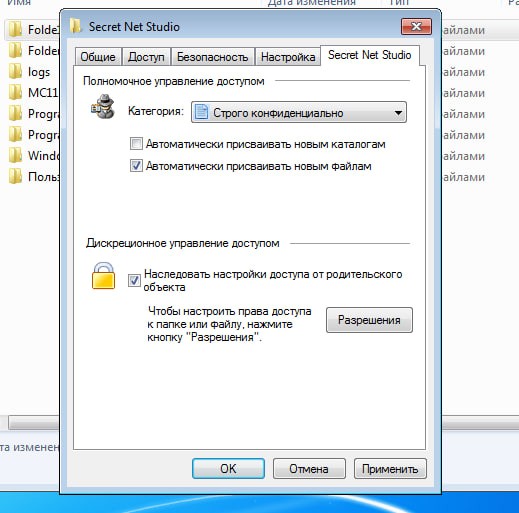
Папки Folder1 и Folder2, а также все файлы, которые в них содержатся, имеют наи- высший уровень конфиденциальности — «строго конфиденциально». Для этих папок уста- новлена опция автоматического присвоения такой же категории конфиденциальности вновь создаваемым файлам.

Рис. 8: Категории конфиденциальности для Folder1

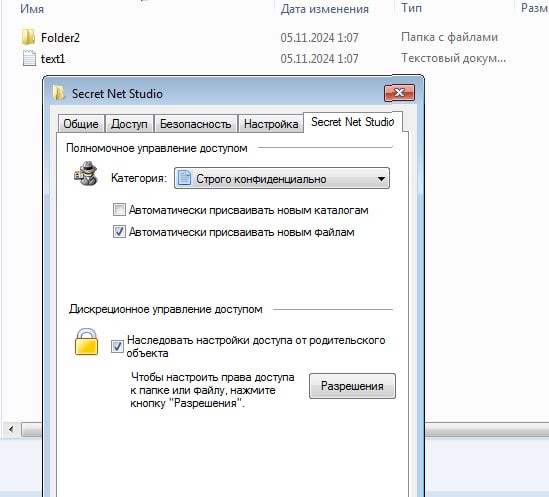


Рис. 9: Категории конфиденциальности для Folder2

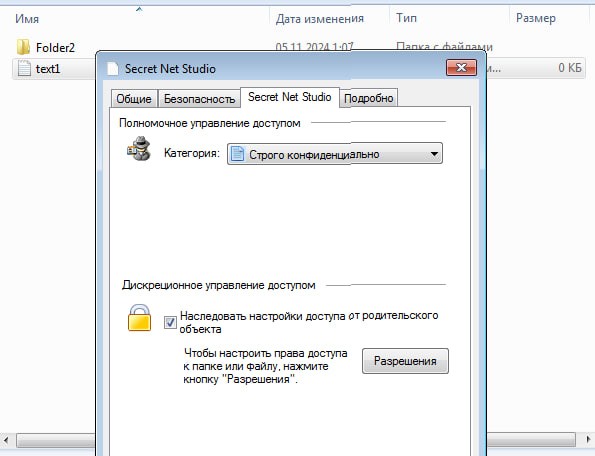


Рис. 10: Категория конфиденциальности для text1

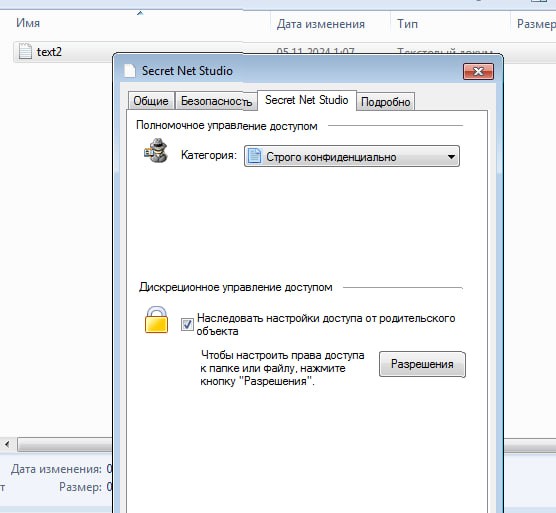


Рис. 11: Категория конфиденциальности для text2

Папка Folder3 и содержащийся в ней файл имеют категорию конфиденциаль- ности «конфиденциально». В настройках папки 3 отмечено, что новые файлы будут автома- тически иметь такую же категорию.

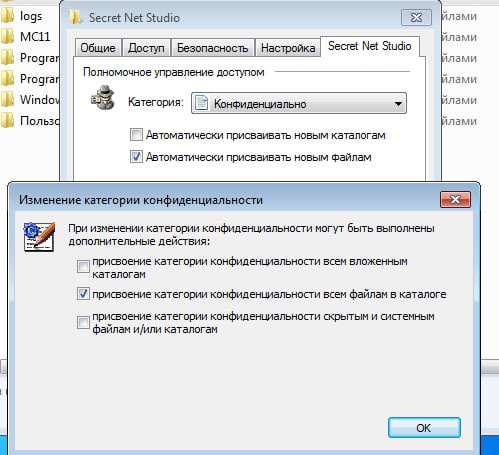


Рис. 12: Категория конфиденциальности для Folder3

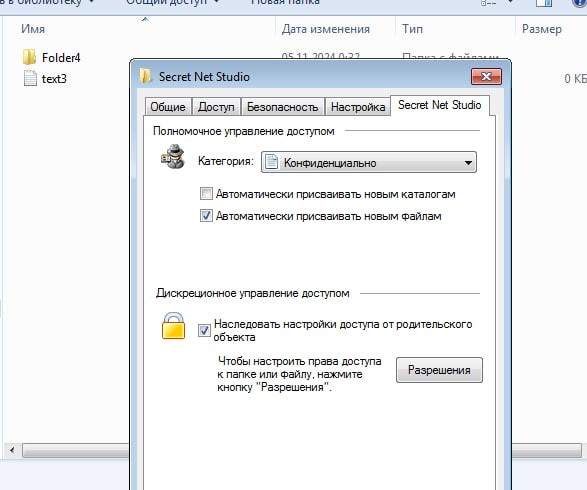


Рис. 13: Категория конфиденциальности для text3

Folder4 и входящий в него файл имеют категорию конфиденциальности –

«неконфиденциально».

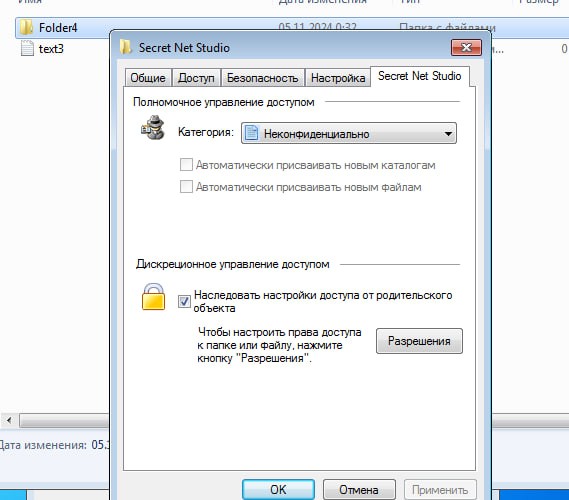


Рис. 14: Категория конфиденциальности для Folder4

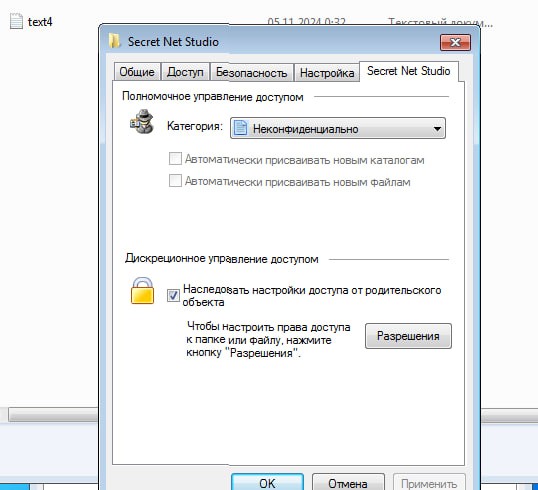


Рис. 15: Категория конфиденциальности для text4

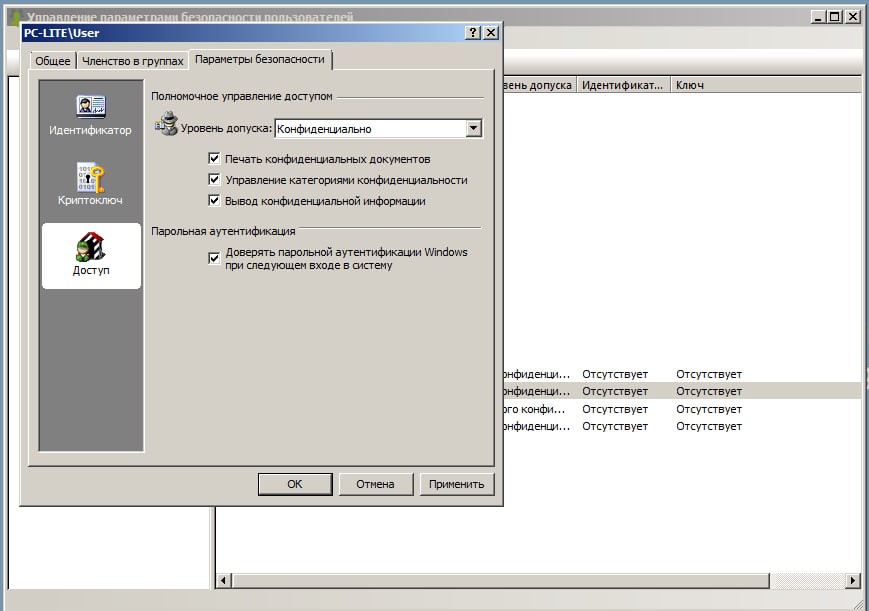


Рис. 16: Предоставление пользователю user доступа к конфиденциальности

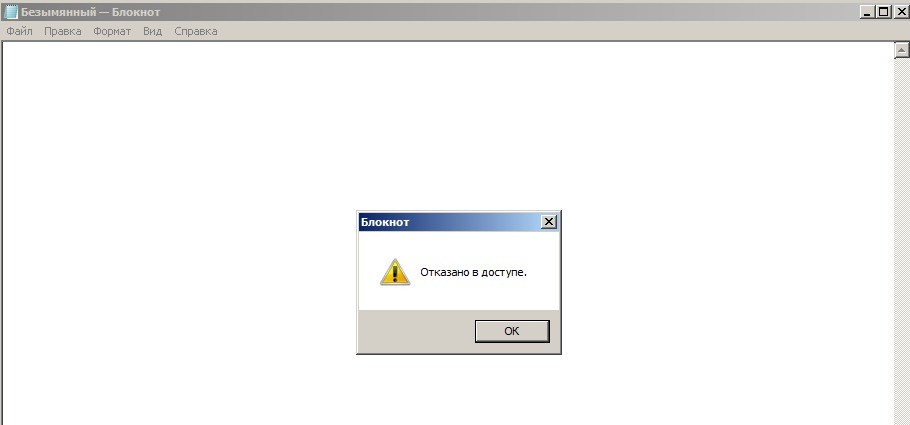


Рис. 17: Попытка доступа пользователя с уровнем ниже

## Настройка параметров избирательного разграничения доступом

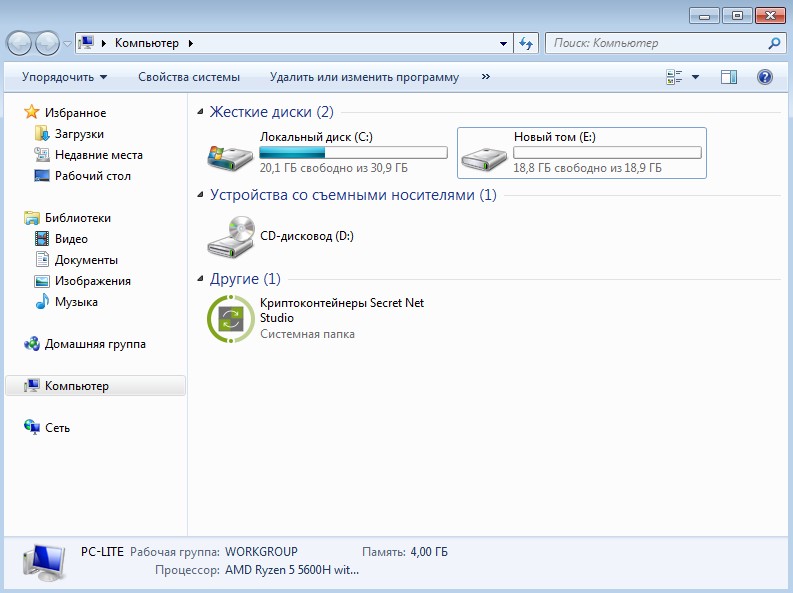


Рис. 18: Добавим новый жесткий диск

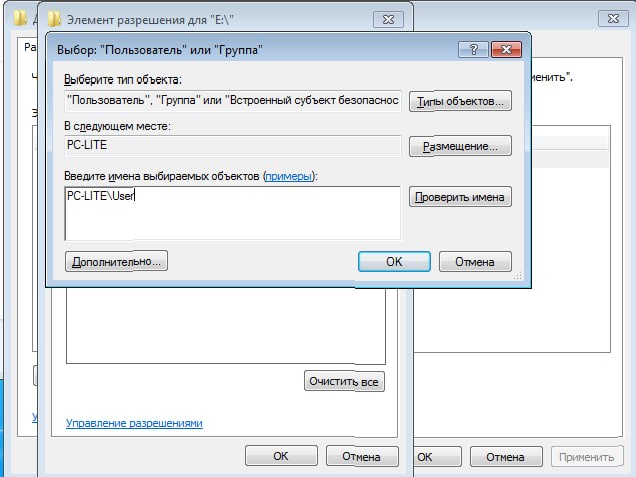


Рис. 19: Указание пользователя User в натройках доступа к новому диску

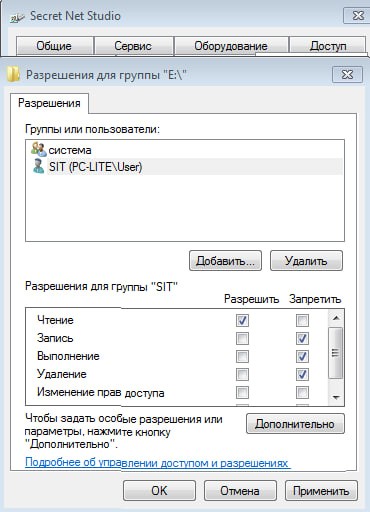


Рис. 20: Разрешения только на чтения для пользователя User для нового диска

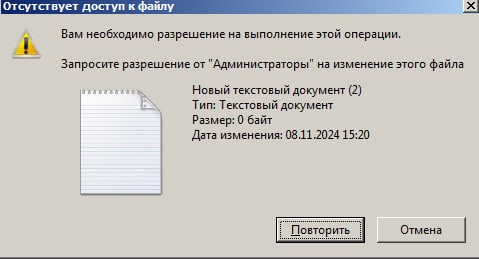


Рис. 21: Попытка удалить файл на диске Е от лица пользователя User

## Попытка изменения доступа на Системный диск С

Как мы видим поменять права на системный диск С невозможно:

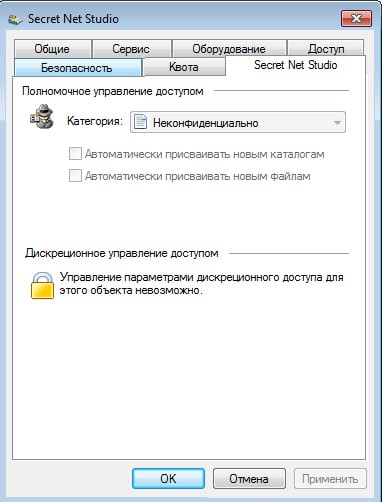


Рис. 22: Попытка смены прав доступа на системный диск С

## Предварительная настройка механизма замкнутой програмной сре- ды

Настроим запрет на приложение ”Калькулятор”.

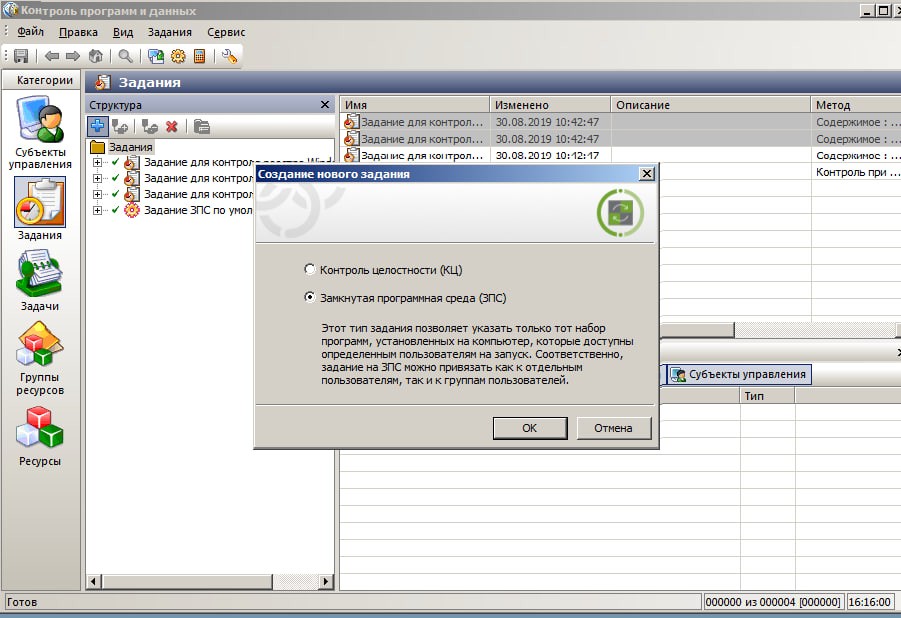


Рис. 23: Создание ЗПС

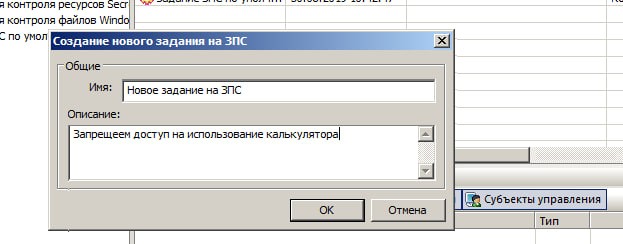


Рис. 24: Создание задания

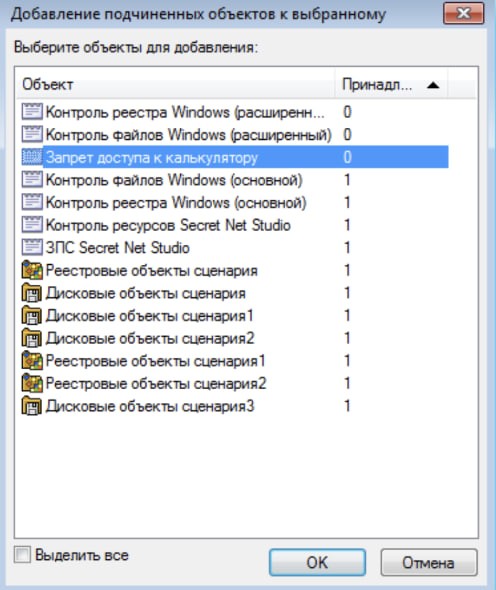


Рис. 25: Подключения задания

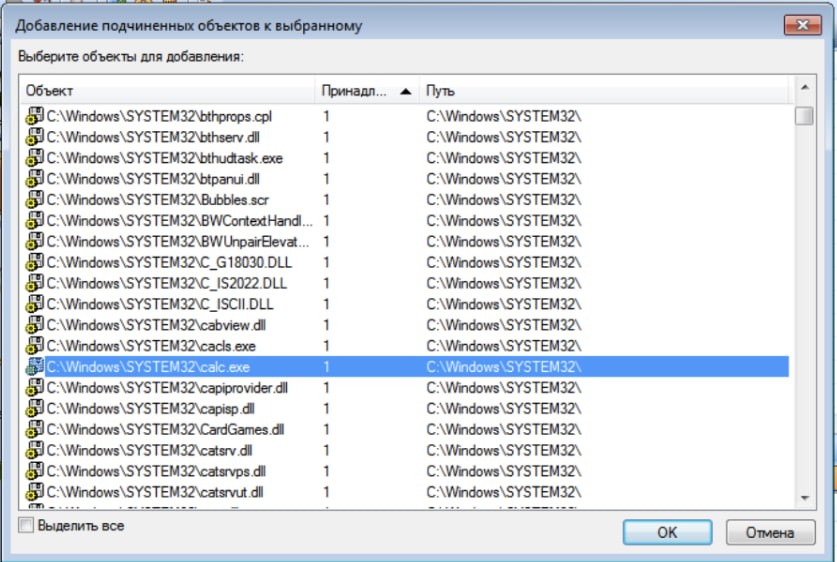


Рис. 26: Добавление ресурсов

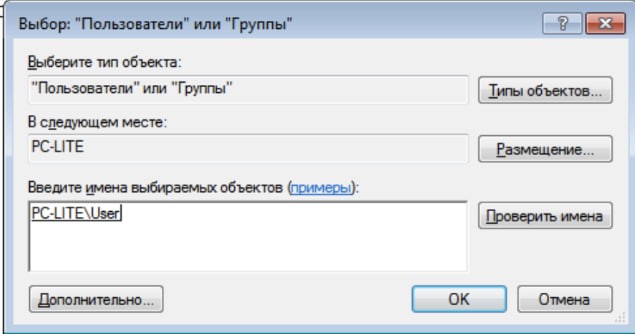


Рис. 27: Добавление субъекта

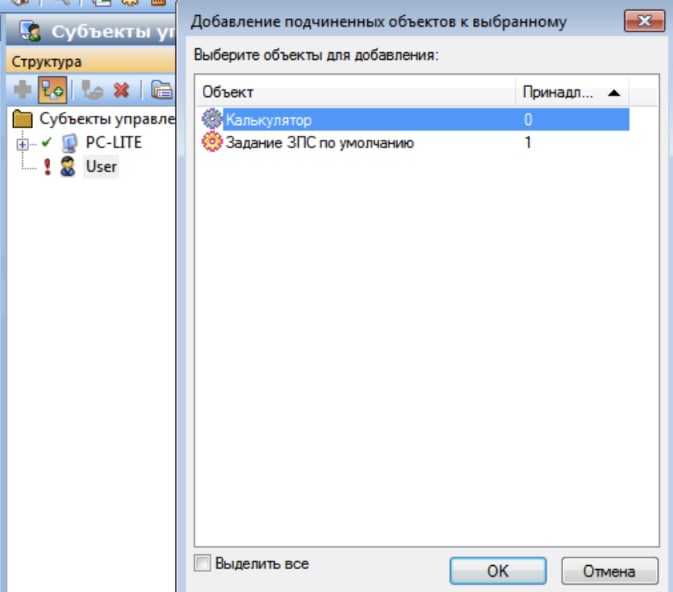


Рис. 28: Добавление задания пользователю

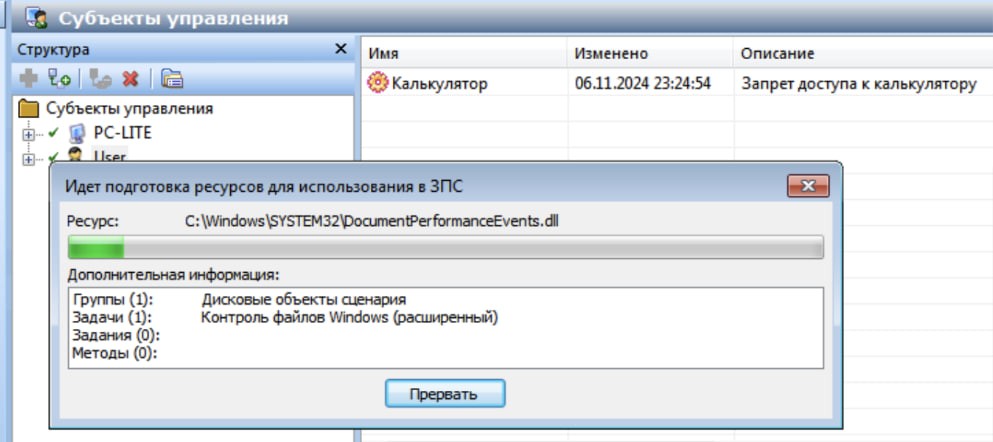


Рис. 29: Подготовка ресурсов для использования ЗПС

# Заключение

В ходе лабораторной работы мы познакомились с программой Secret Net. Мы научились управлять конфиденциальностью каталогов и рассмотрели функции защиты си- стемного диска. Кроме того, мы настроили замкнутую программную среду с ограниченным доступом для пользователей.

# Список литературы

1. Secret Net Руководство по эксплуатации.