**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 №3

«Системы обеспечения информационной безопасности от НСД. Secret Net»

**Выполнили:**

Суханкулиев Мухаммет,

студент группы N3346

_____

(подпись)

Бардышев Артём Антонович,

студент группы N3346

_____

(подпись)

**Проверил:**

Чешев Никита Игоревич

_____

(отметка о выполнении)

_____

(подпись)

Санкт-Петербург

2025 г.

**СОДЕРЖАНИЕ**

# ВВЕДЕНИЕ

Цель работы – изучить и практически настроить в Secret Net 5.1 мандатное разграничение (категории и допуски), дискреционный контроль доступа к устройствам и замкнутую программную среду, проверив действие политик на тестовых объектах и пользователях.

Для достижения поставленной цели были решены следующие задачи:

- Подготовлены тестовые учётные записи и структура каталогов/файлов на NTFS.
- Настроены категории конфиденциальности и режим «Автоматически присваивать новым файлам».
- Назначен уровень допуска пользователю и проверено влияние на доступ к объектам.
- Реализован дискреционный контроль доступа к устройствам (право «Чтение» на D:, защита системного C:).
- Включена замкнутая программная среда; создано задание, задача и группа ресурсов.
- Сформирован «белый список» исполняемых файлов; подготовлены ресурсы ЗПС.
- Проанализированы журналы безопасности; применены фильтры (неделя/месяц/год) и выполнен экспорт.
- Создана отчётная сводка по назначенным правам/параметрам.
- Сформулированы выводы о корректности настроек и их соответствии требованиям.

# 1 SECRET NET

Для выполнения лабораторной работы была использована предоставленная виртуальная машина с предустановленной ОС Windows 7 и СЗИ от НСД Secret Net 5.1. Вход в систему осуществлялся под учетной записью администратора admin.

На рабочей станции установлена и функционирует система защиты информации Secret Net Studio. Рабочая станция работает в локальном режиме, управление осуществляется через SNS ЛЦУ. В составе системы активированы следующие подсистемы: функциональный контроль, блокировка, вход в систему, дискреционное управление, затирание данных, контроль устройств, замкнутая программная среда, полномочное управление, контроль печати, защита дисков и шифрование, межсетевой экран, обнаружение вторжений, антивирус (подсистема не установлена), паспорт ПО. Вход в систему выполняется пользователем PC-LITE\User с правами администратора. Аутентификация – стандартная, идентификация – смешанная. Служба Secret Net загружена, конфигурация функционирует корректно. Система готова к дальнейшей настройке политик безопасности и выполнению последующих заданий лабораторной работы.

## 1.1 Подготовка окружения и пользователя

В среде Windows 7 подготовим тестовое окружение:

- проверяем работоспособность служб Secret Net 5.1

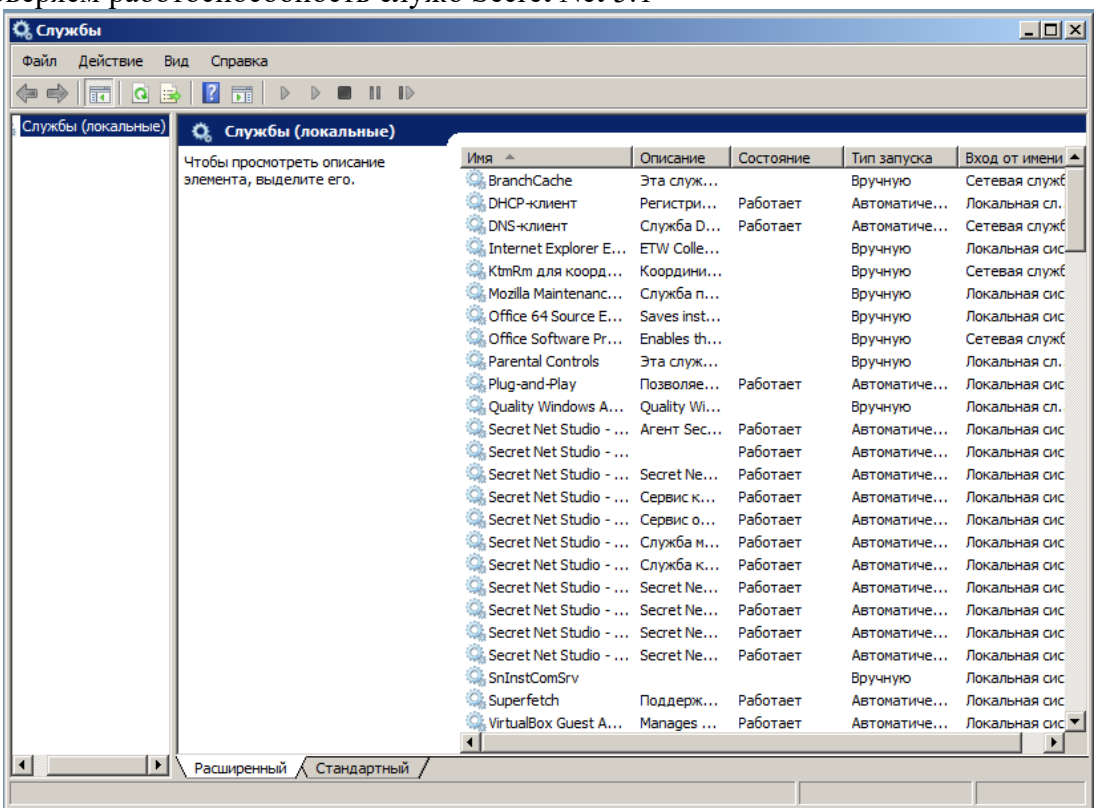

Рисунок 1 – Учетные записи существующие в системе

- создаем тестовую учётную запись user1 (обычный пользователь без административных прав). Учётная запись используется для проверки действия политик мандатного и дискреционного разграничения, а также замкнутой программной среды (ЗПС).

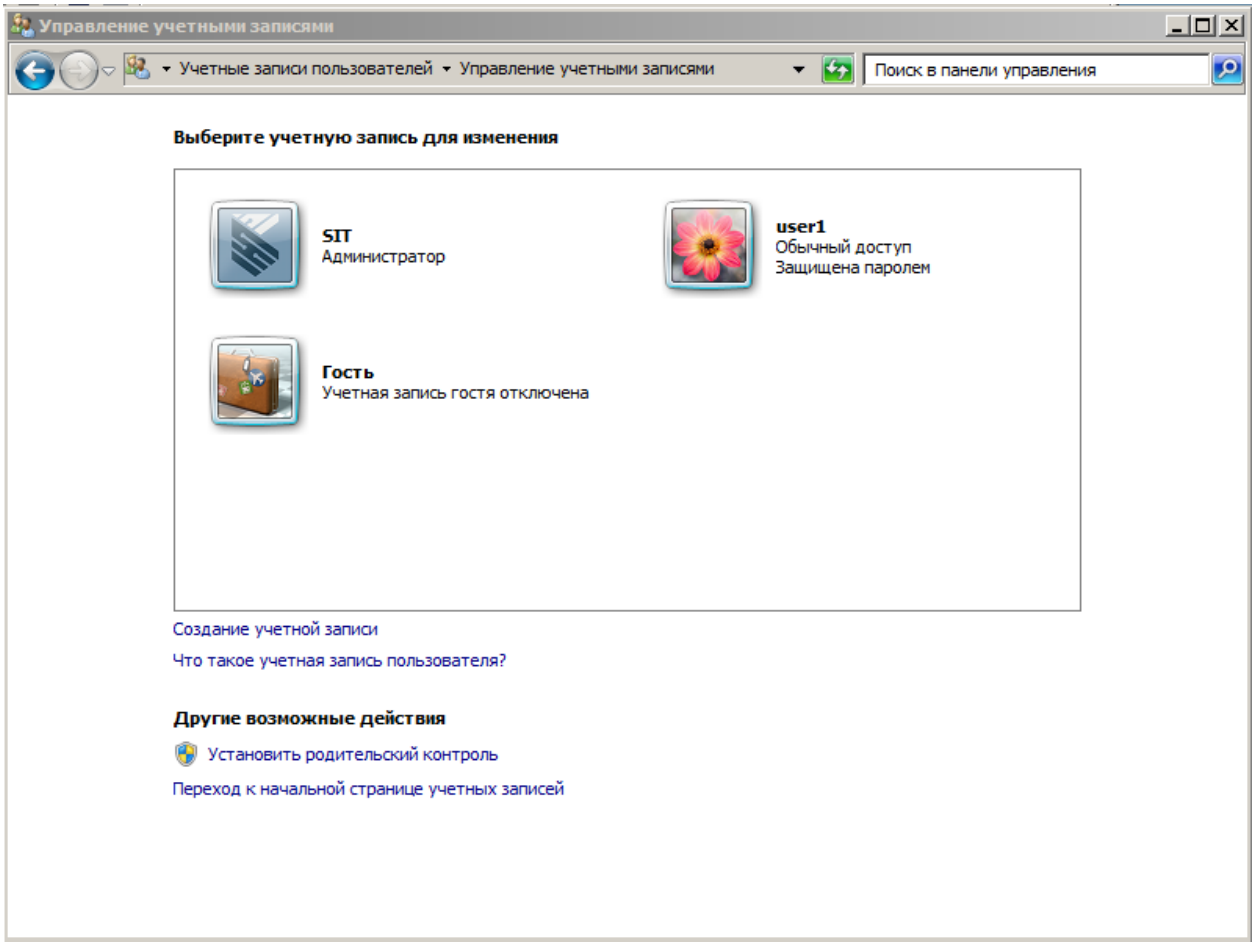


Рисунок 2 – Учетные записи существующие в системе

Учетная запись Гость – отключена, она не потребуется.

# 2 МАНДАТНАЯ МОДЕЛЬ

## 2.1 Создание структуры каталогов и файлов

Создаем эталонную структуру каталогов и файлов для проверки наследования категорий конфиденциальности и действия режима «Автоматически присваивать новым файлам»: C:\1\2, C:\3\4, файлы 1.txt, 2.txt, 3.txt, 4.txt.

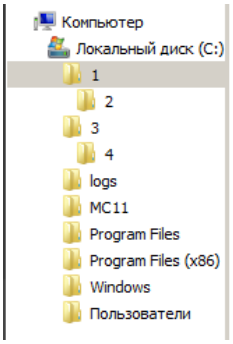


Рисунок 3 – Дерево папок в проводнике

## 2.2 Настраиваем категории конфиденциальности

Так как в мандатном доступе у администратора должен быть уровень схож или выше того, что он назначает, нам необходимо проверить данный факт. В настройках SNS УП можно увидеть, что мы обладаем слишком малым грифом – изменим это.

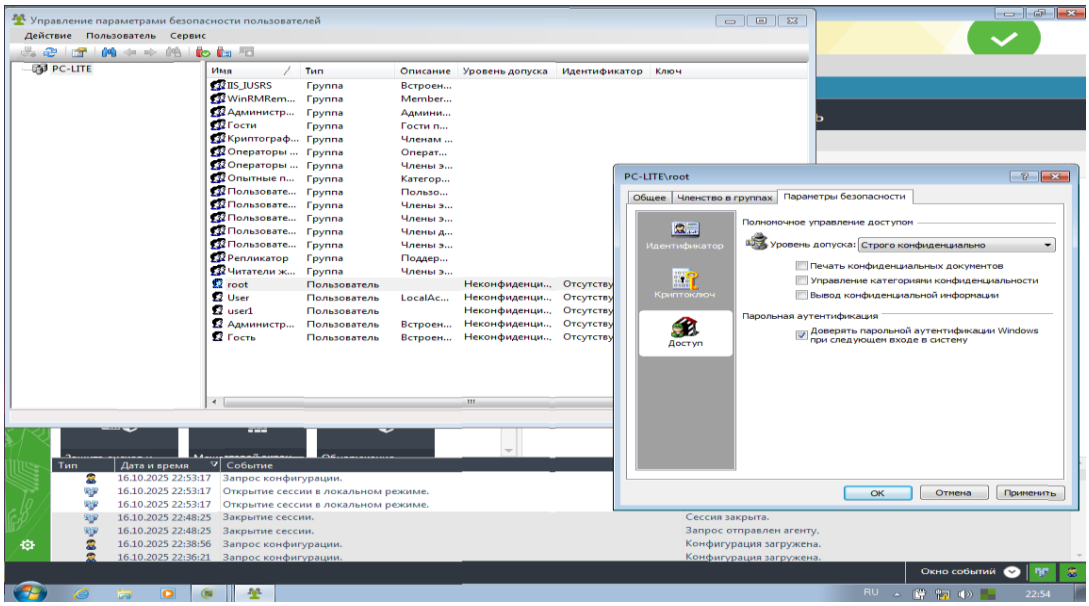


Рисунок 4 – Мандатный доступ пользователя

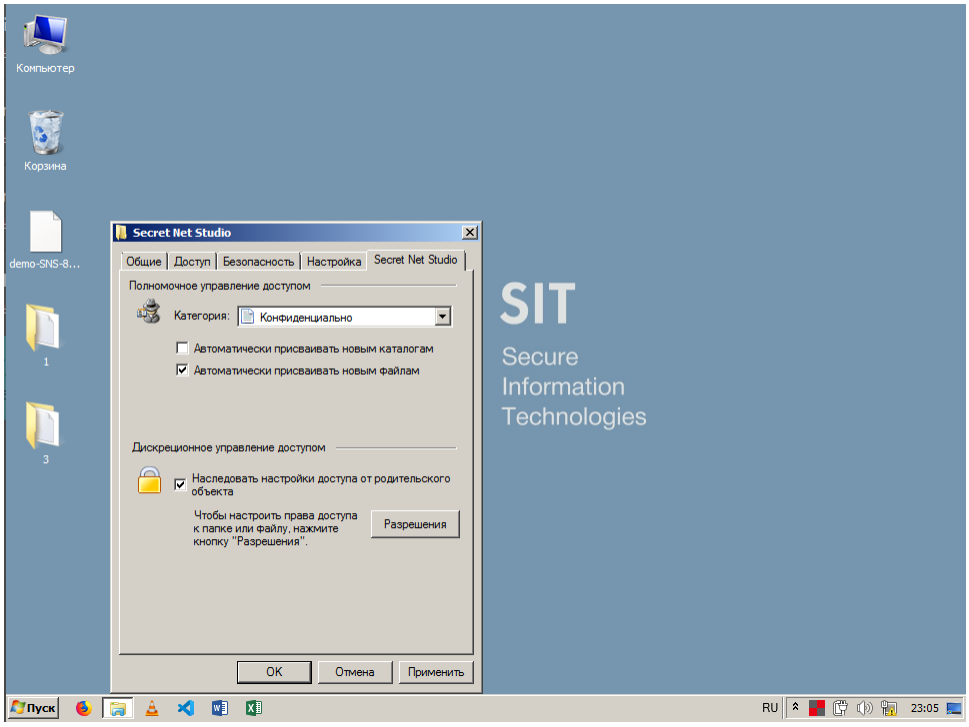


Рисунок 5 – C:\1 помечаем как «конфиденциально» с автоприсвоением новым файлам

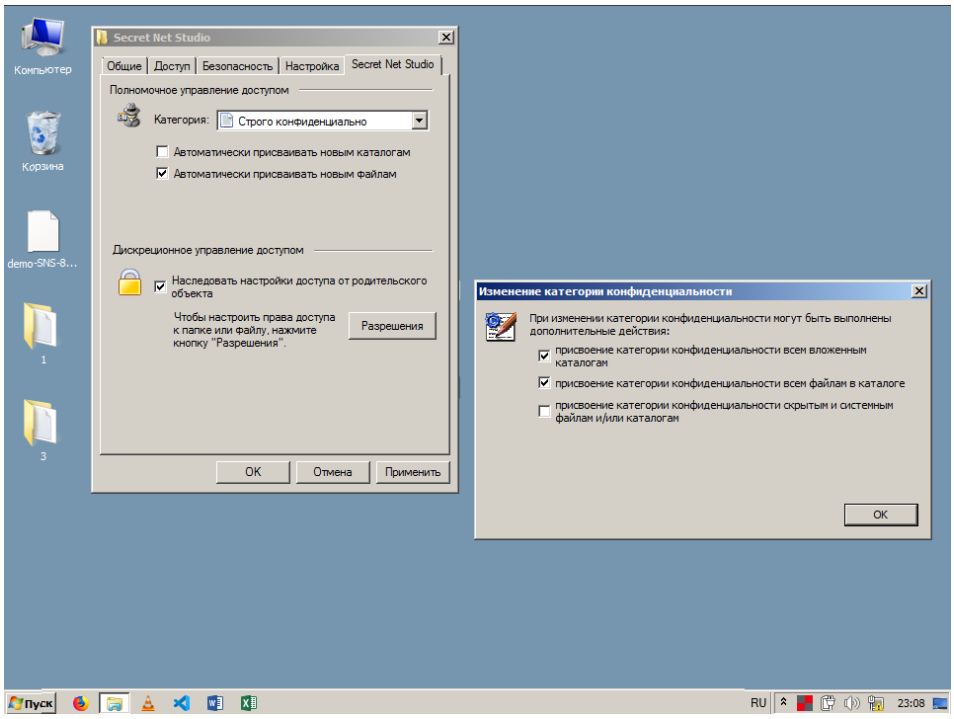


Рисунок 6 – C:\3 — как «строго конфиденциально» с применением метки ко всем вложенным каталогам и файлам

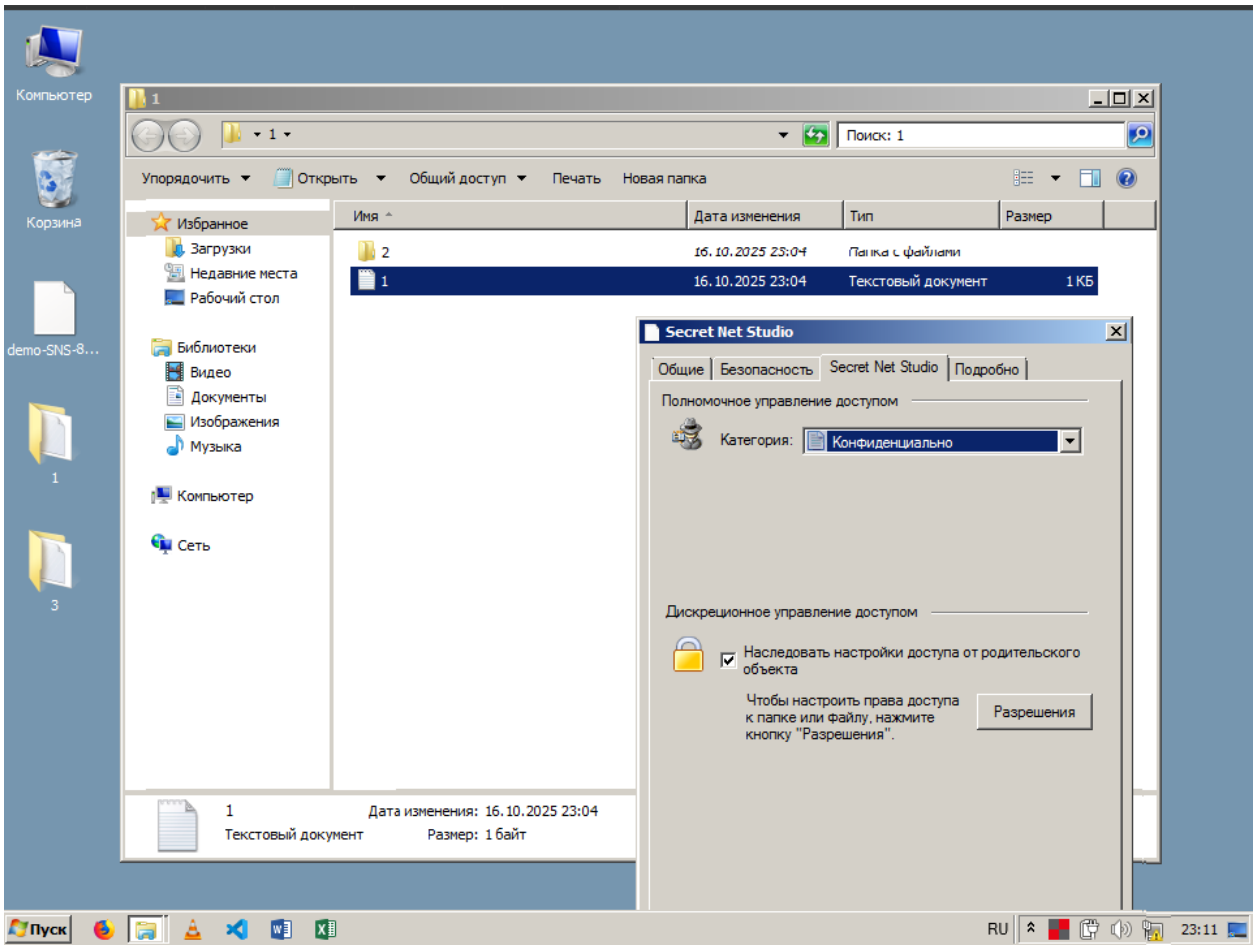


Рисунок 7 – Проверяем применились ли настройки к самим файлам

После успешного применения настроек конфиденциальности приступаем к следующему этапу

На втором этапе переназначаем:

- C:\3 ставим «конфиденциально» (только файлам текущего каталога)

- C:\1 — «строго конфиденциально» (всем вложенным каталогам и файлам).

В результате C:\1, C:\1\2, C:\1\1.txt, C:\1\2\2.txt имеют метку «строго конфиденциально»; C:\3, C:\3\3.txt — «конфиденциально»; C:\3\4, C:\3\4\4.txt — «неконфиденциально». Для C:\1, C:\1\2, C:\3 режим «Автоматически присваивать новым файлам» включён, что подтверждает корректное наследование и авто-присвоение.

### 2.3 Назначение уровня допуска пользователю

Назначаем пользователю user1 уровень допуска «конфиденциально» и проверяем влияние этого допуска на доступ к объектам.

Файлы и каталоги со статусом «строго конфиденциально» для данного пользователя недоступны, а объекты уровня «конфиденциально» открываются без ошибок. Таким

образом демонстрируется работа мандатной модели: допуск пользователя определяет уровень информации, к которой он имеет доступ.

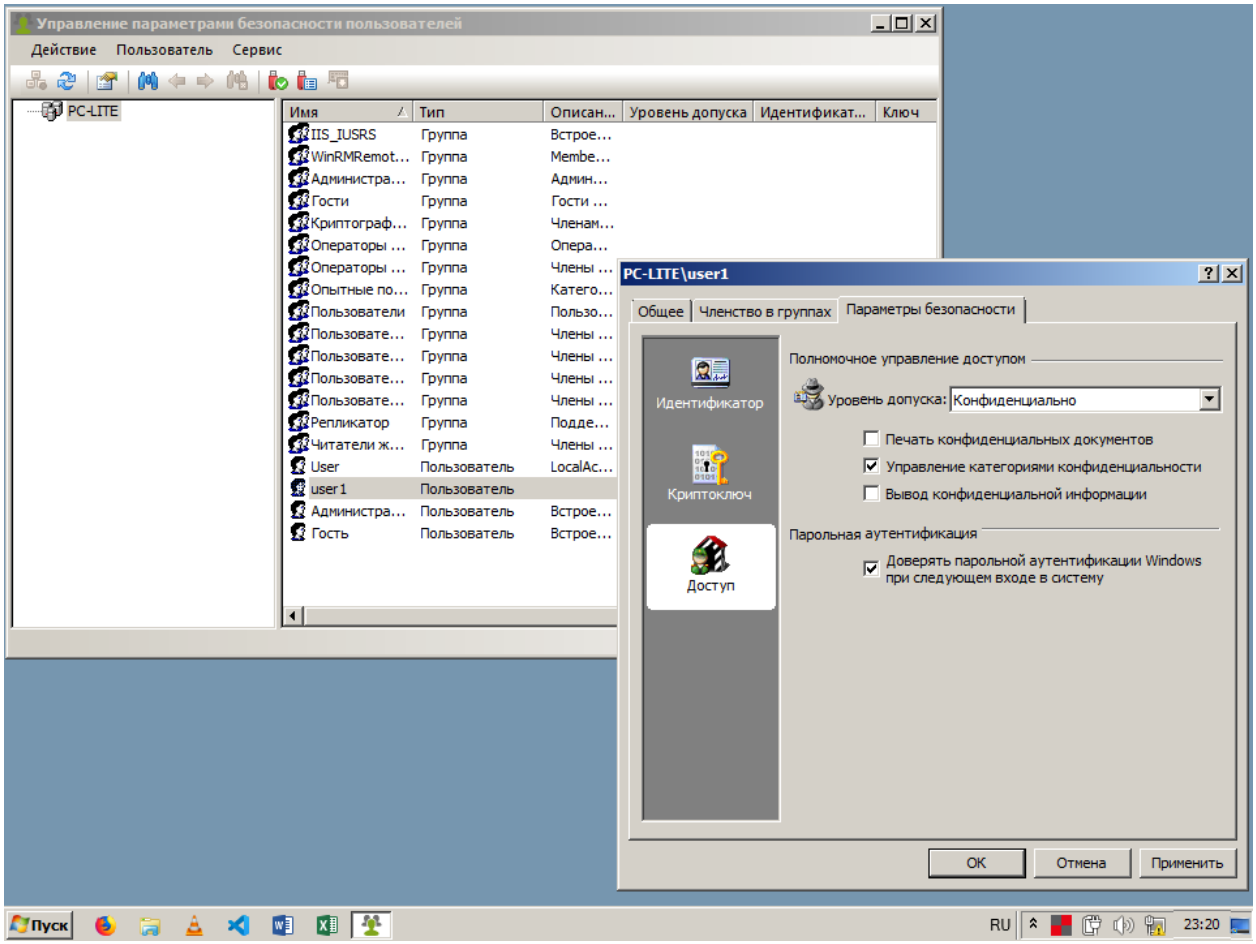


Рисунок 8 – Мандатный уровень доступа пользователя user1

# 3 ДИСКРЕЦИОННОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА К УСТРОЙСТВАМ (DAC)

## 3.1 Изменения политики контроля устройств

Настраиваем дискреционный контроль устройств.

Для диска D: пользователю user1 назначаем право «Чтение», что позволяет просматривать содержимое, но запрещает запись и изменение файлов. Присваиваем User права на «Чтение».

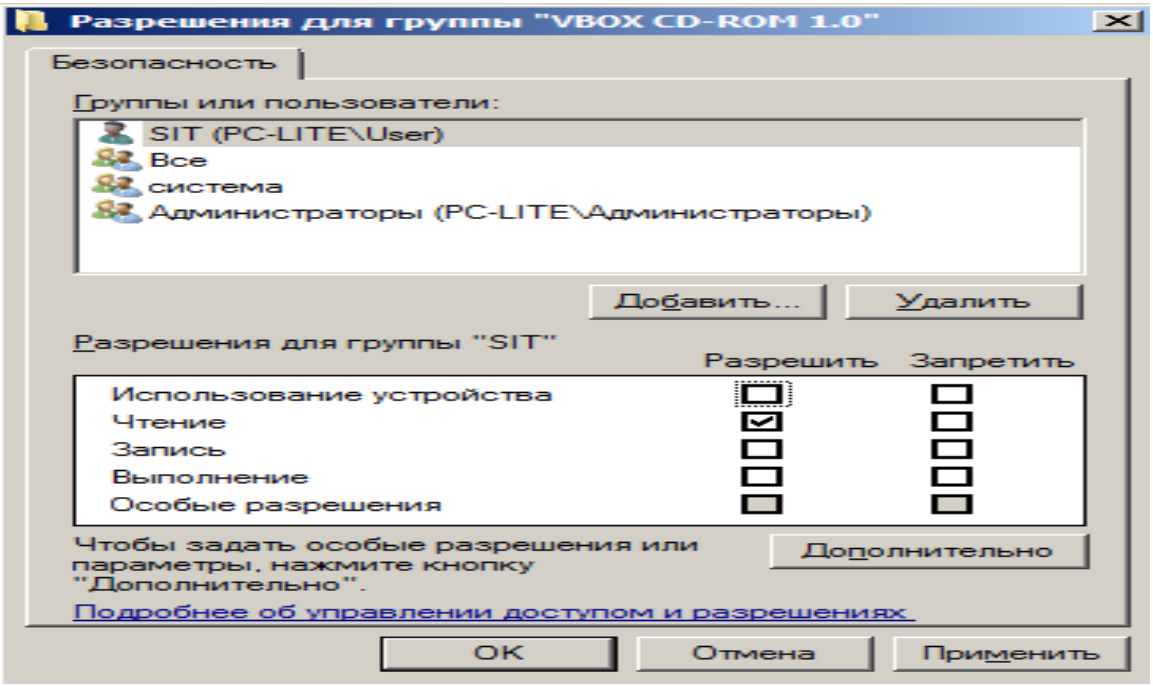


Рисунок 9 – Настройка разрешений для пользователя User в CD-ROM

# 4 ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА (ЗПС) В «ЖЁСТКОМ» РЕЖИМЕ

Настраиваем замкнутую программную среду (ЗПС) для пользователя user1 в «жёстком» режиме. Формируем «белый список» разрешённых исполняемых файлов и исключаем calc.exe. В жёстком режиме разрешается запуск только утверждённых программ; все остальные попытки блокируются и фиксируются в журнале безопасности. Это демонстрирует принцип «разрешено только явно разрешённое».

В техническом задании оглашены следующие требования – запретить пользователю User запуск программы «Word».

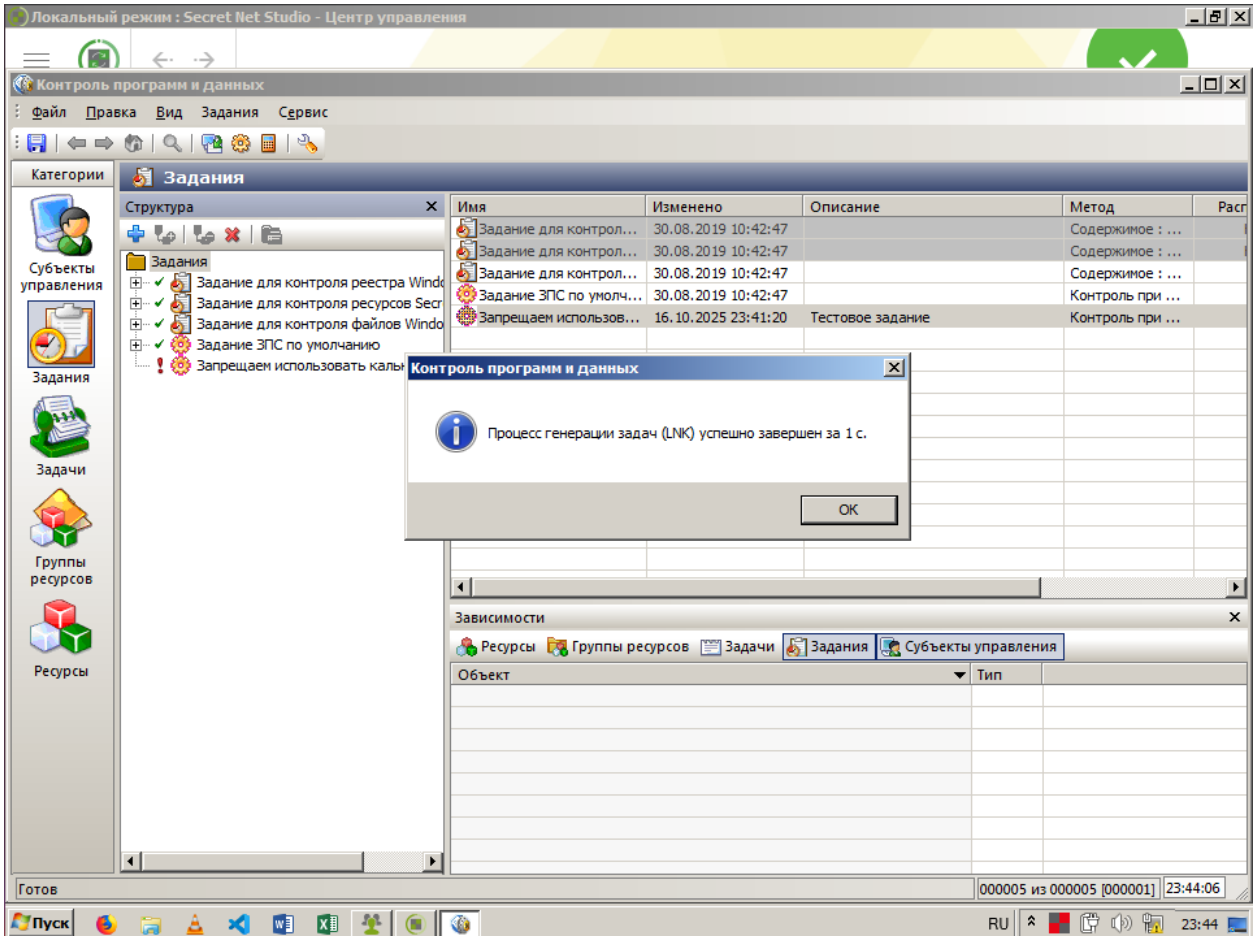


Рисунок 10 – Генерация задания

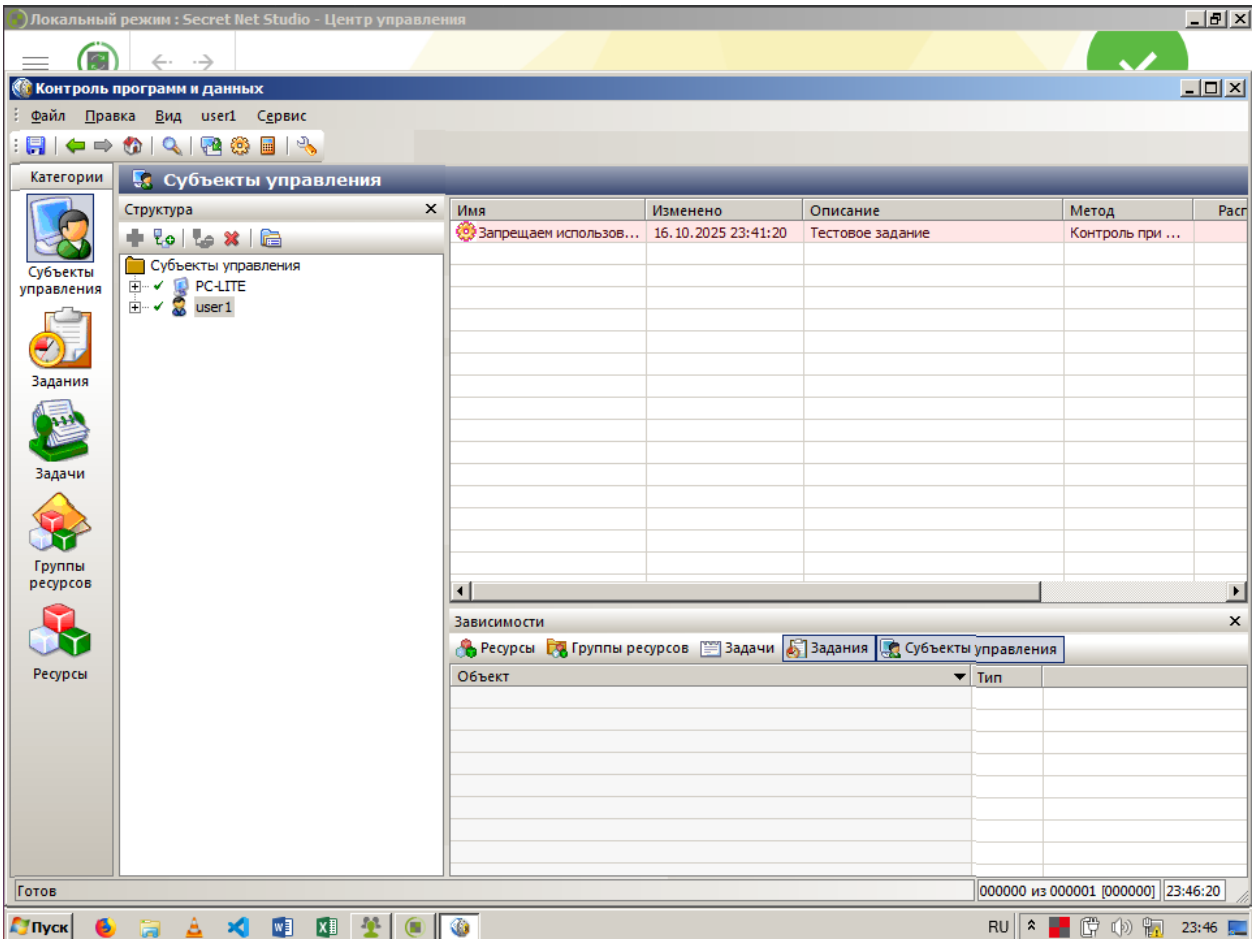


Рисунок 11 – Добавление существующего задания пользователю user1

# 5 ЖУРНАЛИРОВАНИЕ ДЕЙСТВИЙ

Открываем Secret Net Studio Локальный центр управления, на странице “Состояние” внизу находится журнал действий, в нем находится запись о всех действиях всех пользователей по времени и дате

Просматриваем журналы безопасности Secret Net для подтверждения результатов настроек. В журнале отображаются записи о попытках доступа к объектам «строго конфиденциально», попытках записи на защищённые носители и блокировках запуска. Журналы служат доказательством корректной работы мандатной, дискреционной и программной политик безопасности.

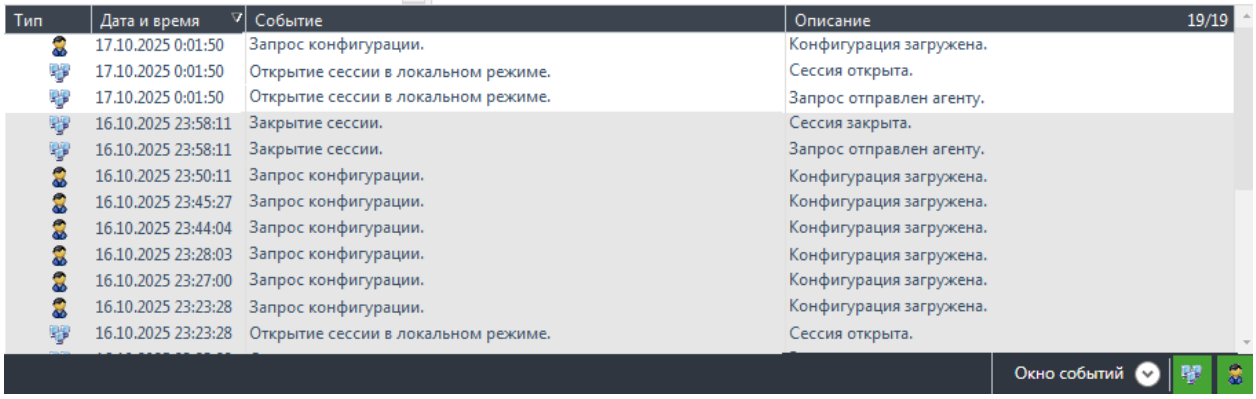


Рисунок 12 – Журнал Secret Net

## ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы мы изучаем принципы построения и практического применения средств защиты от несанкционированного доступа в системе **Secret Net 5.1**.

На тестовом стенде с Windows 7 нами последовательно реализованы три ключевых механизма безопасности:

- **Мандатное разграничение доступа**, основанное на категориях конфиденциальности и уровнях допуска пользователей;
- **Дискреционный контроль устройств**, обеспечивающий выборочный доступ к носителям информации;
- **Замкнутая программная среда (ЗПС)**, ограничивающая запуск приложений в соответствии с утверждённым «белым списком».

В процессе работы мы проверяем корректность присвоения категорий объектам, влияние уровня допуска пользователя на доступ, ограничение записи на защищённые устройства, а также блокирование неразрешённых программ. Все настройки подтверждаются записями в журналах безопасности Secret Net, что свидетельствует о правильной работе системы защиты.

В результате проделанной работы мы осваиваем основные методы администрирования Secret Net 5.1, закрепляем знания о мандатных и дискреционных моделях безопасности и на практике убеждаемся в эффективности комплексного подхода к защите информации.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1. Средство защиты информации **Secret Net 6. Принципы построения.** Руководство администратора RU.88338853.501410.007 91 1. — СПб. : АО «Код Безопасности». — Текст : непосредственный.
2. Средство защиты информации **Secret Net 6. Установка, обновление и удаление.** Руководство администратора RU.88338853.501410.007 91 2. — СПб. : АО «Код Безопасности». — Текст : непосредственный.
3. Средство защиты информации **Secret Net 6. Управление. Основные механизмы защиты.** Руководство администратора RU.88338853.501410.007 91 3. — СПб. : АО «Код Безопасности». — Текст : непосредственный.
4. Средство защиты информации **Secret Net 6. Управление. Полномочное управление доступом и контроль печати.** Руководство администратора RU.88338853.501410.007 91 4. — СПб. : АО «Код Безопасности». — Текст : непосредственный.
5. Средство защиты информации **Secret Net 6. Аудит.** Руководство администратора RU.88338853.501410.007 91 5. — СПб. : АО «Код Безопасности». — Текст : непосредственный.
6. Лазутин А. И. *Курс лекций по дисциплине «Программно-аппаратные средства защиты информации»* / А. И. Лазутин. — Армавир, 2023. — Текст : непосредственный.
7. Методические указания к лабораторной работе «Система защиты информации Secret Net 5.x». — Армавир, 2025. — Текст : рукопись