

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра комплексной информационной безопасности электронно–
вычислительных систем (КИБЭВС)

SECRET NET. ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА. КОНТРОЛЬ
ЦЕЛОСТНОСТИ

Отчет по лабораторной работе №2
по дисциплине «Управление средствами защиты информации»

Выполнил

Студент гр. 728–2

_____ Геворгян Д.Р.

____.____.2021

Принял

Доцент кафедры БИС

_____ Рахманенко И. А.

оценка

подпись

____.____.2021

1 Введение

Целью данной работы является изучение и приобретение навыков настройки и управления основными защитными механизмами СЗИ от НСД «Secret Net». Рассмотрены принципы обеспечения замкнутой программной среды и настройки контроля целостности.

Вариант 2

2 Ход работы

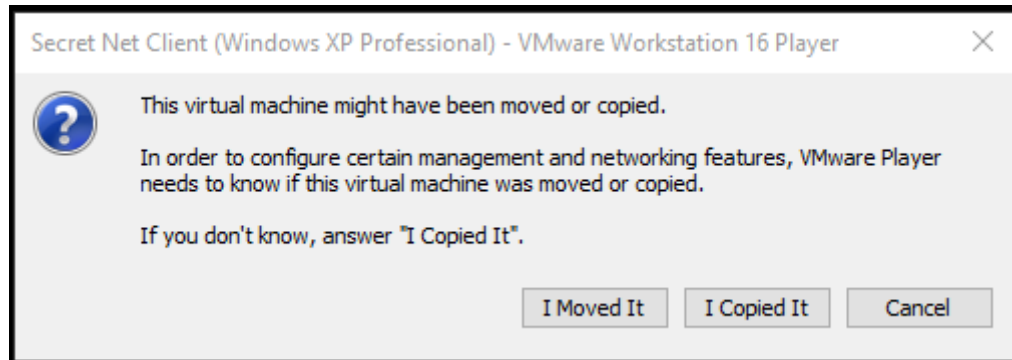


Рисунок 1– Запрос конфигурации при запуске виртуальной машины

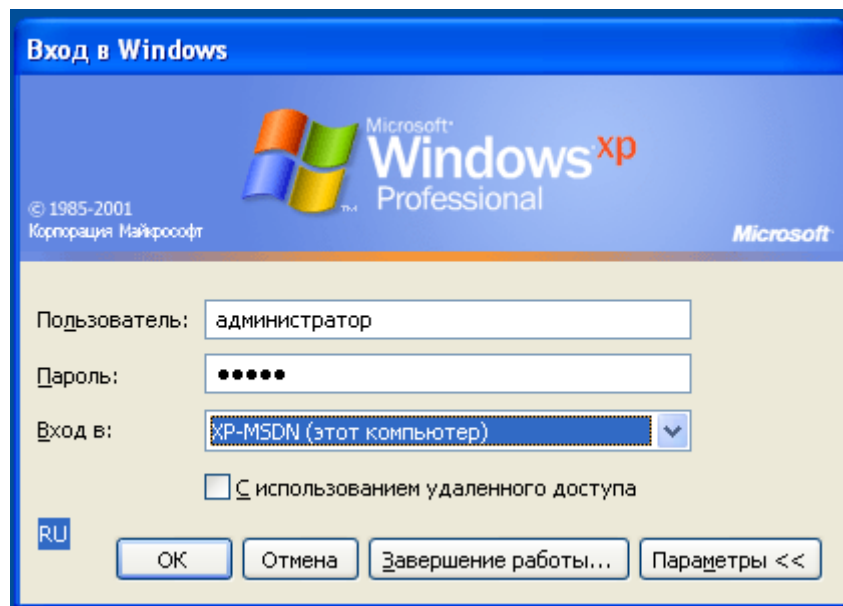


Рисунок 2 – Вход в систему под локальной учетной записью

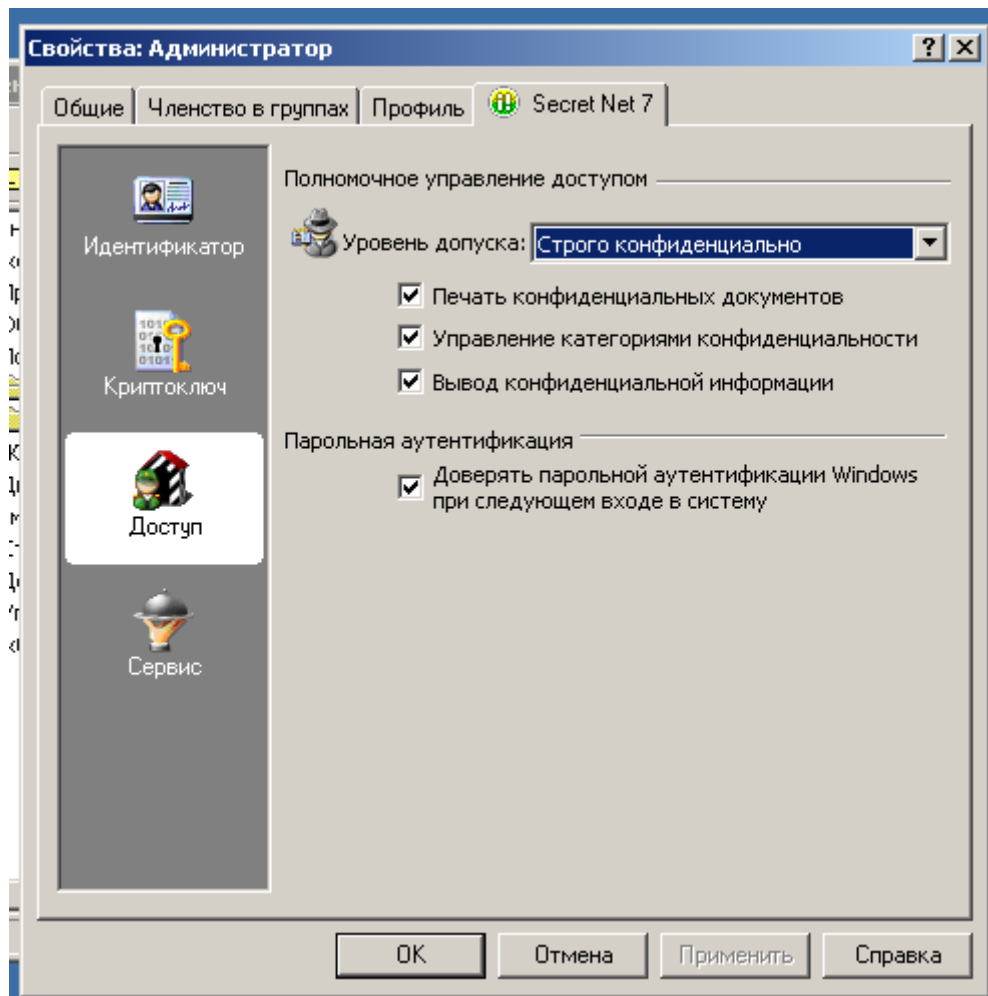


Рисунок 3 – Параметры управления полномочным доступом для пользователя Администратор

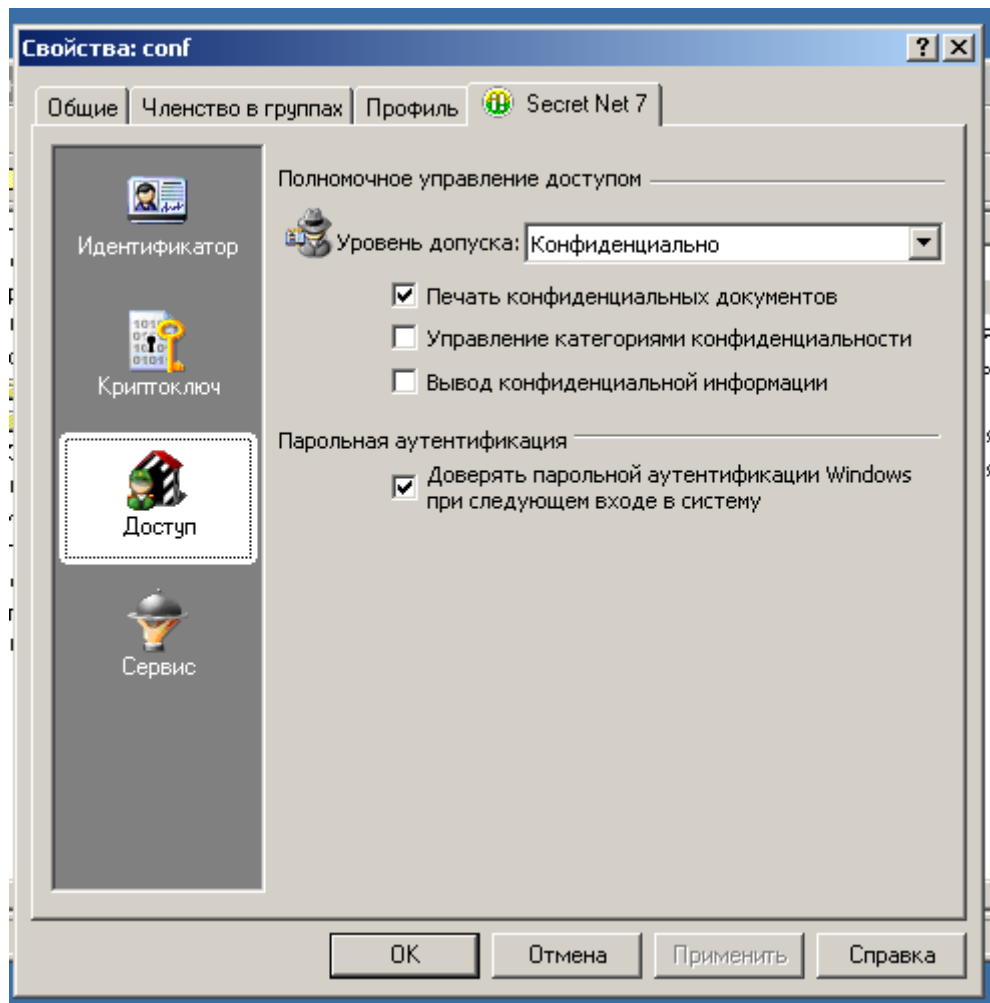


Рисунок 4 – Параметры управления полномочным доступом для пользователя conf

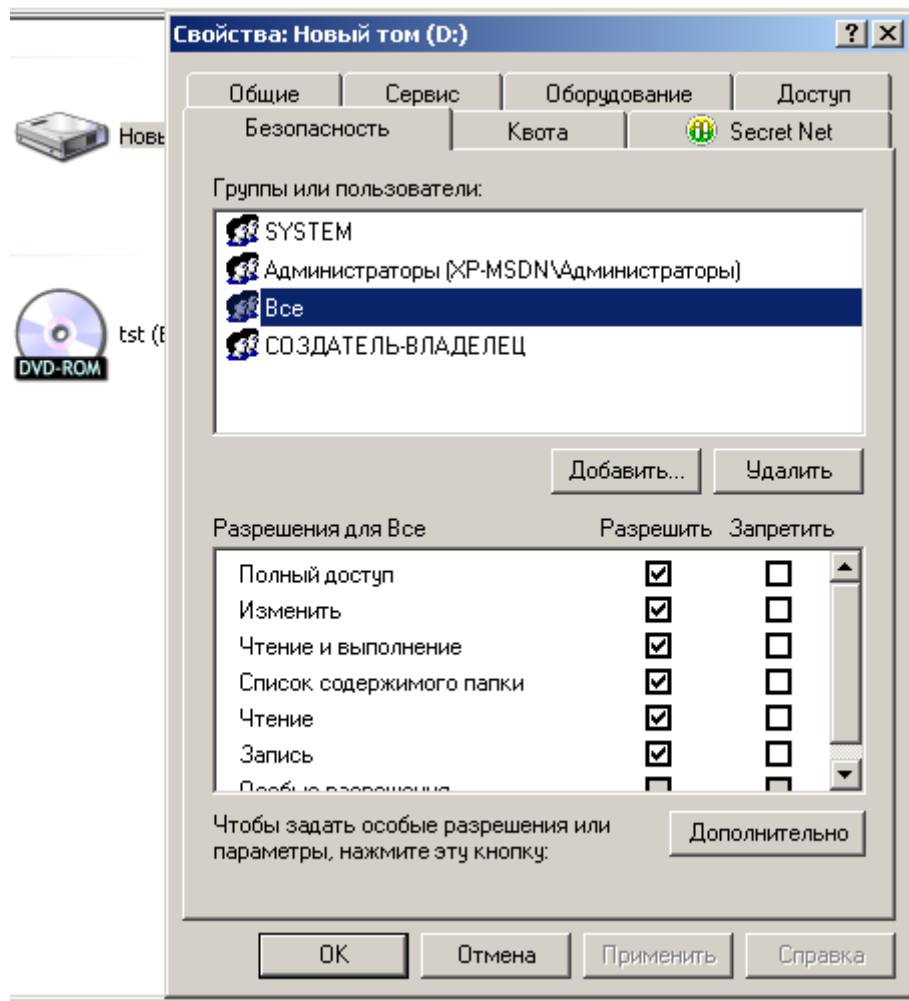


Рисунок 5 – Изменение разрешения на доступ к диску “D:\”

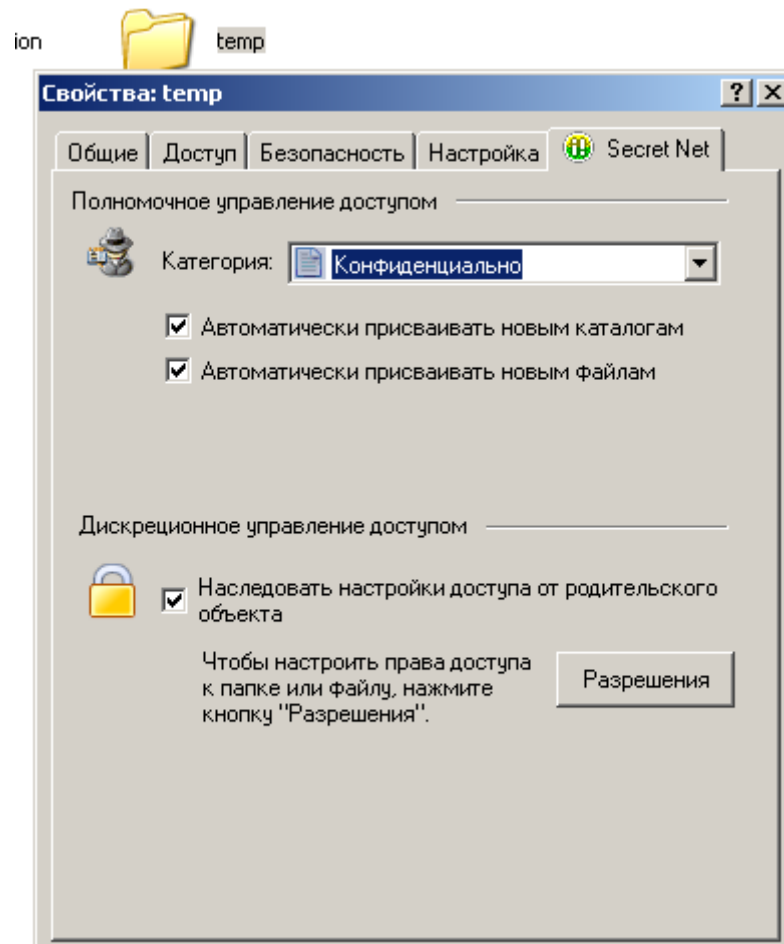


Рисунок 6 – Изменение уровня конфиденциальности папки temp

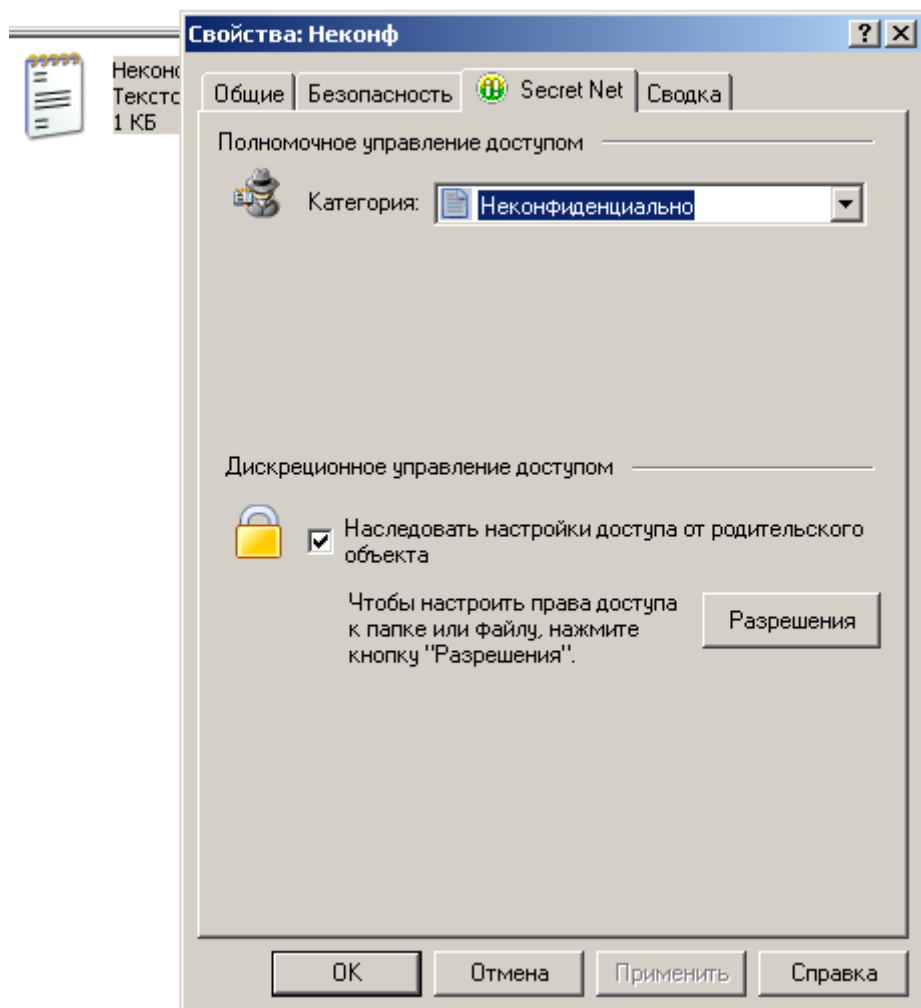


Рисунок 7 – Изменение уровня конфиденциальности файла Неконф.txt

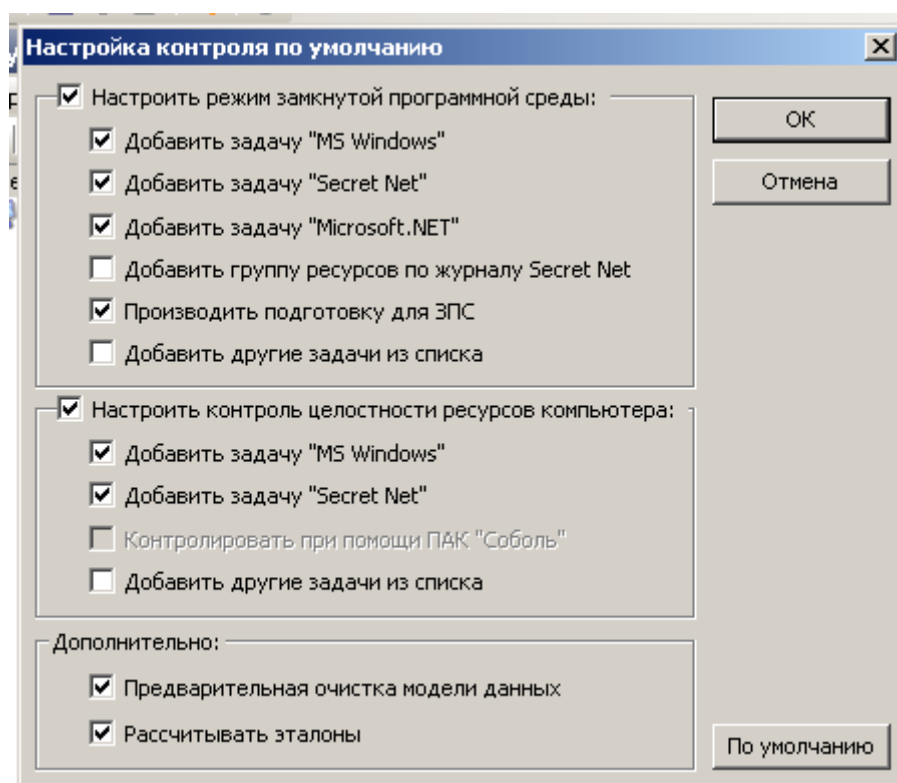


Рисунок 8 – Настройка контроля целостности и ЗПС для стандартных объектов.

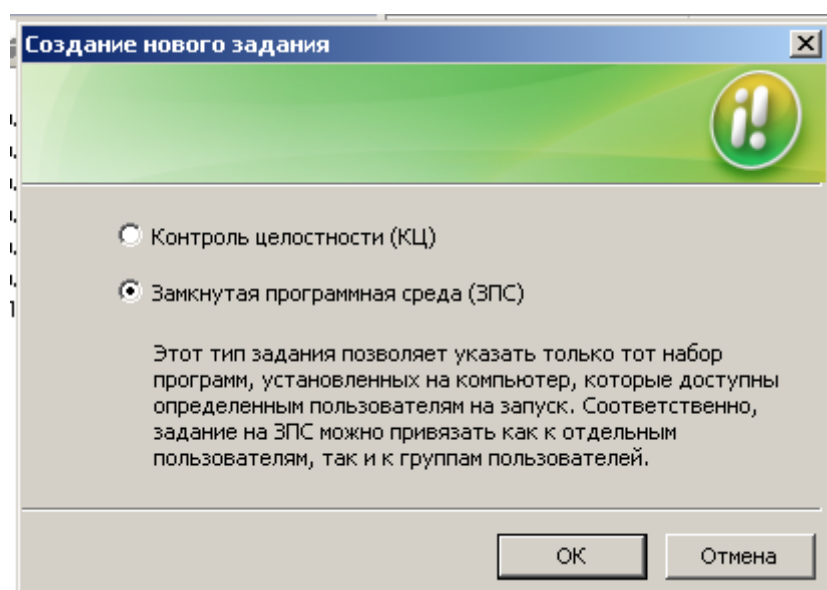


Рисунок 9 – Выбор типа задания

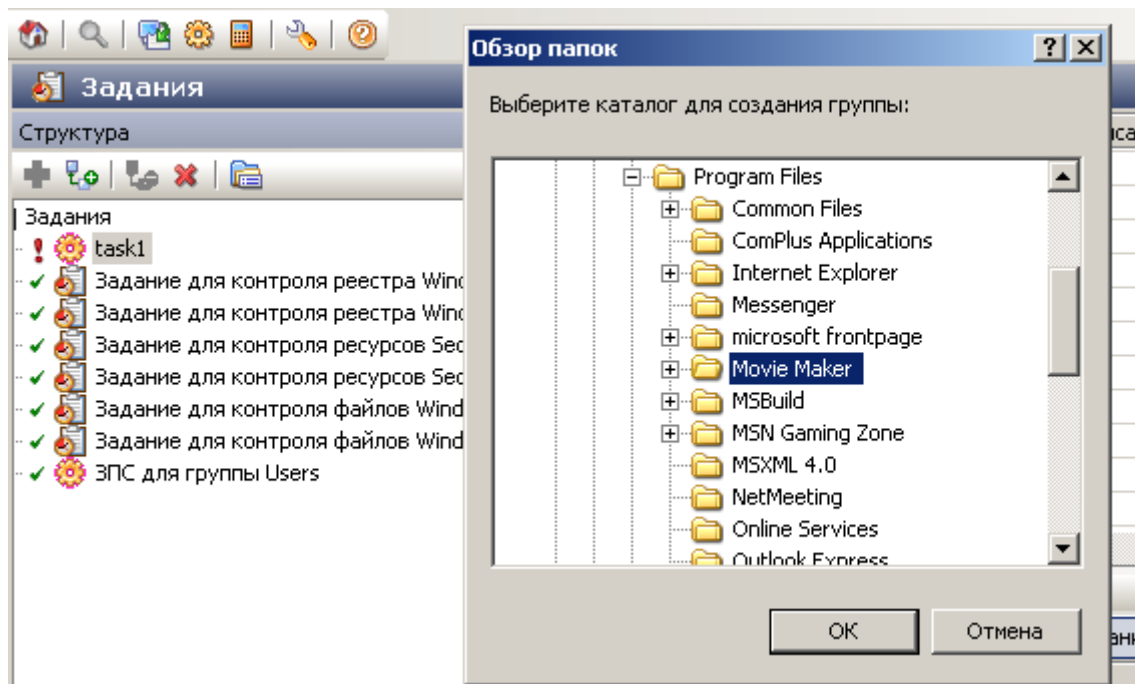


Рисунок 10 – Добавление группы ресурсов в задание на ЗПС

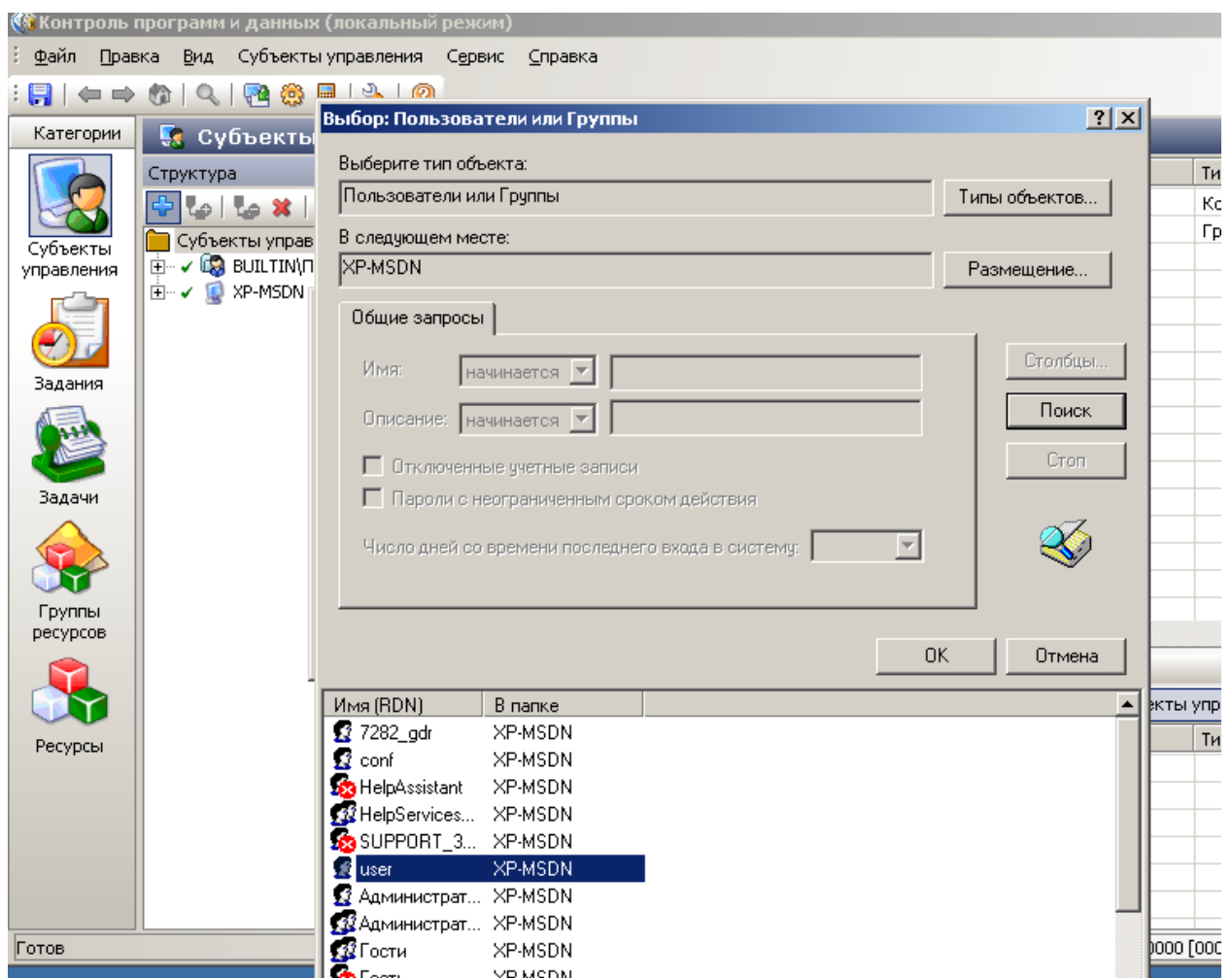


Рисунок 11 – Выбор пользователя user

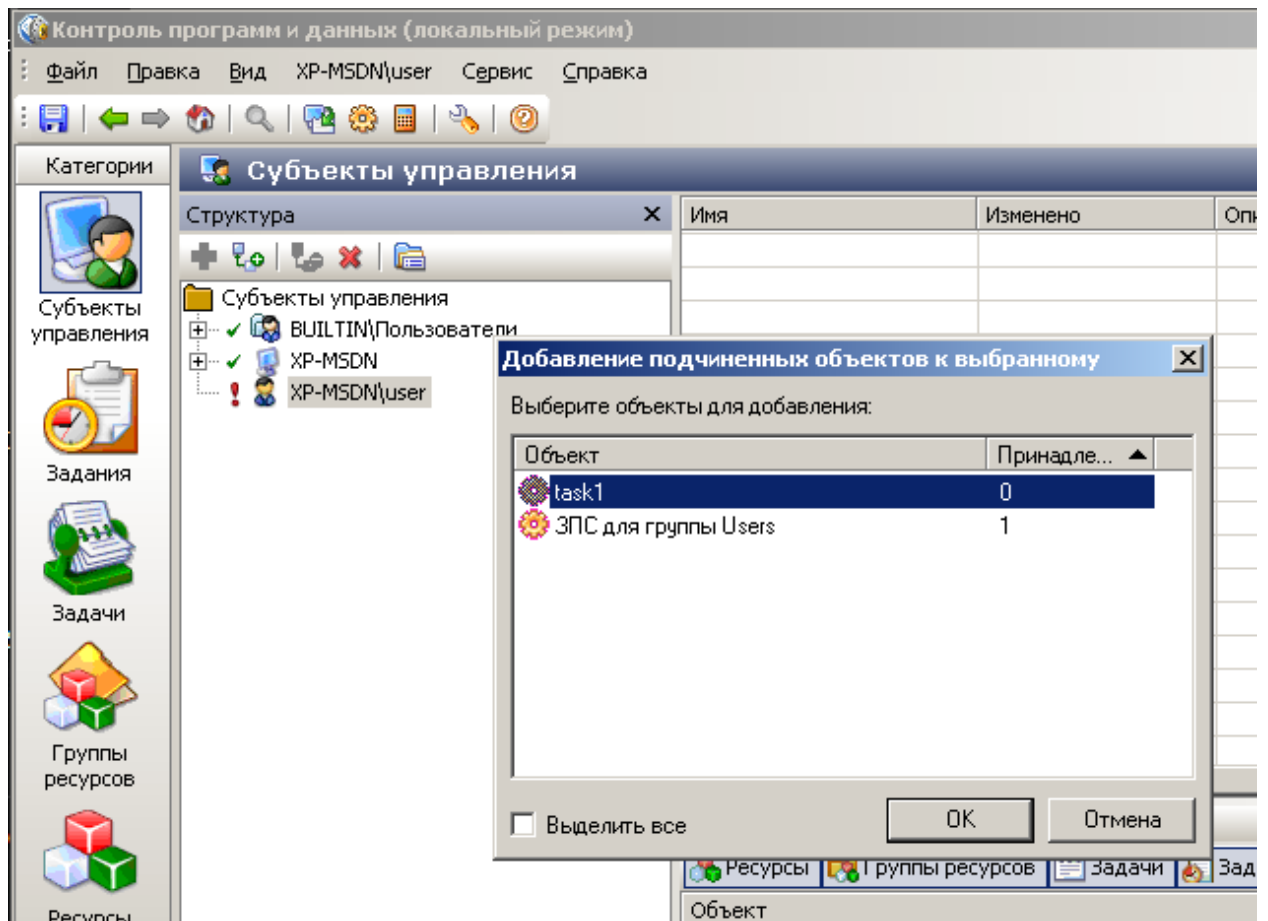


Рисунок 12 – Добавление задания

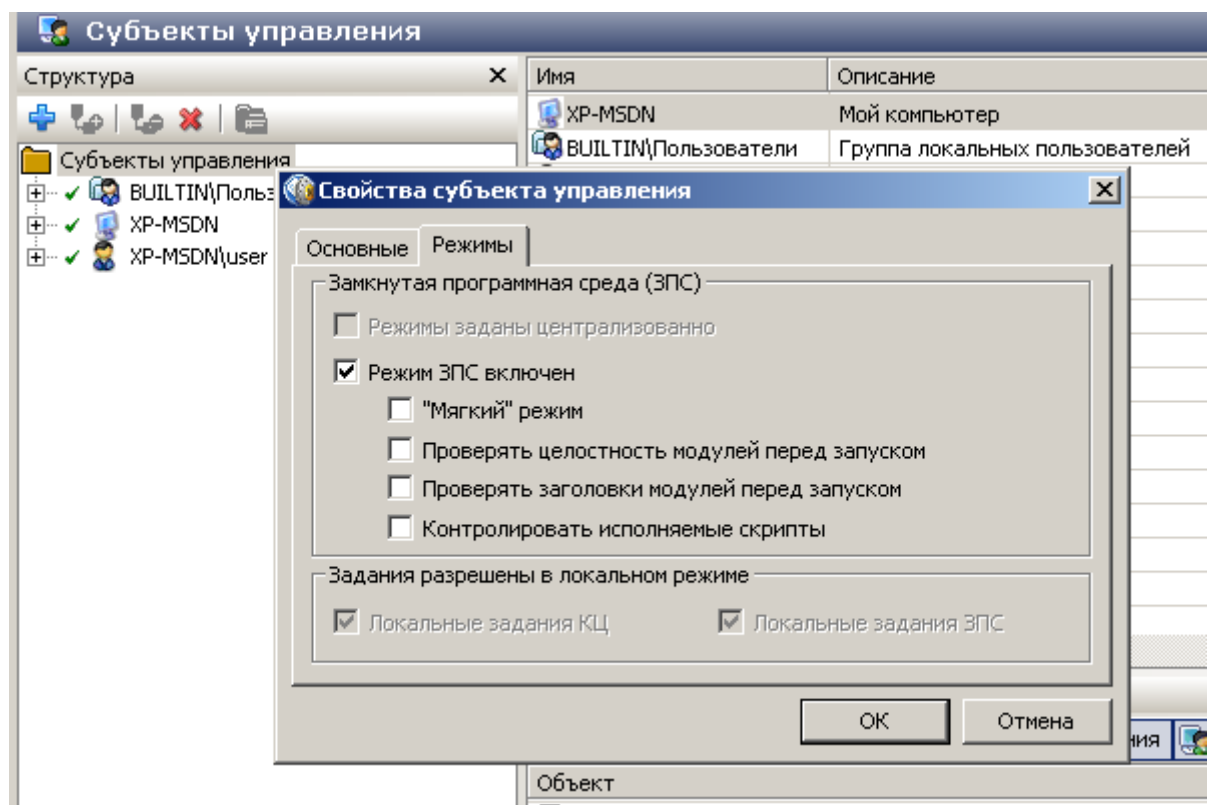


Рисунок 13 – Настройка режима ЗПС

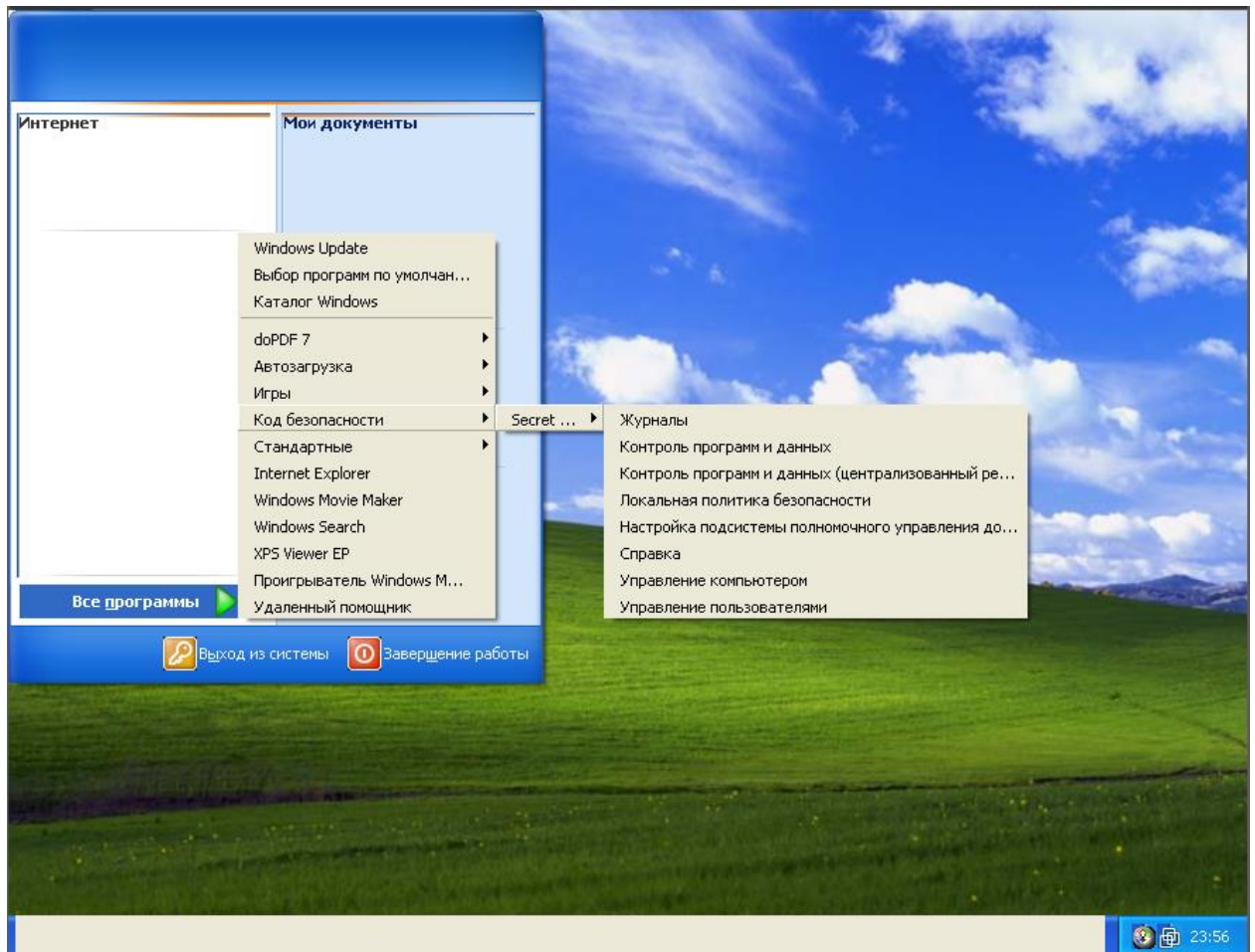


Рисунок 14 – Некорректный интерфейс Windows

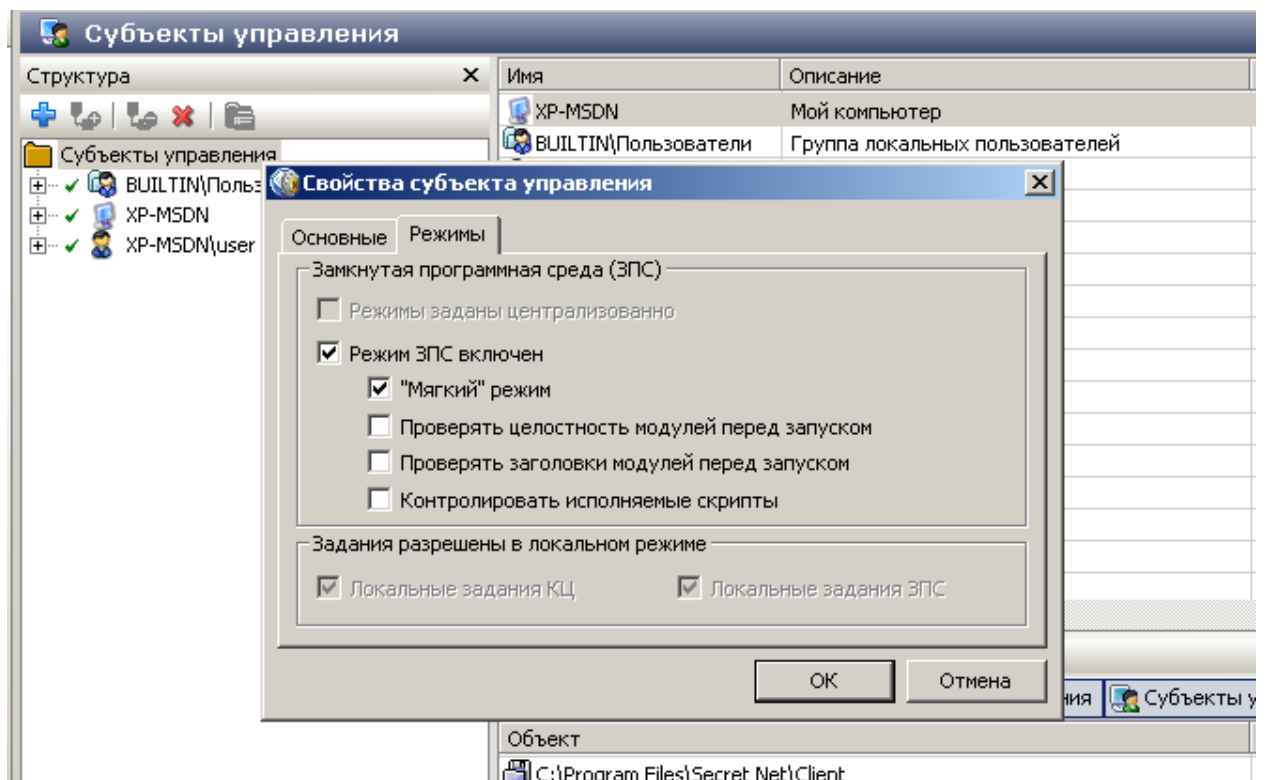


Рисунок 15 – Включение «Мягкого режима»

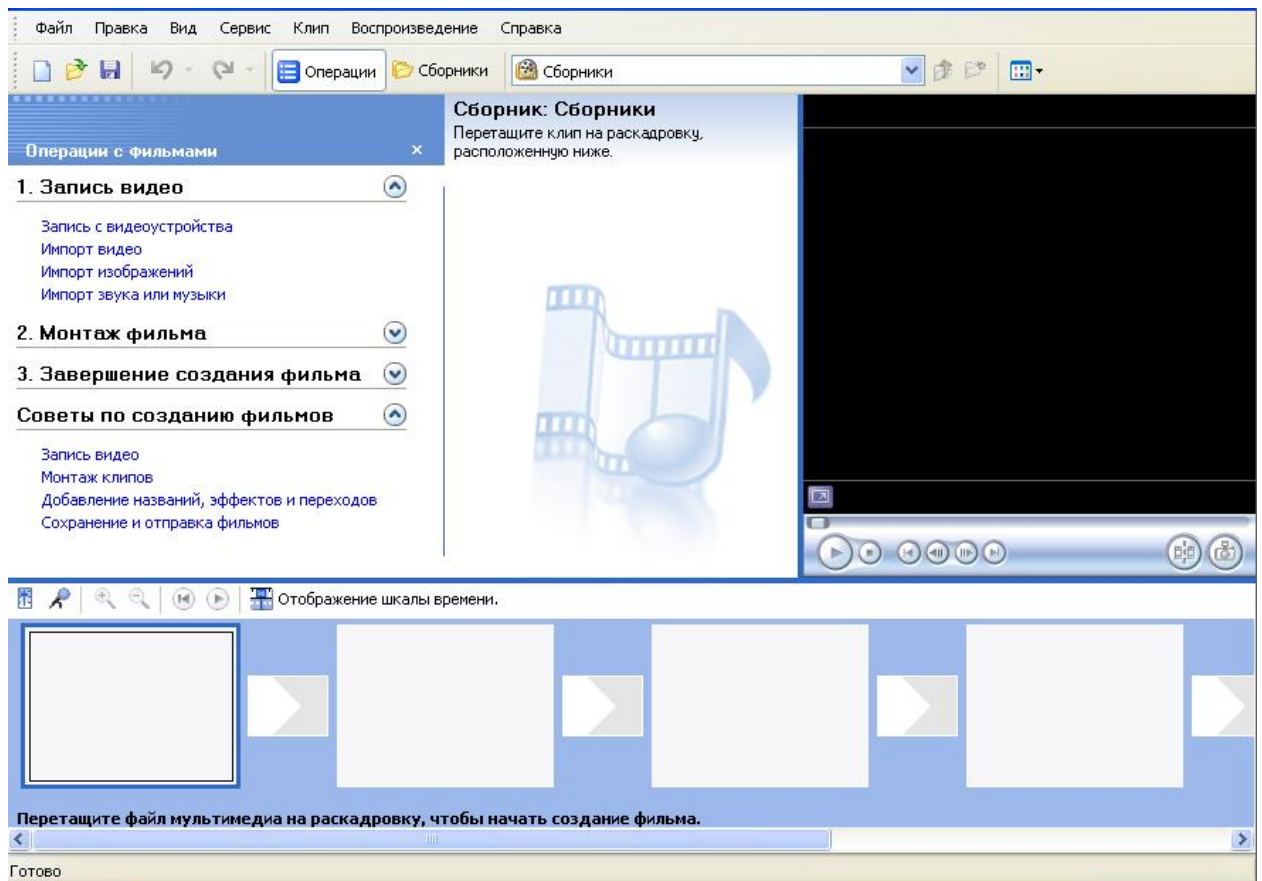


Рисунок 16 – Запуск Movie Maker под учетной записью user

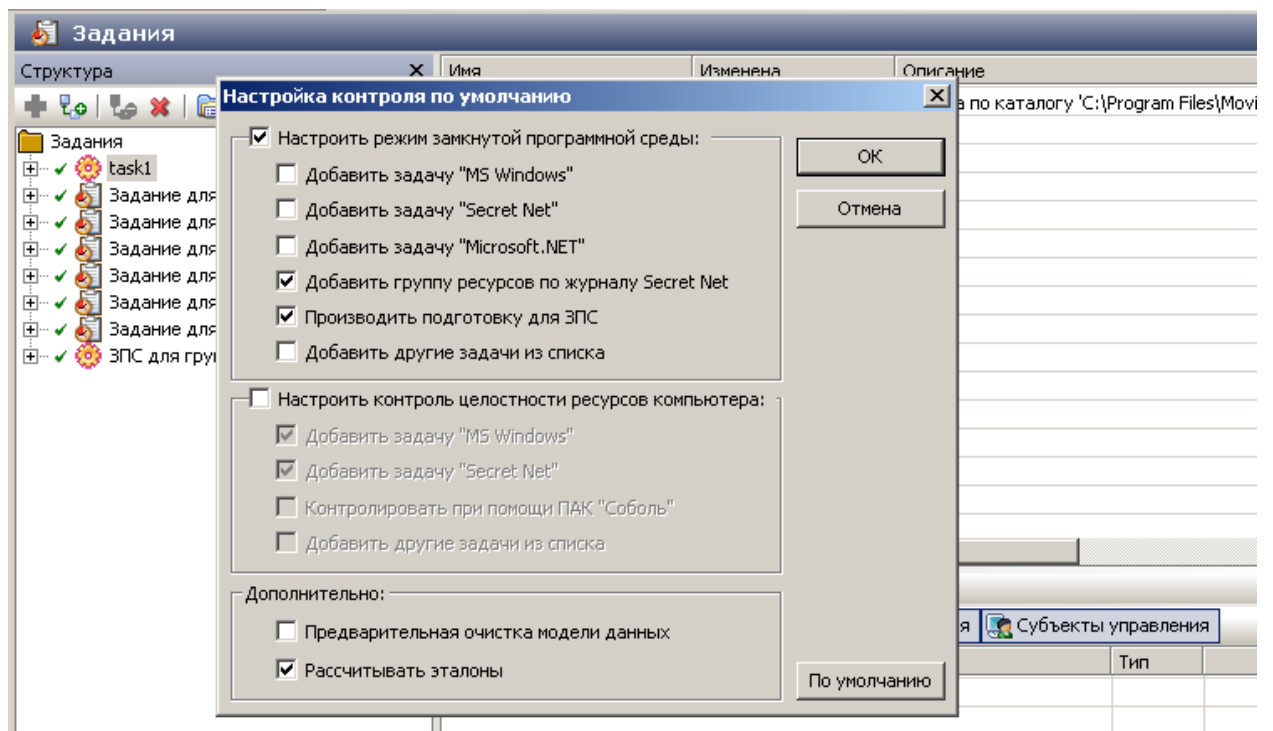


Рисунок 17 – Добавление группы ресурсов по журналу Secret Net

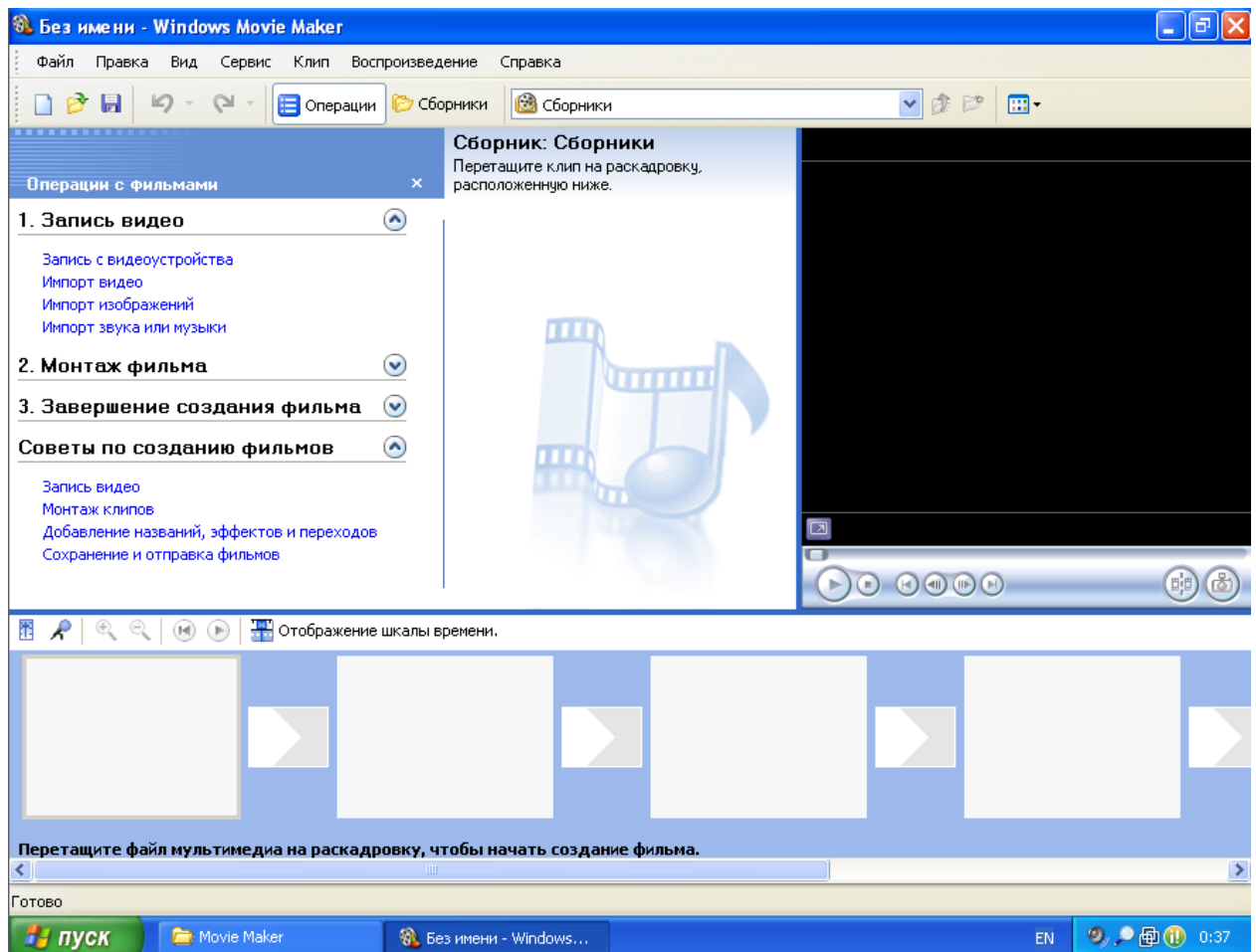


Рисунок 18 – Повторный запуск Movie Maker

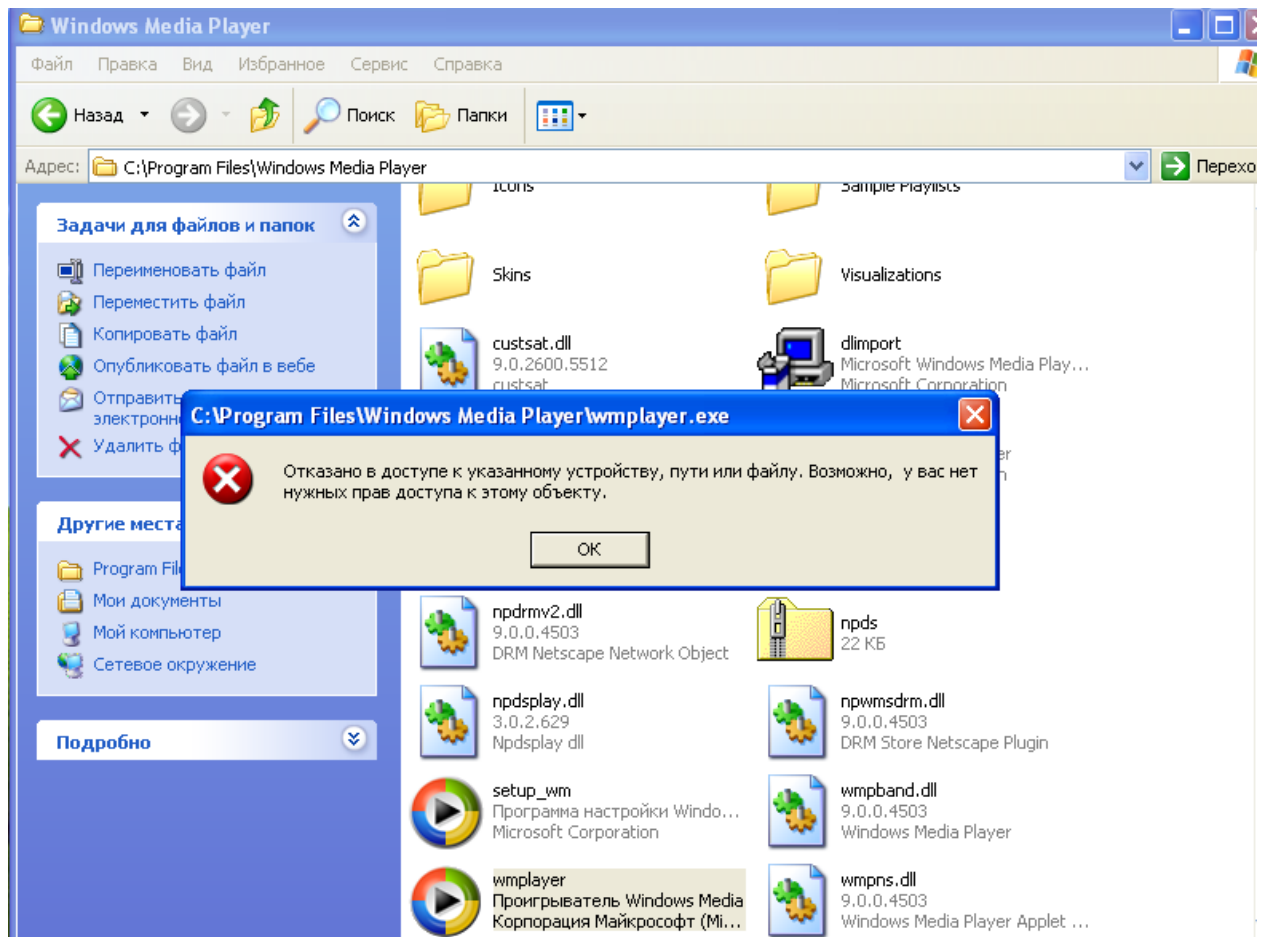
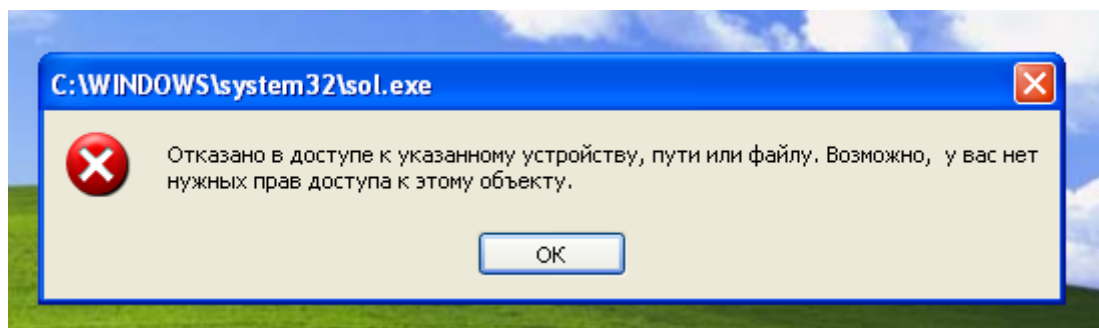
Рисунок 19 – Отказ в доступе к `wmplayer`

Рисунок 20 – Отказ в доступе к «Солитёр»

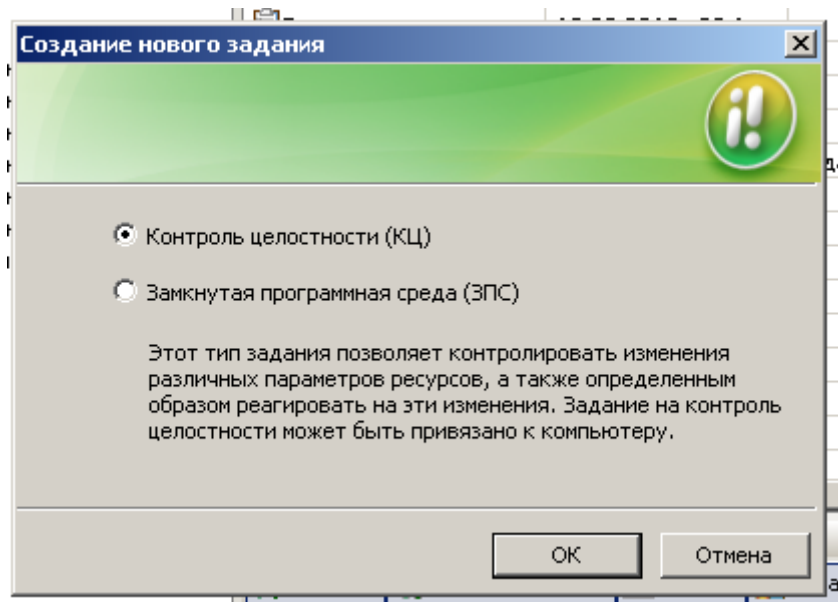


Рисунок 21 – Создание задания на КЦ

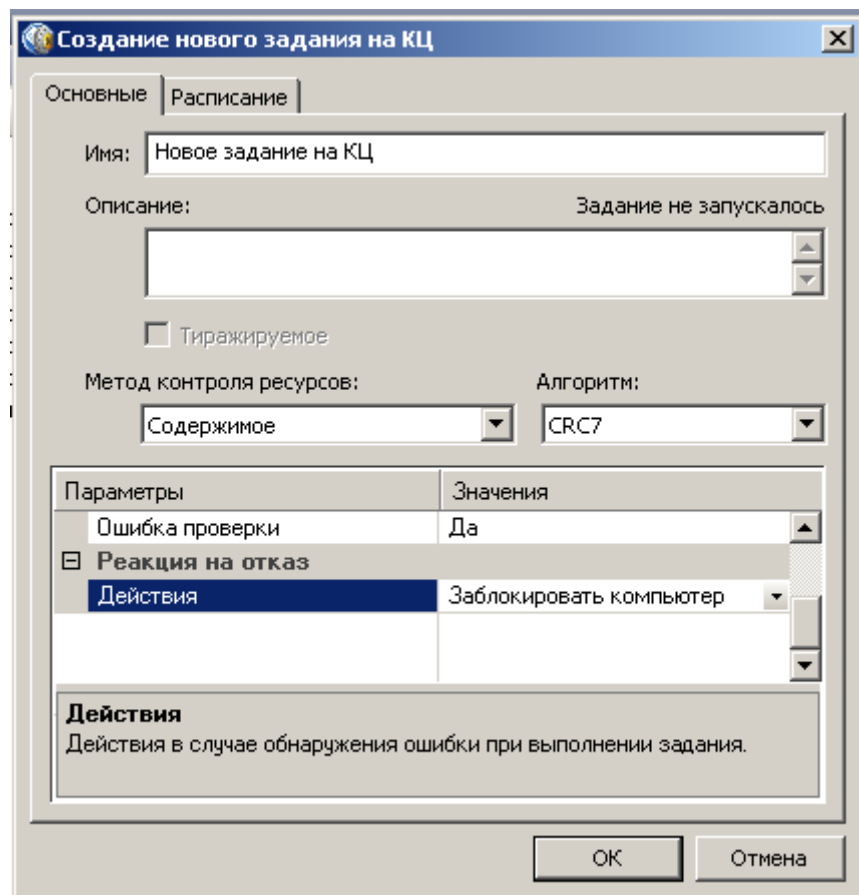


Рисунок 22 – Окно настроек задания на контроль целостности

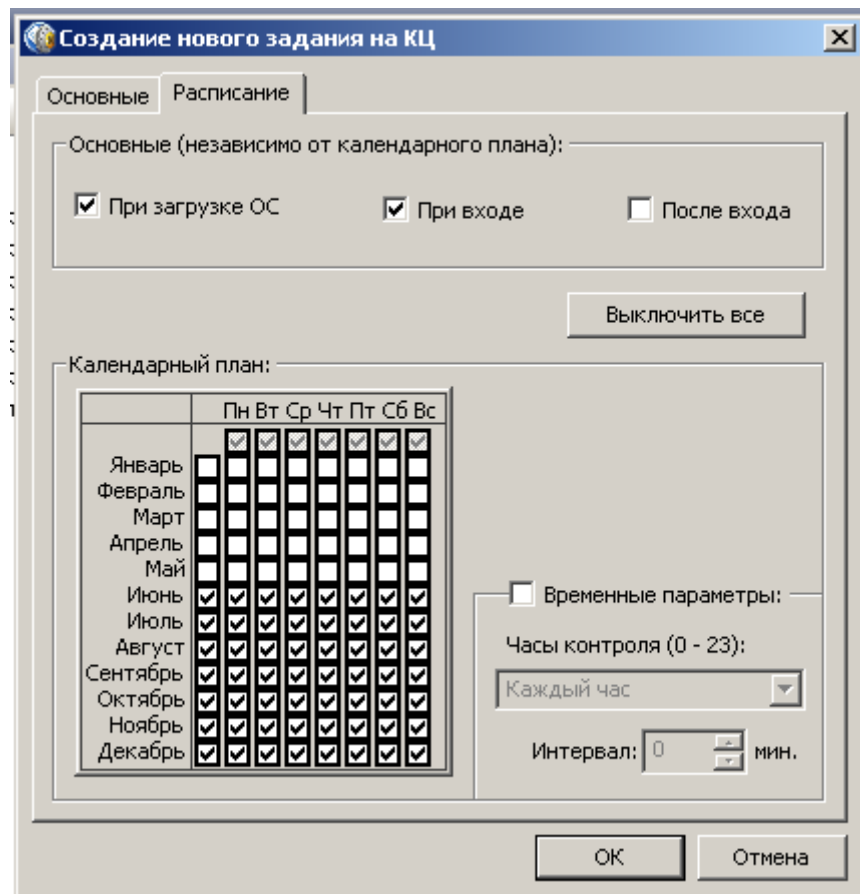


Рисунок 23 – Настройка расписания контроля целостности

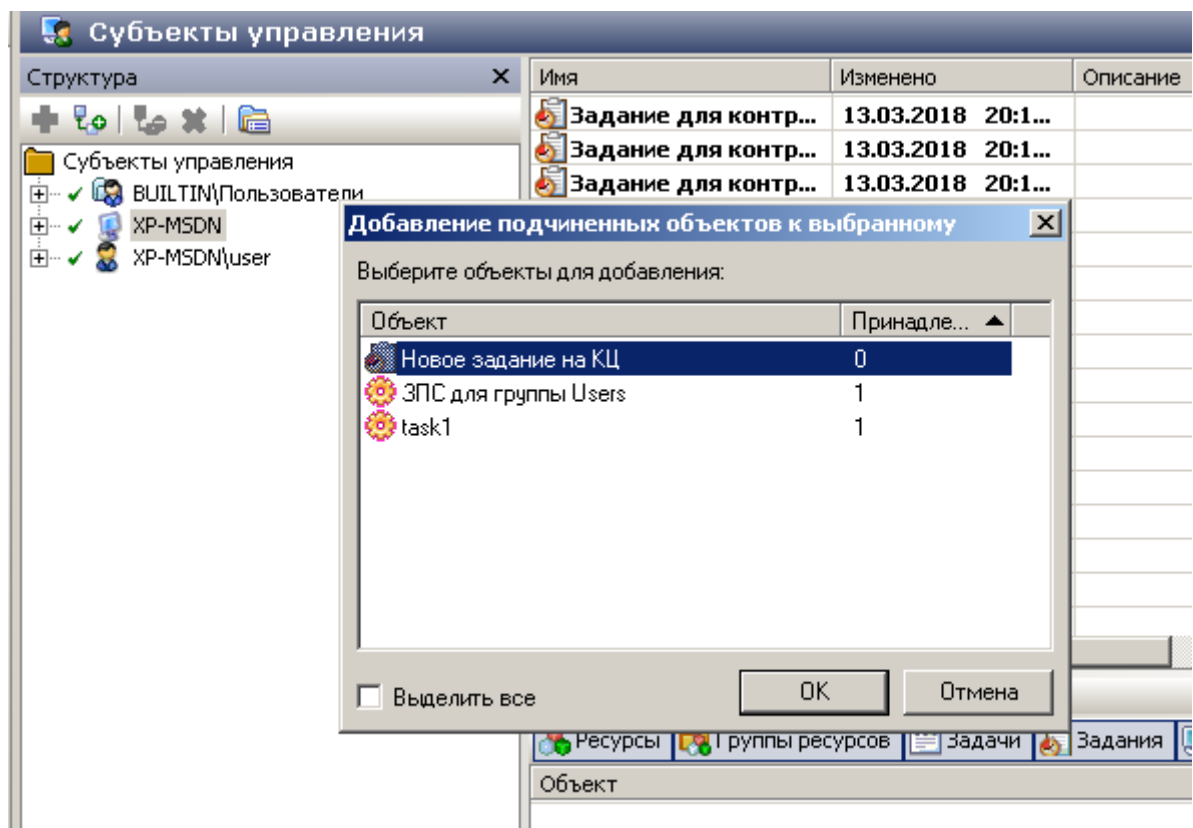


Рисунок 24 – Задание контроля целостности

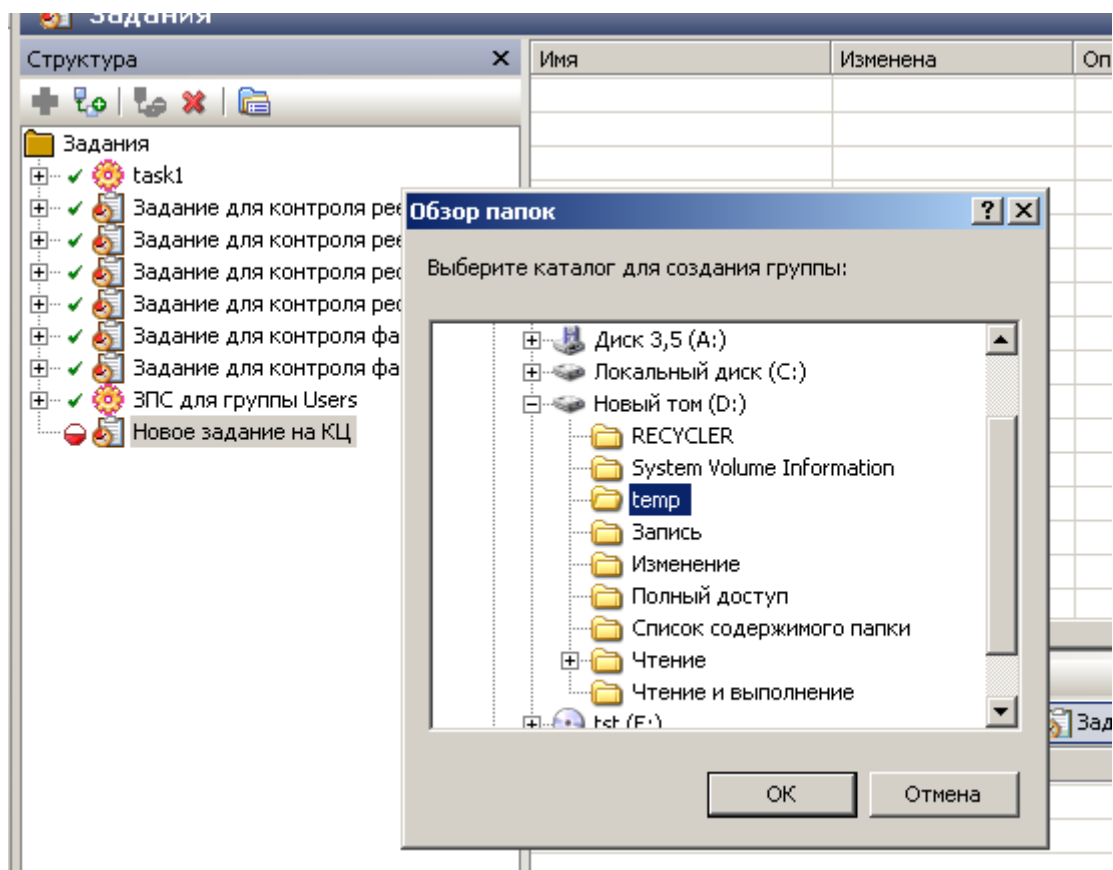


Рисунок 25 – Выбор каталога, проверяемого КЦ

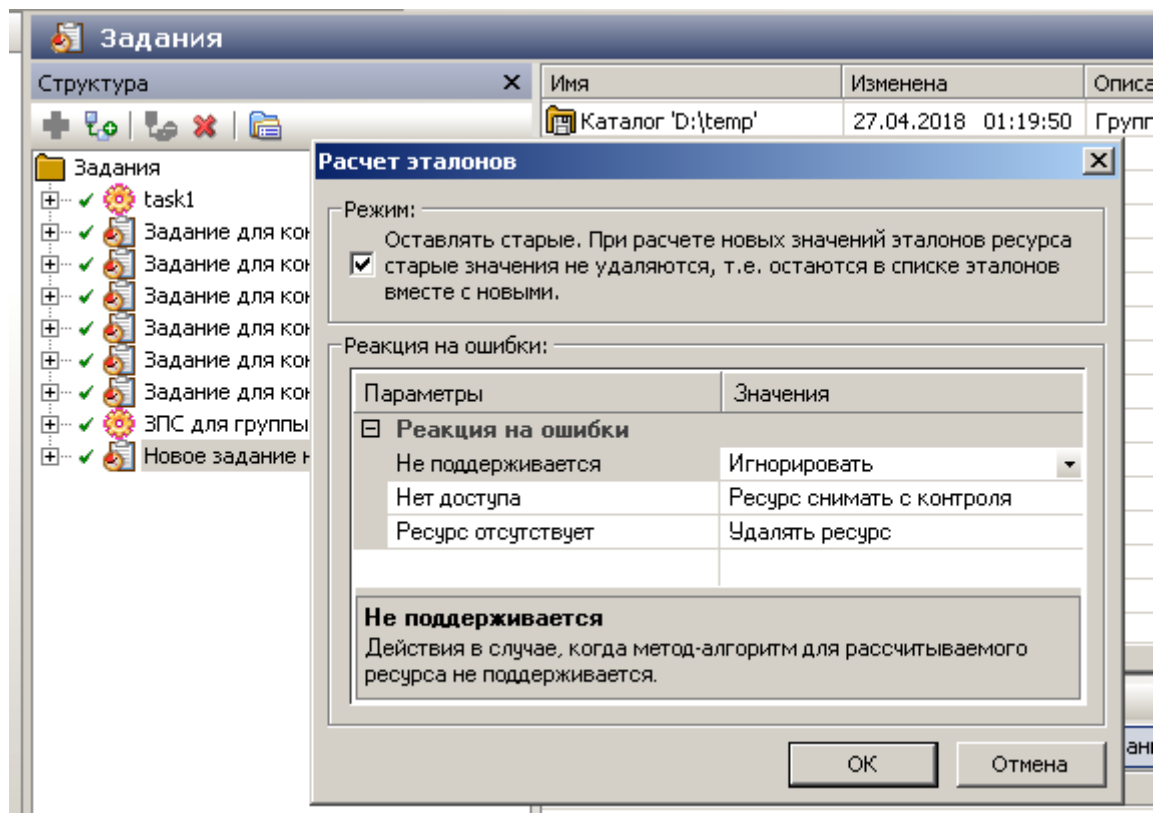


Рисунок 26 – Расчёт эталонов

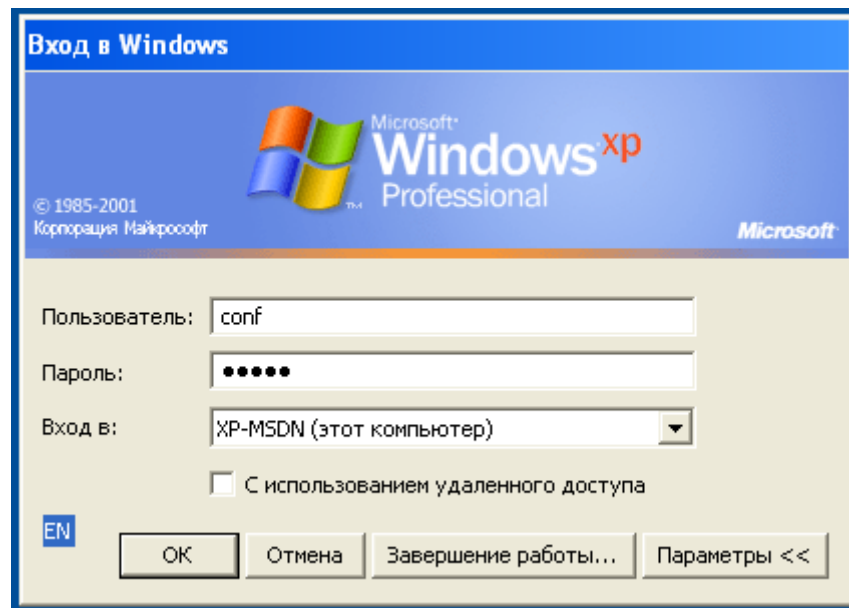


Рисунок 27 – Вход под учётной записью conf

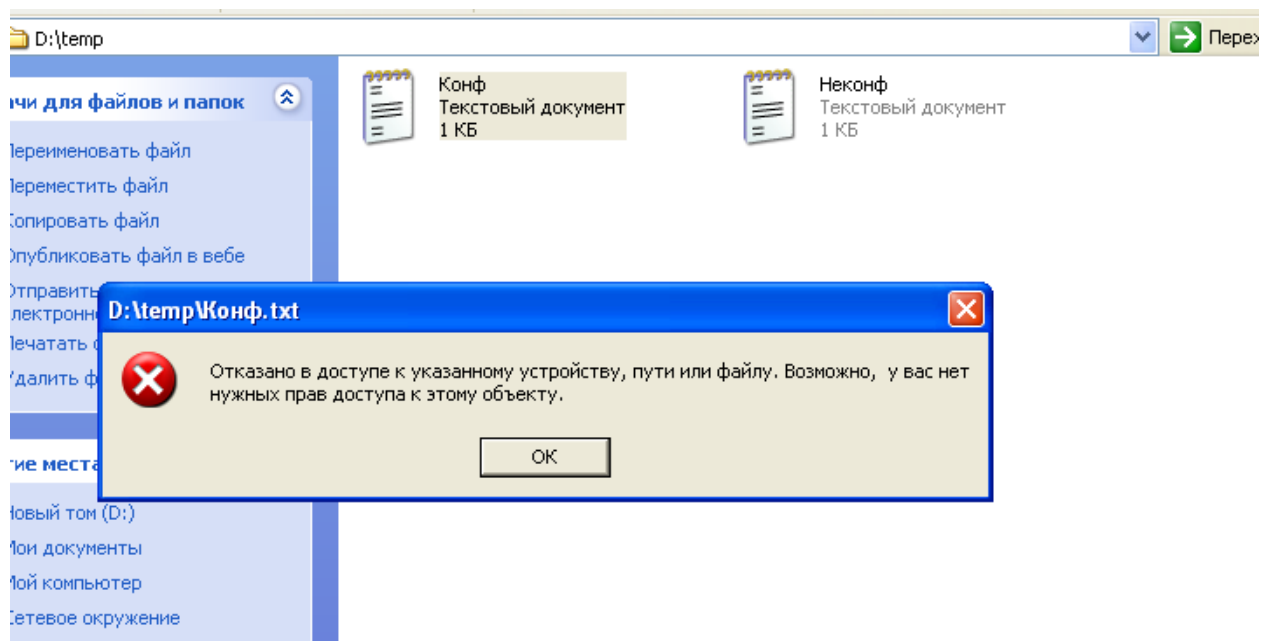


Рисунок 28 – Отказ в доступе

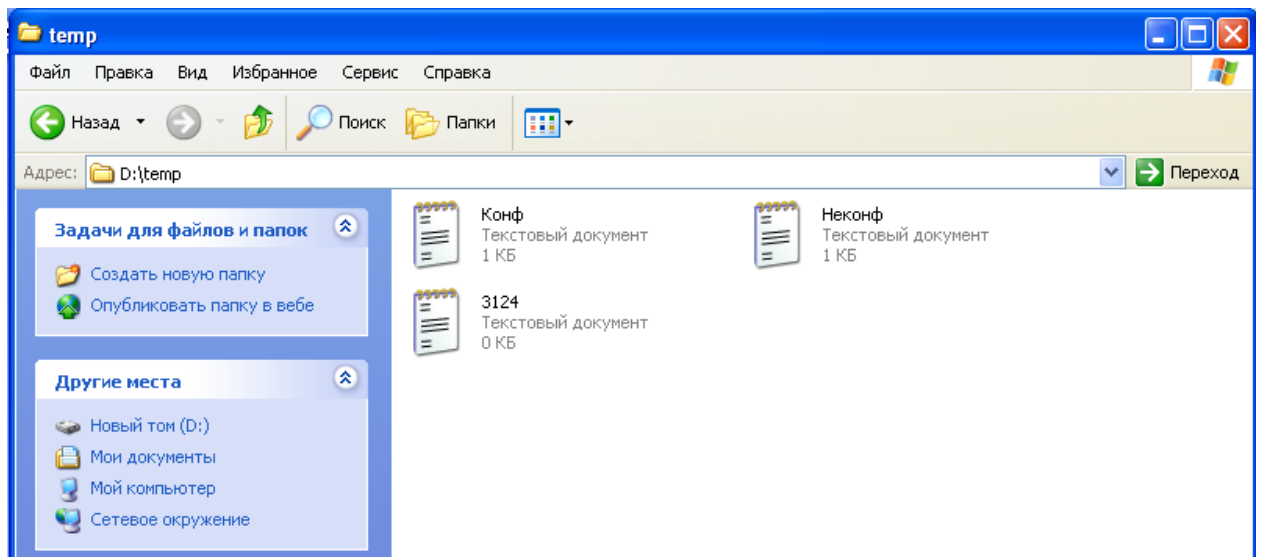


Рисунок 29 – Добавление нового файла в каталог temp

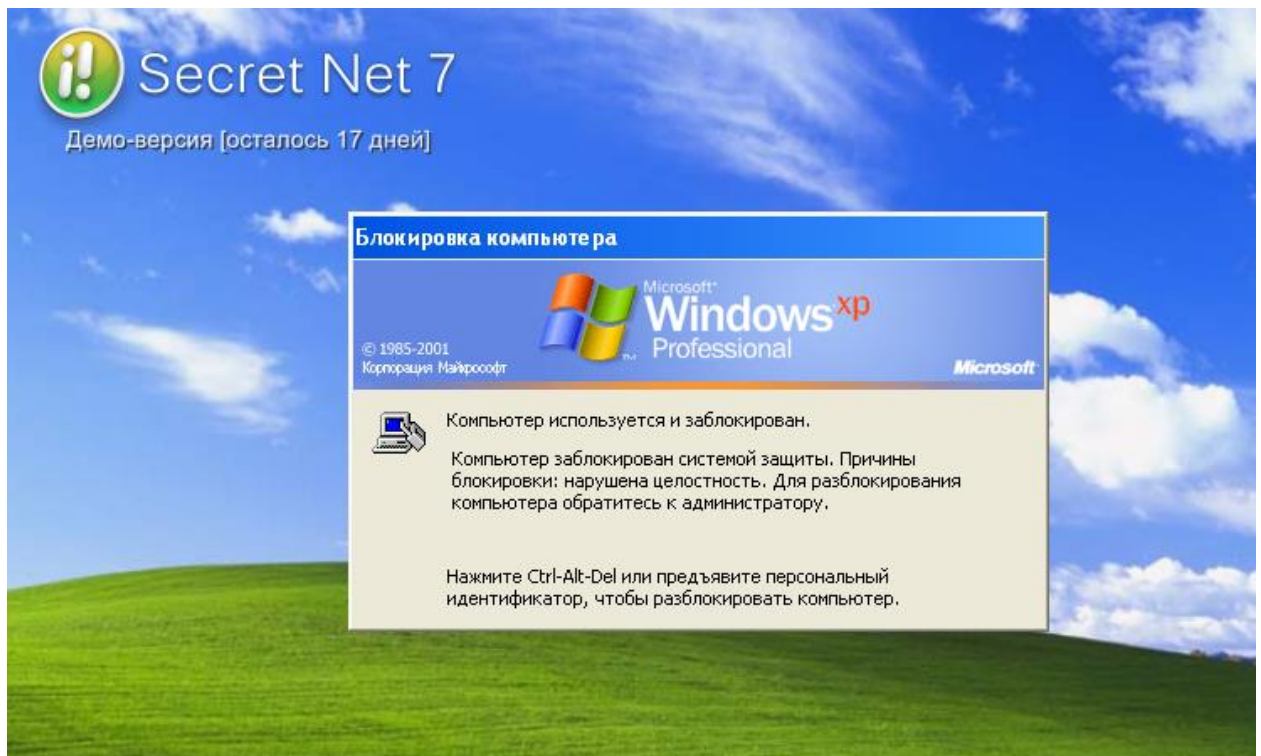


Рисунок 30 – Блокировка компьютера в связи с нарушением целостности

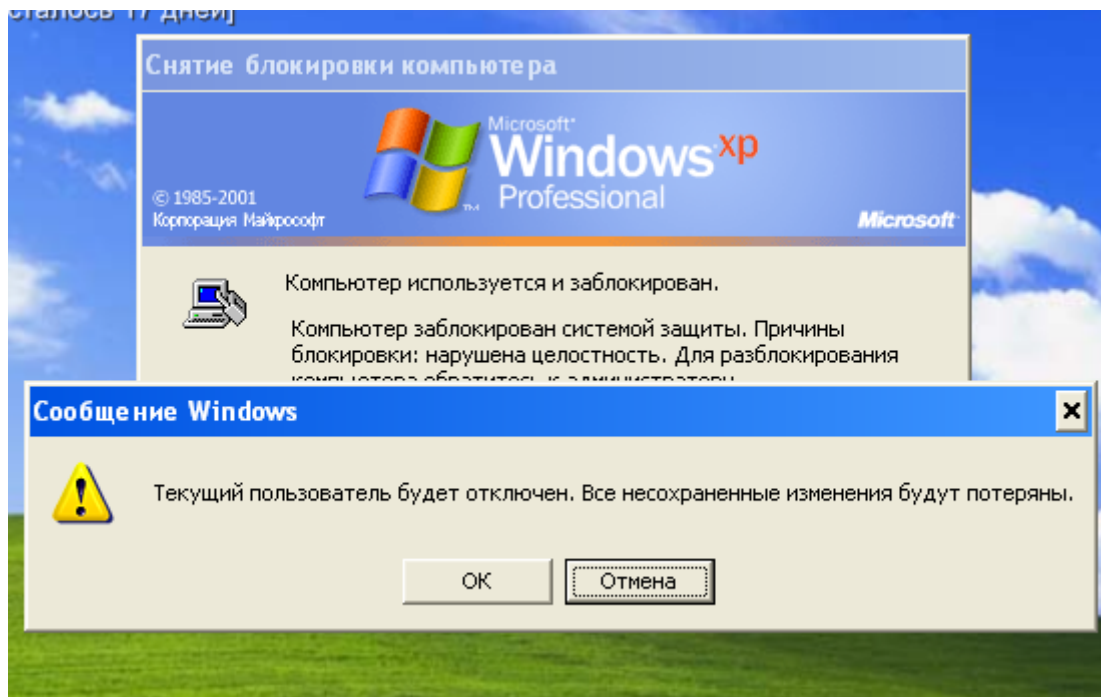


Рисунок 31 – Отключение пользователя

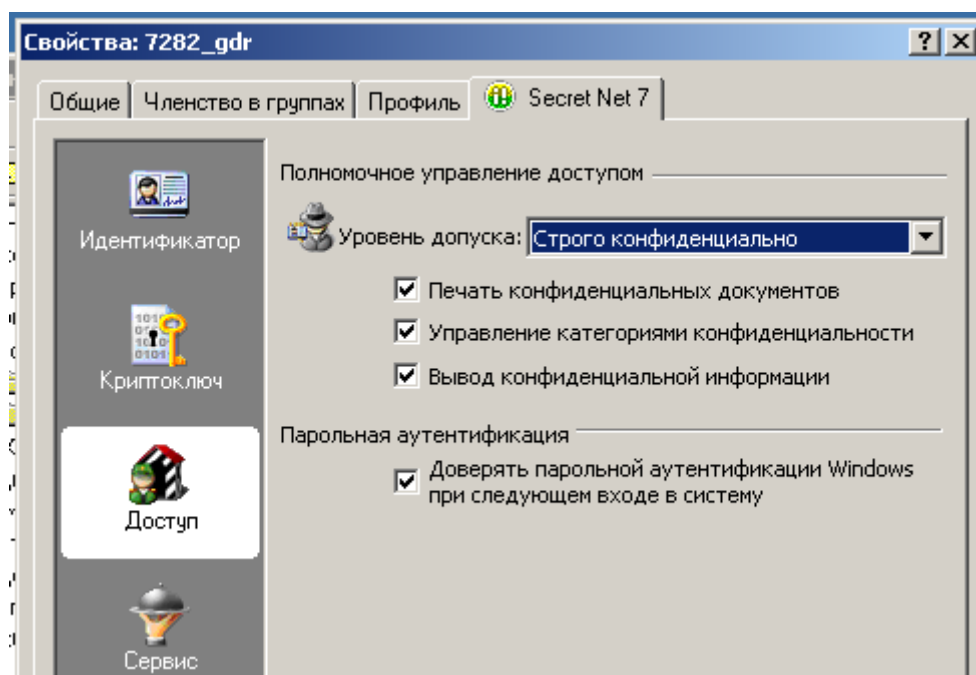


Рисунок 32 – Задание уровня допуска учётной записи

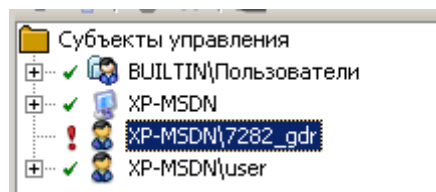


Рисунок 33 – Добавление учётной записи в субъекты управления

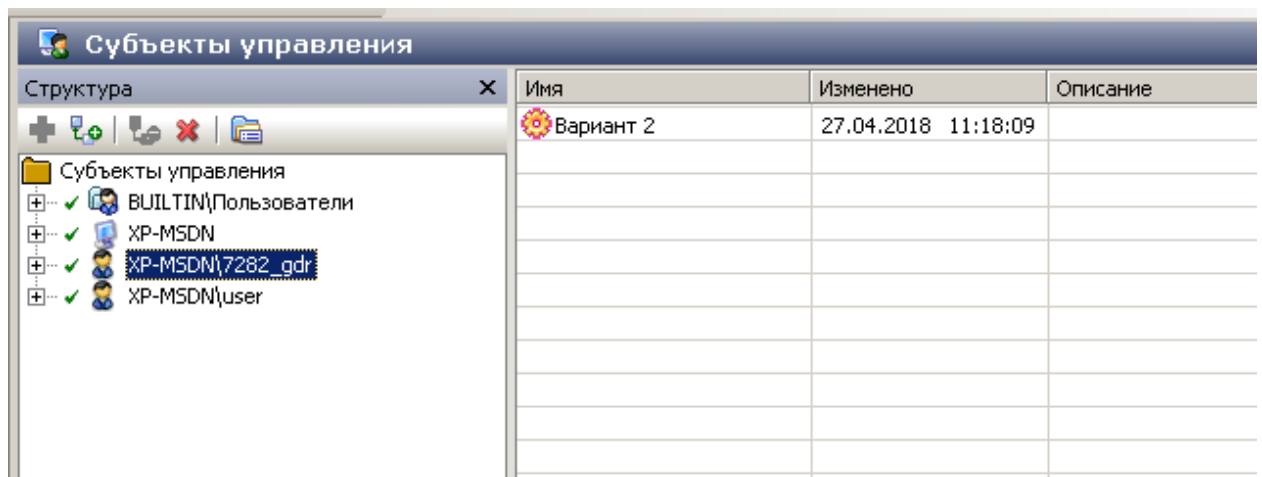


Рисунок 34 – Добавление задания для 7282_gdr

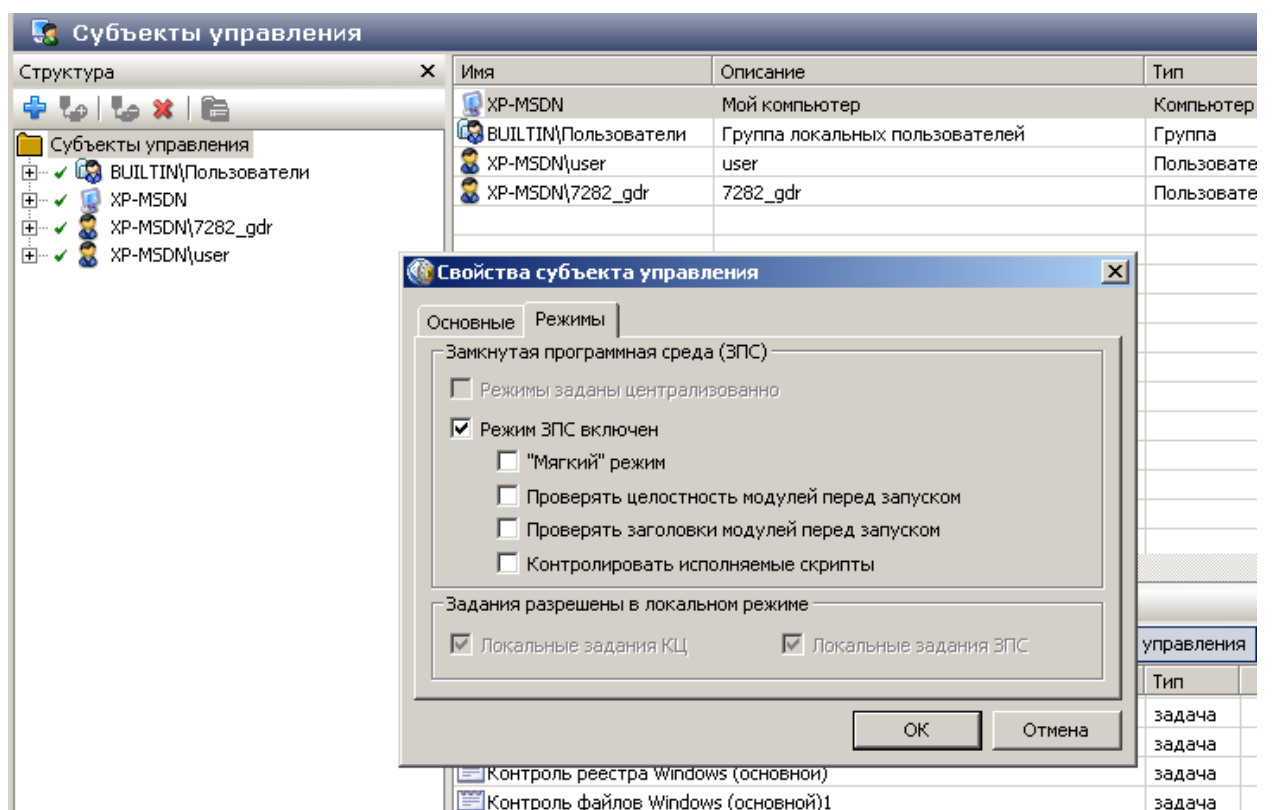


Рисунок 35 – Свойства субъекта управления, «Жёсткий режим»

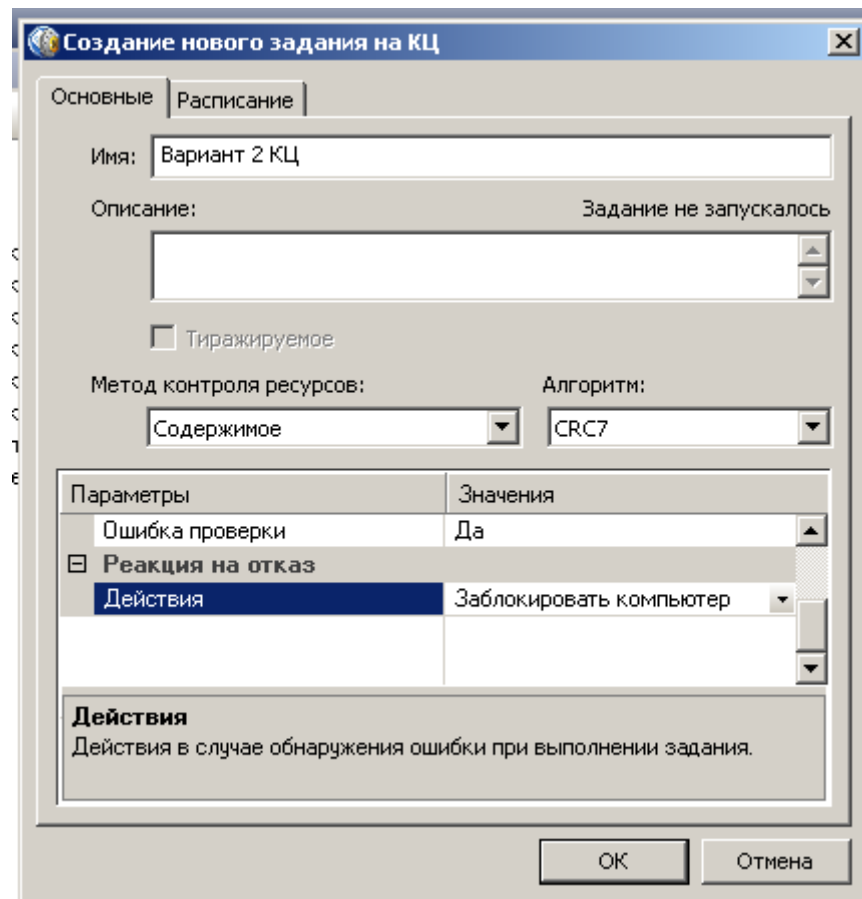


Рисунок 36 – Создание нового задания на КЦ

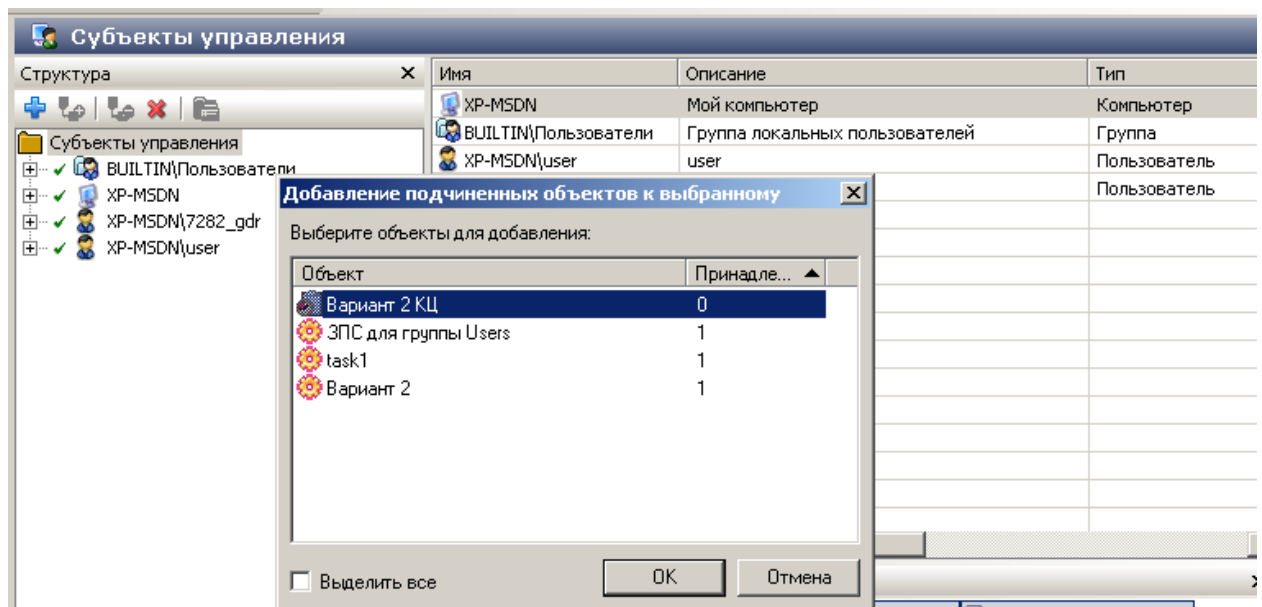


Рисунок 37 – Задание контроля целостности для компьютера

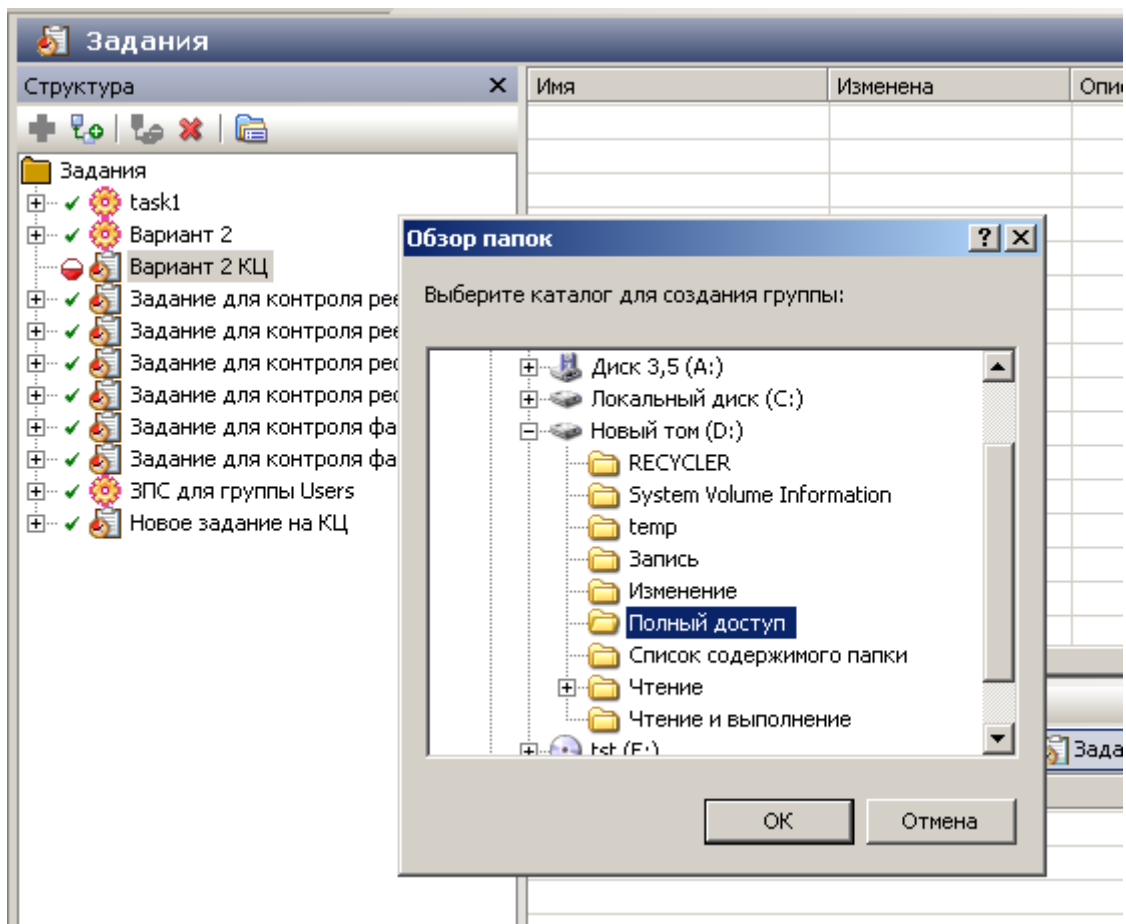


Рисунок 38 – Выбор каталога для контроля целостности

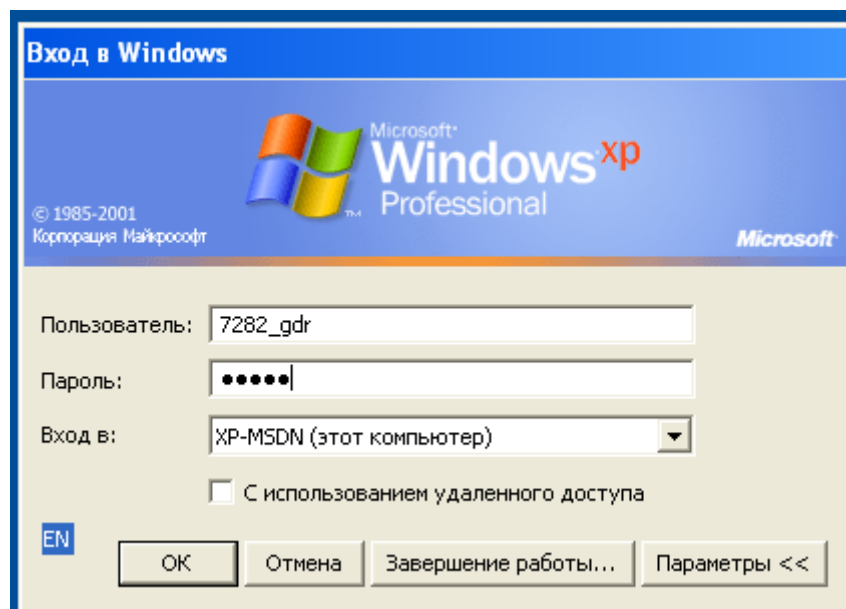


Рисунок 39 – Вход под учётной записью 7282_gdr

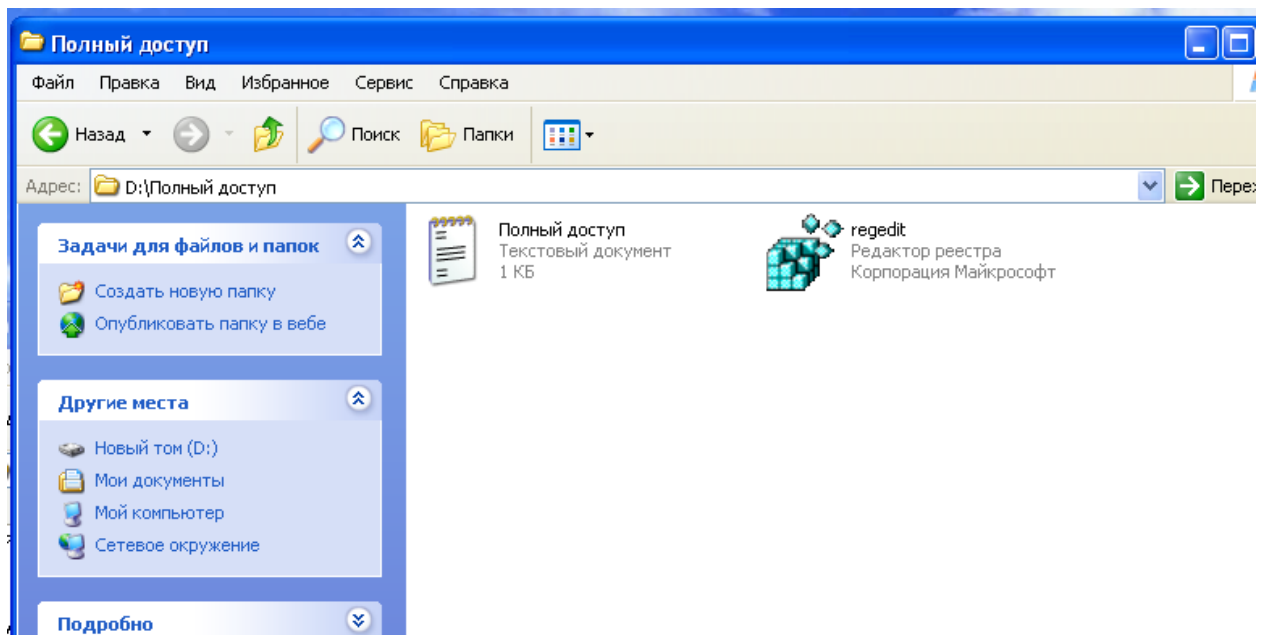


Рисунок 40 – Подмена содержимого каталога, находящегося под контролем целостности



Рисунок 41 – Проверка механизма контроля целостности

3 Заключение

В ходе данной работы были изучены и приобретены навыки настройки и управления основными защитными механизмами СЗИ от НСД «Secret Net». Рассмотрены принципы обеспечения замкнутой программной среды и настройки контроля целостности.