МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
_____ 2017 г.

Администрирование пользователей с помощью програмно–аппаратного комплекса защиты информации «АККОРД-АМДЗ»

Методические указания по выполнению лабораторной работы по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» для студентов укрупненной группы специальностей 10.00.00

п
и
г

Курск 2017

УДК 621.(076.1)
Составители: М.О. Таныгин.

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *И.В. Калуцкий*

Администрирование и управление средствами контроля и фильтрации сетевых пакетов: методические указания по выполнению лабораторной работы по дисциплине «Программно-аппапаратные средства обеспечения информационной безопасности» / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. Курск, 2016. 21 с.: ил., ,Библиогр.: с. 21.

Излагаются методические указания по выполнению лабораторной работы на персональной ЭВМ с программно–аппаратным комплексом защиты информации. Изучается основные возможности системы защиты информации «Аккорд-АМДЗ».

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность автоматизированных систем», «Информационная безопасность».

Предназначены для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения.

Текст печатается в авторской редакции
Подписано в печать . Формат 60x84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ . Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Изучение работы программно-аппаратного комплекса средств защиты информации от несанкционированного доступа "Аккорд-АМДЗ". Реализация заданной политики безопасности на основе "Аккорд-АМДЗ".

2. РАБОТА С ПРОГРАММНО-АППАРАТНЫМ КОМПЛЕКСОМ «АККОРД-АМДЗ»

2.1. Создание пользователей

- Запустим «Редактор прав доступа» (рис. 1):

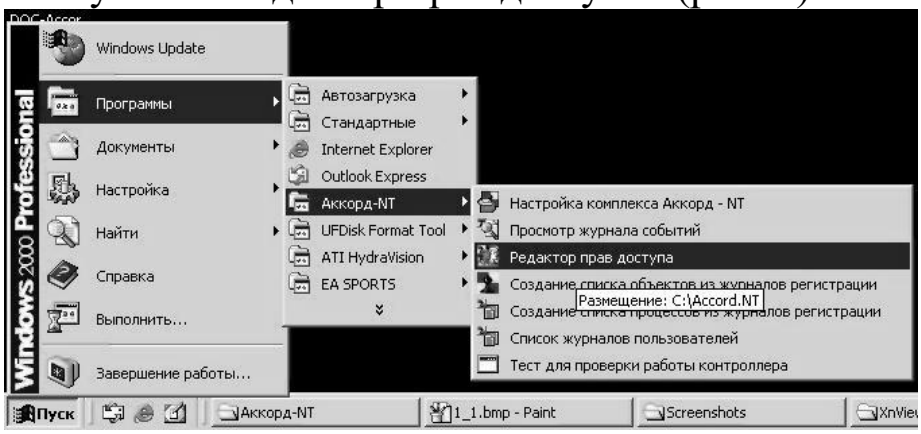


Рис. 1 - Запуск редактора прав доступа

- Появится главное окно программы (рис. 2)

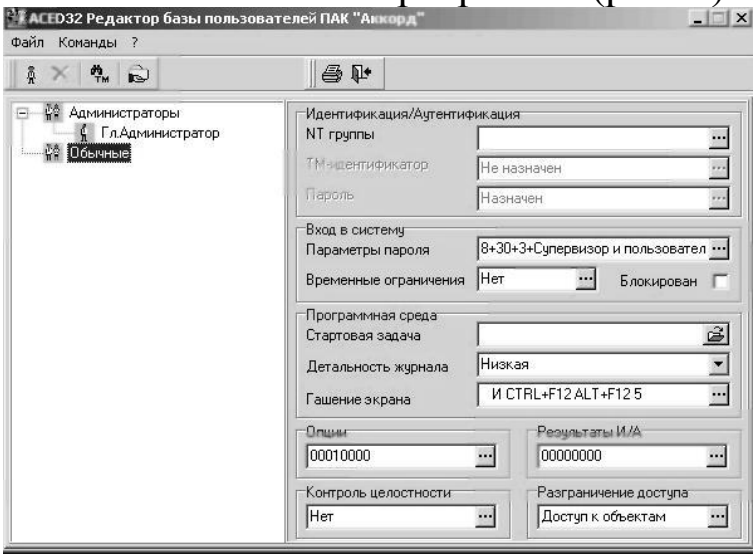


Рис. 2 - Главное окно программы «Редактор прав доступа»

- В меню «Команды» выбрать пункт «Создать».
- Появится окно ввода имени пользователя (рис. 3). Ввести имя пользователя.

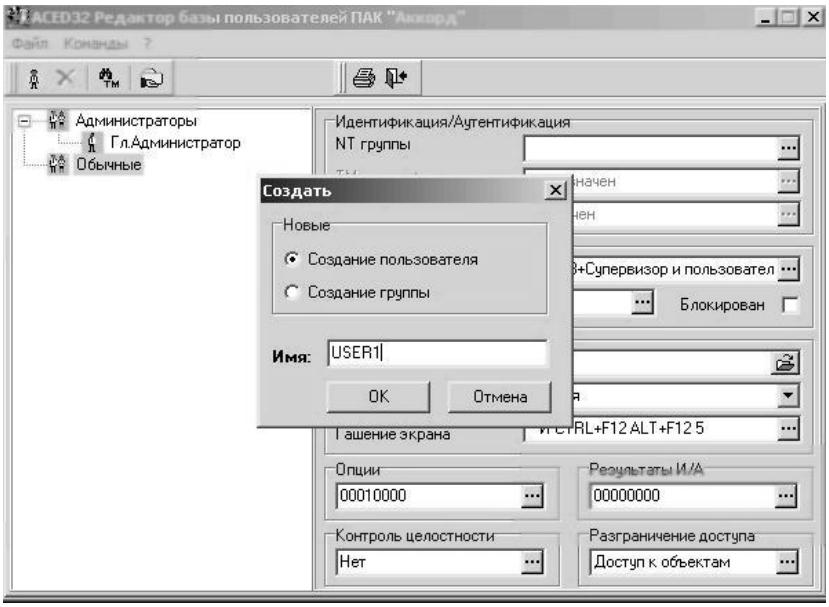


Рис. 3 - Создание пользователя

- После этого запись о новом пользователе появится в окне пользователей (рис. 4)

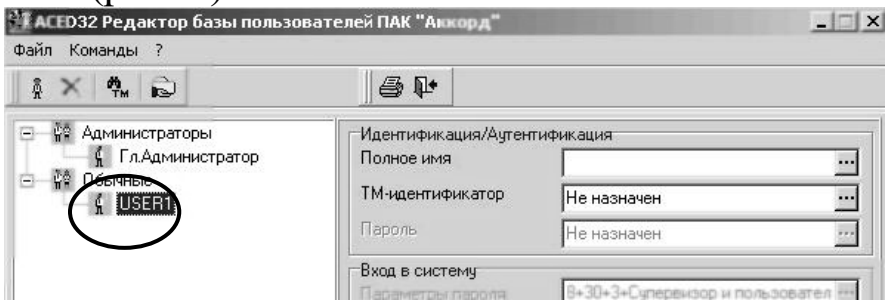


Рис. 4 - Новая запись

- Зарегистрируем ТМ–идентификатор пользователя, нажав соответствующую клавишу на панели (рис. 5). В появившемся окне выбрать необходимый пункт и нажать «Далее»

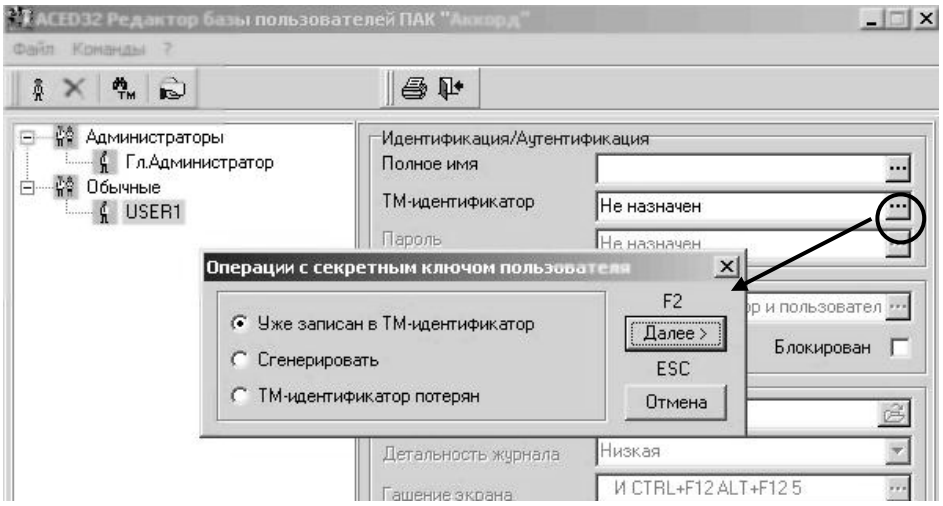


Рис. 5 - Назначение идентификатора

- Появится запрос на ТМ–идентификатор. Прислонив ключ к считывателю подождать несколько секунд. После этого в окне «ТМ–идентификатор» появится номер присвоенного созданному пользователю идентификатора (рис. 6)

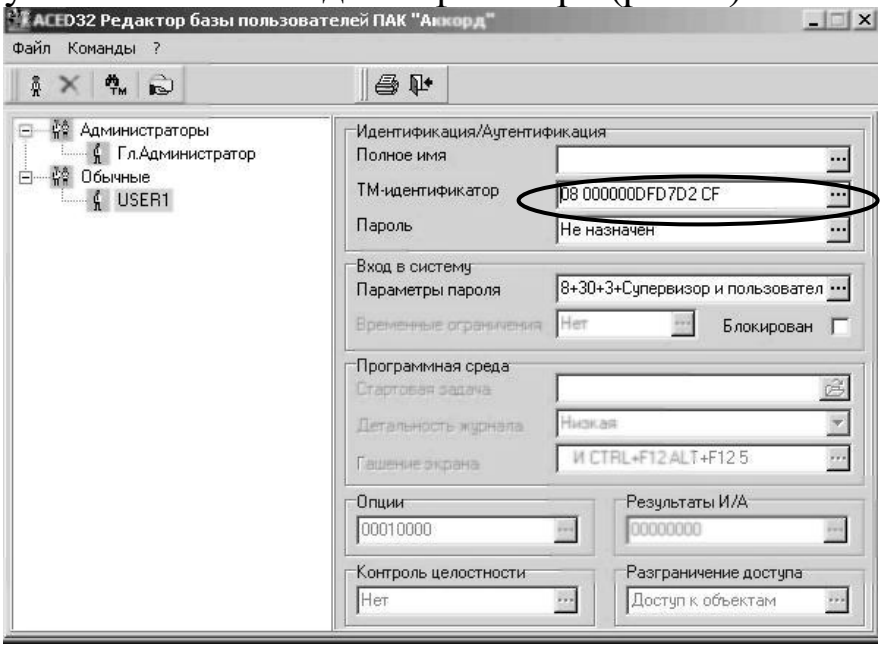


Рис. 6 - Регистрация ТМ–идентификатора

- Пользователю можно задать пароль. Для этого вначале необходимо задать параметры вводимого пароля, нажав соответствующую клавишу в окне редактора. (Рис. 7)

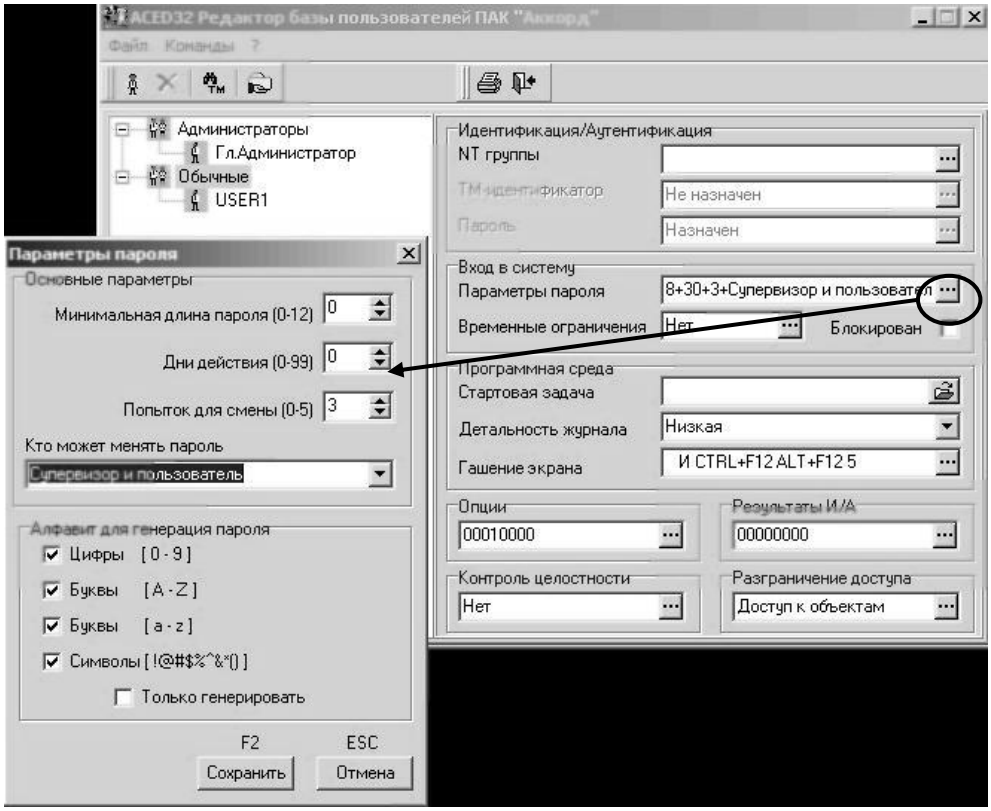
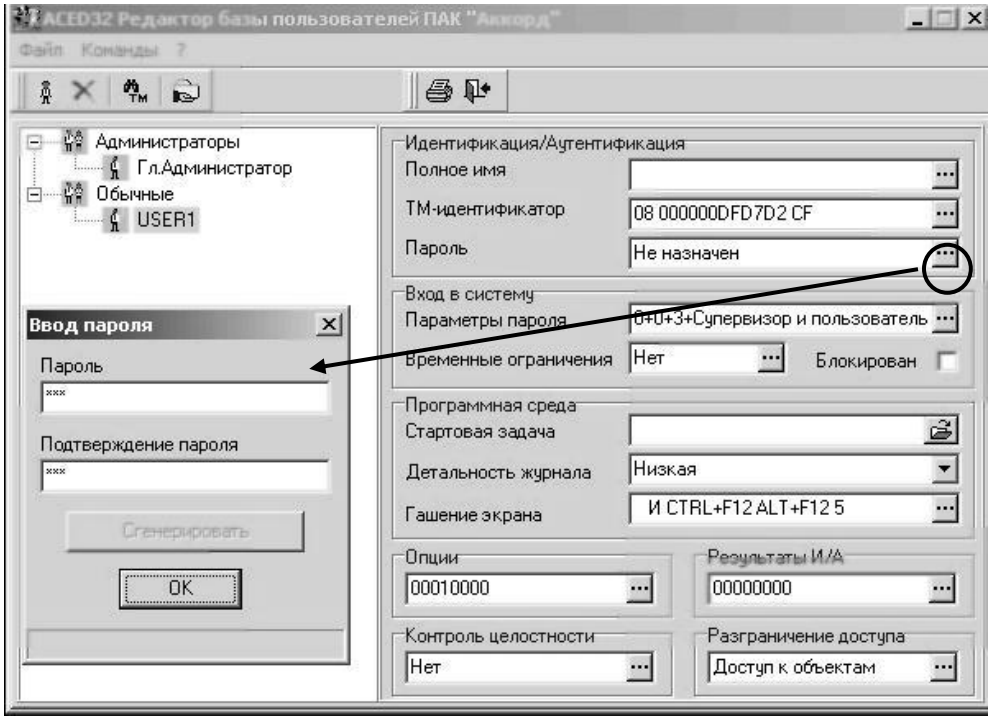


Рис. 7 - Задание параметров пароля

- Задав требуемые параметры, ввести пароль пользователя (рис. 8)



2.2. Установка параметров входа в систему

2.2.1. Установка временных ограничений на авторизацию

- Нажать кнопку напротив окна «Временные ограничения» (рис. 8)

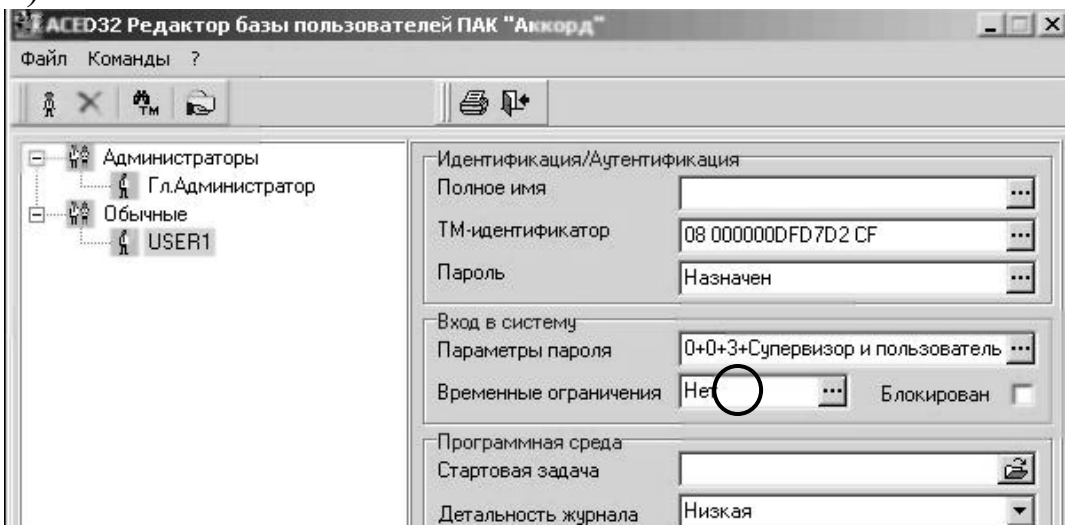


Рис. 8 - Установка временных ограничений

- Появится окно установки ограничений на время входа (рис. 9). Для запрещения/разрешения времени входа выделить требуемые ячейки и нажать кнопку «Запретить»/«Разрешить».

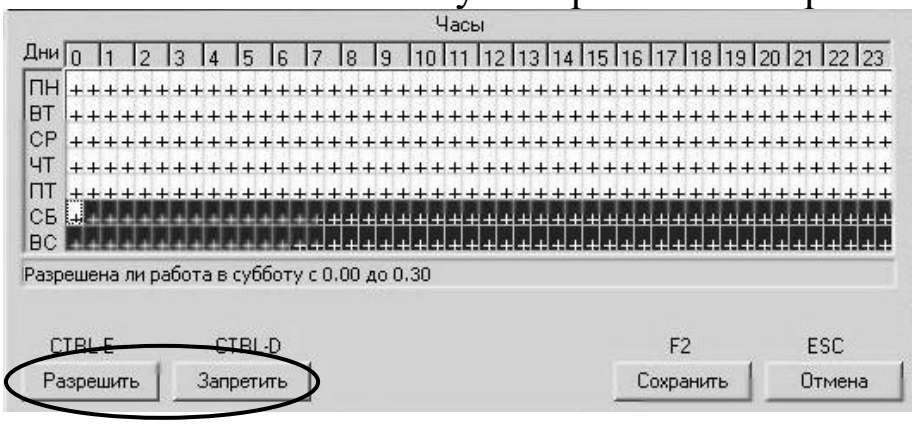


Рис. 9 - Окно установки временных ограничений

- Плюсы в ячейках соответствуют возможности входа пользователя в данное время, минусы – невозможности.
- После установки ограничений нажать кнопку «Сохранить»

2.2.2.Назначение стартовой задачи

- Нажать кнопку напротив окна «Стартовая задача» (рис. 10)

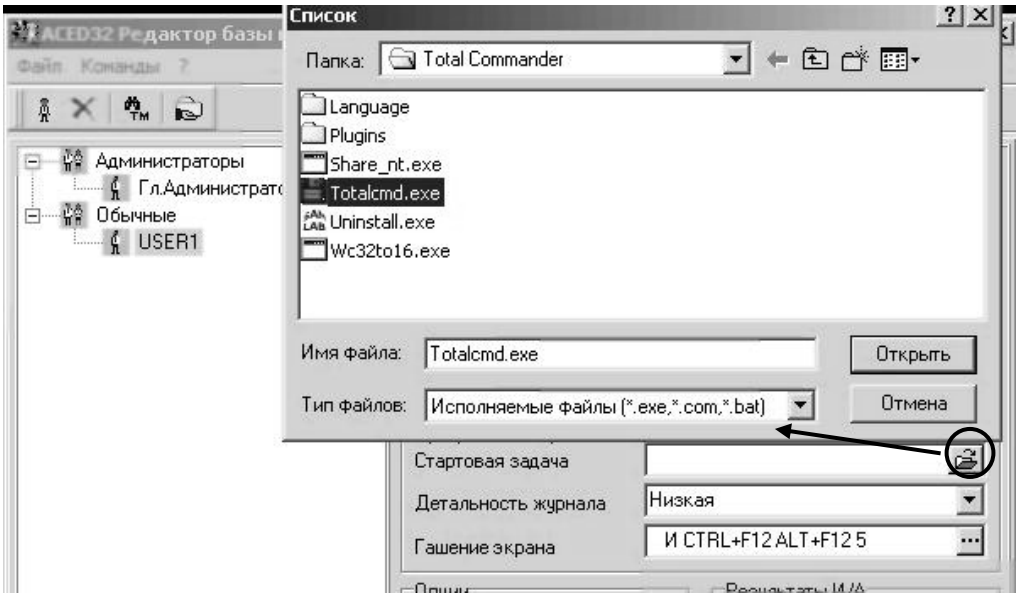


Рис. 10 - Назначение стартовой задачи

- Выбрать приложение, которое будет автоматически запускаться в начале работы пользователя
- Данное приложение появится в окне «Стартовая задача» (рис. 11)

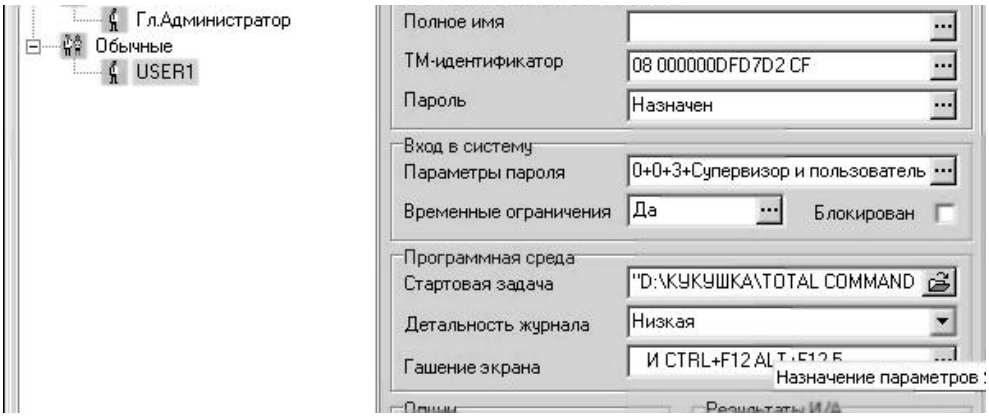


Рис. 11 - Установленная стартовая задача

2.3. Установка ресурсов, доступных пользователей

- Нажать клавишу напротив окна «Доступ к объектам» (рис. 12)

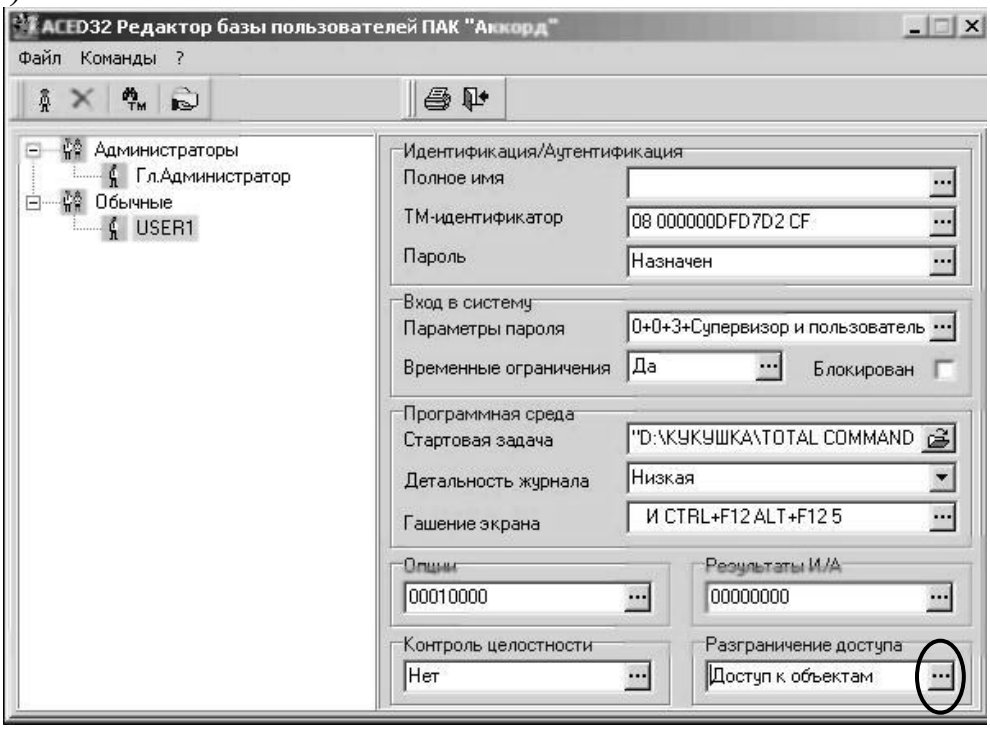


Рис. 12 - Установка ограничений на доступ к ресурсам

- Появится окно редактирования доступных ресурсов (рис. 13).

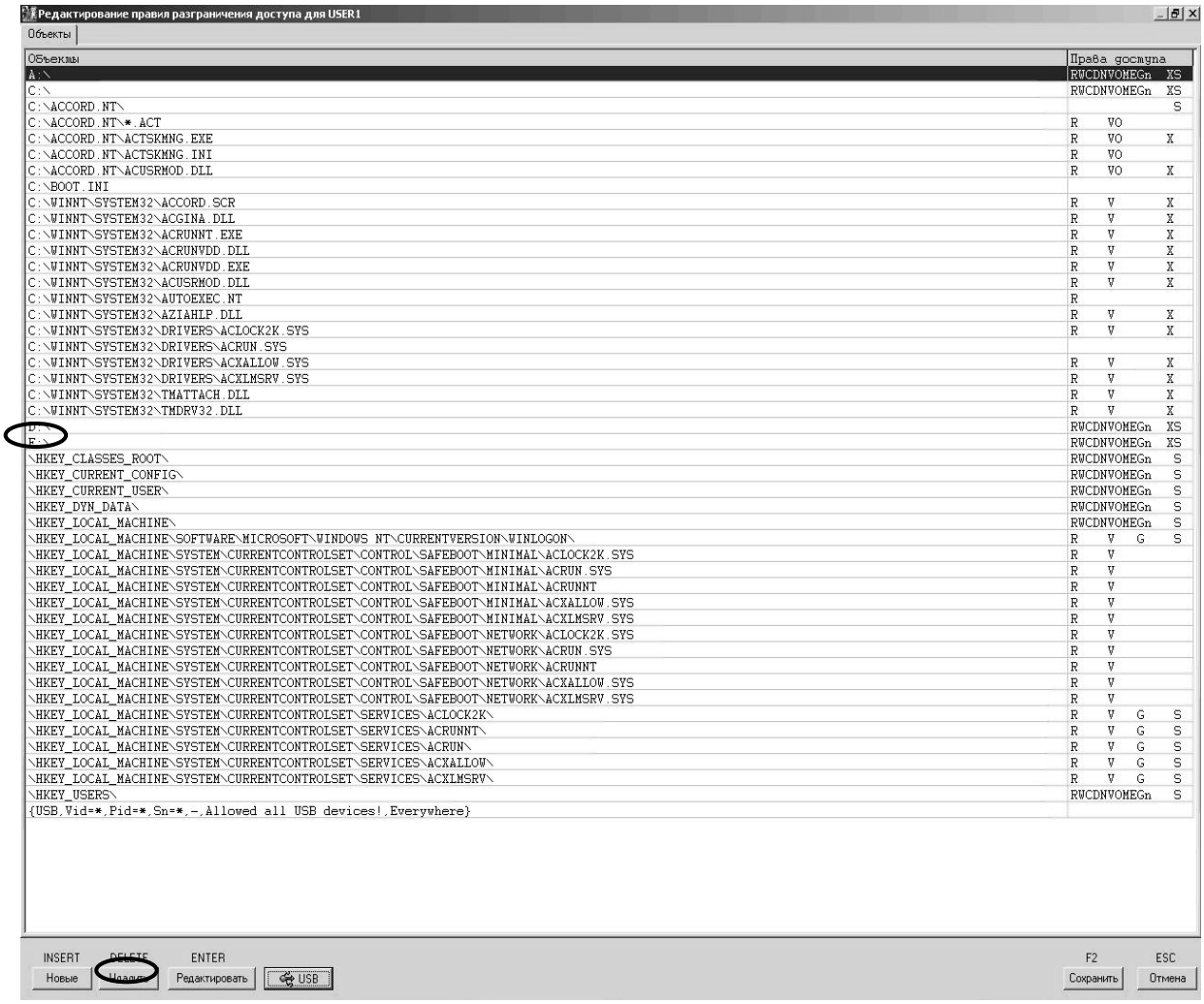


Рис. 13 - Окно редактирования доступных ресурсов

В появившемся окне приведён список всех доступных пользователю ресурсов и виды доступа к ним, которые разрешены. Список возможных прав доступа приведен в таблице 1.

Таблица 1 – Права доступа к ресурсу

Обозначение	***Вид доступа***
Операции с файлами	
R	Файлы могут быть открыты для чтения
W	Файлы могут быть открыты для записи
C	Можно создавать файлы в каталоге
D	Можно удалять файлы из каталога
N	Можно переименовывать файлы в каталоге
V	Содержимое каталога можно просматривать
O	Файлы могут быть дописаны

Обозначение	*Вид доступа*
Операции с подкаталогами	
M	Разрешено создавать подкаталоги
E	Разрешено удалять подкаталоги
G	Разрешено входить в подкаталоги
n	Разрешено переименовывать подкаталоги
Операции наследования прав	
0	Права доступа не наследуются в подкаталогах
S	Права доступа наследуются в подкаталогах любого уровня
1	Права доступа наследуются в подкаталогах лишь на один уровень
Операции с программами	
X	Разрешён запуск программ
Операции регистрации событий	
r	Регистрировать операции чтения
w	Регистрировать операции записи

- Для удаления ресурсов выделить строки с именем требуемых ресурсов и нажать кнопку «Удалить» (рис. 13).
- Для добавления нового ресурса нажать клавишу «Новый». Появится окно добавления ресурсов (рис. 14).

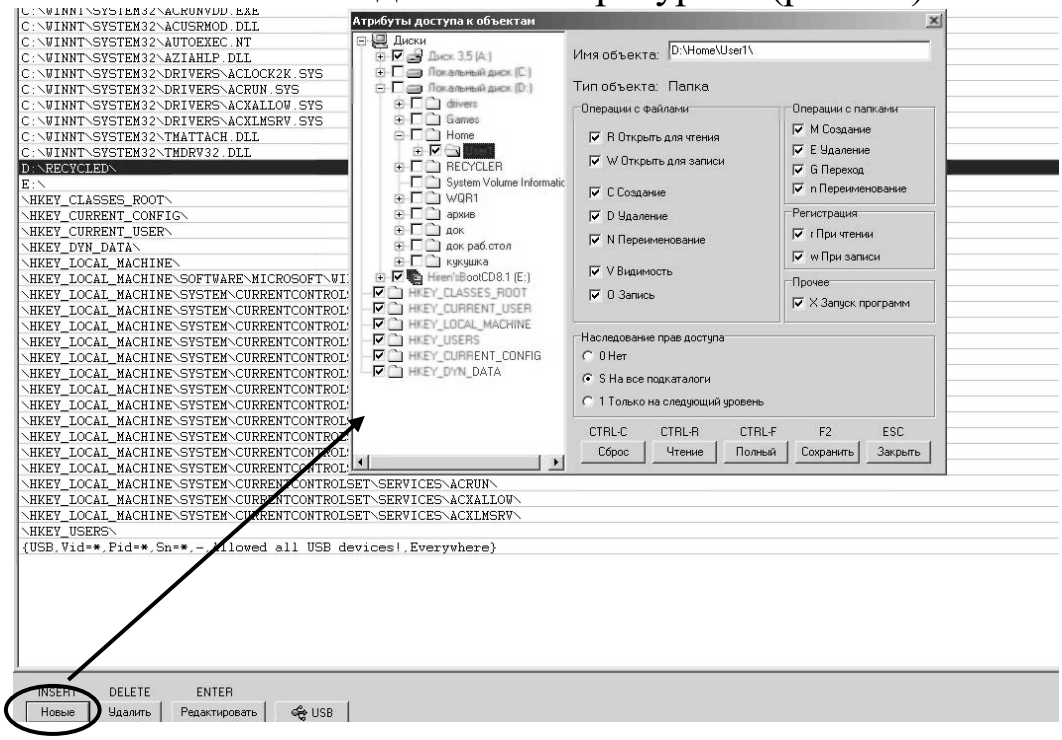


Рис. 14 - Добавление нового ресурса

- Выбрать необходимый каталог, установить требуемые права доступа к нему, нажать кнопку «Сохранить».
- Для разрешения доступа к USB–устройствам нажать клавишу «USB»
- Для сохранения изменений в списке доступных ресурсов в окне редактирования ресурсов нажать кнопку «Сохранить» (рис. 13).

2.4. Установка контроля целостности объектов

- Нажать кнопку напротив окна «Контроль целостности» (рис. 15)

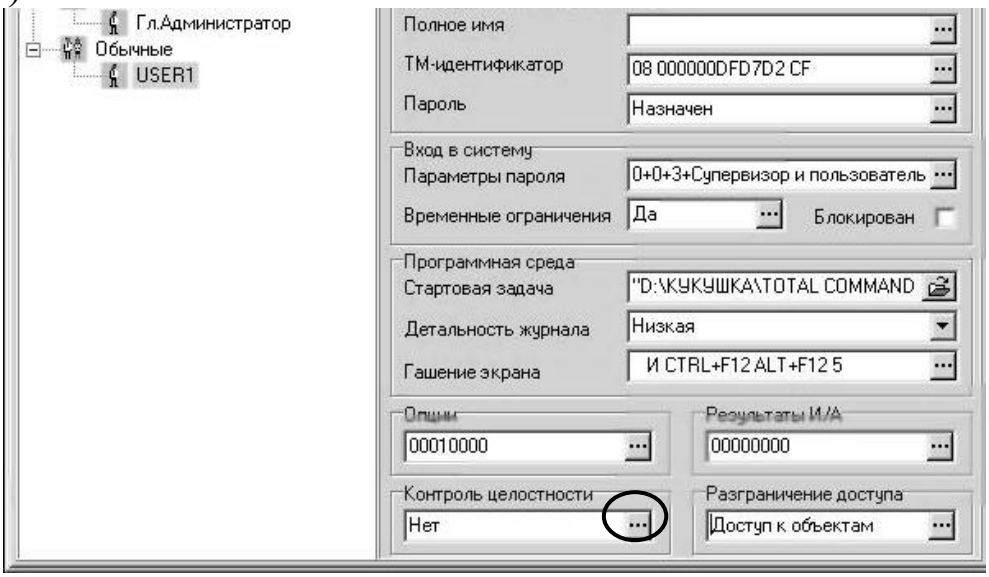


Рис. 15 - Установка контроля целостности объектов

- В появившемся окне редактирования контроля целостности объектов выбрать нужный каталог и добавить его в список контролируемых объектов (рис. 16)

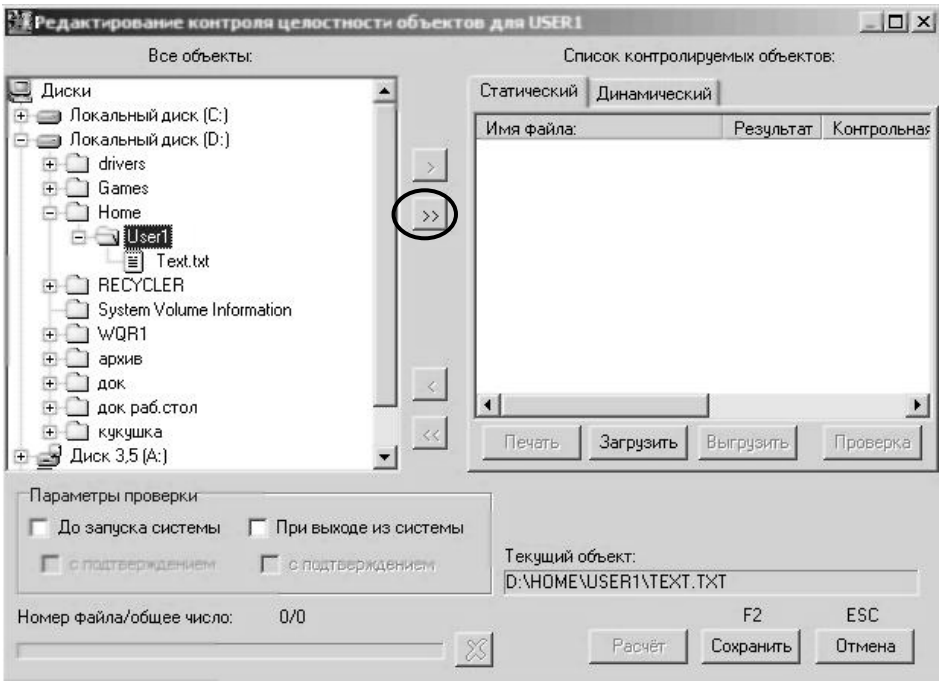


Рис. 16 - Добавление ресурсов в список контролируемых объектов

- Для установки контроля целостности над всеми файлами выбранной директории оставить фильтр по умолчанию (рис. 17). Если надо контролировать отдельные файлы каталога, в фильтр вводится требуемое значение.

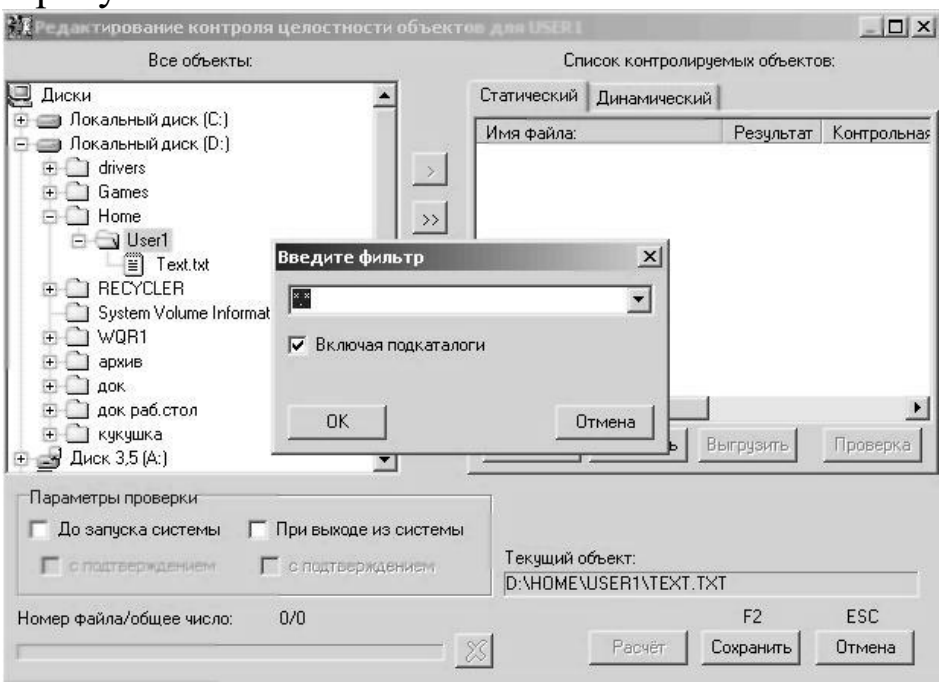


Рис. 17 - Фильтр контроля целостности

- Для расчёта контрольной суммы нажмите кнопку «Расчёт» (рис. 18).

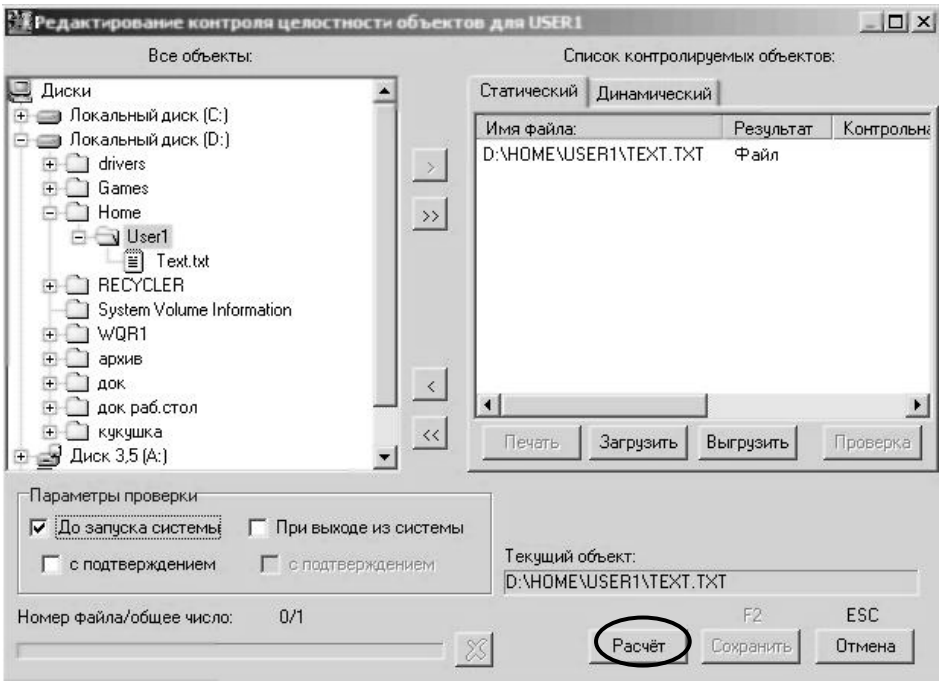


Рис. 18 - Расчёт контрольной суммы

- По запросу прислонить ТМ–идентификатор пользователя.
- После этого контроль целостности будет установлен.

2.5. Установка политики безопасности

2.5.1. Установка детальности журнала

Система Аккорд позволяет задавать различные уровни детальности журнала аудита безопасности (рис. 19). При выборе уровня детальности следует исходить из соображений требований политики безопасности, а также их удобства просмотра регистрируемых сведений с помощью программы просмотра журнала безопасности. Очевидно, что высокая детальность журнала затрудняет анализ регистрируемых данных и увеличивает размер журнала безопасности. Поэтому применять её в некоторых случаях нецелесообразно. С другой стороны, если речь идёт о защите высокосекретных данных с высокой степенью надежности, то тут необходим более высокий уровень детальности журнала.

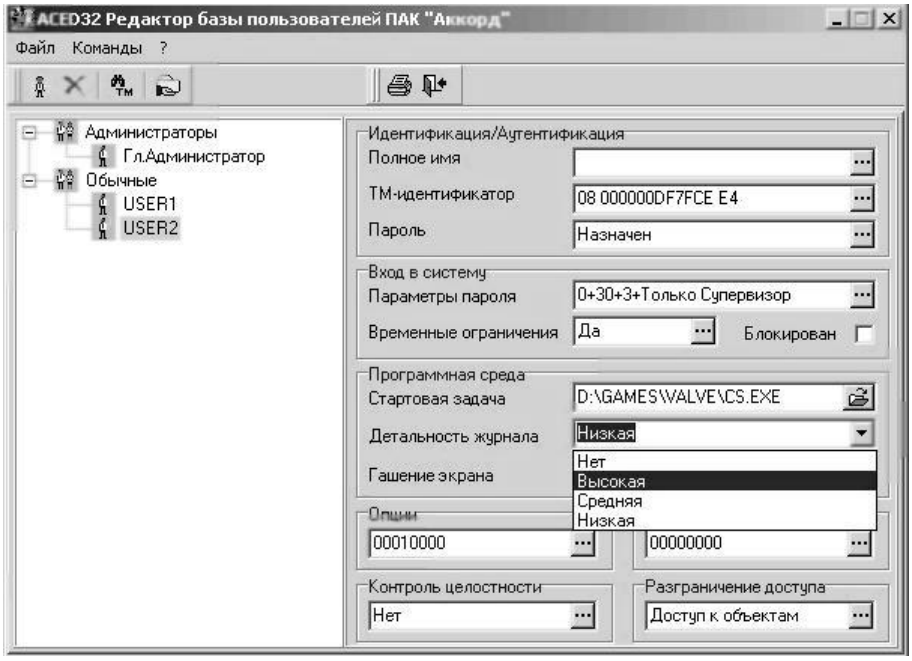


Рис. 19 - Установка детальности журнала

2.5.2. Установка дополнительных опций

При работе с системой защиты информации, в зависимости от требуемого уровня защищённости данных, иногда требуется устанавливать дополнительные параметры безопасности, такие как затирание удаляемых с диска файлов, возможность изменения времени и даты и т. д.

- Для установки дополнительных опций безопасности нажмите кнопку напротив окна «Опции». Появится окно редактирования дополнительных опций безопасности (рис. 20).

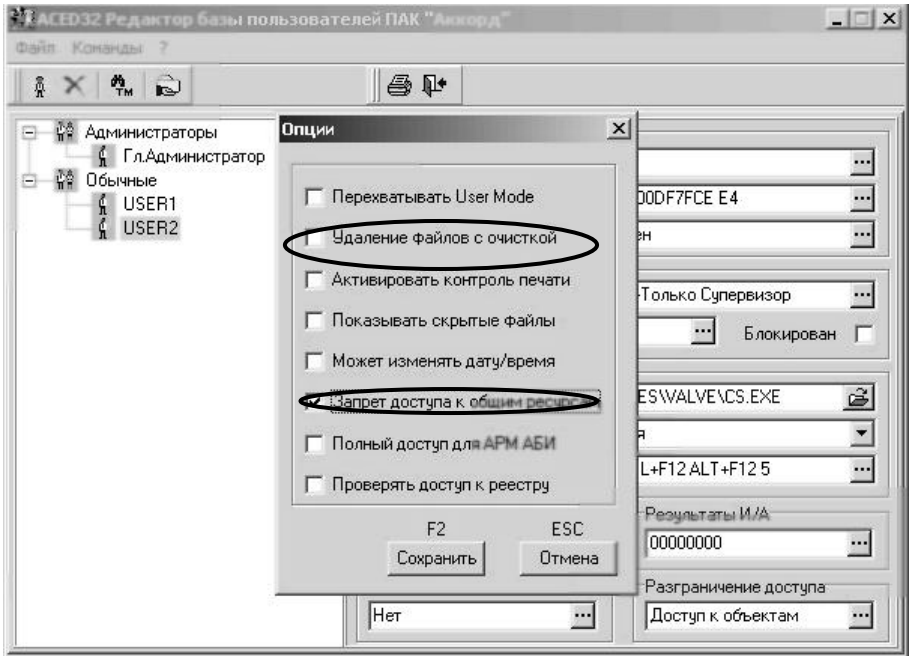


Рис. 20 - Окно установки дополнительных опций безопасности

- Поставить галочки в нужных пунктах и нажать «Сохранить» (рис. 20)
- Установленные опции опции будут отображены в окне «Опции» (рис. 21).

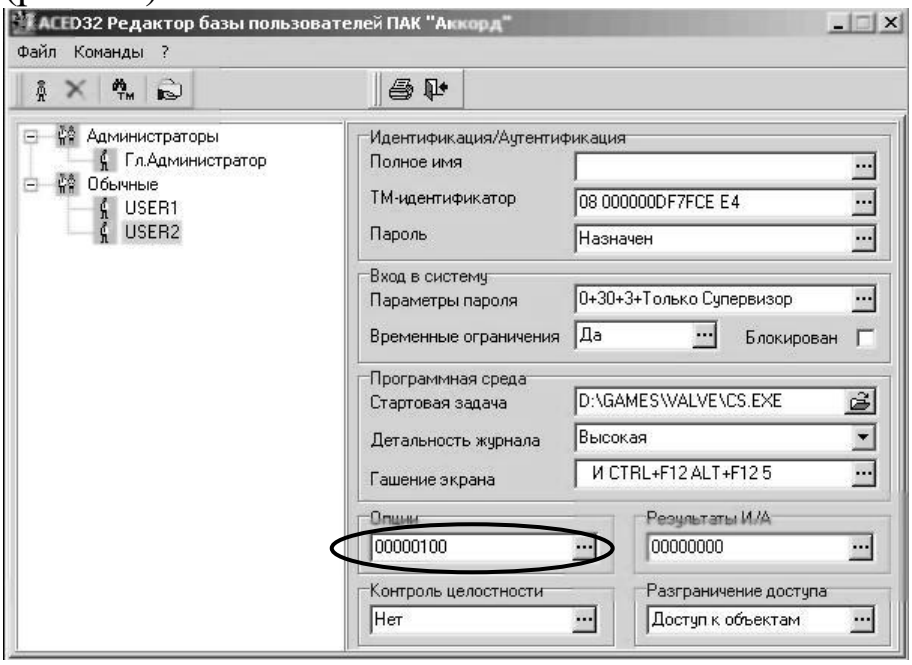


Рис. 21 - Установленные опции безопасности

2.5.3. Установка регистрируемых событий

- Для установки регистрируемых событий нажать кнопку напротив окна «Результаты И/А»
- В появившемся окне отметить галочками требуемые пункты, нажить «Сохранить» (рис. 21)

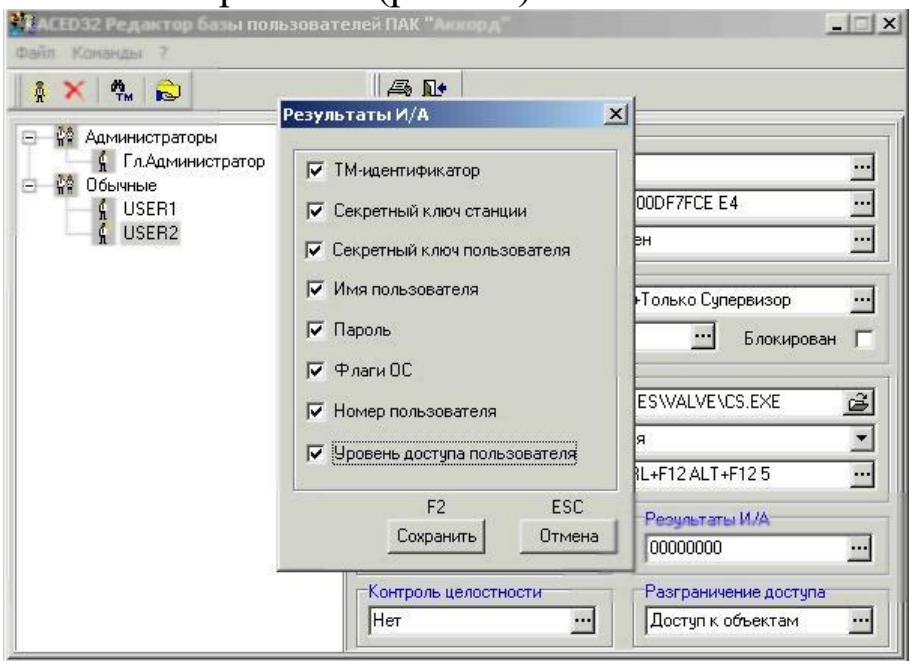


Рис. 22 - Установка регистрации результатов идентификации/аутентификации

2.6. Определение ресурсов, доступных для общего доступа

- В меню «Команды» «Редактора прав доступа» выбрать пункт «Имена общих ресурсов». Появится окно, в котором отображены все общедоступные ресурсы (рис. 23).
- Для запрещения общего доступ к ресурсам выделить нежелательные строки и нажать «Удалить».

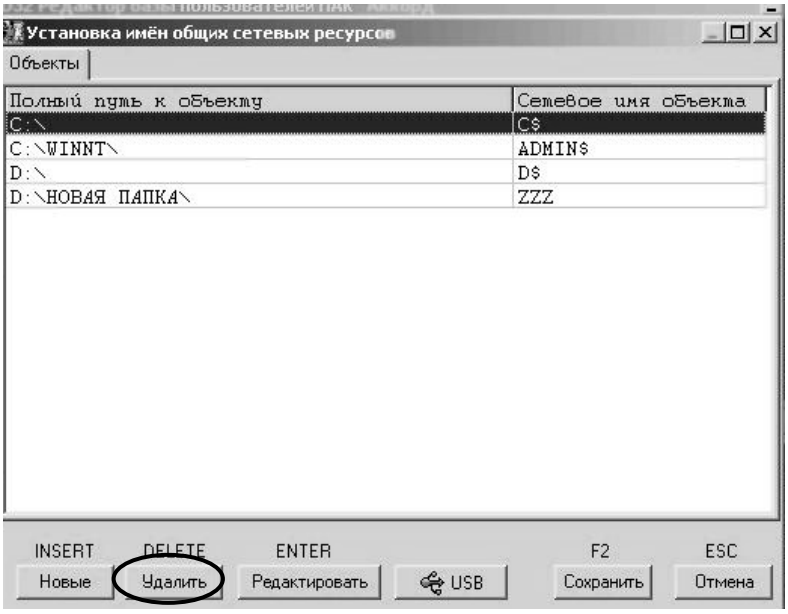


Рис. 23 - Удаление ресурса из списка общедоступных

- Для добавления затем нажмем «Новые», чтобы разрешить общий доступ к новым ресурсам.

1. Выбрать каталог, к которому хотите открыть общий доступ и нажать «Сохранить» (рис. 24)

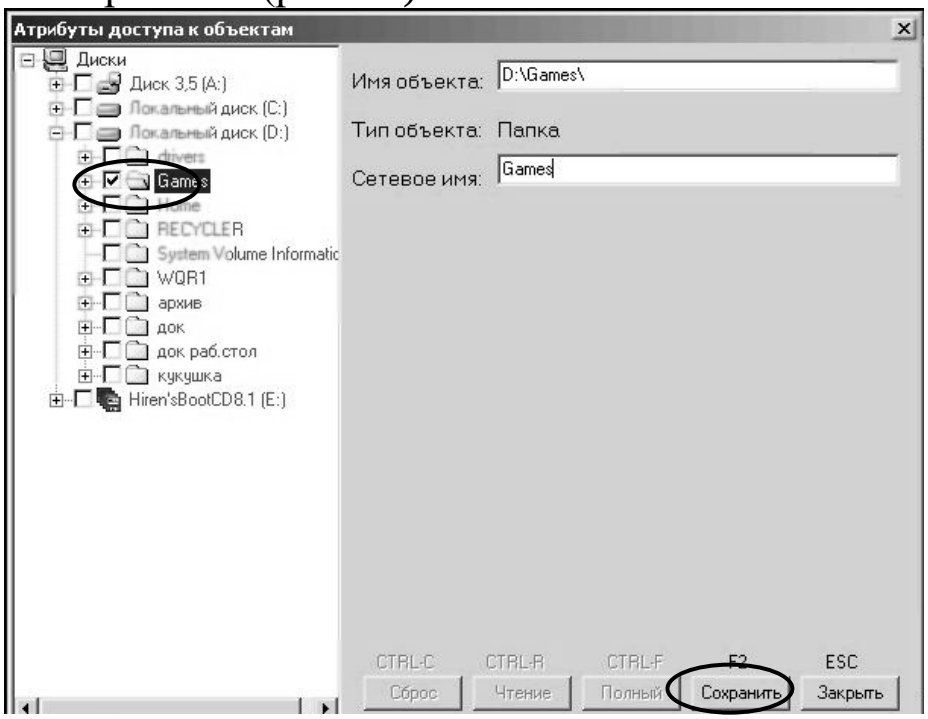


Рис. 24 - Добавление ресурса в список общедоступных

3. ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

Лабораторная работа выполняется бригадой студентов в составе 2–х человек. В ходе выполнения лабораторной работы им предстоит создать пользователей. Имена пользователей формируются по следующему правилу:

<номер группы>_<первые буквы фамилии, имени, отчества первого студента>_<первые буквы фамилии, имени, отчества второго студента>_<номер создаваемого пользователя>.

Общие ресурсы компьютера должны включать, кроме прочего папку с именем <номер группы>_<первые буквы фамилии, имени, отчества первого студента>_<первые буквы фамилии, имени, отчества второго студента>.

1. Создать новые учетные записи двух пользователей:
   - Первый пользователь может работать в течение всего учебного занятия все дни кроме выходных, он имеет доступ к сменным носителям информации, доступ к общим ресурсам и полный доступ к своему рабочему каталогу. Авторизуется ТМ-ключом и паролем.
   - Второй пользователь может авторизоваться только в течении последнего часа учебного занятия и имеет полный доступ только к своему рабочему каталогу. Авторизуется ТМ-ключом.
2. Каждому пользователю назначить стартовое приложение
3. Авторизироваться под каждым пользователем и проверить возможность доступа к различным ресурсам компьютера.
4. Авторизироваться под учётной записью администратора и просмотреть журнал безопасности. Найти в нём записи, соответствующие ранее произведённым действиям созданных пользователей.

4. СОДЕРЖАНИЕ ОТЧЁТА

1. Скриншоты процесса создания новых пользователей.
2. Скриншоты работы под учётными записями созданных пользователей.
3. Результаты аудита.

5. ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. Назовите основные механизмы идентификации/ аутентификации пользователей, применяемые в системе «Аккорд».
2. Назовите основные возможности программы «Редактор прав доступа».
3. Что такое «общие ресурсы» компьютерной системы?
4. Как происходит назначение прав доступа к ресурсам компьютера в системе «Аккорд»?
5. Для чего необходим контроль целостности данных и как он реализуется средствами системы «Аккорд»?

6. БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Информационная безопасность офиса. Выпуск 1. Технические средства защиты информации [Текст] : учеб. пособие / : ТИД «ДС», 2003, 216 с.
2. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей [Текст]: учеб.пособие / Платонов В.В.: Академия, 2006, 416 с.
3. Черкесов, Г.А. Надежность аппаратно-программных комплексов [Текст]: учеб. пособие / Г.А.Черкесов, С.-Петербург,: Питер, 2004, 510 с.
4. Конявский, В.А. Управление защитой информации на базе СЗИ НСД «Аккорд» [Текст] / Конявский, В.А., 1999, 325 с.: ил.