ОКБ АПР ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

СПО «АККОРД- Win64 К»

Инструкция
по исключению возможности запуска системных команд LogOff, Shutdown и др. (наследование ПРД от группы)

Москва

2020

В данной инструкции приведены сведения о том, как исключить для пользователя возможность запуска системных команд типа Logoff, Shutdown и т.п. при использовании дискреционного метода с формированием списка контролируемых процессов.

1. Запустить программу «Настройка комплекса «Аккорд» (Пуск–> Программы–> Аккорд–> Настройка комплекса Аккорд).

В главном окне программы в поле «Механизмы разграничения доступа» установить флаги в строках «Дискреционный», «Контроль процессов» и «Наследование ПРД от группы» (рисунок **1**).

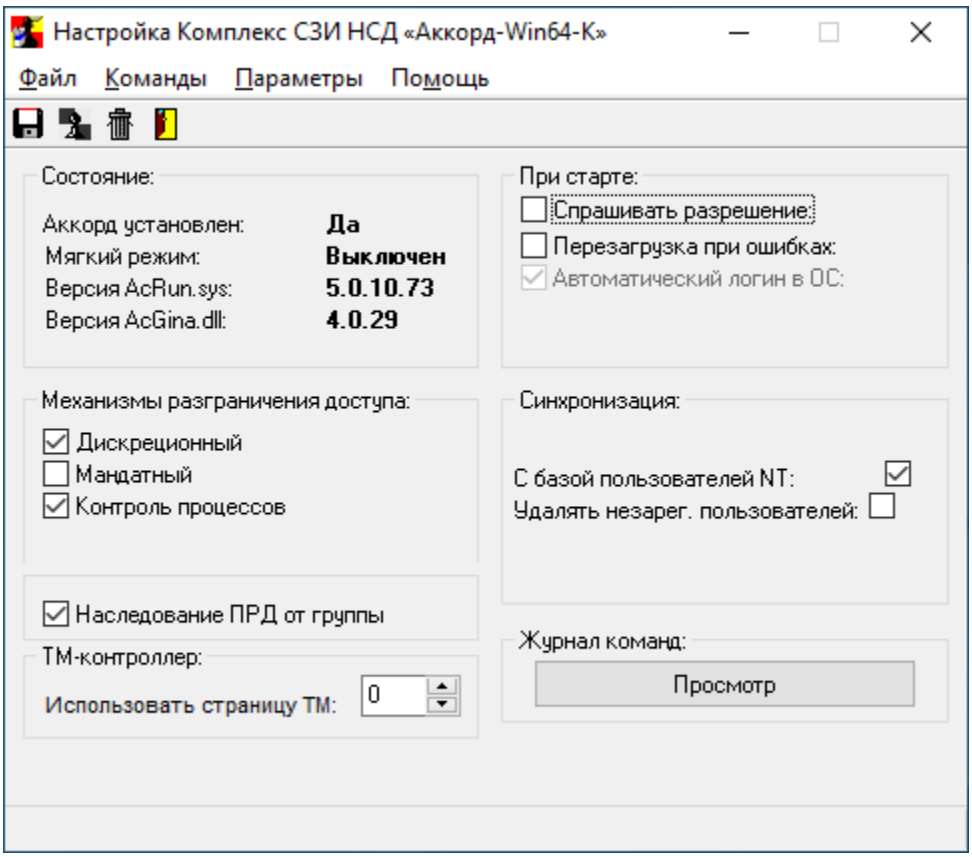

Рисунок 1 - Главное окно программы настройки комплекса «Аккорд»

2. В меню «Параметры» выбрать пункт «Дополнительные опции...» На вкладке «Разное» открывшегося окна установки дополнительных опций убрать флаг «Использовать полный путь процесса» (рисунок 2).

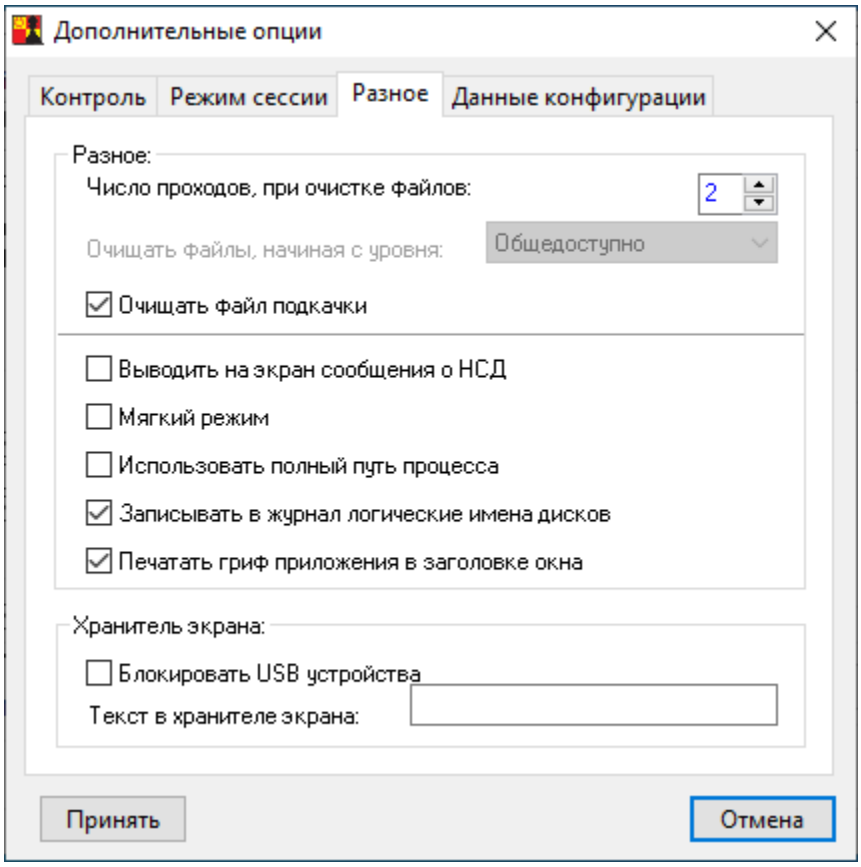

Рисунок 2 - Убрать опцию «Использовать полный путь процесса»

3. На вкладке «Режим сессии» окна установки дополнительных опций установить флаг «Завершать сессию только полной перезагрузкой» (рисунок 3).

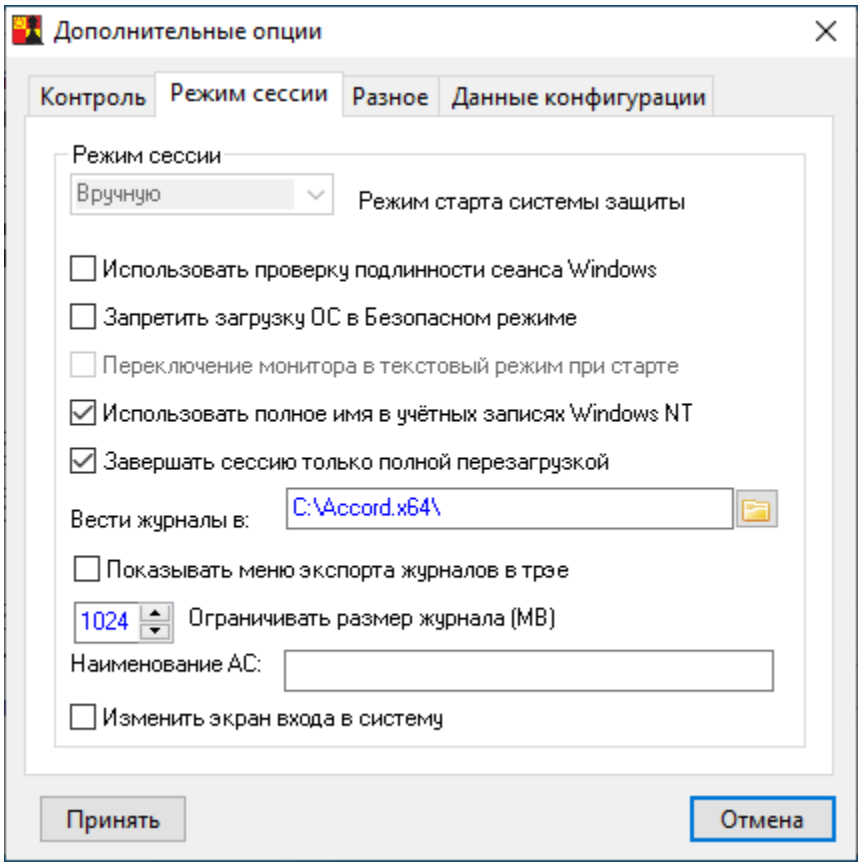

Рисунок 3 – Установка опции «Завершать сессию только полной перезагрузкой»

4. Завершить работу приложения с сохранением изменений.

5. Запустить утилиту «Редактор прав доступа» (Пуск–> Программы–> Аккорд–> Редактор прав доступа). В поле «Программная среда» установить в строке «Детальность журнала» значение «Сбор статистики», выбрав его из выпадающего списка (рисунок 4). Удаляем в Разделении доступа — Объекты и Процессы (рисунок 5).

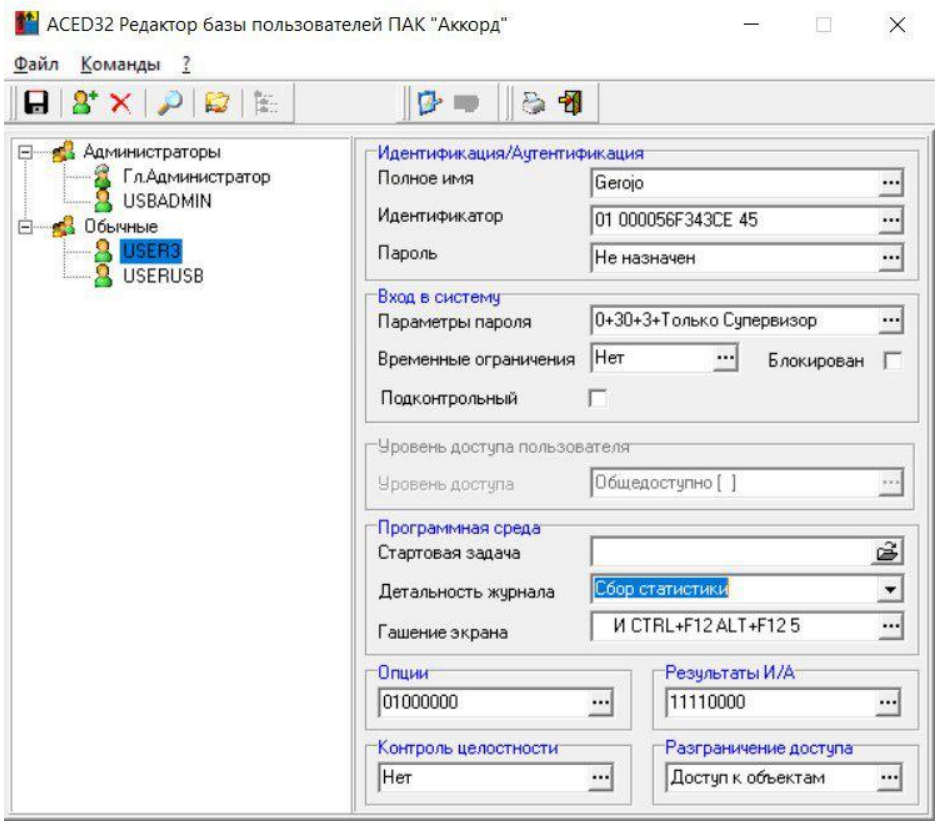

Рисунок 4 - Установка детальности журнала «Сбор статистики»

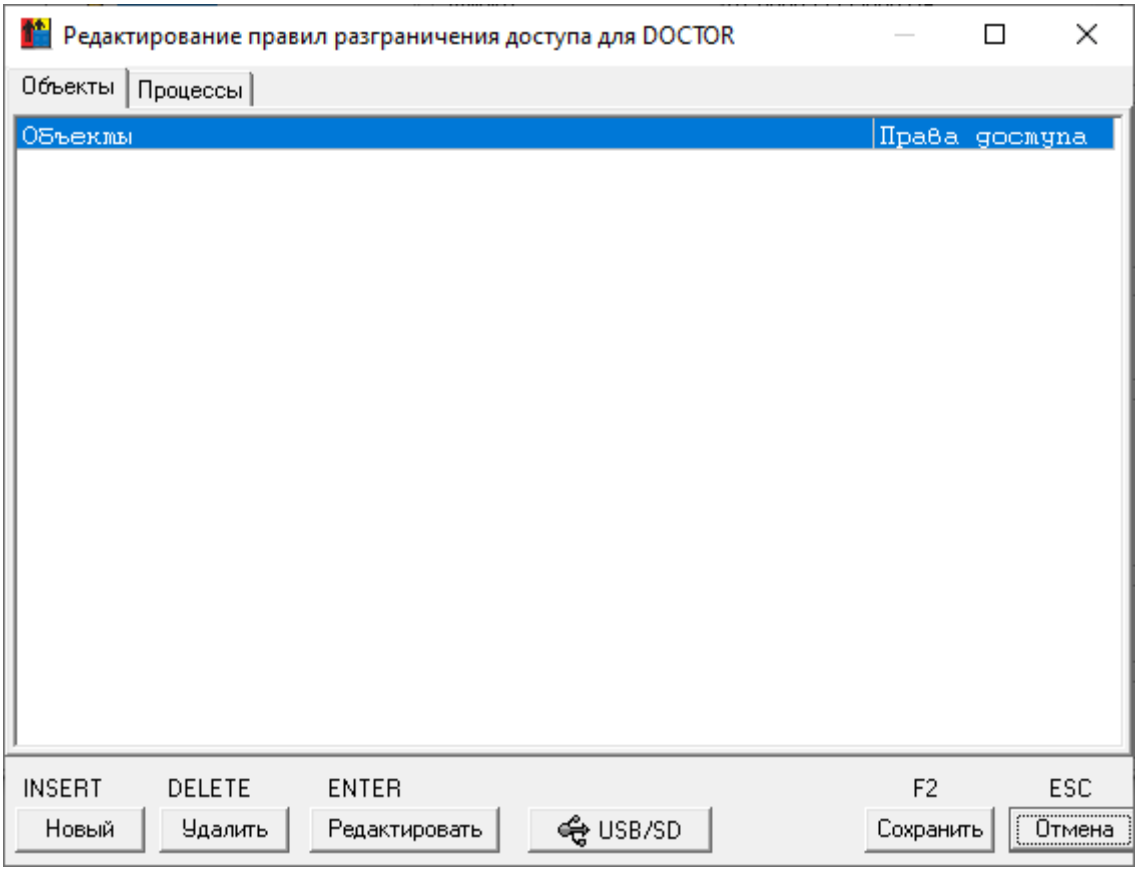

Рисунок 5 — Очищаем содержимое Объекты и Процессы

6. Перезагрузить компьютер.

7. Войти в ОС под учетной записью пользователя (при запуске будет оповещение о специальном режиме работы комплекса «Аккорд»). Запустить процессы, необходимые для выполнения должностных обязанностей пользователя. Завершить сеанс пользователя. Выйти из ОС. Повторить данную процедуру несколько раз, для получения подробной статистики.

8. Войти в ОС под учетной записью администратора.

9. Запустить программу LogBase.exe (по умолчанию — C:\Accord.x64\LogBase.exe). Выбрать файлы журнала предыдущих сеансов под учетной записью пользователя (рисунок 6). Запустить из меню Команды — Запуск AcProc.

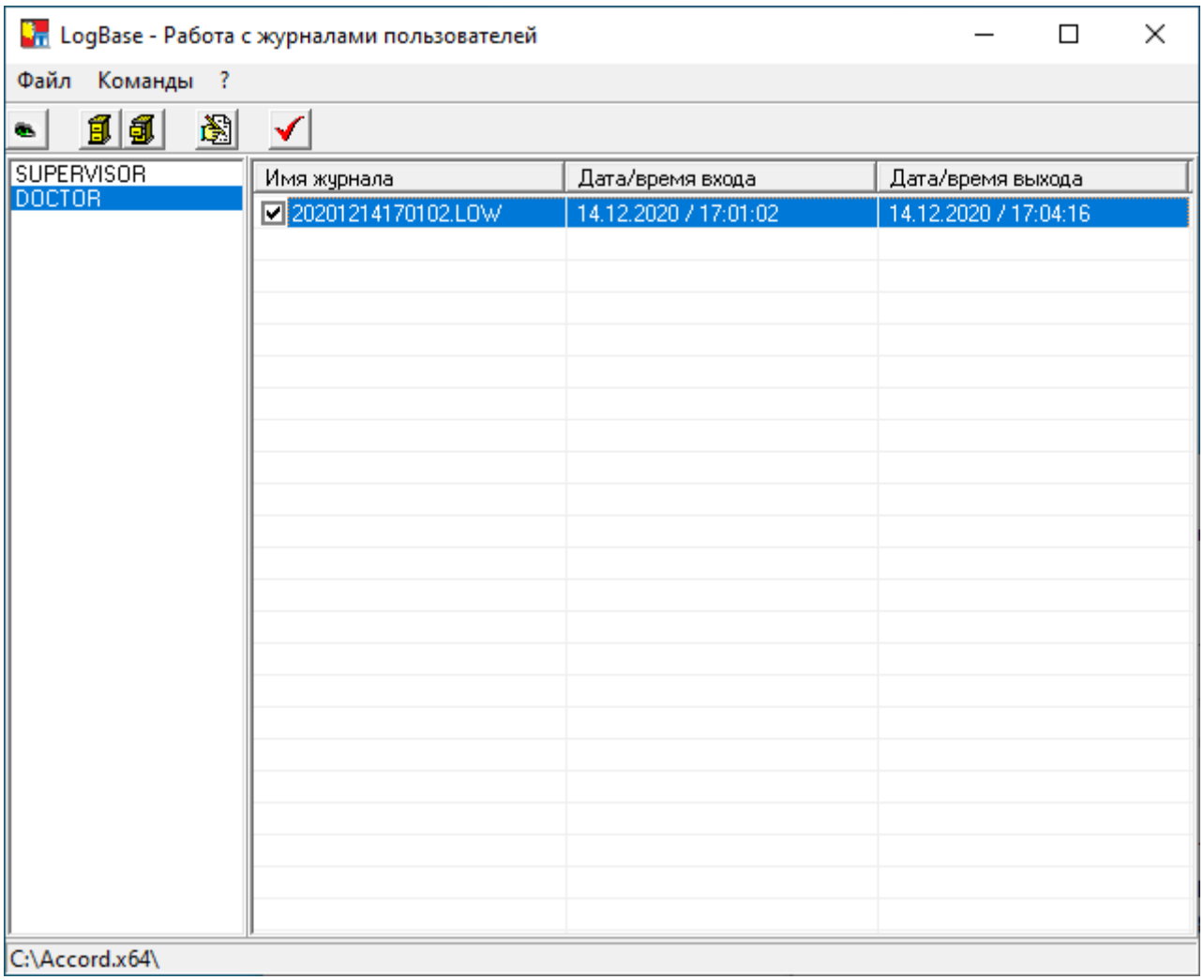

Рисунок 6 – Выбор журнала для формирования списка

В появившемся окне (рисунок 7) отметить только необходимые (для работы пользователя) процессы (вкладка 'Процессы') и нажать кнопку <Экспортировать>. Т.о появится файл *.prd в котором будут прописаны все процессы используемые пользователем (рисунок 8).

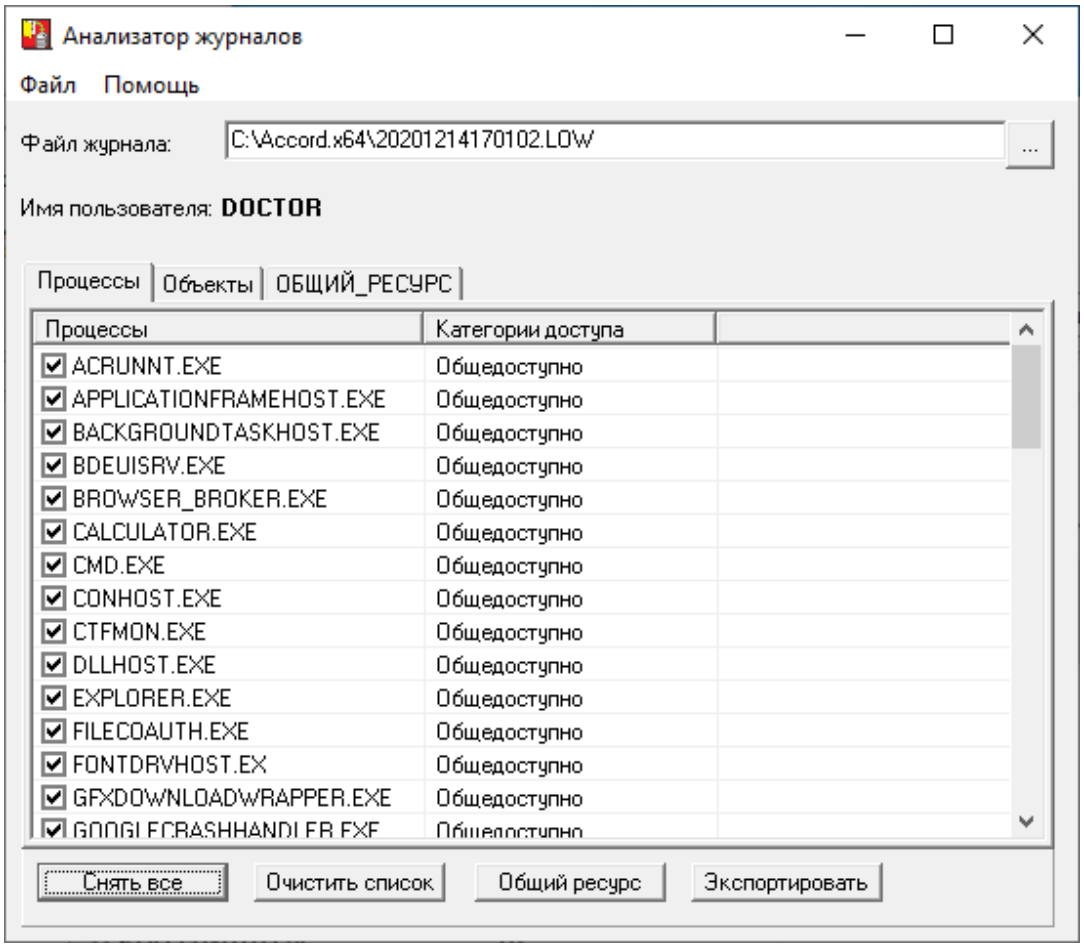

Рисунок 7 – Выбор процессов для контроля

10. Нажать кнопку "Экспортировать". При нажатии кнопки появляется окно, в котором следует указать путь, имя файла и нажать кнопку <Сохранить> (рисунок 8).

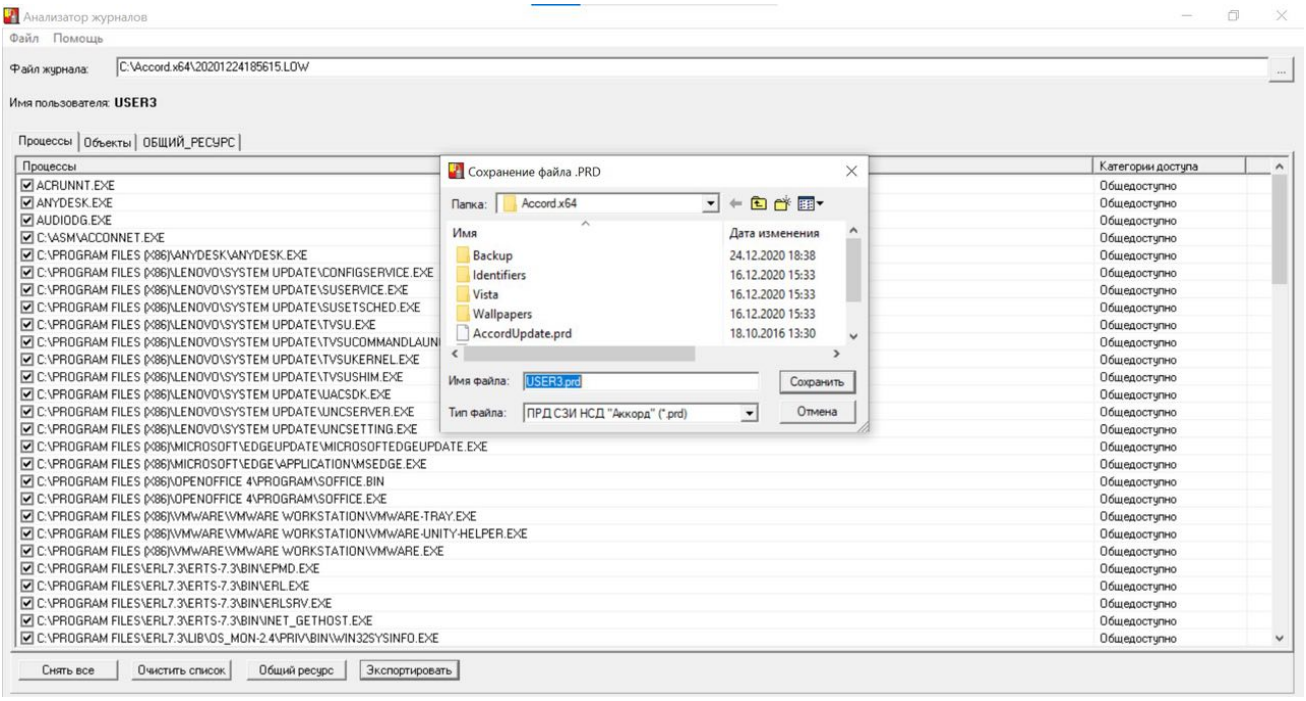

Рисунок 8 – Сохранение файла .PRD

11. Выйти из приложения Анализатор журналов.

12. Запустить утилиту «Редактор прав доступа». Выбрать пользователя, нажать на него правой кнопкой мыши. Отметить «Импорт ПРД» (рисунок 9). Появится окно выбора файла со списком процессов (рисунок 10).

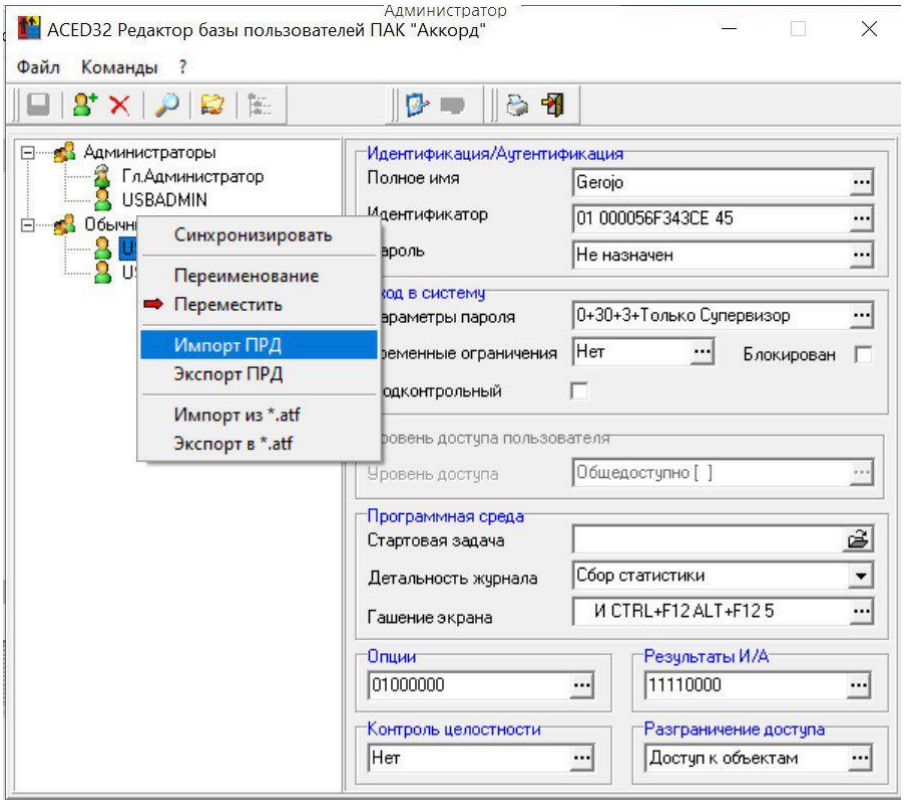

Рисунок 9 – Импорт ПРД

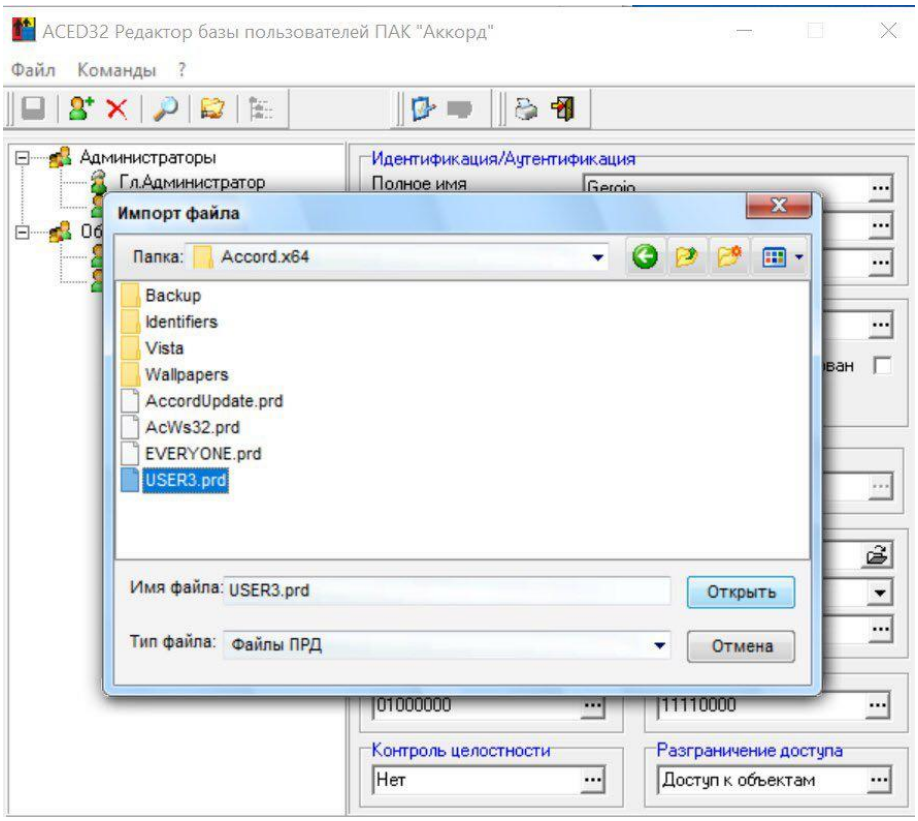

Рисунок 10 – Выбор файла со списком процессов

13. Выбрать нужный файл .prd. и нажать кнопку <Открыть>.

В появившемся окне установить флаг «Для процессов» и нажать кнопку <Импорт> (рисунок 11). В окне со списком импортированных процессов (рисунок 12) отметить строку «Заменить».

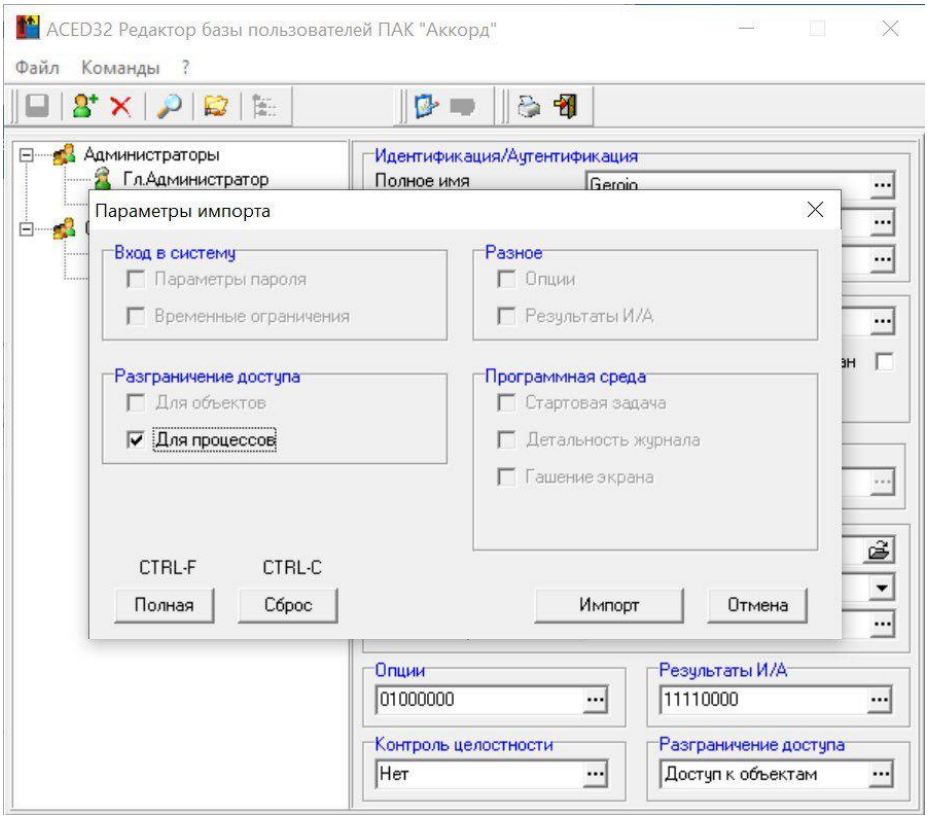

Рисунок 11 – Выбор параметров импорта

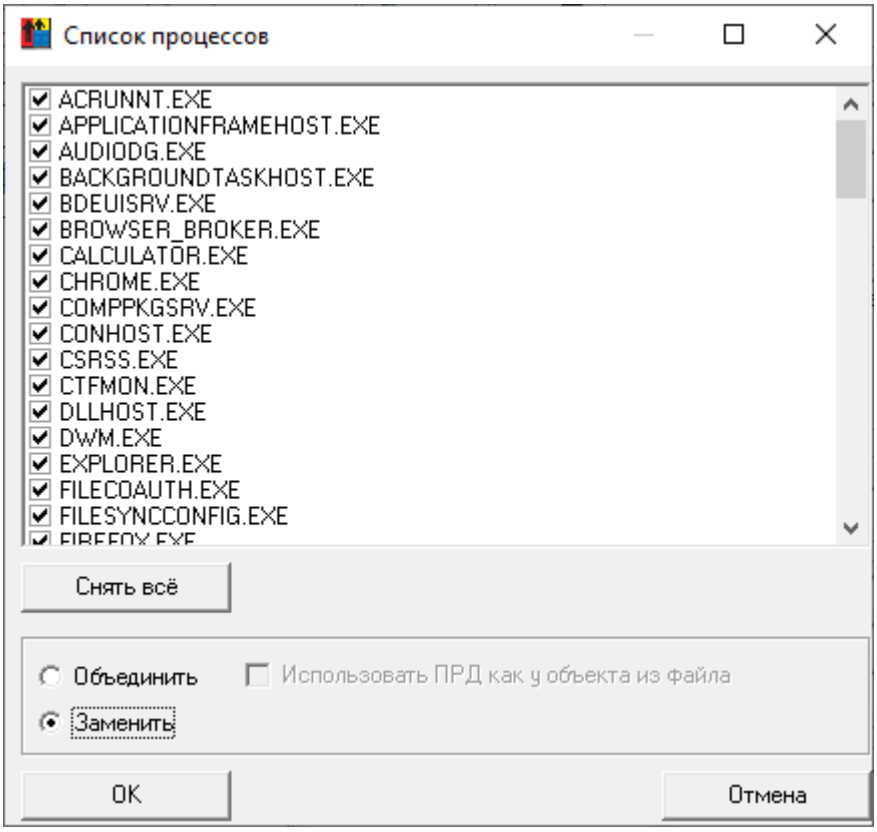

Рисунок 12 - Окно со списком импортированных процессов

14. Переходим в Разделение доступа — Процессы и проверяем импортированные процессы, в случае необходимости можно их скорректировать (рисунок 13)

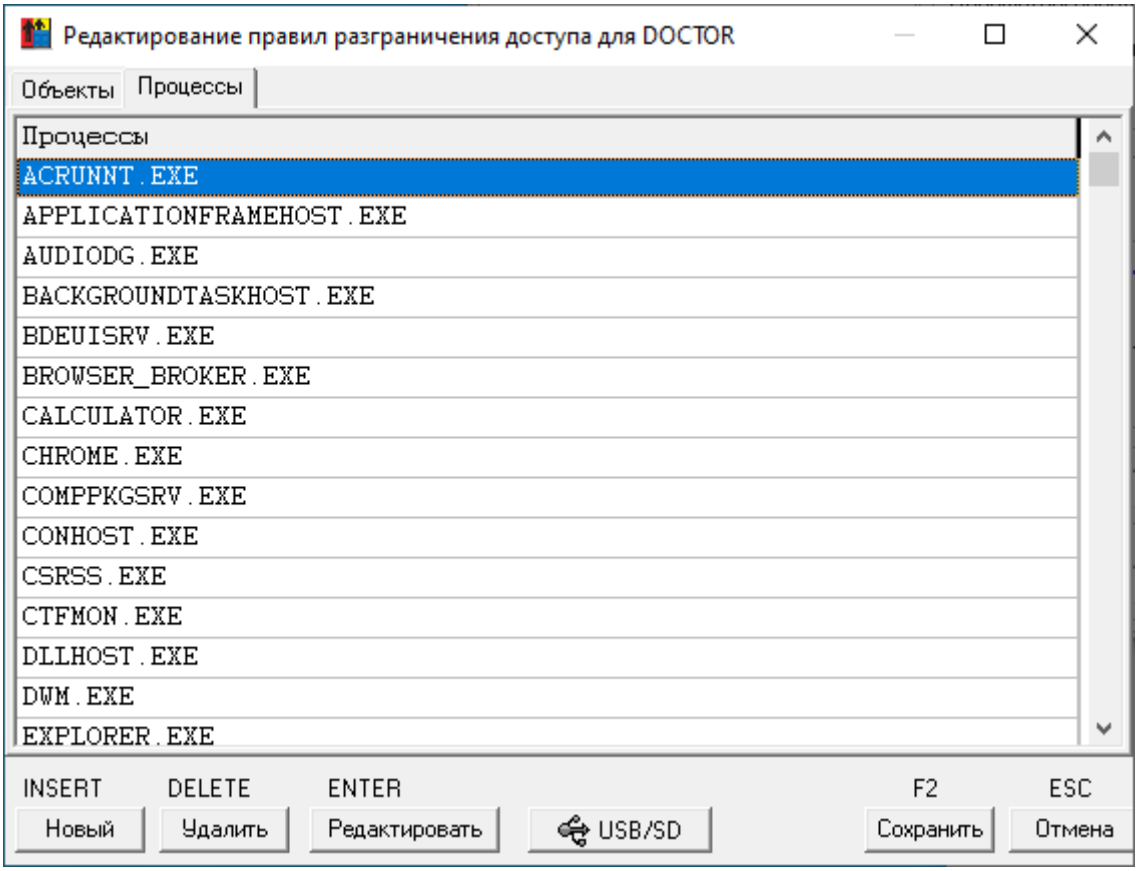

Рисунок 13 - Окно со списком импортированных процессов

15. Установить запрет на запуск процесса Shutdown.exe можно следующим образом: в главном окне утилиты ACED32 (рисунок 4) нажать кнопку справа в поле «Разграничение доступа» для группы Обычные, найти в списке Shutdown.exe, нажать кнопку <Редактировать> (Enter) и в появившемся окне атрибутов доступа поле «Прочее» оставить пустым (рисунок 14).

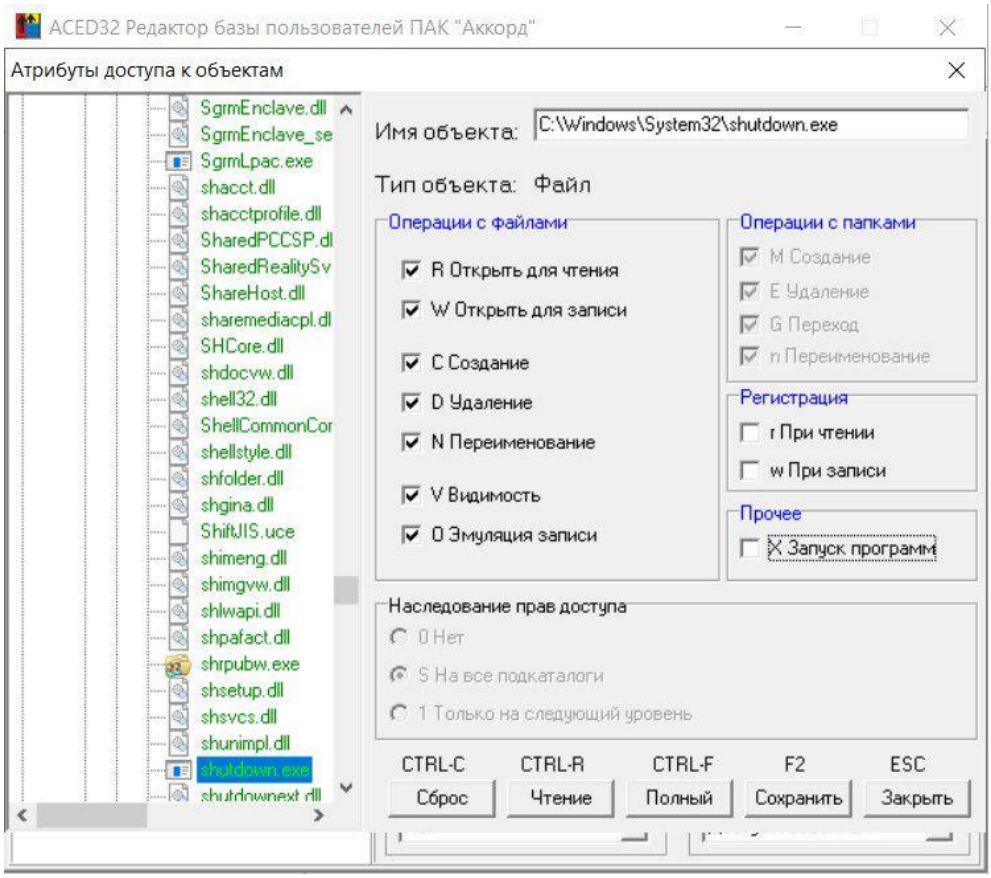

Рисунок 14 – Окно атрибутов доступа к объектам

16. Сменить детализацию журнала пользователя на значение «Низкая» (рисунок 15).

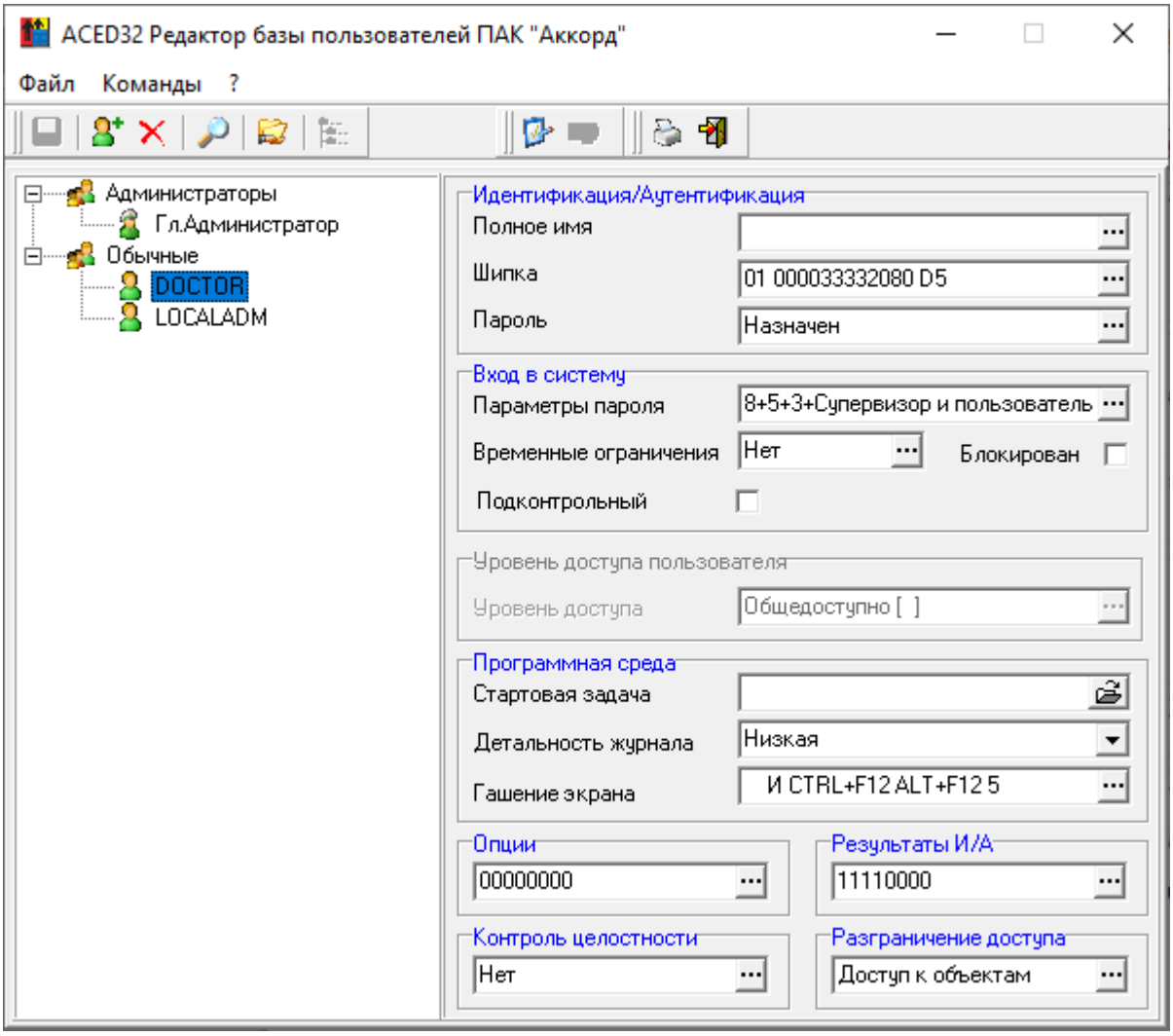

Рисунок 15 – Установка низкого уровня детальности журнала пользователя

17. Выйти из приложения ACED32. Перезагрузить компьютер.