СОЗДАНИЕ «БЕЛОГО» СПИСКА ПРОЦЕССОВ С ПОМОЩЬЮ МАНДАТНОГО МЕХАНИЗМА РАЗГРАНИЧЕНИЯ ДОСТУПА С КОНТРОЛЕМ ПРОЦЕССОВ И ДИНАМИЧЕСКОГО КОНТРОЛЯ ЦЕЛОСТНОСТИ ФАЙЛОВ ИЗ ЭТОГО СПИСКА

В ПО ПАК «Аккорд» имеется возможность создания списков разрешенных для пользователей процессов («белого» списка процессов). В целях исключения возможности возникновения несанкционированного доступа (НСД) к процессам из «белого» списка (например, при несанкционированной модификации процесса) рекомендуется выполнять процедуру создания «белого» списка процессов с помощью мандатного механизма разграничения доступа с контролем процессов и динамического контроля целостности файлов из этого списка.

Формирование списков процессов выполняется в соответствии со следующим порядком:

1) запустить утилиту «Настройка комплекса «Аккорд» (Программы\Аккорд\Настройка комплекса Аккорд);

2) в главном окне программы установить флаги «Мандатный» и «+процессы» (рисунок 1);

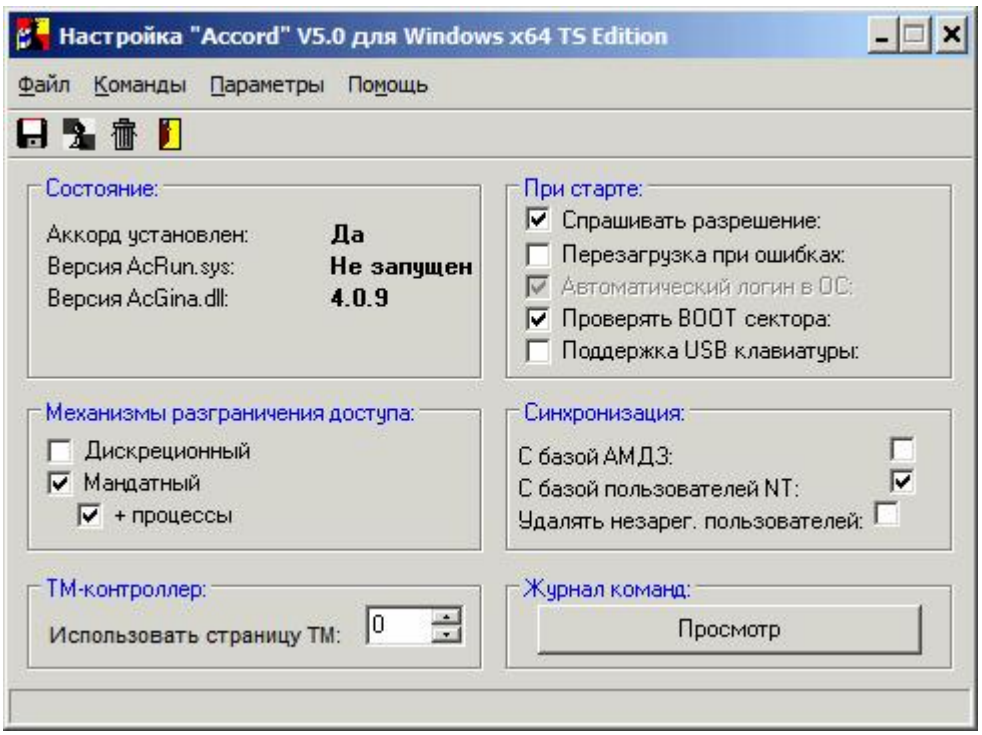

Рисунок 1 – Главное окно утилиты «Настройка комплекса Аккорд»

3) завершить работу приложения с сохранением изменений;

4) запустить утилиту «Редактор прав доступа» (Программы\Аккорд\Редактор прав доступа), в которой установить в уровень детальности журнала «Сбор статистики» для одного из пользователей, входящего в состав группы пользователей СЗИ от НСД «Аккорд», с использованием учетной записи которого будут формироваться списки. При этом пользователю автоматически присваивается высокий уровень детальности журнала, а его работа выполняется в мягком режиме;

5) осуществить от имени пользователя запуск и работу с приложениями, необходимыми для выполнения его должностных обязанностей;

6) завершить сеанс пользователя, запустить от имени Администратора СЗИ от НСД «Аккорд» программу AcProc.exe (Программы\Аккорд\Создание списка процессов из журналов регистрации, рисунок 2);

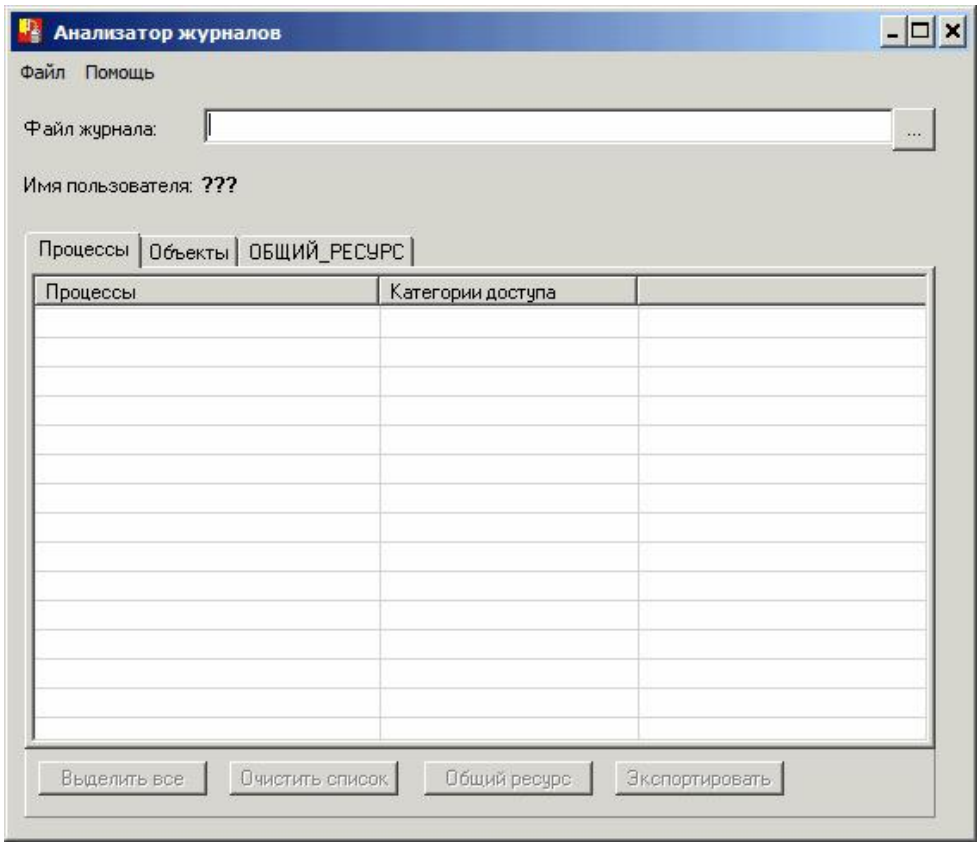

Рисунок 2 – Главное окно утилиты AcProc.exe

7) во вкладке «Процессы» загрузить журнал последнего сеанса работы пользователя (в окне программы AcProc.exe (рисунок 2) нужно нажать на раскрывающийся список в поле «Файл журнала»), далее в появившемся на экране окне (рисунок 3) выбрать файл журнала (или несколько файлов);

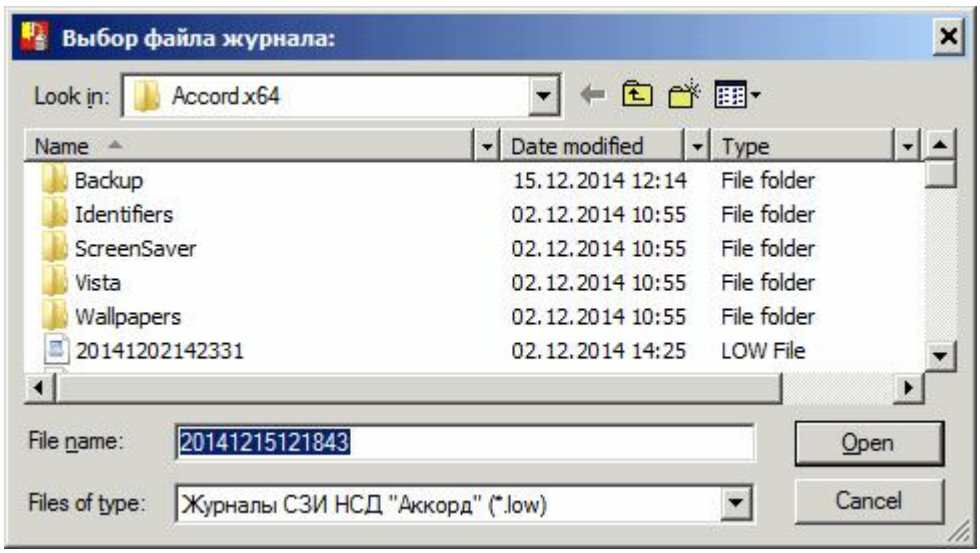

Рисунок 3 - Выбор файла журнала регистрации событий

8)далее в главном окне программы AcProc.exe выбрать процессы, которые необходимы для выполнения должностных обязанностей пользователя и нажать кнопку <Экспортировать> (рисунок 4);

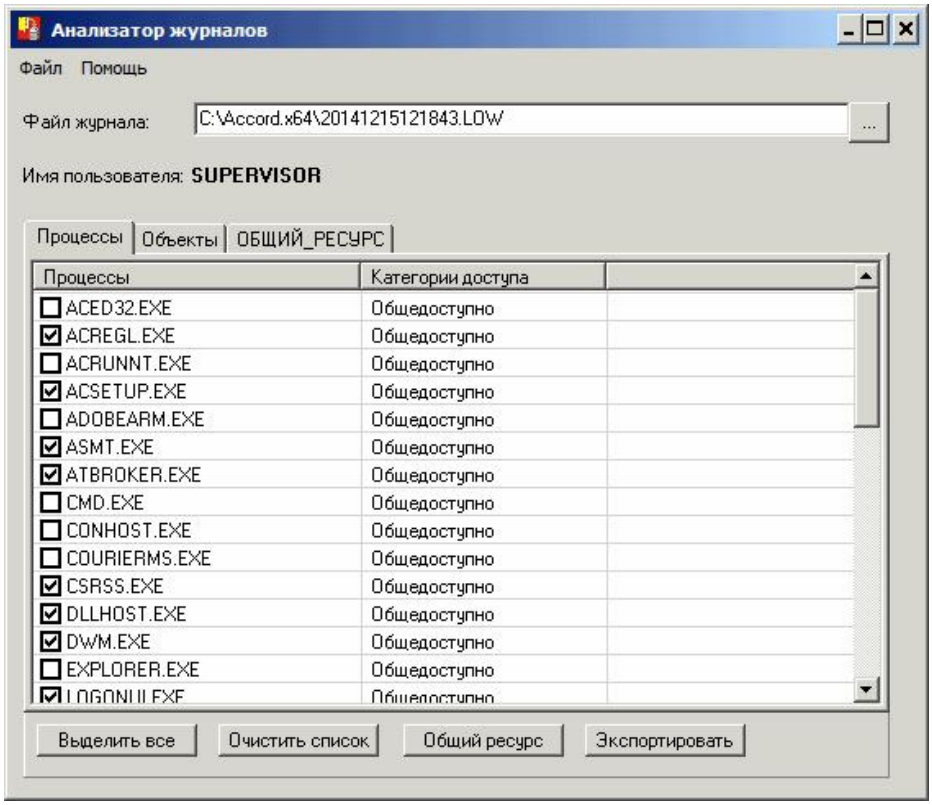

Рисунок 4 - Главное окно программы AcProc.exe. Выбор процесса

9)далее в появившемся на экране окне следует нажать кнопку <Сохранить> (по умолчанию имя файла соответствует имени учетной записи пользователя, для которого формируется список процессов, однако при необходимости можно изменить имя файла, рисунок 5);

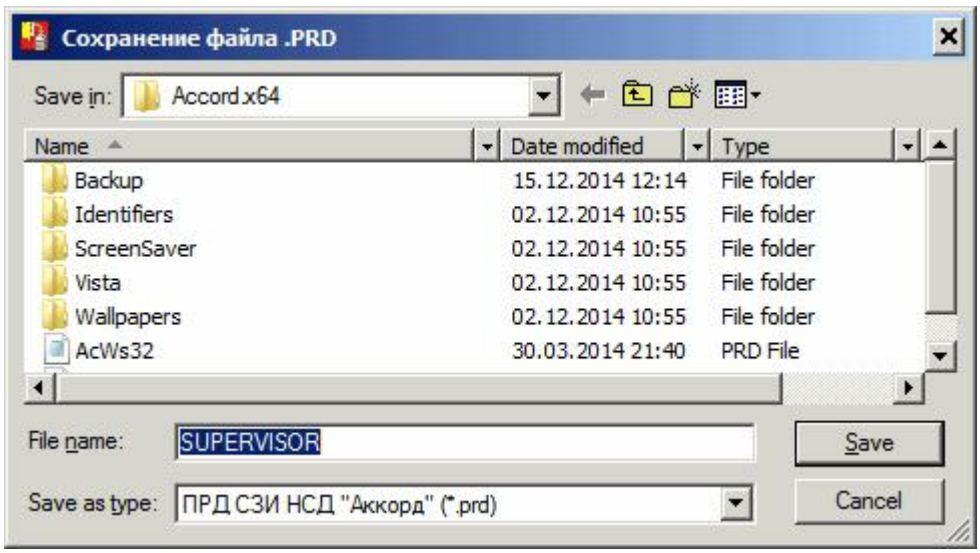

Рисунок 5 – Сохранение процессов в файл .prd

10) далее в главном окне программы AcProc.exe перейти во вкладку «Объекты» и сохранить список объектов, к которым обращался пользователь во время выполнения должностных обязанностей, нажав кнопку <Экспортировать> (рисунок 6);

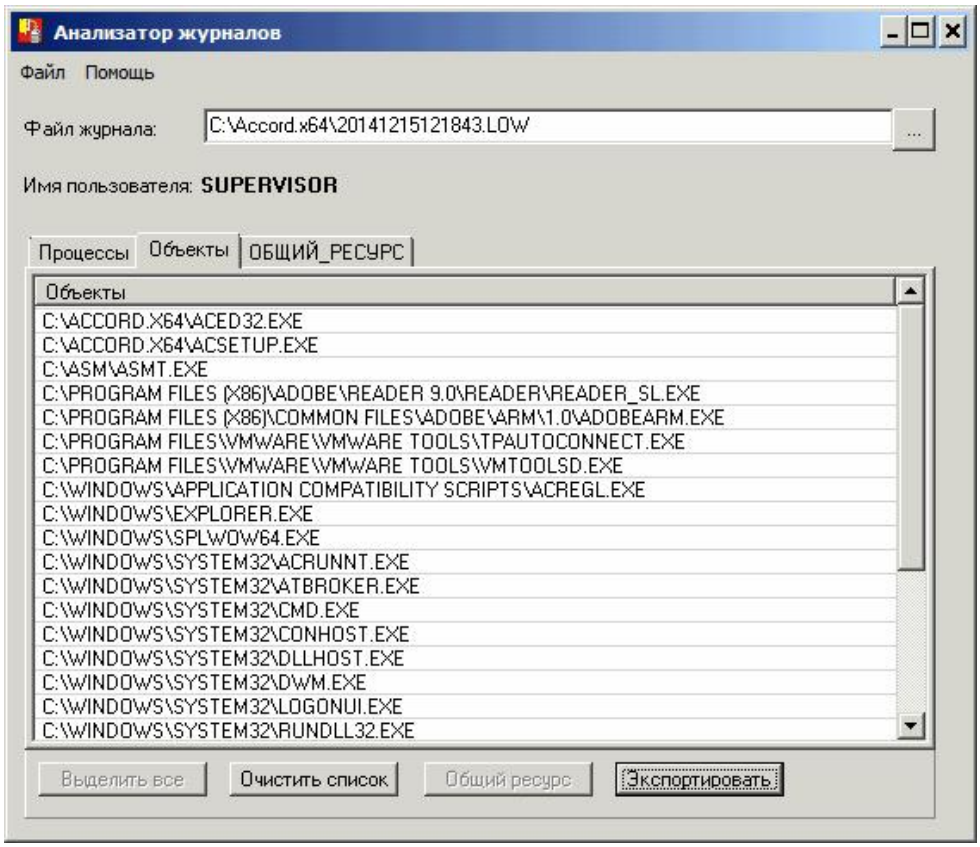

Рисунок 6 – Главное окно программы AcProc.exe. Вкладка «Объекты»

11) далее в появившемся на экране окне следует нажать кнопку <Сохранить> (по умолчанию имя файла соответствует имени учетной записи пользователя, для которого формируется список объектов, однако при необходимости можно изменить имя файла, рисунок 7);

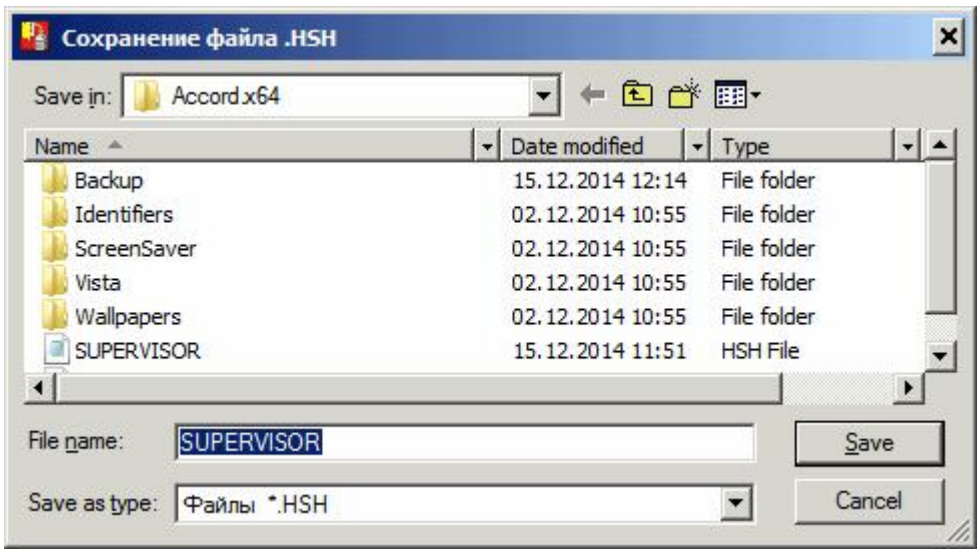

Рисунок 7 – Сохранение объектов в файл .hsh

12) затем необходимо вновь запустить утилиту «Редактор прав доступа» (Программы\Аккорд\Редактор прав доступа) и выбрать меню Файл\Импорт ПРД (рисунок 8);

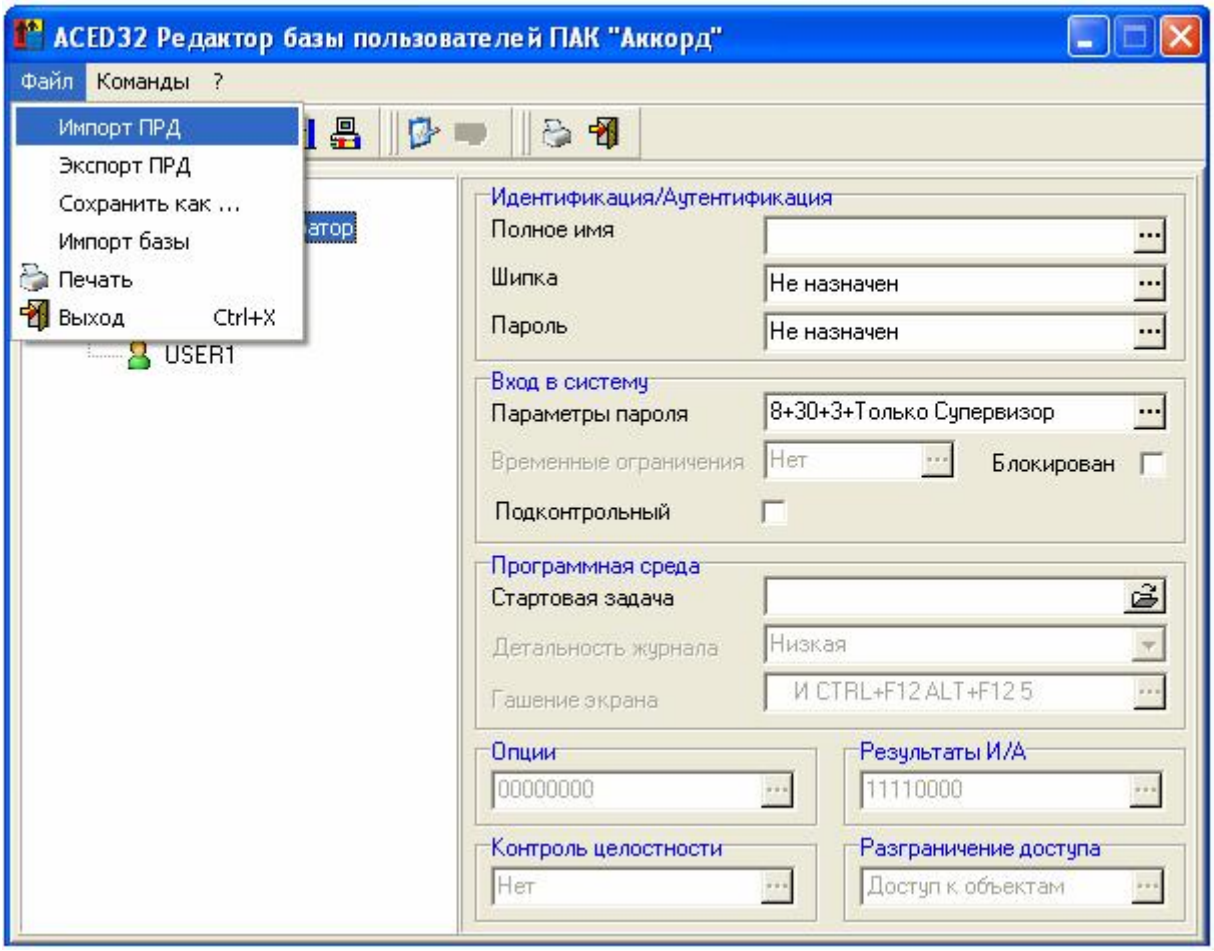

Рисунок 8 – Импорт мандатных меток

13) после этого на экране появляется окно выбора файла со списком процессов (рисунок 9);

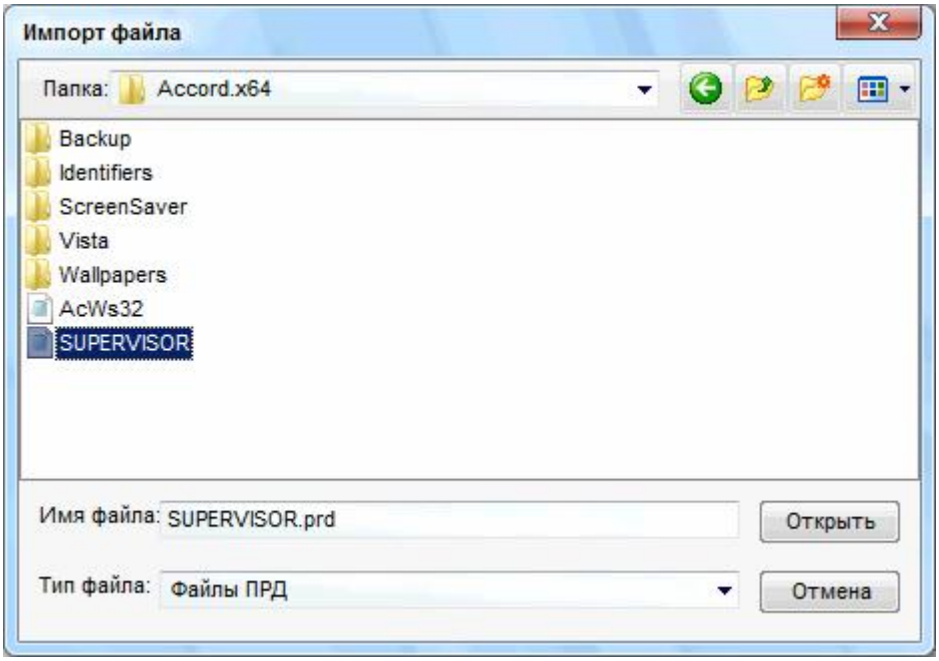

Рисунок 9 – Окно выбора файла со списком процессов

14) необходимо выбрать файл (рисунок 9) и нажать кнопку <Открыть>;

15) в появившемся на экране окне нажать кнопку <Импорт> (рисунок 10);

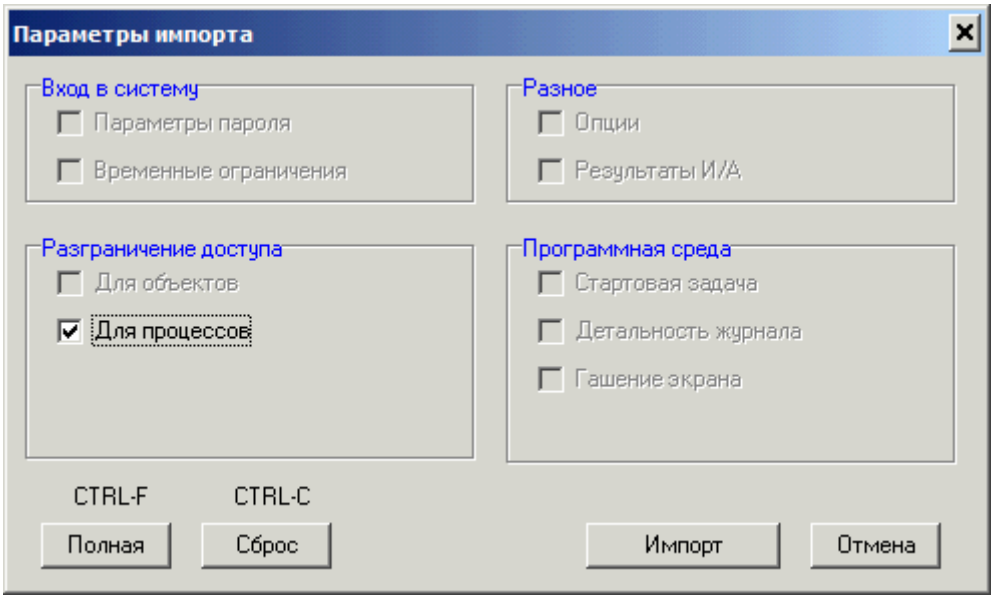

Рисунок 10 – Параметры импорта

16) далее на экране появляется окно со списком импортированных процессов (рисунок 11), следует отметить необходимые (или же выбрать все процессы, нажав кнопку <Выбрать все>), а также (в случае необходимости) отметить флаги, показанные внизу окна 11, и нажать кнопку <OK>;

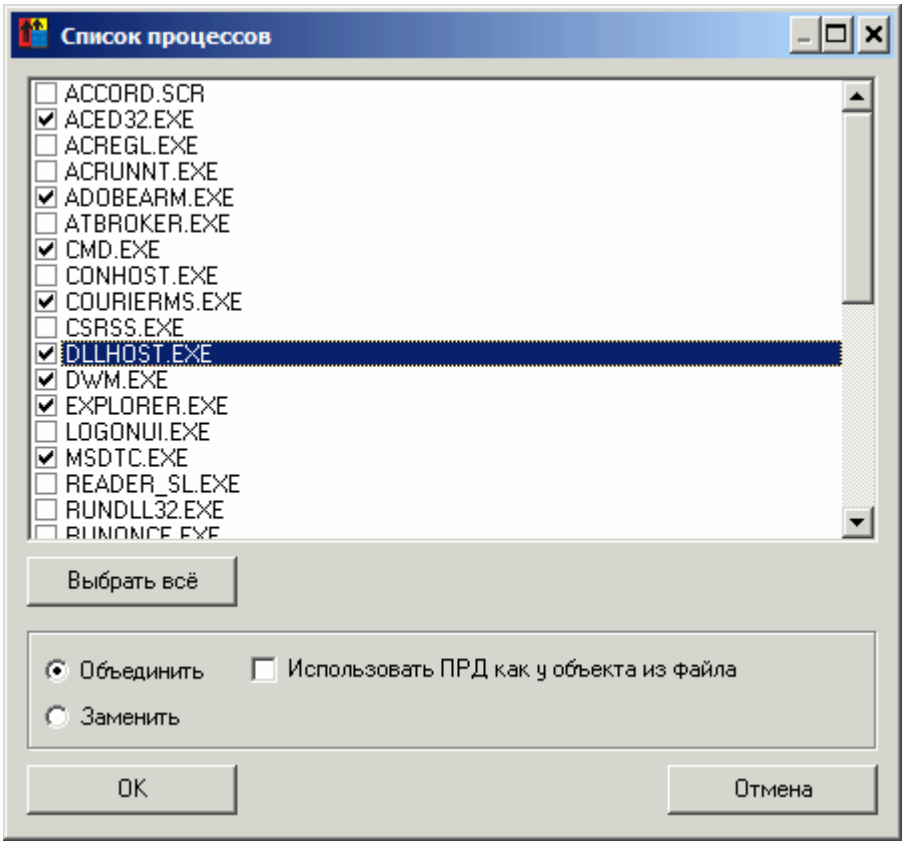

Рисунок 11 – Список импортированных процессов

17) далее в меню разграничения доступа для пользователя следует установить соответствующие уровни доступа импортированным процессам (рисунок 12);

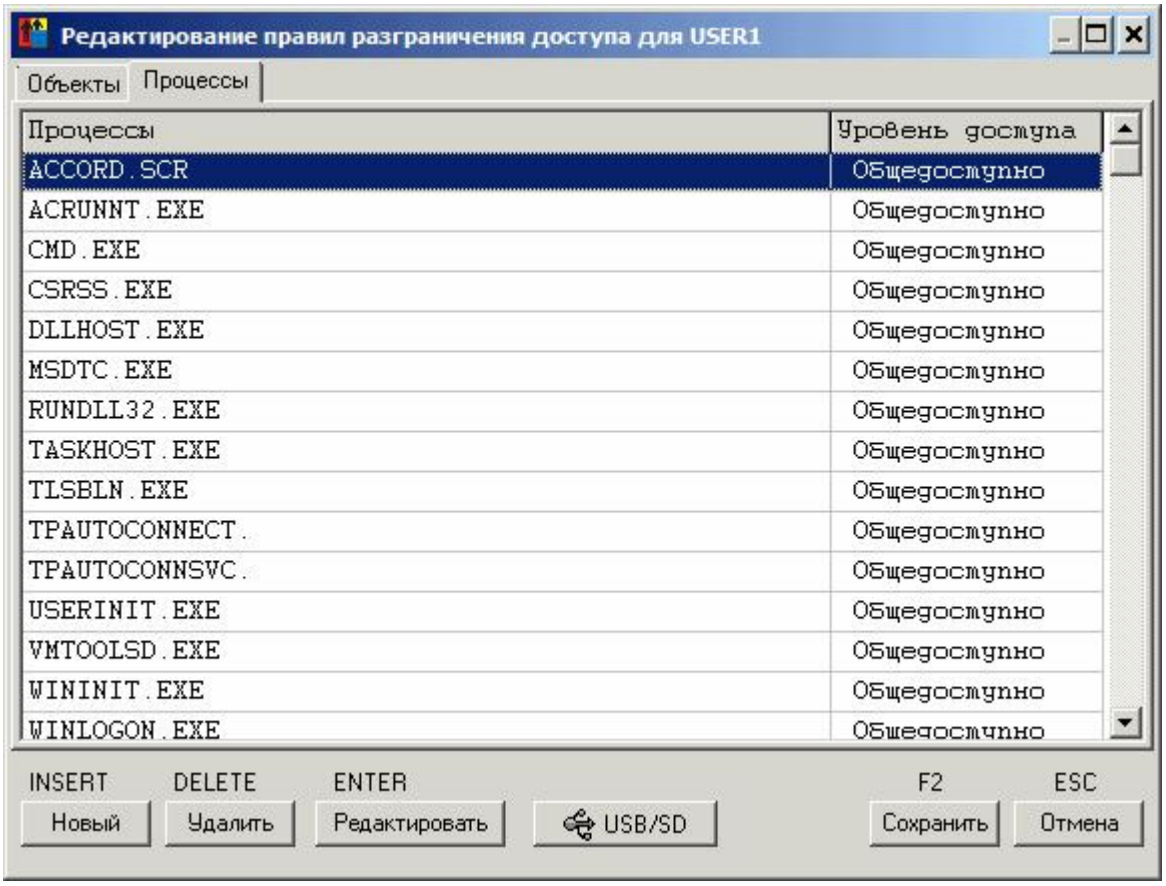

Рисунок 12 – Установка уровней доступа импортированным процессам

18) затем в главном окне редактора прав доступа нужно перейти в меню «Контроль целостности»;

19) в появившемся окне перейти во вкладку «Динамический» и нажать кнопку <Загрузить> (рисунок 13);

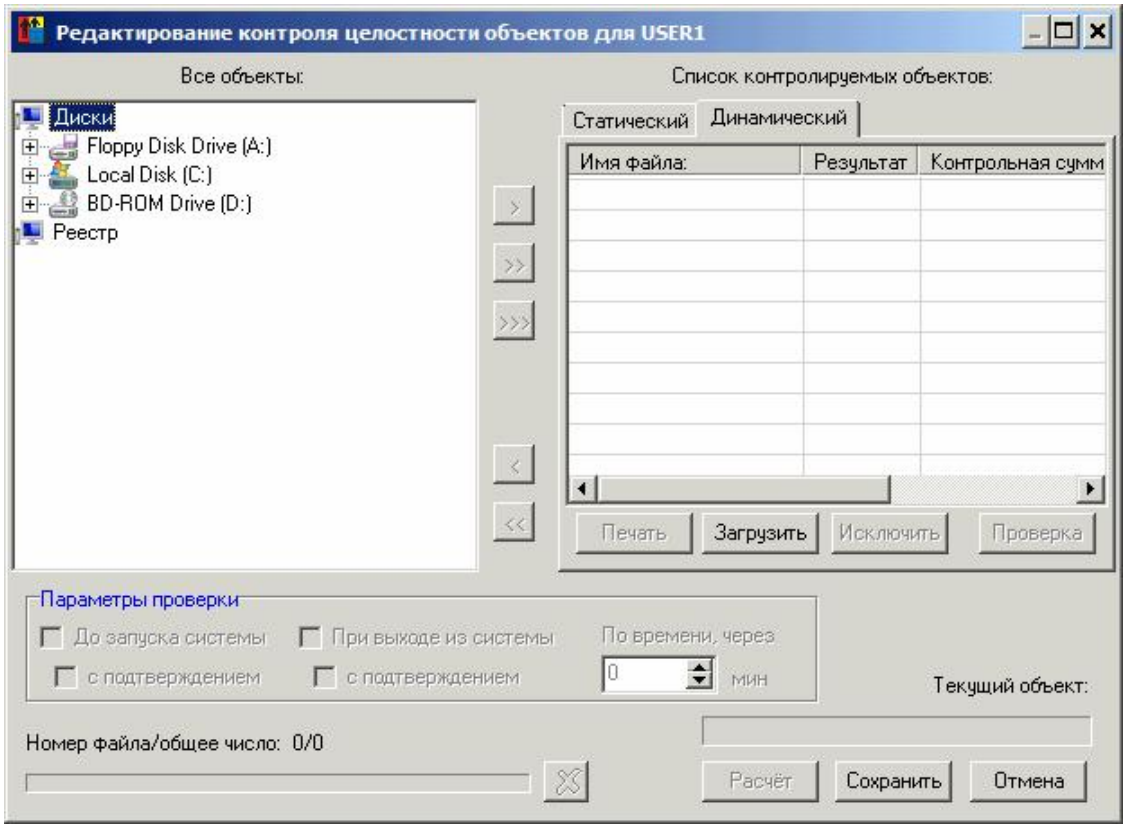

Рисунок 13 – Редактирование списков для контроля целостности пользователя

20) по нажатии кнопки на экране появляется окно выбора файла (рисунок 14). Необходимо выбрать файл со списком импортированных объектов, с которыми работал пользователь при выполнении должностных обязанностей (файл .hsh) и нажать кнопку <Открыть>;

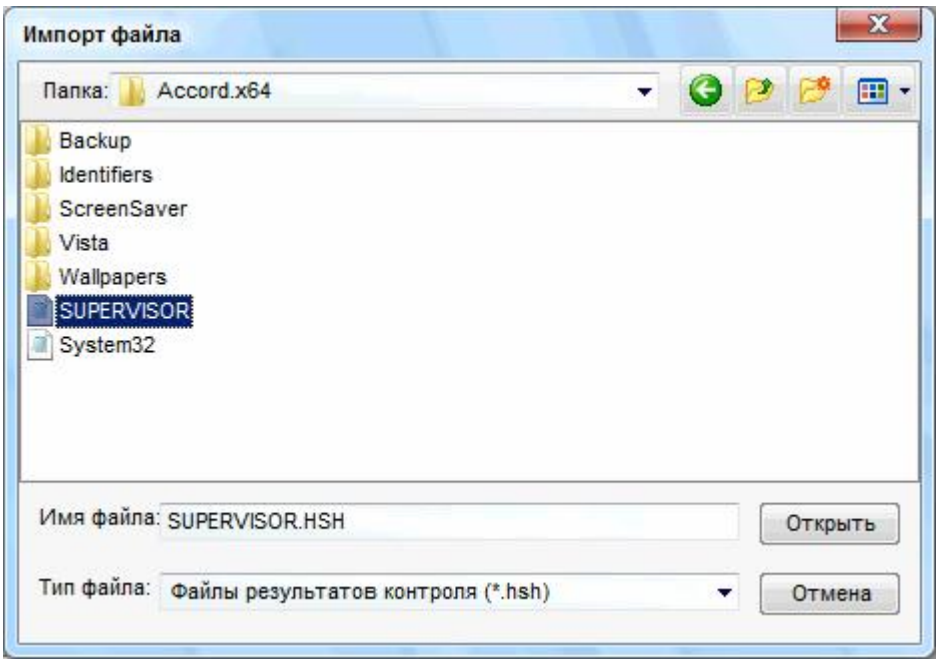

Рисунок 14 – Импорт файла со списком импортированных объектов

21) после этого окно для редактирования списков для контроля целостности примет вид (рисунок 15):

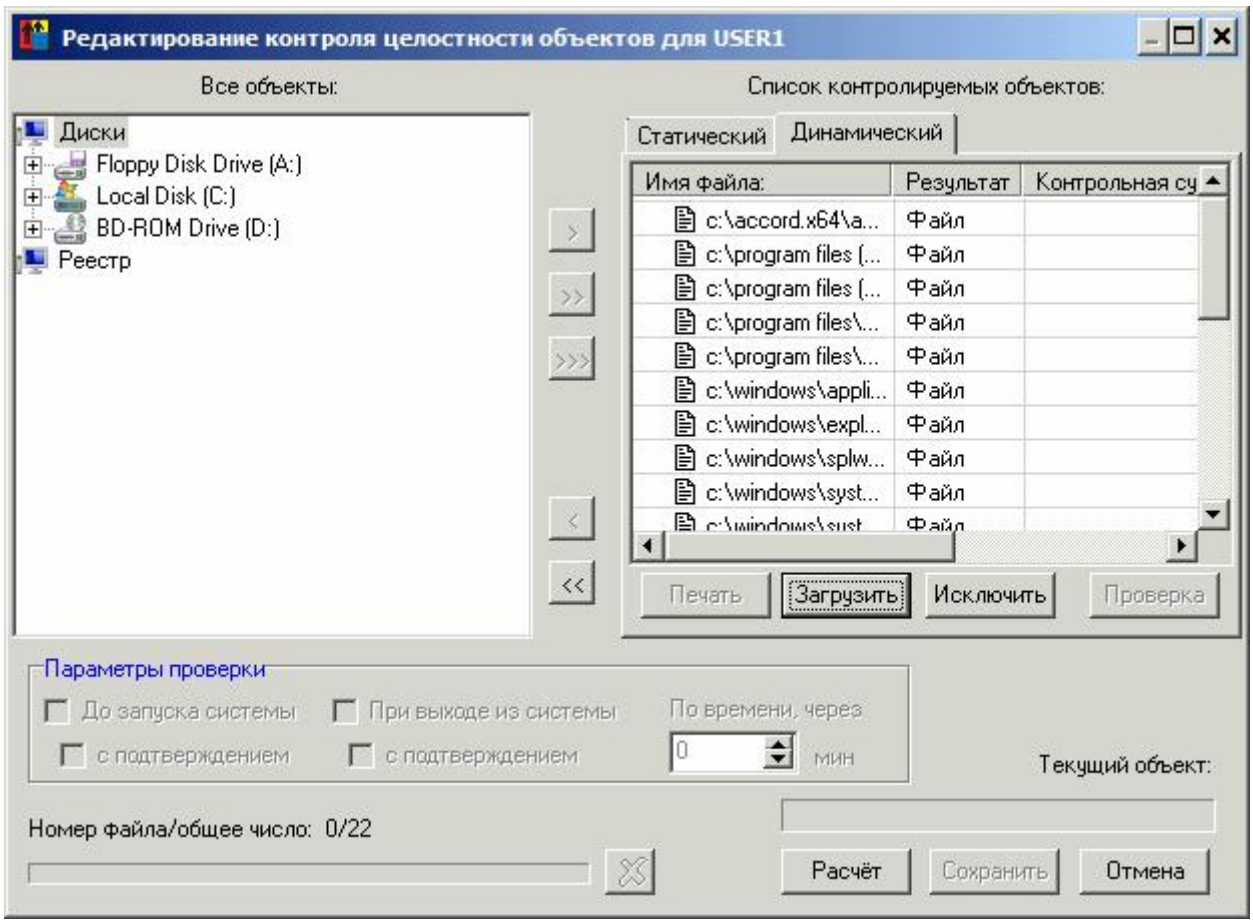

Рисунок 15 - Редактирование списков для контроля целостности. Импорт списка контролируемых объектов

22) затем необходимо выбрать объекты и нажать кнопку <Расчет> (рисунок 15);

23) на запрос идентификатора предъявить идентификатор пользователя, для которого выполняется процедура редактирования контроля целостности объектов;

24) после этого в графе «Контрольная сумма» появляются эталонные значения КС (рисунок 16);

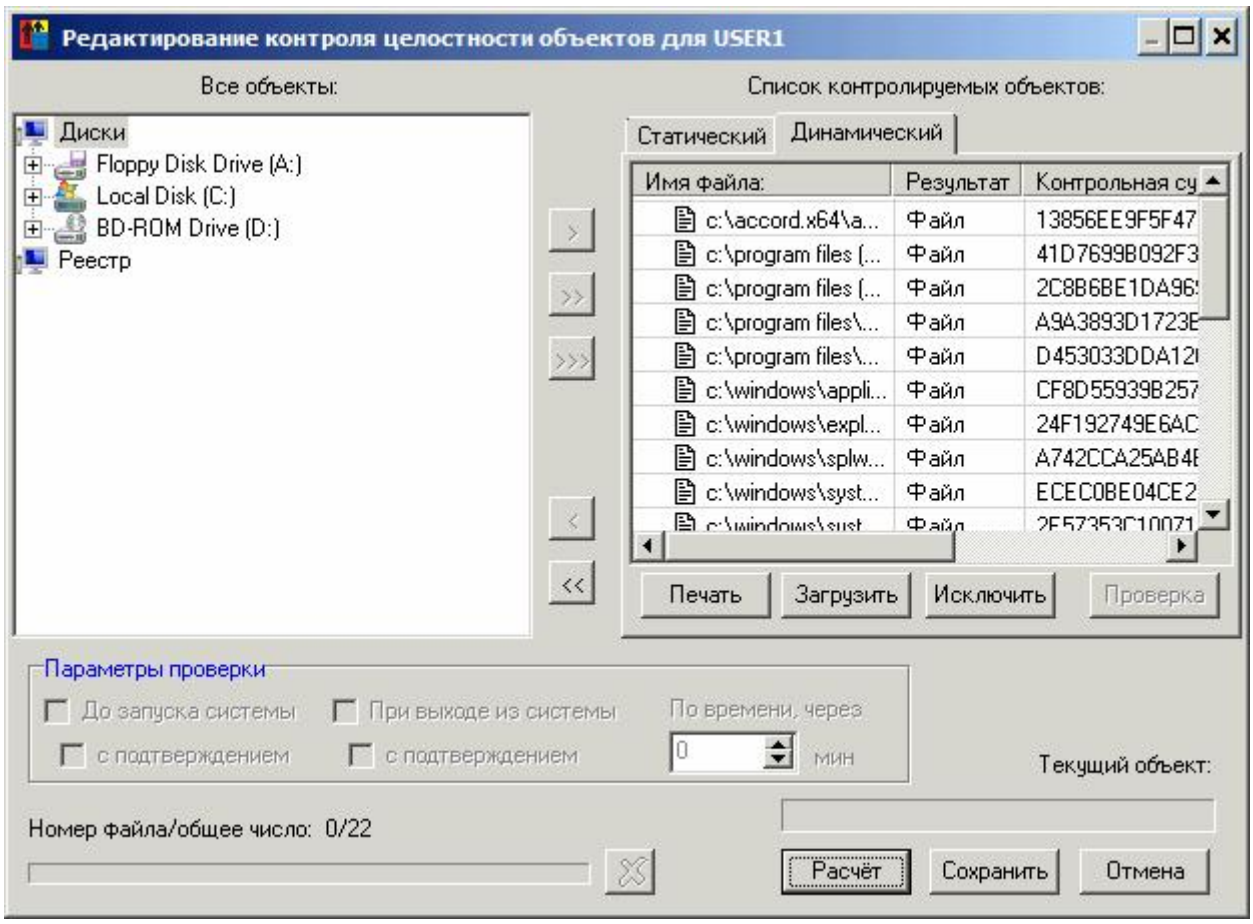

Рисунок 16 - Редактирование списков для контроля целостности. Контрольные суммы рассчитаны

25) по завершении процедуры расчета КС нужно нажать кнопку <Сохранить> (рисунок 16).

После выполнения описанной в документе последовательности действий для пользователя создается список разрешенных процессов, необходимых для выполнения его должностных обязанностей. Для каждого из процессов рассчитывается контрольная сумма и сохраняется в памяти идентификатора пользователя.

После запуска монитора разграничения доступа пользователю будут доступны только процессы из «белого» списка.

В случае несанкционированной модификации имени (при замене имени неразрешенного процесса именем разрешенного) процесс не запустится, так как КС модифицированного процесса не совпадет с эталонным значением КС исходного, добавленного в список разрешенных, процесса.

Таким образом, возможность несанкционированного доступа к процессам исключается.