

ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО



★ ОКБ

систем автоматизированного
проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.4012-019 97 02-ЛУ

**Программно-аппаратный комплекс
средств защиты информации от
несанкционированного доступа
“АККОРД-НТ/2000”
(версия 3.0)**

**УСТАНОВКА ПРАВИЛ
РАЗГРАНИЧЕНИЯ ДОСТУПА
ПРОГРАММА ACED32**

11443195.4012-019 97 02

Литера О₁

АННОТАЦИЯ

Программа ACED32.EXE - редактор параметров (атрибутов) доступа пользователей к объектам доступа СВТ или АС - предназначена для описания (установки) правил разграничения доступа (ПРД) пользователей в соответствии с их полномочиями.

Программа используется администратором БИ комплекса СЗИ НСД "Аккорд-NT/2000" v.3.0 (ТУ 4012-019-11443195-02) при настройке подсистемы разграничения доступа комплекса в соответствии с принятыми ПРД и входит в состав специального ПО комплекса.

Настоящее руководство предназначено для конкретизации действий администратора БИ (либо субъектов доступа, наделенными правами администратора) и содержит описание программы ACED32.EXE и порядок ее применения при установке комплекса.

Перед эксплуатацией комплекса необходимо внимательно ознакомиться с комплектом эксплуатационной документации на комплекс, а также принять необходимые организационные меры защиты, рекомендуемые в документации.

Применение защитных механизмов комплекса должно дополняться общими мерами технической безопасности, а также физической охраной СВТ.

СОДЕРЖАНИЕ

1	НАЗНАЧЕНИЕ ПРОГРАММЫ	5
2	ЗАПУСК РЕДАКТОРА ПРАВ ДОСТУПА	5
2.1	Порядок запуска программы ACED32	5
2.2	Выход из программы	7
3	ИНФОРМАЦИЯ О ПРОГРАММЕ	7
4	РЕГИСТРАЦИЯ НОВОЙ ГРУППЫ ПОЛЬЗОВАТЕЛЕЙ.....	8
5	РЕДАКТИРОВАНИЕ ПАРАМЕТРОВ ПОЛЬЗОВАТЕЛЕЙ (ПРАВ ДОСТУПА).....	8
5.1	Регистрация нового пользователя.....	8
5.2	Печать параметров пользователя.....	9
5.3	Удаление пользователя из списка зарегистрированных	9
5.4	Переименование пользователя в списке	9
5.5	Поиск пользователя по ТМ-идентификатору	10
5.6	Синхронизация параметров пользователя с параметрами группы.....	10
6	АДМИНИСТРИРОВАНИЕ ПОДСИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА	11
6.1	Задание имени пользователя	11
6.2	Регистрация ТМ пользователя	12
6.3	Установка параметров пароля	13
6.4	Задание пароля пользователя	13
6.5	Установка детальности протокола работы пользователей.....	15
6.6	Установка режима гашения экрана.	15
6.7	Установка временных ограничений для сеанса работы пользователя	16
6.8	Блокировка пользователя	17
6.9	Установка стартовой задачи пользователя	17
6.10	Установка правил разграничения доступа (ПРД) к объектам доступа	20
6.10.1	<i>Установка доступа к объектам с использованием дискреционного метода ПРД.</i>	<i>20</i>
6.10.2	<i>Установка доступа к объектам с использованием мандатного метода контроля ПРД.</i>	<i>25</i>
6.11	Контроль целостности файлов.....	29
6.11.1	<i>"Статический" контроль целостности файлов</i>	<i>30</i>
6.11.2	<i>"Динамический" контроль целостности файлов.....</i>	<i>31</i>
6.12	Установка опций настройки.....	34
6.13	Установка фиксированных сетевых имен ресурсов общего пользования	35
6.14	Экспорт/импорт базы данных пользователей и правил разграничения доступа	36
6.14.1	<i>Сохранение/загрузка базы данных пользователей</i>	<i>36</i>
6.14.2	<i>Экспорт/импорт правил разграничения доступа.....</i>	<i>38</i>
6.15	Формирование списка разрешенных USB устройств	41
6.16	Формирование правил доступа для отдельных программ (процессов)	43
6.17	Групповая политика и особенности установки ПРД на контроллере домена Windows	47
7	ЗАКЛЮЧЕНИЕ.....	48
8	ПРИЛОЖЕНИЕ 1. ФАЙЛ ACCORD.INI – ФАЙЛ КОНФИГУРАЦИИ СЗИ НСД «АККОРД».....	49

ПРИНЯТЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

Администратор	- администратор службы безопасности информации
Имя_пользователя	- имя, под которым пользователь зарегистрирован в системе
Использовать ТМ-идентификатор	- приложить ТМ-идентификатор к контактному устройству съемника информации
Объект доступа	- под объектом доступа понимается один из перечисленных ресурсов СВТ: диск, каталог, файл, раздел или ключ реестра, процесс (задача), драйвер устройства.
Параметры пользователя	- идентифицирующие признаки пользователя (имя, № ТМ, пароль) и его права по доступу к ресурсам СВТ в соответствии с его полномочиями
Пользователь	- субъект доступа к объектам (ресурсам) СВТ
ПРД	- правила разграничения доступа
Удаление пользователя	- удаление имени, под которым пользователь зарегистрирован в системе, из списка зарегистрированных пользователей в ЭНП контроллера "Аккорд"
Синхронизация параметров пользователя	- сопоставление БД пользователей в ЭНП контроллера "Аккорд" с параметрами БД пользователей подсистемы разграничения доступа и учетными записями пользователей Windows NT/2000
Создать пользователя	- зарегистрировать пользователя в подсистеме разграничения доступом
Сообщения	- информация, выводимая на дисплей, которая сообщает о действиях пользователя, о состоянии программы и нормально завершенных действиях, сбоях в системе и др.
ТМ-идентификатор (или ТМ)	- персональный идентификатор DS-199x ("Touch-memory" - "Память касания") пользователя
Число проходов при удалении	- количество записи случайной последовательности по содержимому файла при его удалении с очисткой
ЭНП	- энергонезависимая память контроллера "Аккорд" [™]

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

Программа ACED32.EXE – редактор параметров (атрибутов) доступа пользователей, используемых в комплексе СЗИ НСД "Аккорд-NT/2000" v.3.0. дискреционного и мандатного механизмов доступа субъектов (пользователей) к объектам СВТ или АС – предназначена для администрирования подсистемы разграничения доступом комплекса.

Программа используется администратором БИ системы защиты информации на базе комплекса (или субъектами доступа, наделенными правами администратора) при установке и эксплуатации комплекса для описания (определения пользователям) принятых в организации (учреждении и т.п.) правил разграничения доступа (ПРД) в соответствии с полномочиями пользователей.

Программа ACED32.EXE входит в состав специального ПО комплекса, устанавливается на жесткий диск СВТ (PC) при установке комплекса.

2 ЗАПУСК РЕДАКТОРА ПРАВ ДОСТУПА

ВНИМАНИЕ!

Доступ к редактору прав доступа обеспечивается только Администратору БИ

2.1 Порядок запуска программы ACED32

Для запуска редактора параметров (атрибутов) доступа пользователей комплекса необходимо запустить программу C:\ACCORD.NT\ACED32.EXE. При этом выполняется синхронизация базы данных редактора прав доступа с базой данных пользователей, находящейся в ЭНП контроллера "Аккорд-АМДЗ". На экран выводится окно для идентификации пользователей, показанное на Рис.1.

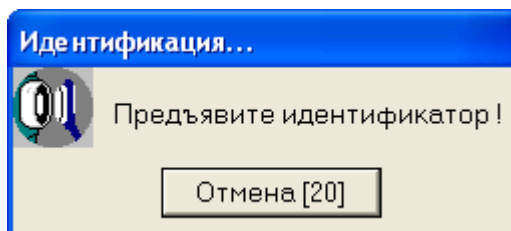


Рис. 1. Окно идентификации пользователей.

Далее программой запрашивается ТМ-идентификатор администратора БИ и его пароль (когда пароль определен при установке комплекса "Аккорд-АМДЗ" и хранится в ЭНП контроллера).

Если идентификации/аутентификация администратора прошла успешно, то на экран выводится главное окно программы, показанное на Рис.2.

Главное окно программы состоит из следующих разделов:

- меню команд;
- управляющие кнопки, дублирующие действия меню команд;
- список пользователей (левая половина окна);
- информация о выделенном пользователе (правая половина окна).

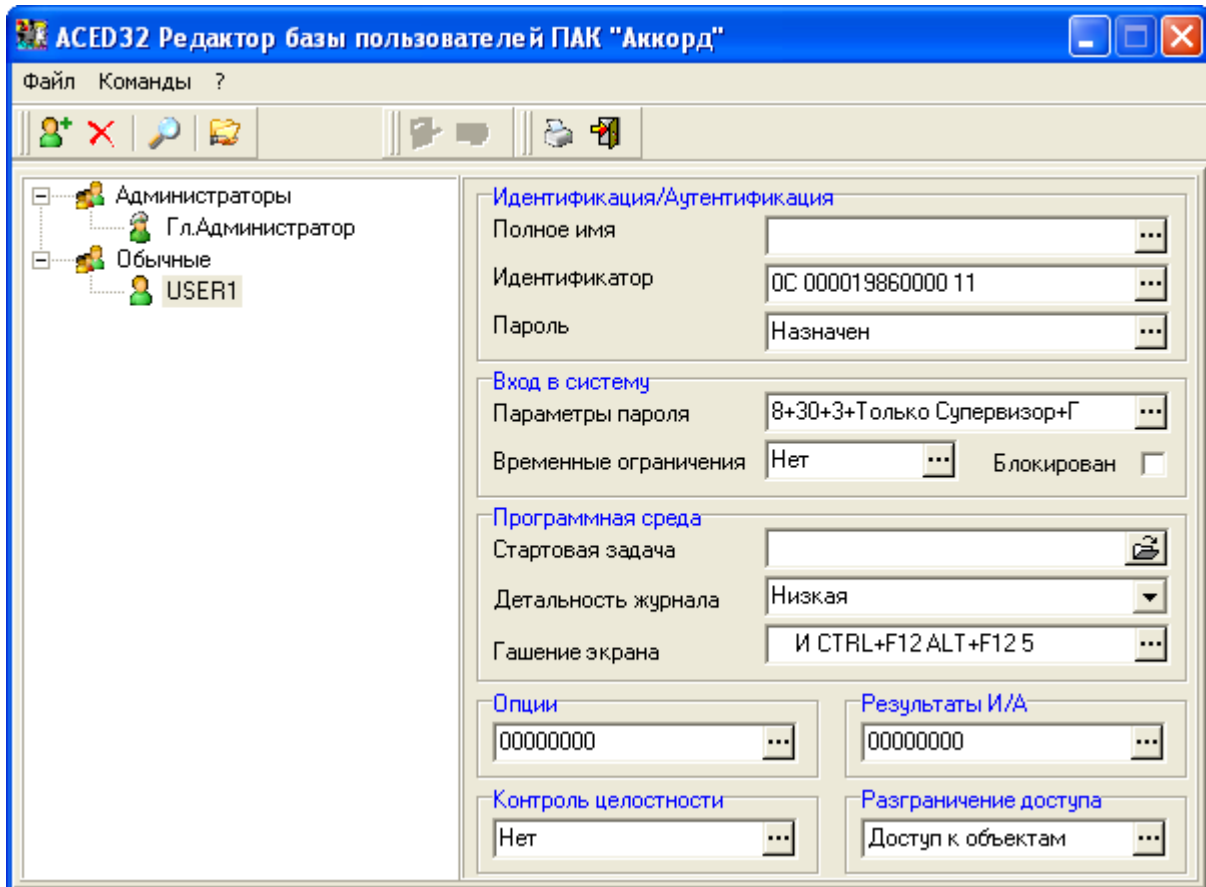


Рис. 2. Главное окно программы.

Сообщения, выдаваемые программой при ее запуске, и порядок действий по ним:

Сообщение	Причина	Порядок действий
«Неверный или старый файл списка пользователей»	БД пользователей ACED32 не соответствует БД пользователей контроллера "Аккорд"	Нажмите кнопку «ОК». Удалите файл C:\ACCORD.NT\Accord.amz. Запустите программу ACED32.EXE.
«ТМ не зарегистрирован!»	Использован ТМ, не зарегистрированный в ACED32.EXE	Используйте зарегистрированный ТМ-идентификатор администратора
«Неверный пароль !!!»	Введен пароль не соответствующий данному ТМ-идентификатору.	Введите правильный пароль
«Редактор может использовать только Администратор»	Попытка запуска редактора лицом, не являющимся администратором.	Используйте зарегистрированный ТМ-идентификатор администратора
Выход из ACED32 без предупреждения	Истекло время (строка «Отмена (X)», где X – время в секундах) для использования ТМ	Перезапустите программу ACED32. Используйте ТМ-идентификатор в течение времени, отведенного для этой операции

2.2 Выход из программы

В подменю <Файл> (см. Рис.2.) выберите команду <Выход>¹ или на панели инструментов нажмите кнопку «Выход из программы».

Если были внесены изменения в ПРД любого пользователя, то на экран выводится запрос на подтверждение сохранения изменений. При выборе кнопки <ДА> все изменения базы пользователей будут сохранены. При вводе, или изменении пароля в программе ACED32 в процессе сохранения настроек выводится окно с требование повторно ввести пароль пользователя. Связано это с тем, что формат хранения учетных записей пользователей в системе «Аккорд» кардинально отличается от ОС Windows, и программа ACED32 не хранит пароли в открытом виде в процессе работы. Некоторое неудобство, связанное с повторным вводом пароля, компенсируется высокой стойкостью защитных процедур к попыткам перехвата парольной информации. Если выбрать кнопку <Отмена>, то произойдет выход из программы без сохранения изменений в списке пользователей.

Сообщения, выдаваемые программой при выходе из нее, и порядок действий по ним:

Сообщение	Причина	Порядок действий
«Назначьте пользователю (указывается имя_пользователя) ТМ-идентификатор !»	Пользователю с именем (указывается имя пользователя) не назначен ТМ-идентификатор, но корректировались другие параметры доступа	Назначить пользователю (указывается имя_пользователя) ТМ-идентификатор. См. "Руководство по установке" комплекса СЗИ НСД "Аккорд-АМДЗ"
«Назначьте пользователю (указывается имя_пользователя) пароль!»	Пользователю с именем (указывается имя пользователя) не назначен пароль.	Назначить пользователю (указывается имя_пользователя) пароль или отменить использование пароля: в поле «Параметры пароля» (установить минимальную длину пароля - 0).

3 ИНФОРМАЦИЯ О ПРОГРАММЕ

Выберите команду <?> в меню главного окна программы (Рис. 2). В подменю <?> выберите команду <О программе>. На экран выводится окно, показанное на Рис. 3.

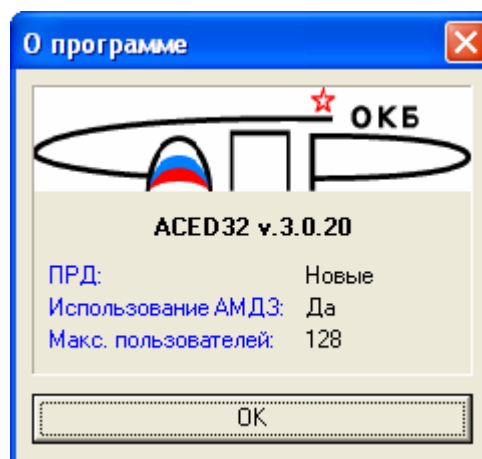


Рис. 3. Информация о программе

Информация о программе содержит сведения о версии программы; типе ПРД (см. приложение accord.ini); использовании базы данных контроллера "Аккорд-АМДЗ"; максимальном количестве пользователей, которые могут быть зарегистрированы; типе БД

¹ команде <Выход> в подменю <Файл> соответствуют клавиши <Alt+X>.

11443195.4012-019 97 02

контроллера; разработчике программы. Для продолжения работы нажмите кнопку «ОК» или клавишу <Enter>.

4 РЕГИСТРАЦИЯ НОВОЙ ГРУППЫ ПОЛЬЗОВАТЕЛЕЙ.

В подменю <Команды> выберите команду <Создать>. На экран выводится окно, предлагающее выбрать тип создаваемого объекта. Установите отметку на строке «Группа» и введите имя новой группы пользователей. После этого следует выбрать кнопку «ОК». В главном окне программы появится новая группа. Для группы можно задать параметры доступа к ресурсам СВТ. В строке «Группа в NT» можно выбрать группу в составе ОС, в которую будут включаться пользователи группы СЗИ «Аккорд» при синхронизации с базой данных пользователей операционной системы.

Следует отметить, что параметры, заданные для группы, присваиваются пользователю, созданному в данной группе, но для каждого пользователя их можно изменить в индивидуальном порядке.

5 РЕДАКТИРОВАНИЕ ПАРАМЕТРОВ ПОЛЬЗОВАТЕЛЕЙ (ПРАВ ДОСТУПА)

5.1 Регистрация нового пользователя

В подменю <Команды> главного меню программы ACED32 (Рис. 2) На экран выводится окно, предлагающее выбрать тип создаваемого объекта. Установите отметку на строке «Пользователь» и введите имя нового пользователя (Рис. 4). После этого следует выбрать кнопку «ОК». В главном окне программы появится новый пользователь.

Примечание: если список пользователей активен, то при нажатии клавиши <Insert> также можно "создать" нового пользователя.

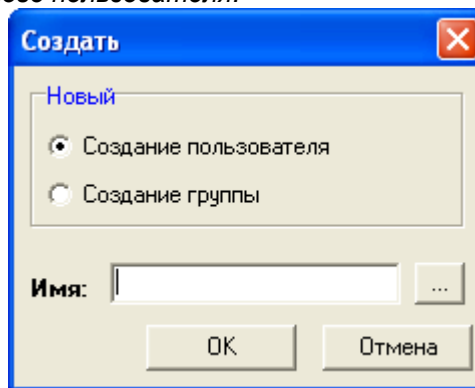


Рис. 4. Окно регистрации нового пользователя.

При нажатии на кнопку «Отмена» регистрация нового пользователя производиться не будет.

Сообщения, выдаваемые при регистрации пользователей, и порядок действий по ним:

Сообщение	Причина	Порядок действий
«Пользователь с таким именем уже есть».	Пользователь с таким именем уже есть в списке пользователей.	Назначьте новому пользователю уникальное имя.
«Задайте имя, пожалуйста».	Имя пользователя не задано.	Назначьте новому пользователю имя

5.2 Печать параметров пользователя

Для хранения и учета параметров пользователей используется команда <Печать> из подменю <Команды> главного меню программы (см. Рис.2).

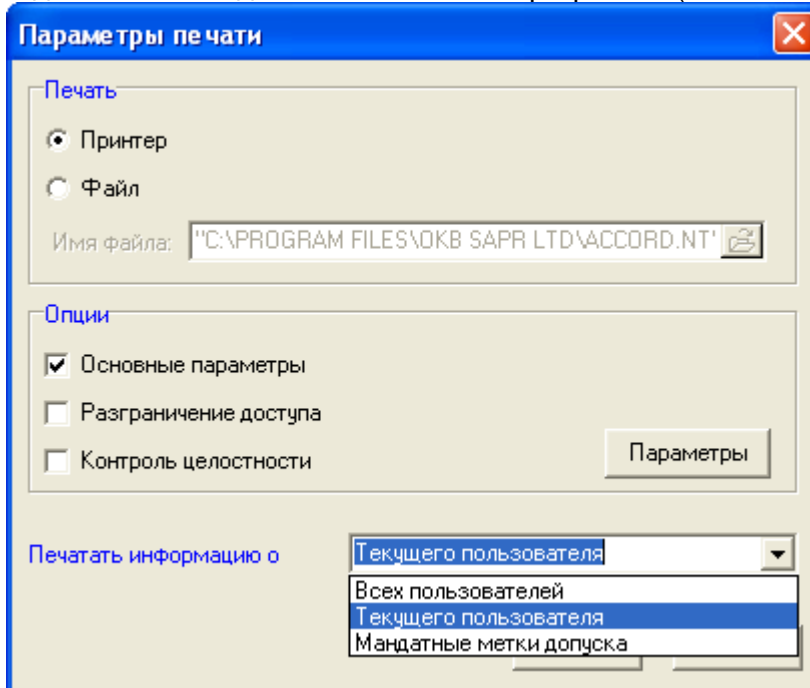


Рис. 5. Окно для выбора параметров пользователя и устройства печати.

Команда <Печать> предназначена для вывода списка параметров пользователя на твердый носитель (принтер) или в файл (магнитный носитель).

В подменю <Команды> главного меню программы выберите команду <Печать>, или на панели инструментов - нажмите кнопку «Печать информации» - выводится окно «Параметры печати», показанное на Рис. 5.

Выберите параметры пользователя, необходимые для вывода и устройство, на которое будут они записаны. Далее нажмите кнопку «ОК» или клавишу <F2>, для отмены операции следует нажать кнопки «Отмена» или <Esc>.

Примечание: Если осуществляется запись параметров пользователя в файл, то по умолчанию ему присваивается имя USER.LST в рабочем каталоге.

5.3 Удаление пользователя из списка зарегистрированных

С помощью мыши или клавиатуры выделите пользователя, которого Вы хотите удалить. В подменю <Команды> выберите <Удалить>, или на панели инструментов нажмите кнопку «Удалить пользователя». Программа выдает запрос «Вы действительно хотите удалить пользователя (указывается имя_пользователя)?» Подтвердите или отмените удаление.

Примечание: Если список пользователей активен, то можно удалить выделенного пользователя, нажав на клавишу <Delete>.

ВНИМАНИЕ!

Нельзя удалить группы «Администраторы» и «Обычные», а также пользователя «Гл.администратор».

5.4 Переименование пользователя в списке

С помощью мыши или клавиатуры выделите пользователя, которого Вы хотите переименовать. В подменю <Команды> выберите <Переименовать> или щелкните правой кнопкой мыши на выделенном пользователе и выберите из всплывшего меню команду <Переименовать>.

11443195.4012-019 97 02

На экран выводится окно (Рис. 6), предлагающее ввести новое имя пользователя.

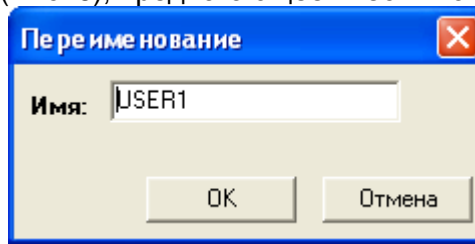


Рис. 6. Переименование пользователя

«ОК» или <Enter> - изменение имени, «Отмена» - отмена операции переименования.

Примечание: Если список пользователей активен, то можно переименовать выделенного пользователя, нажав на клавишу <F2>.

Сообщения, выдаваемые программой при регистрации пользователей, и порядок действий по ним:

Сообщение	Причина	Порядок действий
«Пользователь с таким именем уже есть».	Пользователь с таким именем уже есть в списке пользователей.	Назначьте новому пользователю уникальное имя.
«Задайте имя, пожалуйста».	Имя пользователя не задано.	Назначьте новому пользователю имя

5.5 Поиск пользователя по ТМ-идентификатору

По ТМ-идентификатору можно найти соответствующего ему пользователя. Для этого необходимо выбрать в подменю <Команды> пункт <Поиск> или на панели инструментов нажать кнопку «Поиск пользователя по ТМ-идентификатору» - на экран выводится окно (Рис. 7) с запросом ТМ-идентификатора.

Если прислонить ТМ-идентификатор к считывателю в отведенный интервал времени, то в списке пользователей активизируется (выделяется) пользователь, которому принадлежит данный ТМ-идентификатор.

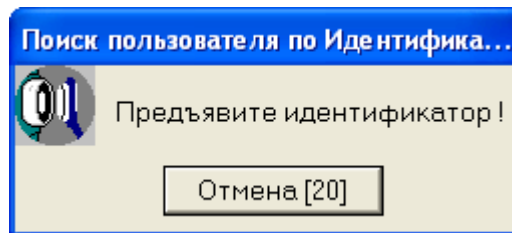


Рис. 7. Запрос ТМ-идентификатора для поиска.

Сообщения, выдаваемые программой и порядок действий по ним:

Сообщение	Причина	Порядок действий
«ТМ никому не принадлежит!»	Предъявленный ТМ-идентификатор не принадлежит ни одному из зарегистрированных пользователей	Попробуйте использовать другой ТМ-идентификатор

5.6 Синхронизация параметров пользователя с параметрами группы

Синхронизация может понадобиться при изменении параметров группы и последующем присвоении этих параметров пользователю. В списке пользователей с помощью мыши или клавиш «стрелка вверх», «стрелка вниз» выделите пользователя, параметры которого Вы хотите синхронизировать. Правой кнопкой мыши щелкните на

11443195.4012-019 97 02

имени выделенного пользователя, на экране появится всплывающее меню. Выберите из него пункт <Синхронизировать> - на экране появится окно «Выбор параметров синхронизации», показанное на Рис. 8. В этом окне перечислены параметры, являющиеся общими для синхронизируемых объектов. Установите те параметры пользователя, которые будут синхронизированы. Для выполнения синхронизации нажмите кнопку «Синхронизация» или клавишу <F2>, для отмены - «Отмена» или <Esc>.

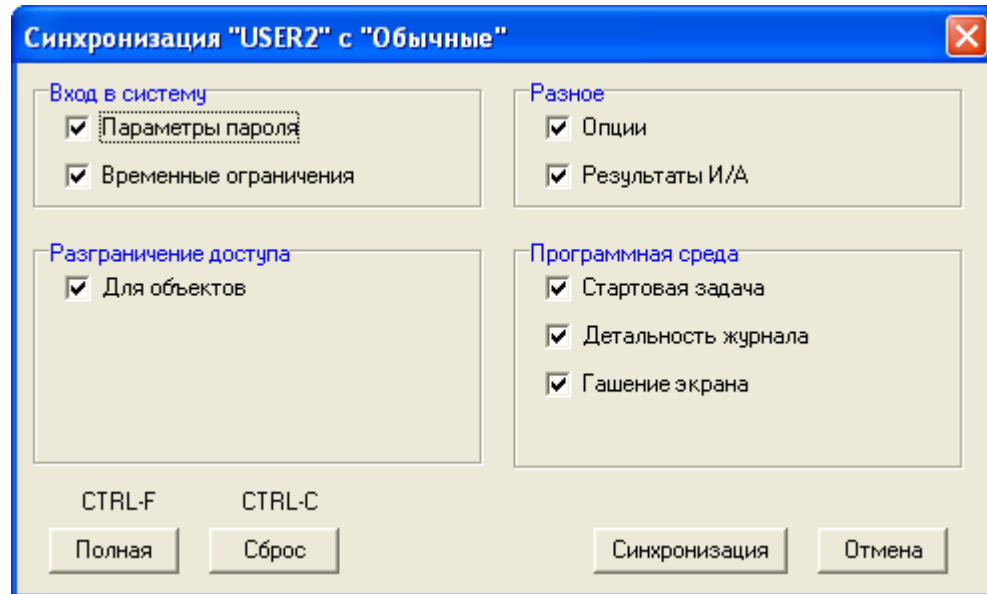


Рис. 8. Параметры синхронизации.

Примечание: Для группового манипулирования параметрами синхронизации пользуйтесь кнопками «Полная» или клавишами <Ctrl+F> - устанавливает все параметры; и «Сброс» или <Ctrl+C>- сбрасывает все параметры.

Сообщения, выдаваемые программой при синхронизации параметров пользователей, и порядок действий по ним:

Сообщение	Причина	Порядок действий
«Выберите, пожалуйста, объект для синхронизации».	Не выбран объект для синхронизации	Выберите объект для синхронизации в окне «Выбор объекта», щелкнув левой кнопкой мыши на его имени

6 АДМИНИСТРИРОВАНИЕ ПОДСИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА

Администратор БИ может производить изменение параметров доступа субъектов к объектам СЗИ. Для этого в списке пользователей выберите имя пользователя, параметры которого необходимо отредактировать.

Примечание: Некоторые «Параметры пользователя» являются обязательными, без которых невозможен ввод остальных, (например – «ТМ-идентификатор» и «Пароль»). Группы «Администраторы» и «Обычные» создаются при инициализации БД пользователей контроллера «Аккорд», и их нельзя переименовать или удалить. Параметры группы являются универсальным шаблоном для задания «Параметров пользователя», и присваиваются по умолчанию каждому создаваемому пользователю.

6.1 Задание имени пользователя

Администратор должен присваивать каждому пользователю уникальное в данной вычислительной среде (отдельный компьютер или локальная сеть) имя. Имя пользователя задается только при регистрации нового пользователя. Параметр «Полное имя» не является обязательным параметром, задается по желанию администратора, и может использоваться для идентификации пользователя в ОС, если в программе настройки комплекса установлен параметр «Использовать полное имя в учетных записях NT».

6.2 Регистрация ТМ пользователя

В поле «ТМ-идентификатор» главного окна (Рис. 2) отображается информация о ТМ-идентификаторе активного (выделенного) пользователя. Выберите режим редактирования, нажав на кнопку, расположенную справа в поле «ТМ-идентификатор» или клавишу <Enter>. На экране появится окно «Работа с ключом пользователя» (Рис. 9).

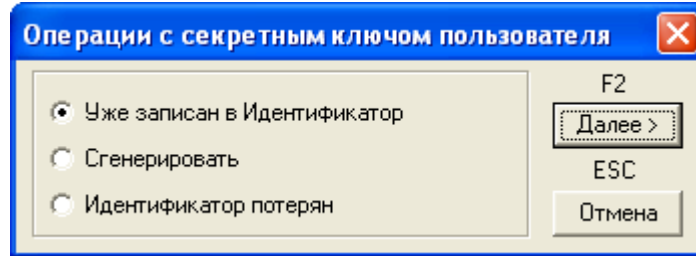


Рис. 9. Работа с ключом пользователя.

Секретный ключ пользователя генерируется с использованием датчика случайных чисел (ДСЧ), установленного на плате контроллера «Аккорд-АМДЗ», и записывается в энергонезависимую память ТМ-идентификатора.

ТМ-идентификатор, в котором не записан ключ пользователя, считается недопустимым в СЗИ «Аккорд». По этой причине не допускается использование ТМ-идентификаторов типа DS-1990 и DS-1991, т.к. они не имеют внутренней памяти.

Возможны три варианта работы с ключами пользователей:

1). "Уже записан в ТМ"

Секретный ключ может быть уже записан в ТМ, например, при перерегистрации пользователя, который был уже зарегистрирован в составе комплекса «Аккорд» на другой СВТ (РС), или секретный ключ уже был сгенерирован при регистрации ТМ в контроллере "Аккорд-АМДЗ" из состава комплекса.

Нажав кнопку «Далее» или клавишу <F2>, выдается запрос на считывание серийного номера ТМ-идентификатора - выводится окно, показанное на Рис. 7. Следует приложить ТМ-идентификатор пользователя к контактному устройству съемника информации - происходит перерегистрация предъявленного ТМ-идентификатора.

2). "Сгенерировать"

В этом случае, при нажатии кнопки «Далее» или клавиши <F2>, генерируется секретный ключ и выдается запрос на считывание ТМ-идентификатора (Рис. 7). Используйте ТМ-идентификатор пользователя. Происходит регистрация ТМ-идентификатора и запись в него секретного ключа пользователя.

3). "Потерян"

В этом случае, после нажатия кнопки «Далее» или клавиши <F2> поле «ТМ-идентификатор» данного пользователя примет значение «Не назначен».

Сообщения, при регистрации ТМ пользователей, и порядок действий по ним:

Сообщение	Причина	Порядок действий
«ТМ принадлежит пользователю (указывается имя_пользователя)»	Данный ТМ-идентификатор уже зарегистрирован для пользователя (указывается имя).	Нажмите кнопку «ОК». Используйте другой ТМ-идентификатор
«Ошибка чтения секретного ключа!»	Ошибка чтения ТМ, или секретный ключ не записан в ТМ идентификаторе.	Нажмите кнопку «ОК», повторите операцию. Если ошибка повторится, сгенерируйте секретный ключ.
«Неверный тип ТМ-идентификатора»	Тип ТМ не поддерживается комплексом «Аккорд».	Нажмите кнопку «ОК». Используйте другой ТМ.
«Ошибка создания ключа!»	Ошибка записи в ТМ-идентификатор.	Нажмите кнопку «ОК». Повторите операцию.

11443195.4012-019 97 02

6.3 Установка параметров пароля

В главном окне (Рис. 2) щелкните левой кнопкой мыши в поле «Параметры пароля». Выберите режим редактирования, нажав на кнопку, расположенную справа в поле «Параметры пароля», или клавишу <Enter>. На экран выводится окно «Параметры пароля» (Рис.10.).

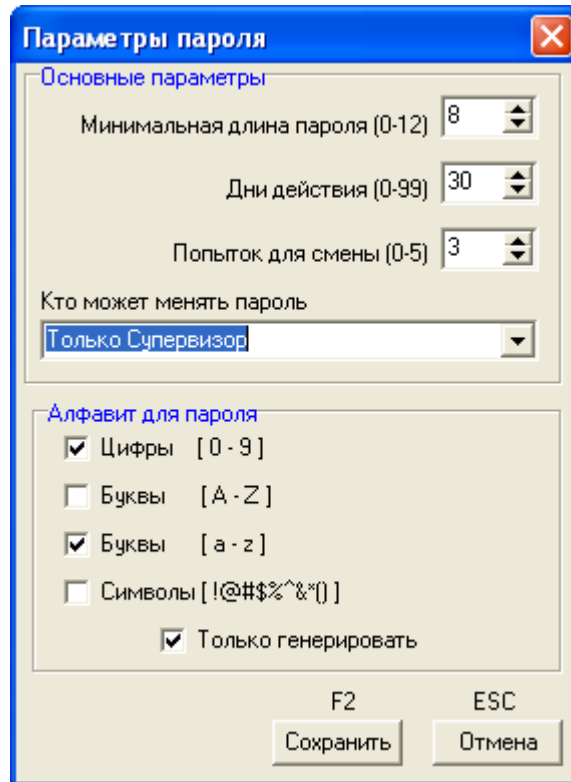


Рис.10. Параметры пароля пользователя.

Параметры пароля включают в себя следующие поля:

"*Длина пароля*" - минимальная длина пароля – 0 (пароль задавать не обязательно), максимальная - 12 символов.

"*Время действия*" - время действия пароля до смены: от 0 (нет смены пароля) до 99 дней.

"*Попыток для смены*" - количество попыток смены пароля: от 0 (бесконечное) до 5.

"*Кто может менять пароль*" - установка прав на смену пароля (только администратор или администратор и пользователь).

"*Алфавит для генерации пароля*" - определяет набор символов, из которого возможна генерация пароля пользователя. При установке флага «Только генерировать» пароль будет генерироваться случайным образом из символов заданного алфавита при смене пароля пользователя.

Обратите внимание! Если пароль уже задан, то изменения его параметров вступят в силу только при смене пароля.

Для выхода из режима редактирования с сохранением измененных параметров нажмите кнопку «Запись» или клавишу <F2>, без сохранения – «Отмена» или <Esc>.

6.4 Задание пароля пользователя

В поле «Пароль» главного окна (Рис. 2) отображается информация о том, назначен или нет пароль выделенному пользователю. Выберите режим редактирования, нажав на кнопку, расположенную справа в поле «Пароль» или клавишу <Enter>. На экране появится окно «Ввод пароля» (Рис. 11).

11443195.4012-019 97 02

Рис. 11. Задание пароля пользователя.

Введите пароль и повторите ввод пароля для подтверждения. Нажмите клавишу <Ок>. Можно воспользоваться клавишей «Сгенерировать», даже в том случае, когда не установлен флаг «Только генерировать» в параметрах пароля. При использовании клавиши «Сгенерировать» полученная последовательность символов автоматически вводится в первое поле пароля, а в нижней части окна выводится значение пароля и требуется его повторный ввод для подтверждения (см. Рис. 12).

Рис. 12. Ввод пароля с использованием процедуры генерации.

Сообщения при вводе пароля пользователя, и порядок действий по ним:

Сообщение	Причина	Порядок действий
«Такую комбинацию символов недопустимо использовать в качестве пароля»	При вводе пароля контролируется нажатие последовательно расположенных клавиш	Используйте другой пароль
«Не следует в качестве пароля использовать имя пользователя или его часть»	В пароле использовано имя пользователя	Используйте другой пароль.
«Не следует в качестве пароля использовать старый пароль или его часть».	При смене пароля в качестве нового введен опять старый пароль	Используйте другой пароль.
«Длина пароля должна быть не менее (указывается число) символов».	Количество введенных символов меньше установленной минимальной длины пароля	Введите пароль из большего количества символов, или уменьшите минимальную длину в параметрах пароля.
«Вы ошиблись - начинаем все сначала».	Ошибка при повторном вводе пароля.	Повторите процедуру ввода пароля заново.

6.5 Установка детальности протокола работы пользователей

Во время каждого сеанса работы пользователя ведется журнал регистрации событий, в котором отображаются действия пользователя, прикладного и системного ПО. Администратору рекомендуется в текущей работе использовать низкую детальность ведения журнала. Среднюю и высокую детальность следует использовать при изучении работы вновь используемых задач с целью определения особенностей задачи, а именно: создание новых постоянных и временных каталогов и файлов, используемых устройств и т.д. Выберите команду «Детальность журнала» в окне «Параметры пользователя» (Рис. 2). Значение поля «Детальность журнала» выбирается из списка, который раскрывается при щелчке мышью по кнопке, расположенной справа.

Детальность журнала:

"Нет" - регистрация входа/выхода из системы.

"Низкая" - регистрация входа/выхода из системы, попытки несанкционированного доступа, запуск задач.

"Средняя" - то же, что и низкая детальность, плюс операции доступа к файлам и каталогам.

"Высокая" - то же, что и при средней детальности и выполнение функций просмотра каталогов.

6.6 Установка режима гашения экрана.

Гашение экрана используется для временного отключения экрана и доступа к клавиатуре и мыши по истечении установленного интервала в работе пользователя, либо по нажатию комбинации клавиш «Гашение» (по умолчанию установлена комбинация <Ctrl+F12>). Вернуться в рабочий режим можно только при помощи ТМ-идентификатора пользователя, чьи права доступа выполняются в данном сеансе работы. Для редактирования параметров гашения экрана щелкните мышью на кнопке, расположенной справа в поле «Гашение экрана» (Рис. 2), или нажмите клавишу <Enter>. Выводится окно «Параметры Screen Saver» (Рис. 13).

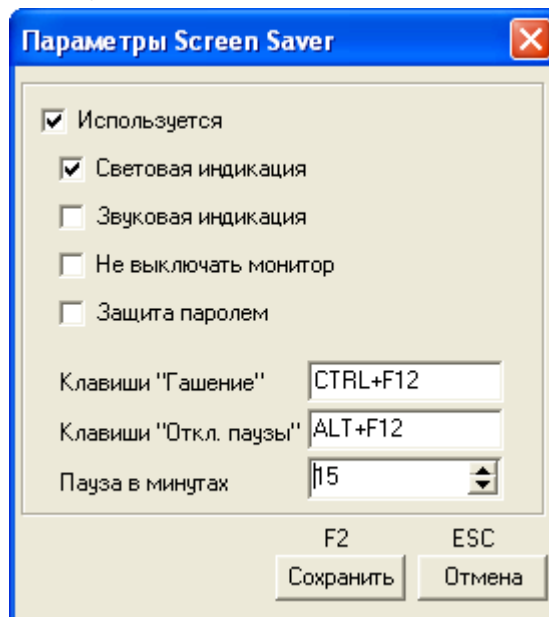


Рис. 13. Параметры гашения экрана.

С помощью мыши задайте необходимые параметры гашения. Если необходимо включить режим гашения экрана, установите параметр «Используется» (этот параметр имеет наиболее высокий приоритет). Затем, если необходимо, установите параметры:

«Световая индикация» - мигание индикаторов <Num Lock>, <Caps Lock> и <Scroll Lock> в режиме гашения)

«Звуковая индикация» - звуковые сигналы в режиме гашения).

«Не выключать монитор» - режим, при котором блокируется клавиатура и мышь, но заставка экрана не включается. Такой режим может быть полезен на рабочих станциях, которые осуществляют мониторинг сети, почты и т.д.

11443195.4012-019 97 02

Интервал времени, через который выполняется переход в режим гашения экрана, если клавиатура и мышь не используются, устанавливается в строке «Пауза в минутах» (по умолчанию – 5 минут).

Можно установить комбинацию клавиш принудительного включения Screen-saver – «Гашение» (по умолчанию <Ctrl+F12>). Предусмотрена установка комбинации клавиш «Откл. паузы» (по умолчанию <Alt+F12>), при нажатии которой отключается режим срабатывания хранителя экрана по времени и для включения используется только клавиатура, или мышь. Для выхода с сохранением установленных параметров нажмите кнопку «Запись» или клавишу <F2>, выход без сохранения – «Отмена» или <Esc>.

Примечание: для установки другой комбинации клавиш «Гашение» или «Откл. паузы» необходимо перейти в поле «Гашение» или «Откл. паузы» соответственно и одновременно нажать клавиши, Shift, Ctrl или Alt и одну из клавиш F1..F12.

Сообщения, выдаваемые программой при установке режима гашения экрана, и порядок действий по ним:

Сообщение	Причина	Порядок действий
«Такая комбинация клавиш уже назначена»	Выбранная Вами комбинация клавиш уже назначена.	Назначьте другую комбинацию клавиш.

6.7 Установка временных ограничений для сеанса работы пользователя

В списке пользователей с помощью мыши или клавиатуры выделите пользователя.

В поле «Временные ограничения» окна «Параметры пользователя» (Рис. 2) отображается информация о наличии временных ограничений у активного (выделенного) пользователя. Выберите режим редактирования, нажав на кнопку, расположенную справа в поле «Временные ограничения», или клавишу <Enter>. На экран выводится окно «Временные ограничения для (указывается имя_пользователя)» (Рис. 14).

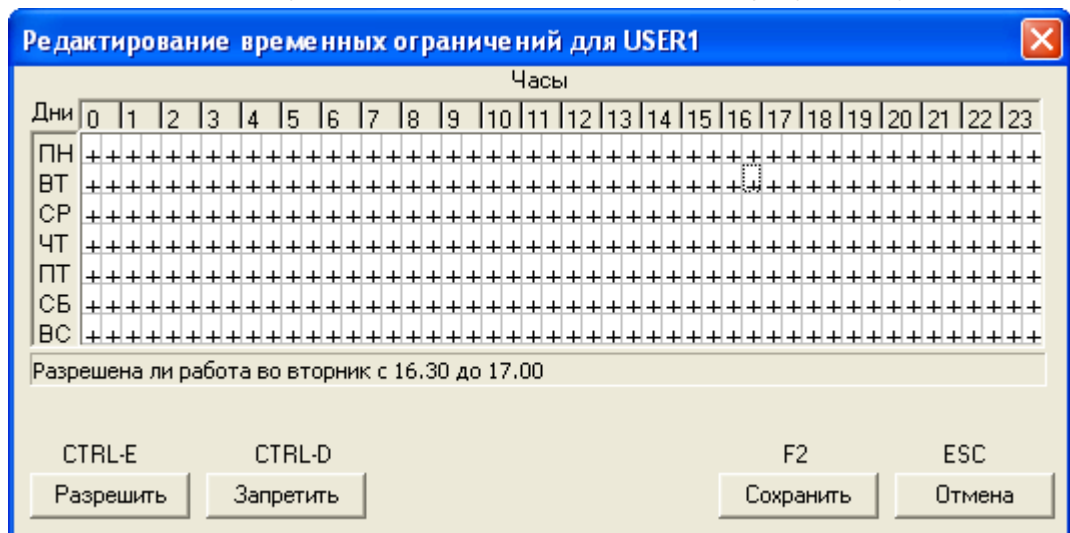


Рис. 14. Окно редактирования временных ограничений

В этом окне отображена таблица со строками, соответствующими дням недели, и столбцами, соответствующими временным промежуткам (часам).

Ячейки таблицы заполнены знаками "+" и "-":

"+" - работа возможна.

"-" - работа невозможна.

11443195.4012-019 97 02

При помощи мыши, удерживая левую кнопку, можно выделить область редактирования. Для того чтобы разрешить пользователю работу в выделенной области, необходимо нажать кнопку «Разрешить» или клавиши <Ctrl+E>. Для запрета работы в выделенной области необходимо нажать кнопку «Запретить» или клавишу <Ctrl+D>. Двойное нажатие мыши (или клавиши <Пробел>) на ячейку меняет ее значение на противоположное. Перемещение по таблице возможно как при помощи мыши, так и при помощи клавиатуры.

Для выхода из режима редактирования с сохранением, нажмите кнопку «Запись» или клавишу <F2>, без сохранения – «Отмена» или <Esc>.

6.8 Блокировка пользователя

В главном окне программы (см. Рис.2) правее поля «Временные ограничения» находится флаг «Блокирован». При установке этого флага все параметры пользователя сохраняются в базе данных, но вход в систему и работа данного будут запрещены. Данный флаг можно использовать для временной блокировки пользователя. После того, как администратор снимет блокировку, работа пользователя восстановится со всеми установленными настройками. Для этого необходимо просто перезагрузить компьютер.

Внимание! Данный флаг поддерживается внутренним ПО «Аккорд АМД3» версии 02.01.005 и выше!

6.9 Установка стартовой задачи пользователя

В главном окне программы (см. Рис.2) нажмите мышкой правую кнопку в строке "Задача для запуска", и на экран выводится окно выбора исполняемого файла (задачи). Выбранная задача запускается для данного пользователя после старта операционной системы в качестве программной оболочки (shell) вместо explorer.exe. При этом пользователь может работать только в загруженной программной среде (рабочий стол Windows, кнопка «Пуск» и панель задач на экран не выводятся). В случае, когда пользователю в рамках его функциональных обязанностей необходимо запускать на выполнение несколько различных задач, то в качестве задачи для запуска можно указать программу AcTskMng.EXE, входящую в состав комплекса СЗИ «Аккорд» (Рис. 15).

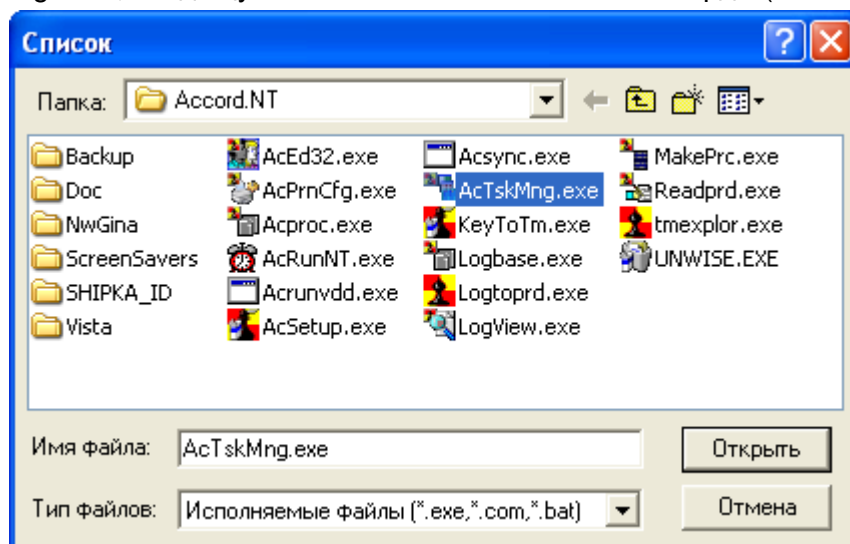


Рис. 15. Выбор стартовой задачи – менеджера приложений СЗИ «Аккорд».

Для успешной работы этой программы необходимо создать текстовый файл – список задач, разрешенных для запуска данному пользователю. Имя этого файла должно совпадать с именем пользователя, расширение файла должно быть .ACT. Задачи пользователя можно объединять в группы по функциональному признаку. Если в файле

11443195.4012-019 97 02

используются русские наименования группы, или задачи, то они должны вводиться в «windows» кодировке. Файл .ACT должен выглядеть следующим образом:

```
[Group1]
GroupName=File managers
[Task1.1]
DisplayName=FAR Manager
ImagePath=C:\Program Files\Far\far.exe
[Task1.2]
DisplayName=Norton Commander
ImagePath=c:\NC\nc.exe
Parameters=/V
[Group2]
GroupName=Офисные приложения
[Task2.1]
DisplayName= Excel
ImagePath=C:\Program Files\Microsoft Office\Office\Excel.exe
[Task2.2]
DisplayName= Winword
ImagePath=C:\Program Files\Microsoft Office\Office\winword.exe
[RUN_BEFORE]
GroupName=Предварительный запуск
[RunTask1]
DisplayName=IntelExtrimGraphics
ImagePath=c:\Program Files\Intel\IEG.exe
[RunTask2]
DisplayName=SoundMax
ImagePath=c:\Program Files\SM\smax3cp.exe
```

В результате при старте монитора разграничения доступа запустится оболочка AcTskMng со списком программ, доступных для выполнения данным пользователем (Рис.16.)

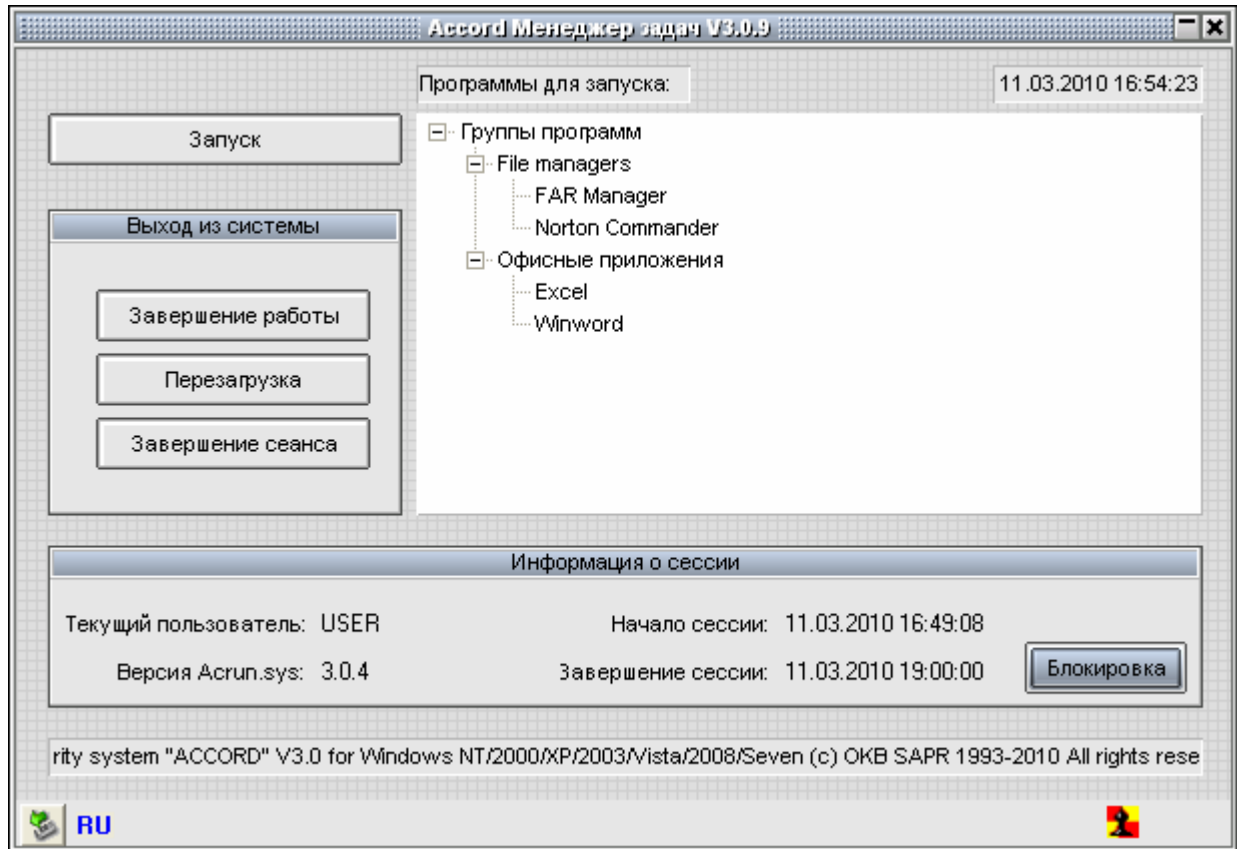


Рис. 16. Менеджер задач СЗИ «Аккорд».

Кроме списка задач пользователю доступны кнопки завершения работы, перезагрузки и завершения сеанса, а также кнопка включения блокировки экрана (Screen Saver). Если пользователь не входит в группу администраторов, то для него также блокируется возможность запуска диспетчера задач Windows (по комбинации клавиш Ctrl-Alt-Del).

Секция [RUN_BEFORE] определяет группу задач, которые запускаются перед загрузкой оболочки AcTskMng.

Если нет необходимости разбивать задачи на группы, то администратор может задать простой список в файле .ACT. В этом случае формат файла следующий:

```
[Task1.1]
#Комментарий
DisplayName=FAR Manager
ImagePath=C:\Program Files\Far\far.exe
[Task1.2]
DisplayName=Norton Commander
ImagePath=c:\NC\nc.exe
Parameters=/V
[Task1.3]
DisplayName= Excel
ImagePath=C:\Program Files\Microsoft Office\Office\Excel.exe
[Task1.4]
DisplayName= Winword
ImagePath=C:\Program Files\Microsoft Office\Office\winword.exe
```

Внимание! В качестве исполняемых задач можно задавать файлы типа .lnk.

11443195.4012-019 97 02

Кроме этого, можно управлять режимом запуска программы AcTskMng.exe. В папке Accord.NT находится файл Actskmng.ini с набором ключей.

Ключ ProceedRegistryKeyRun=Yes управляет загрузкой резидентных программ, запускаемых при старте ОС (обычно они прописаны в секции Run системного реестра и значки этих программ располагаются на панели задач Windows в правом углу).

По умолчанию этот ключ установлен в значение Yes, т.е. запуск таких программ разрешен. Если администратор желает запретить запуск всех приложений кроме AcTskMng.exe, то значение ключа нужно установить в No.

Ключ WaitEndTask=Yes определяет последовательность выполнения задач, включенных в список. Значение ключа «Yes» означает, что запуск следующей задачи из списка будет возможен только после завершения уже запущенного приложения. Значение ключа «No» разрешает запуск одновременно нескольких приложений. Переключаться между запущенными приложениями можно стандартной комбинацией клавиш <Alt-Tab>.

Внимание! Создание списка выполняемых задач в AcTskMng еще не означает реализацию замкнутой программной среды, т.к. запущенное приложение может иметь в своем составе средства запуска других программ. Полностью замкнутую программную среду можно реализовать с использованием механизма мандатного доступа с контролем процессов!

6.10 Установка правил разграничения доступа (ПРД) к объектам доступа

СЗИ НСД «Аккорд» поддерживает два типа управления правилами разграничения доступа:

- дискреционный механизм ПРД;
- мандатный механизм ПРД.

Система атрибутов доступа и особенности ее реализации описаны в «Руководстве администратора» (11443195.4012-019 90 02). Можно использовать отдельно каждый механизм управления. Возможен вариант использования комбинированной политики безопасности с применением обоих механизмов задания ПРД.

6.10.1 Установка доступа к объектам с использованием дискреционного метода ПРД.

Если в файле accord.ini установлены параметры Discrete Access = Yes и Mandatory Access = No то используется только дискреционный механизм задания и контроля ПРД. Выбор механизма управления ПРД можно осуществлять в программе настройки комплекса «Аккорд».

В главном окне программы (см. Рис.2) нажмите мышкой правую кнопку в строке "Разграничение доступа", и на экран выводится окно с правами доступа пользователя к ресурсам СВТ, показанное на Рис.17. По умолчанию выведен перечень всех доступных корневых каталогов (для сетевых корневых каталогов указано полное сетевое имя), ключей реестра (строки, начинающиеся с «\HKEY_»), сетевых и локальных принтеров.

В этом окне нет деления на диски, каталоги, файлы и т.д., а ведется один общий список объектов. Для того, чтобы запретить доступ к логическому диску достаточно исключить корневой каталог этого диска из списка объектов.

Если какой-либо объект (каталог, файл, раздел реестра, сетевой ресурс, устройство или очередь печати) явно прописан в списке, то для него действуют установленные ПРД, независимо от атрибутов наследования объектов вышестоящего уровня.

Для того, чтобы сделать какой-либо файл «скрытым», т.е. полностью запретить к нему доступ, нужно включить его в список объектов, но не назначать ни одного атрибута доступа. Более подробно действие атрибутов доступа описано в «Руководстве администратора» (11443195.4012-019 90 02).

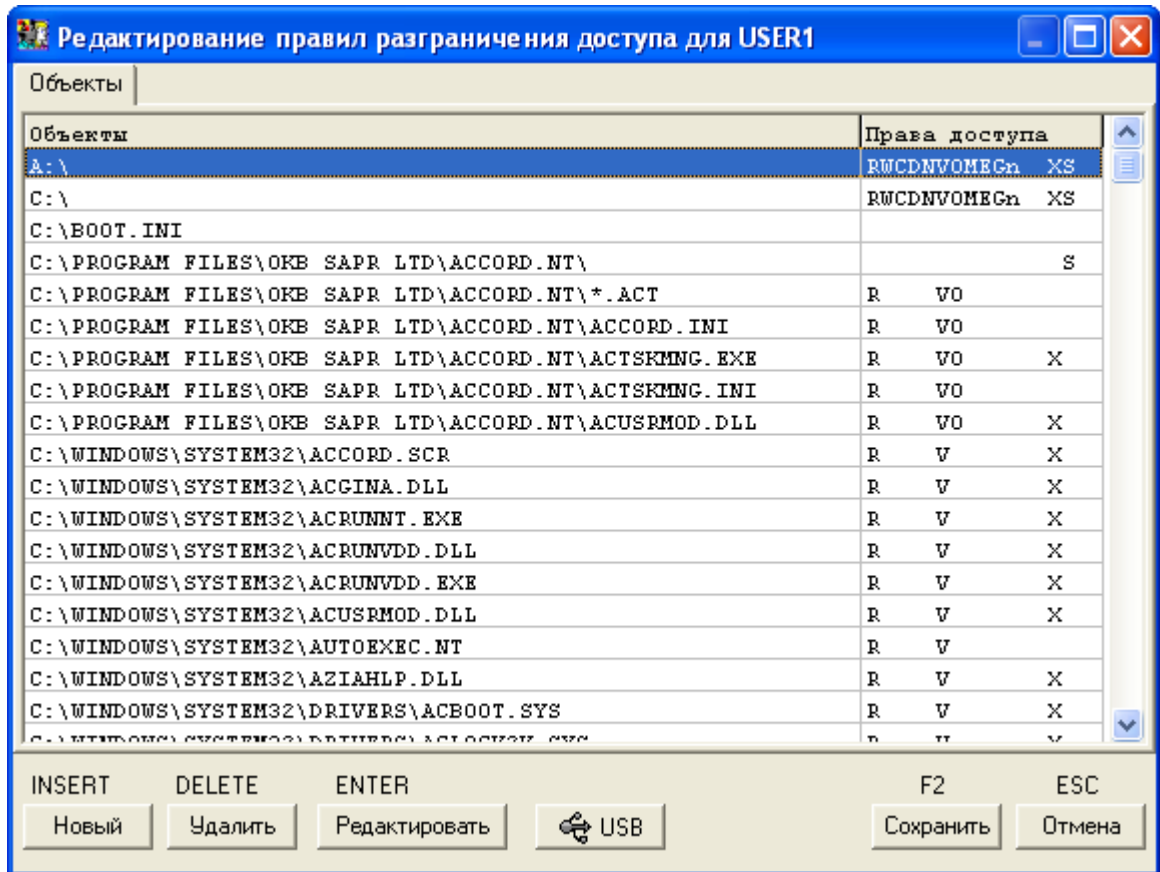


Рис. 17. Окно установки дискреционных ПРД к объектам.

В список объектов для обычных пользователей уже включены ограничения, которые защищают от модификации программные компоненты комплекса «Аккорд». В разделе «Объекты» (Рис.17) выберите строку с нужным именем объекта и нажмите кнопку «Редактировать» или клавишу <Enter> - выводится окно для определения правил доступа к объекту, показанное на Рис. 18. Если Вы хотите удалить какой-либо объект и установленные для него ПРД, то выберите строку с названием объекта, нажмите кнопку «Удалить» или клавишу <Delete>. Подтвердите или отмените удаление.

Для выхода из режима редактирования с сохранением, нажмите кнопку «Запись» или клавишу <F2>, без сохранения – «Закрыть» или <Esc>.

Примечание: при вводе имени файла можно пользоваться простым групповым обозначением имени файла, используя шаблон *.расширение. Например, можно *.bak, *.exe и т.п., **нельзя** *a.exe, a*.bat, &a.dat, ?a.dat, a.* и т.п.

11443195.4012-019 97 02

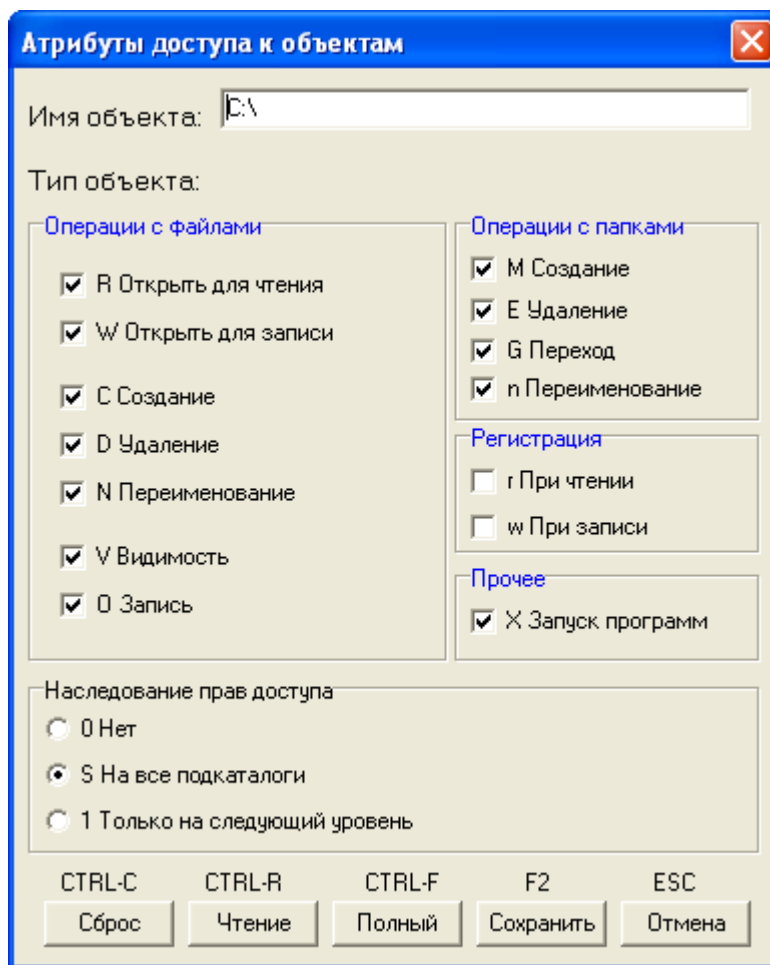


Рис. 18. Атрибуты доступа к объекту.

При установке дискреционных ПРД могут использоваться следующие атрибуты доступа:

I. Операции с файлами:

- R - разрешение на открытие файлов только для чтения.
- W - разрешение на открытие файлов для записи.
- C - разрешение на создание файлов на диске.
- D - разрешение на удаление файлов.
- N - разрешение на переименование файлов.
- V - видимость файлов. Позволяет делать существующие файлы невидимыми для пользовательских программ. Доступ возможен только по полному пути в формате Windows NT. Этот параметр имеет более высокий приоритет, чем R,W,D,N,O.
- O - эмуляция разрешения на запись информации при открытии файла. Этот параметр имеет более низкий приоритет, чем W (открыть для записи). Параметр может пригодиться в том случае, если программа по умолчанию открывает файл для чтения/записи, а мы хотим разрешить пользователю только просмотр файла.

II. Операции с каталогом:

- M - создание каталогов на диске (или подкаталогов в каталоге, для которого устанавливается атрибут).
- E - удаление каталогов на диске (или подкаталогов в каталоге, для которого устанавливается атрибут).
- G - разрешение перехода в этот каталог.

11443195.4012-019 97 02

- n – переименование каталога. В ОС Windows, например, удаление папки в "корзину" – это, на самом деле, переименование каталога.

III. Прочее:

- X - разрешение на запуск программ.

IV. Регистрация:

- r - регистрируются все операции чтения файлов диска (папки) в журнале.
- w - регистрируются все операции записи файлов диска (папки) в журнале.

Примечание: для группового манипулирования параметрами доступа пользуйтесь кнопками «Сброс» (сбрасывает все параметры), «Чтение» (устанавливает параметры R, V, G, X, S), «Полный» (устанавливает все параметры кроме параметров группы «Регистрация») или соответствующими им горячими клавишами - <Ctrl+C>, <Ctrl+R>, <Ctrl+F> (Рис. 18).

Для каталогов, в том числе и корневого каталога диска, устанавливается отдельный параметр, который очень важен для реализации ПРД – это параметр наследования прав доступа.

Параметр наследования прав доступа может принимать три значения:

S - параметры доступа наследуются существующими и созданными в дальнейшем подкаталогами **всех** уровней текущего каталога, т.е. для них устанавливаются те же параметры доступа, что и у "родительского" каталога, при этом для отдельных подкаталогов можно явно определять атрибуты доступа;

1 - параметры доступа текущего каталога наследуются **только** подкаталогами следующего уровня;

0 - параметры доступа текущего каталога не наследуются подкаталогами.

Например, если для корня дерева каталогов диска C:\ установить атрибут 0, доступными будут только файлы в корневом каталоге, а остальные каталоги для данного пользователя как бы не существуют. Каталог на диске C:\ будет доступен пользователю (с любой непротиворечивой комбинацией атрибутов) только при явном его описании в списке прав доступа. Если для корневого каталога C:\ установить атрибут S, то все его файлы, каталоги и подкаталоги доступны пользователю и правила доступа к ним определяется атрибутами, установленными для C:\. В этом случае отдельный каталог можно включить в список ПРД и установить для него персональные атрибуты, отличные от "родительских". Еще раз подчеркиваем, что, если какой-либо объект явно прописан в списке доступа, то для него действуют установленные ПРД, независимо от атрибутов наследования объектов вышестоящего уровня.

Если необходимый Вам объект отсутствует в списке (Рис. 17), нажмите кнопку «Новый» или клавишу <Insert> - на экран выводится расширенное окно «Атрибуты доступа к объектам» (Рис. 19). Справа в этом окне отображен список всех объектов. Каждый объект выделен цветом, соответствующим наследованию прав доступа и наличию объекта в списке разграничения прав доступа (Таблица 1.).

Таблица 1.

Наличие объекта в списке	Атрибут наследования прав доступа	Цвет
Есть	Полное наследование	Зеленый
Есть	Наследование на один уровень	Синий
Есть	Нет наследования	Красный
Нет	Атрибуты доступа наследуются	Коричневый
Нет	Нет доступа	Черный

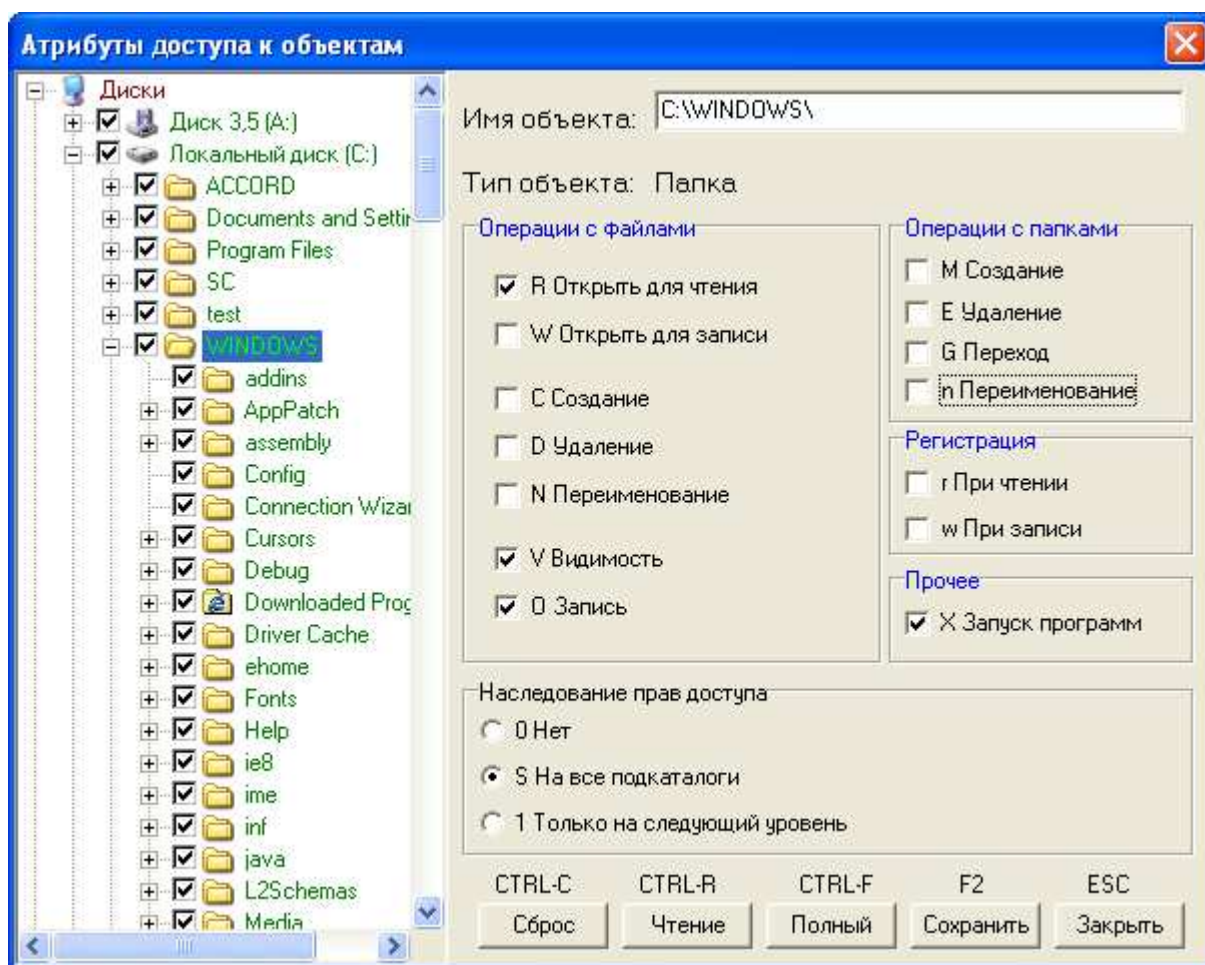


Рис. 19. Выбор нового объекта и установка ПРД.

Введите в поле «Имя объекта» имя объекта и установите для него необходимые атрибуты. С помощью мыши также можно выбрать имя объекта, щелкнув левой кнопкой мыши на имени объекта в дереве объектов, тогда в поле «Имя объекта» отобразится имя выделенного объекта, а в поле «Тип объекта» - его тип (каталог, файл, реестр, съемный диск, принтер). Если у выделенного объекта уже установлены ПРД, то будут отмечены соответствующие флаги, если нет, то все флаги будут сброшены. При установке ПРД можно воспользоваться клавишами <Сброс>, <Чтение>, <Полный> в нижней части панели. Клавиша <Сброс> снимает все флаги атрибутов доступа. Объект с такими атрибутами становится запрещенным, т.е. недоступным для ВСЕХ программ и процессов, включая и системные. Клавиша <Чтение> устанавливает для выбранного объекта «файл» атрибуты R – открыть для чтения, V – видимость и X – запуск программ. Для объекта «папка» добавляется атрибут G – переход в данную папку и S – наследование. Клавиша <Полный> включает все атрибуты для полного доступа. При работе в ОС Windows может случиться такая ситуация, что объект с набором атрибутов «Чтение» не будет открываться некоторыми программами. Это происходит потому, что многие программы (например большинство приложений Microsoft Office) по умолчанию открывают файл на чтение/запись. В этом случае придется добавить атрибут O – запись, который имитирует разрешение на запись при открытии файла, но не позволяет модифицировать файл. Для сохранения изменений ПРД выделенного объекта, нажмите кнопку «Запись» или клавишу <F2>. Более подробно действие атрибутов доступа и их комбинаций описано в документе «Руководство администратора».

По умолчанию все сетевые ресурсы обычному пользователю запрещены. Для разрешения доступа нужно явно указать полное сетевое имя ресурса. Это относится и к сетевым принтерам, или очередям печати. Если правила доступа к сетевым ресурсам

11443195.4012-019 97 02

определяются администратором домена (сервера), то можно задать универсальный сетевой ресурс. Для этого в список нужно включить объект \\ (ввести с клавиатуры), установить ему полный доступ и наследование на все подкаталоги.

ВНИМАНИЕ!

При задании параметров доступа к сетевым ресурсам, необходимо указывать полное сетевое имя ресурса, например: \\SERVER1\VOL2\DOC1\.

При описании правил доступа к съемному устройству (USB флэш-диску, USB Zip-диску) необходимо, чтобы это устройство было подключено к компьютеру. Нажмите кнопку <Новые>, выберите «Съемный диск» в списке, установите ему ПРД и сохраните изменения кнопкой «Запись» или клавишей <F2>. В дальнейшем при работе пользователя после подключения соответствующего устройства для него будут действовать установленные ПРД.

ВНИМАНИЕ! Процедура описания правил доступа к съемным дискам (USB флэш, Zip, floppy, сменные HDD) выполняется корректно только в том случае, когда сменное устройство подключено к компьютеру ДО запуска программы ACED32.EXE и остается подключенным до завершения процедуры сохранения базы данных пользователей. Только в таком варианте редактор ПРД может точно определить соответствие логического диска, под которым съемное устройство отображается в GUI и физического устройства, например Device\Harddisk1\, к которому обращаются запросы уровня ядра операционной системы.

При этом необходимо, чтобы USB устройство предварительно было включено в список разрешенных устройств на данном компьютере. Как выполняется эта операция описано в пункте 6.15 данного руководства. По умолчанию разрешен доступ ко всем USB-устройствам, т.е. в список объектов включена запись «USB, Vid=*, Pid=*, Sn=*, -, Allowed all USB devices!».

Еще один важный момент – регулирование доступа к стационарным устройствам, которые входят в состав компьютера. В список объектов можно включить такие устройства, как Com1, Com2, LPT1. Действует следующее правило, в отличие от дисковых ресурсов, - если устройство включено в список ПРД, то доступ к нему ЗАПРЕЩЕН, независимо от атрибутов доступа. Сделано это из необходимости поддерживать единый формат записи об объекте доступа, а реально установить режим «только чтение», или «только запись» для Com/Lpt порта весьма затруднительно.

Для выхода из режима редактирования нажмите кнопку «Заккрыть» или клавишу <Esc>.

Сообщения, выдаваемые программой при установке дискреционных ПРД, и порядок действий по ним:

Сообщение	Причина	Порядок действий
«Сохранить изменения для объекта (указывается имя_объекта) доступа?»	После изменения ПРД объекта не сохранены изменения	«Да» - сохранить изменения «Нет» - не сохранять изменения.

6.10.2 Установка доступа к объектам с использованием мандатного метода контроля ПРД.

Если в файле accord.ini установлен параметр MandatoryAccess=Yes то включается мандатный механизм задания и контроля ПРД. Этот параметр можно изменить с помощью программы ACSETUP.EXE (см. документ «Руководство по установке»).

В главном окне программы (Рис. 2) появляется кнопка "Уровень доступа" на панели инструментов и пункт "Уровень доступа" в меню "Команды". С помощью этой команды можно установить, или изменить уровень доступа пользователя (Рис. 20).

11443195.4012-019 97 02

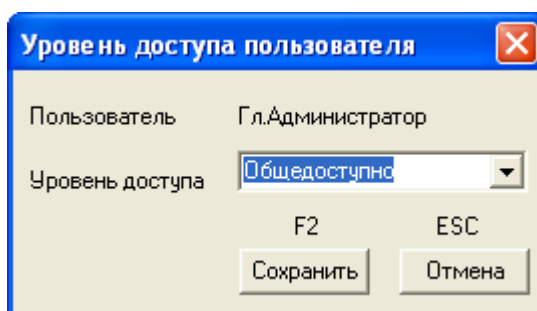


Рис. 20. Установка уровня доступа пользователя.

Мандатный механизм доступа реализуется по следующему правилу: если уровень доступа пользователя (субъекта) выше или равен метке доступа каталога, файла, сетевого ресурса (объекта) то доступ к объекту предоставляется данному субъекту. Если при этом установлены дискреционные ПРД, то операции, которые пользователь может выполнять с разрешенным объектом, определяются этими ПРД.

Для присвоения объектам меток доступа нажмите кнопку на панели инструментов с изображением дерева каталогов, или выберите пункт «Мандатный доступ» в меню "Команды". Выводится окно со списком объектов (Рис. 21).

По умолчанию всем объектам присваивается самый низкий уровень – общедоступно. Для изменения метки доступа установите курсор на нужную строку и нажмите Enter, или мышью кнопку «Редактировать». Откроется окно, в котором для объекта можно изменить только два параметра – уровень доступа и наследование прав доступа. Уровень доступа меняется нажатием мышью на кнопку в строке «Уровень доступа» и выбором значения из списка.

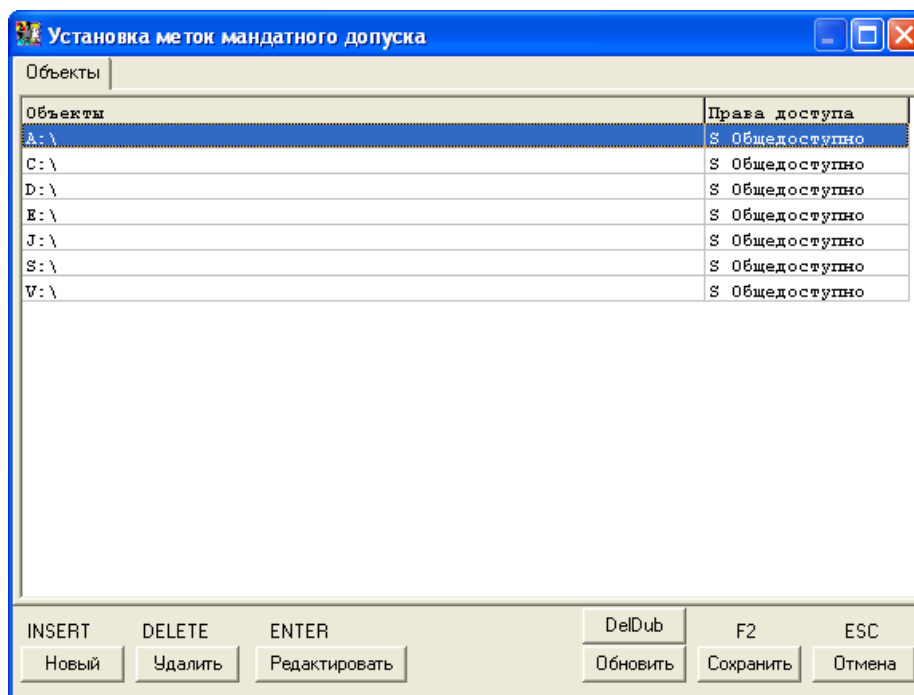


Рис. 21. Установка меток доступа объектов при использовании мандатных ПРД.

Если необходимый Вам объект отсутствует в списке (Рис. 21), нажмите кнопку «Новый» или клавишу <Insert>. На экран выводится расширенное окно «Атрибуты доступа к объектам» (Рис. 22.). Справа в этом окне отображен список всех объектов. Введите в поле «Имя объекта» имя объекта и установите для него необходимые атрибуты. С помощью мыши также можно выбрать объект, щелкнув левой кнопкой мыши на имени объекта, тогда в поле «Имя объекта» отобразится имя выделенного объекта, а в поле «Тип объекта» - его тип (каталог, файл, реестр). В правом нижнем секторе окна доступна функция установке

11443195.4012-019 97 02

меток доступа объекта. Установите указатель мыши на стрелку в правой части строки "Уровень доступа" и нажмите левую кнопку мыши. Появится список, из которого можно выбрать значение метки доступа выбранного объекта. Для сохранения изменений ПРД выделенного объекта, нажмите кнопку «Запись» или клавишу <F2>. Объект, которому не присвоена метка доступа считается недоступным для всех пользователей, кроме администраторов. В этом списке можно создавать записи, которые во время работы системы защиты будут определять переменную среды окружения для процессов с определенным уровнем доступа, например `_SET TEMP=C:\TEMP_1 [Конфиденциально]`. В этом случае процесс будет создавать временные файлы именно в том каталоге, который указал администратор. Единственное ограничение – каталог с заданным именем должен существовать на жестком диске.

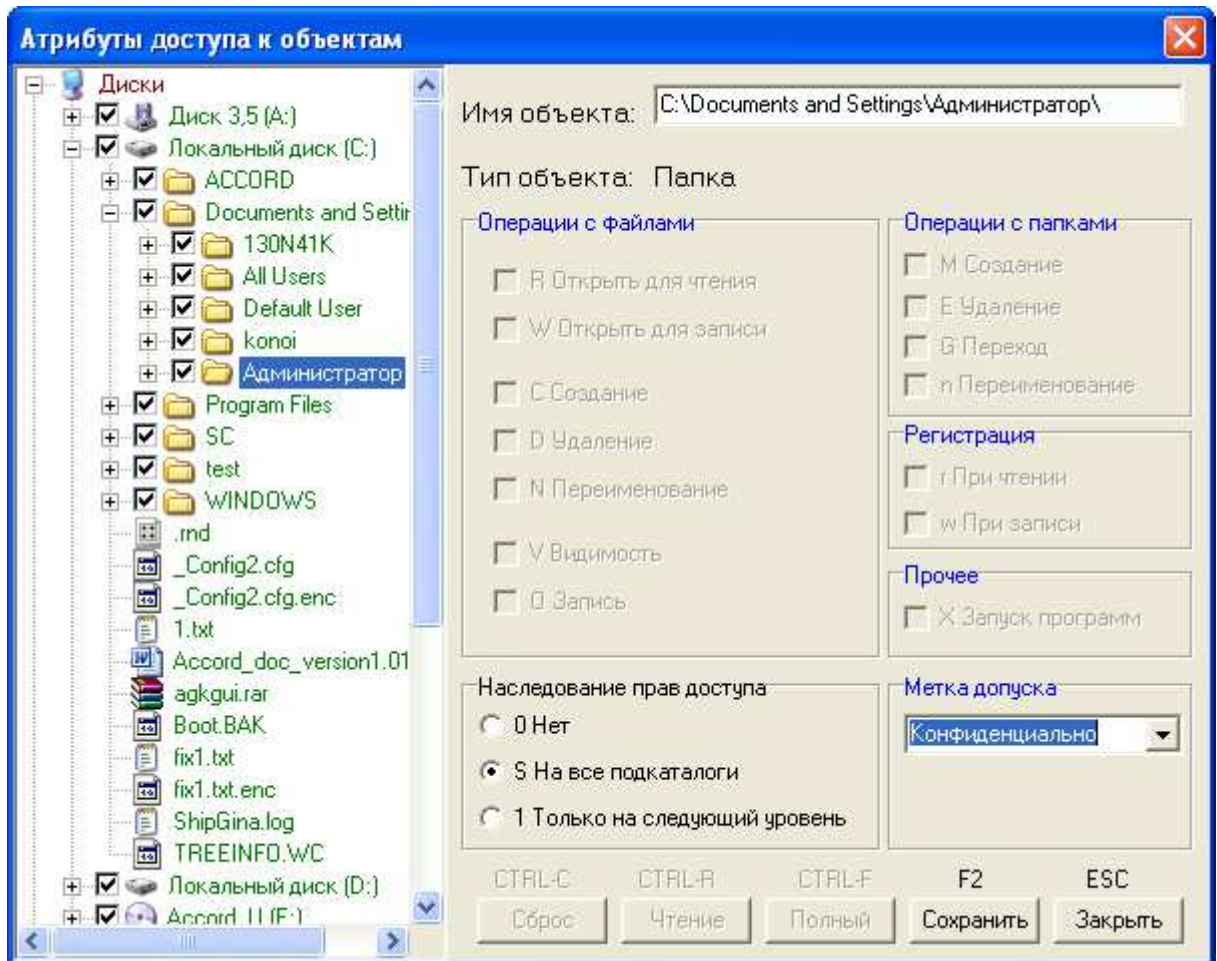


Рис. 22. Определение нового объекта и выбор его метки доступа.

В мандатном механизме доступа СЗИ "Аккорд-NT/2000" реализована весьма важная с точки зрения безопасности и создания ИПС (изолированной программной среды) функция – это мандатный доступ к объектам со стороны такого субъекта, как процесс (задача), который загружен в оперативную память СВТ. Параметр `CheckProcess=Yes` в файле `accord.ini` включает механизм мандатного доступа для процессов. Этот параметр можно изменить с помощью программы `ACSETUP.EXE` (см. документ "Руководство по установке"). В окне описания прав доступа пользователя к ресурсам СВТ кроме закладки "Объекты", появляется закладка "Процессы". Если щелкнуть по ней левой кнопкой мыши, то на экран выводится список процессов (Рис. 23).

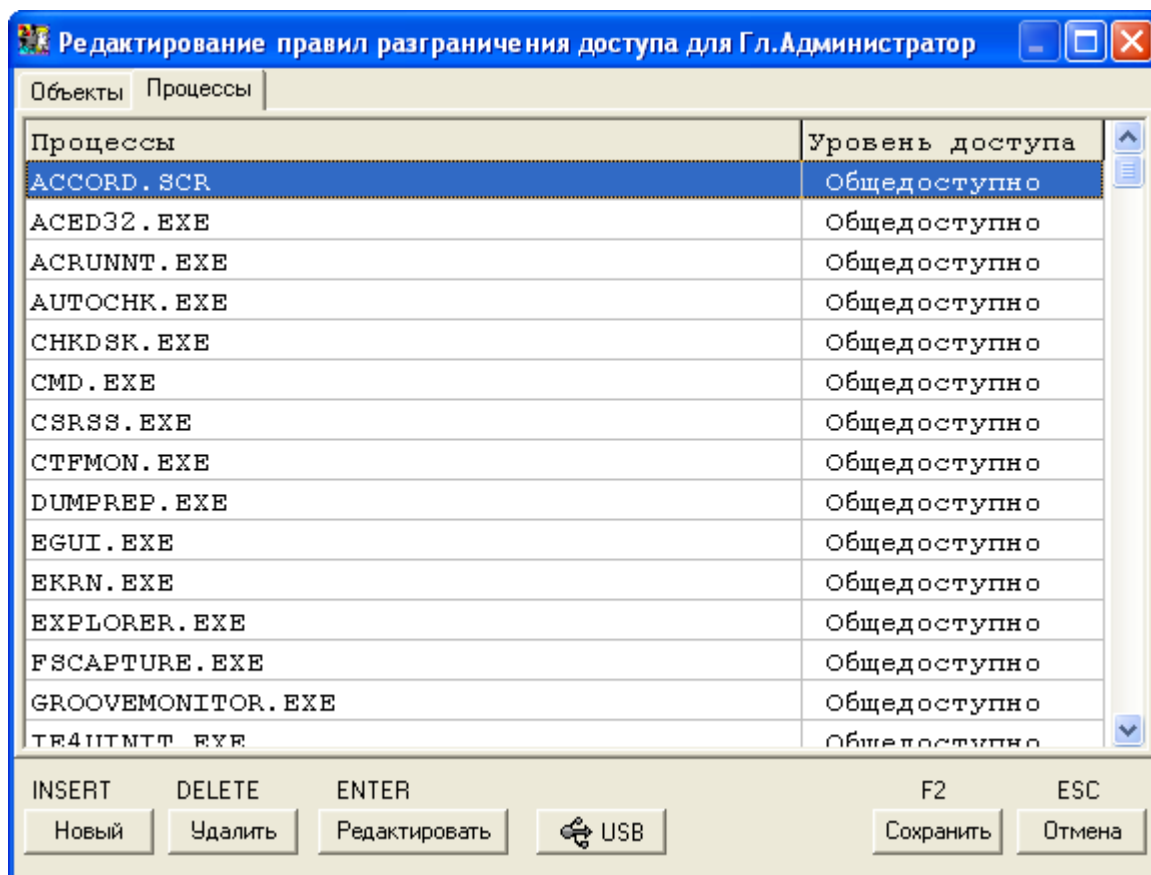


Рис. 23. Установка атрибутов мандатного доступа для процессов.

При первом запуске программы ACED32.EXE с включенной дисциплиной мандатного доступа в список процессов заносятся все процессы, которые в данный момент находятся в оперативной памяти и им устанавливается уровень доступа "Общедоступный", т.е. самый низкий. Если необходимый Вам объект отсутствует в списке (Рис. 23), нажмите кнопку «Новый» или клавишу <Insert>. На экран выводится окно установки уровня доступа (Рис. 24). Имя процесса вводится без указания пути, т.к. это процесс в памяти, но с расширением. Уровень доступа выбирается из списка. Для сохранения изменений ПРД выделенного объекта, нажмите кнопку «ОК». Для изменения уровня доступа процесса в разделе «Процессы» выберите строку с нужным именем и нажмите кнопку «Редактировать» или клавишу <Enter>.

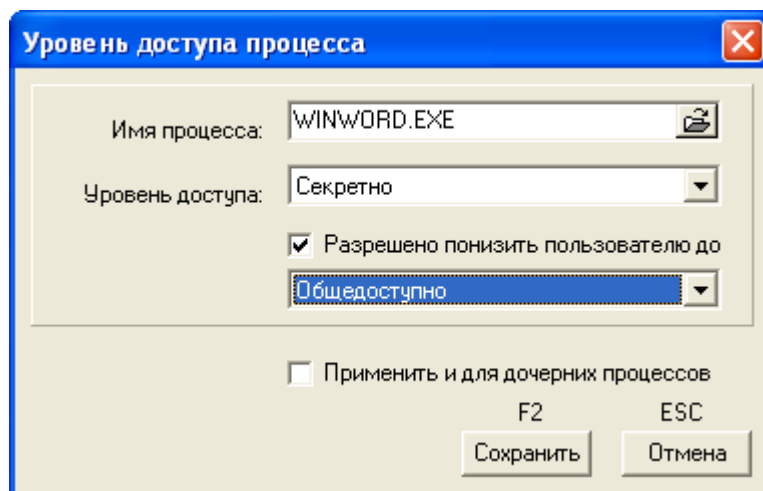


Рис. 24. Установка уровня доступа процесса.

11443195.4012-019 97 02

Администратор может для некоторых процессов установить флаг «Разрешено понизить пользователю». Если этот флаг установлен, то при старте такого процесса выводится окно выбора текущего уровня процесса (конечно при этом уровень доступа можно выбирать только с понижением). При запуске процесса с «динамическим» уровнем подключается и соответствующая переменная среды. Это дает возможность пользователю в одном сеансе работать с документами разных грифов секретности с помощью одной программы, того же Winword, например, но четко соблюдать **правило запрета на «понижение» метки конфиденциальности документа**, т.к. процессу в системе мандатного контроля запрещается запись в любой ресурс с меньшей по уровню меткой доступа.

На момент старта редактора ACED32.EXE некоторые процессы уже завершают свою работу, поэтому более корректно выполнять формирование списка процессов следующим образом:

- установить в программе настройки комплекса «Аккорд» дополнительную опцию «Мягкий режим»;
- некоторое время предоставить пользователю возможность работать на компьютере в этом режиме, но обязательно с загруженным монитором разграничения доступа;
- с помощью программы AcProc.exe («Создание списка процессов») выбрать из журналов используемые при работе программы и сохранить в файле <Имя_пользователя>.PRD;
- импортировать в редакторе из файла .PRD набор исполняемых файлов;
- выключить в настройках комплекса «Мягкий режим».

Список процессов с установленными уровнями доступа в наиболее полном и наглядном виде отражает концепцию изолированной программной среды, т.к. доступ к соответствующим ресурсам получают только процессы из этого списка. При этом процесс не имеет доступа на запись информации в объекты нижестоящего уровня.

В реализации процедуры разграничения доступа СЗИ "Аккорд-NT/2000" исполняемый файл может выступать и как объект, и как субъект. Файл на жестком диске – это объект, которому установлена метка доступа и запустить файл на исполнение может пользователь с соответствующим уровнем доступа. После запуска процесса он уже как субъект имеет установленный уровень доступа к объектам. В такой системе атрибутов возможна реализация такой политики безопасности, когда обработка объектов с определенной меткой доступа возможна только с помощью процессов соответствующего уровня доступа.

Управление потоками информации осуществляется по следующему алгоритму:

- конкретному процессу запись информации разрешена только в том ресурсе, чья метка доступа **равна** уровню доступа процесса;
- все ресурсы с более низкой меткой доступа открыты для этого процесса только на чтение и запуск программ (атрибуты RVOX).

Таким образом, пользователь не может понизить уровень секретности документа, т.е. скопировать секретный документ в несекретную папку с помощью «секретного» процесса, а для всех процессов, которые не имеют соответствующего уровня, объект «секретно» не доступен.

В том случае, когда администратор не имеет возможности собрать полный список процессов, но точно знает, какая программа будет работать со сведениями ограниченного доступа, то он может в список добавить процесс «*» (звездочка). При проверки грифа, если процесс явно не прописан в списке, то ему будет присвоен тот уровень что установлен для объекта «*». В общем случае это будет самый низкий гриф.

6.11 Контроль целостности файлов.

Комплекс СЗИ НСД "Аккорд-NT/2000" v.3.0 позволяет контролировать целостность файлов по индивидуальному списку, созданному администратором для каждого пользователя (или

11443195.4012-019 97 02

группы). Предусмотрены два режима контроля: **"статический"** - это контроль целостности любых файлов, расположенных на жестком диске в момент начала сеанса пользователя и обновление контрольных сумм при завершении сеанса работы пользователя; **"динамический"** - это контроль исполняемых модулей перед их загрузкой в оперативную память СВТ.

6.11.1 "Статический" контроль целостности файлов

Для создания списка контролируемых файлов нажмите кнопку, расположенную справа в поле «Контроль целостности», в главном окне (см. Рис. 2). На экран выводится окно «Контроль целостности файлов для (указывается имя_пользователя)», показанный на Рис. 25.

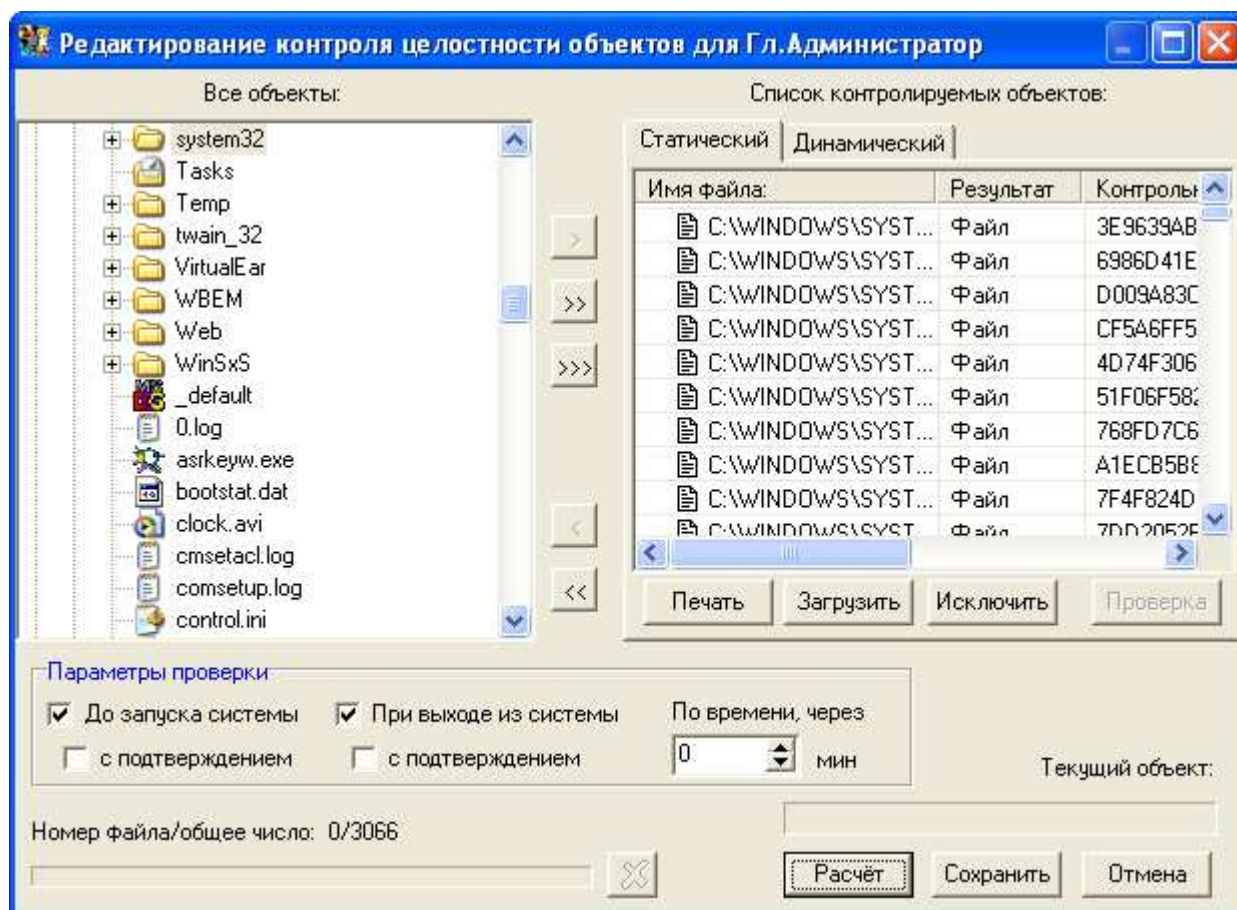


Рис. 25. Окно контроля целостности файлов.

На первом этапе необходимо сформировать список файлов, для которых будет рассчитана контрольная сумма (КС). Возможен выбор отдельного файла, или всех файлов из выбранного каталога. В левой половине окна «Все папки» выберите нужный файл с помощью мыши (левая кнопка). Выбранный файл переместится в правую часть окна в «Список контролируемых файлов» при двойном щелчке мыши или при нажатии на кнопку «>>».

В разделе «Все папки» выберите нужный каталог с помощью мыши (левая кнопка). При нажатии на кнопку «>>>», все файлы данного каталога переместятся в «Список контролируемых файлов». Щелчок правой кнопкой мыши на имени выделенного каталога вызывает всплывающее меню с пунктом «Добавить по фильтру». При выборе данного пункта выводится окно (Рис. 26), предлагающее ввести необходимый фильтр. При нажатии кнопки «ОК» или клавиши <Enter>, все файлы выбранного каталога, удовлетворяющие заданному фильтру, переместятся в «Список контролируемых файлов». Клавиша <Esc> отменяет операцию «Добавить по фильтру».

11443195.4012-019 97 02

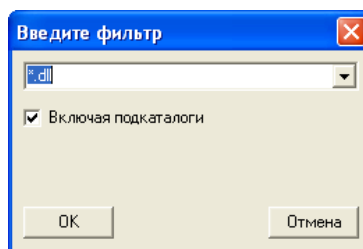


Рис. 26. Задание фильтра для выбора контролируемых файлов.

Очистить «Список контролируемых файлов» можно нажав на кнопку «<<<». Удалить файл из «Списка контролируемых файлов» можно с помощью на кнопки «<» после выделения, или двойным щелчком мыши на выделенном файле.

На втором этапе осуществляется установка режимов контроля целостности.

Выбор режимов осуществляется установкой флагов в нижней панели окна. Возможны следующие варианты:

- *До запуска системы* - контроль целостности до запуска операционной системы.
- *С подтверждением* - запрос подтверждения контроля целостности до запуска ОС (пользователь может отказаться от выполнения процедуры контроля).
- *После завершения задачи* - обновление КС после завершения сеанса работы пользователя (при выходе из системы).
- *С подтверждением* - запрос подтверждения обновления КС после завершения сеанса работы.

На третьем этапе производится расчет КС выбранных файлов при нажатии кнопки «Расчет». В процессе расчета запрашивается идентификатор данного пользователя. В алгоритме расчета используется секретный ключ, записанный в идентификатор при регистрации пользователя. Тем самым исключается возможность подделки результирующей КС при несанкционированном изменении файлов. Расчет КС производится только при установленных режимах контроля целостности (должен быть установлен хотя бы один флаг). При попытке рассчитать контрольную сумму без установки режимов выводится сообщение об ошибке (Рис. 27.).

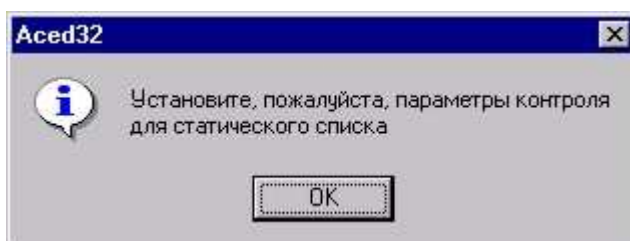


Рис. 27. Предупреждение о необходимости установки режимов контроля.

Выход из процедуры контроля с сохранением результатов расчета - нажатие кнопки «Запись» или клавиши <F2>, без сохранения – кнопки «Отмена» или клавиши <Esc>.

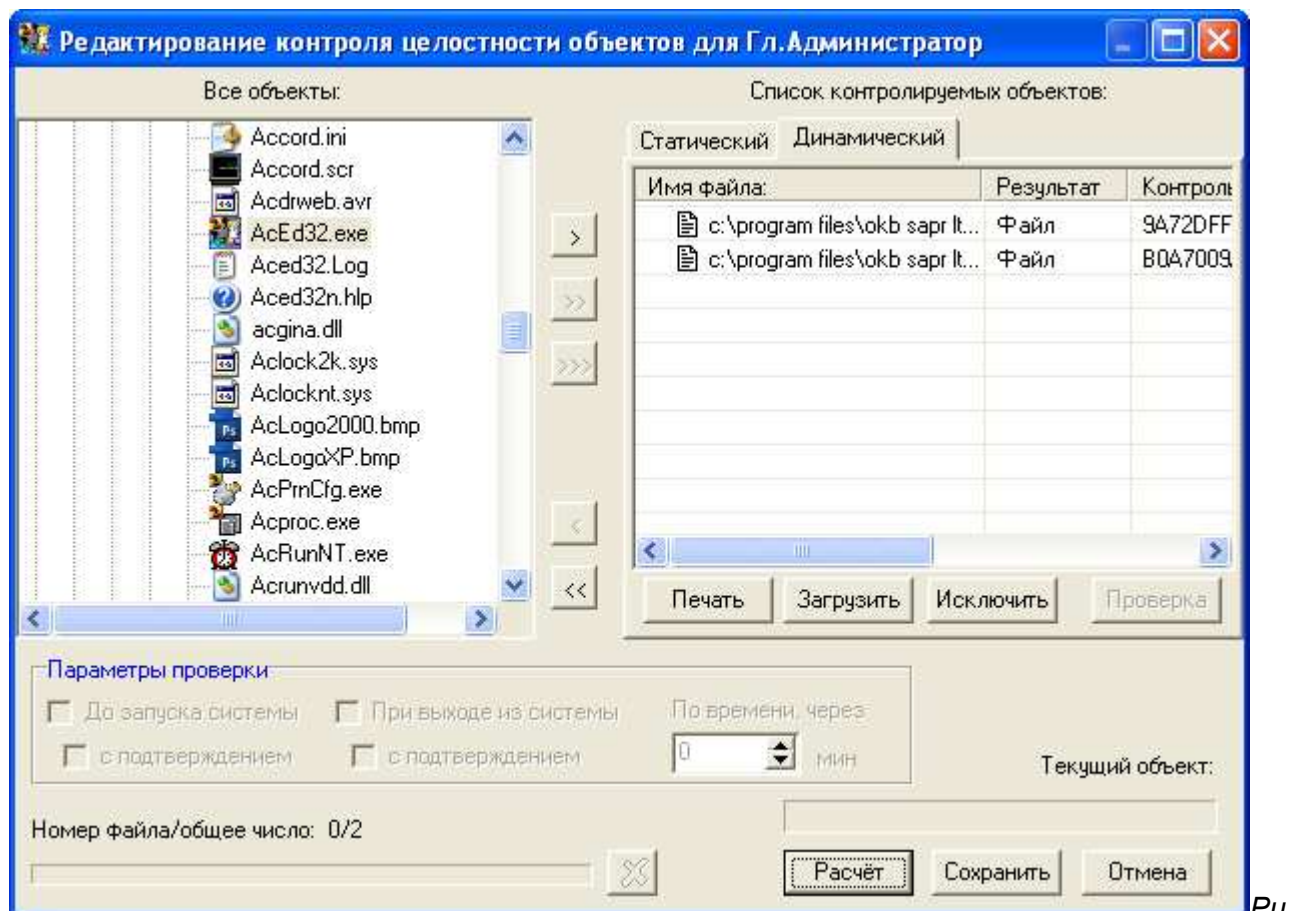
6.11.2 "Динамический" контроль целостности файлов

Эта операция выполняется при **каждом** запуске процесса (исполняемого модуля). Для создания списка контролируемых процессов нажмите кнопку, расположенную справа в поле «Контроль целостности», в главном окне (Рис. 2). На экран выводится окно

«Контроль целостности файлов для (указывается имя_пользователя)».

11443195.4012-019 97 02

Щелкните мышью на закладке "Динамический" и откроется список файлов для динамического контроля, показанный на Рис. 28.



С этим списком можно работать так же, как и со "статическим", но не требуется задания параметров контроля.

Список контролируемых объектов можно задавать как для отдельного пользователя, так и для группы. В этом случае контроль будет выполняться при начале сеанса любого пользователя из группы.

Как для статического, так и для динамического режима контроля возможна загрузка списка контролируемых файлов из специального файла, подготовленного с помощью программы AcProc.EXE (См. документ «Подсистема регистрации. Программа работы с журналами регистрации 11443195.4012-019 99 02») на основе анализа журналов регистрации событий. Список файлов для контроля имеет расширение HSH. Для выполнения этой операции щелкните мышкой по кнопке <Загрузить>, откроется окно выбора файла (Рис.29).

11443195.4012-019 97 02



Рис.29. Выбор файла со списком контролируемых объектов.

Отметьте необходимый файл и нажмите кнопку <Открыть>. Файлы будут добавлены в соответствующий список контроля (Рис.30).

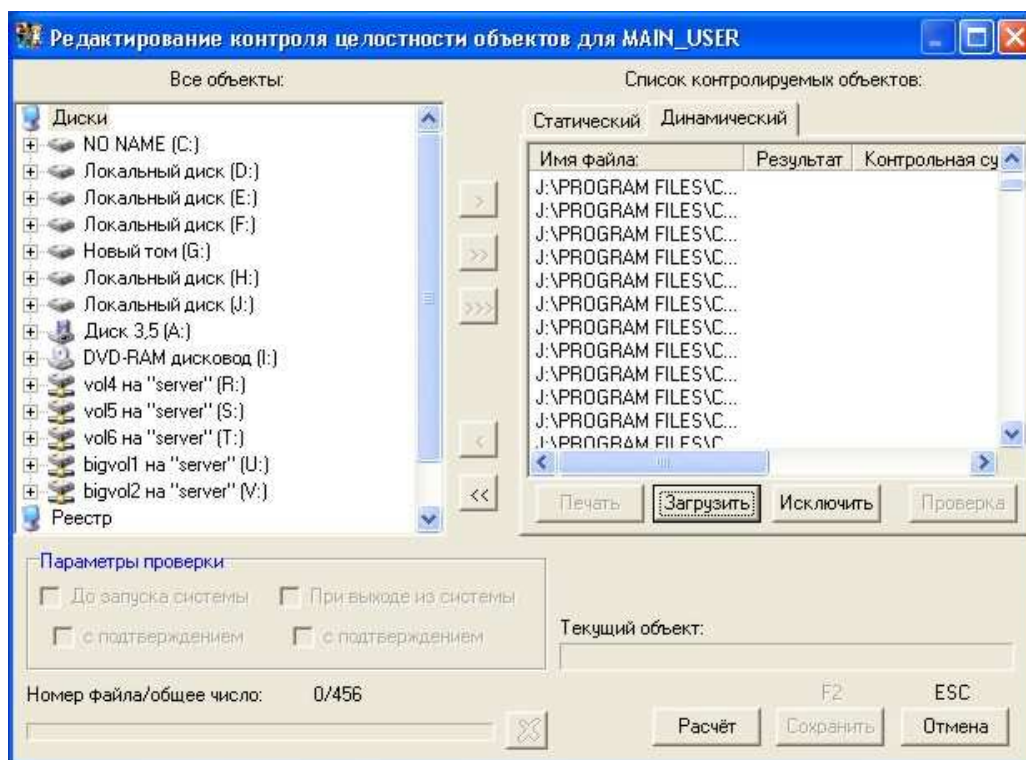


Рис. 30. Загрузка файлов в список контроля.

После этого необходимо выполнить расчет контрольных сумм файлов. После выполнения расчета список файлов с контрольными суммами можно сохранить (становится доступной кнопка <Печать>, и файл можно распечатать на принтере, или записать на диск в виде файла с расширением .HSH). Этот файл можно использовать на других защищаемых СВТ с идентичным составом прикладного ПО, чтобы не вводить каждый раз список вручную. Не забудьте только выполнить пересчет контрольных сумм для конкретного пользователя или группы.

Если список контролируемых объектов не пуст, то становится доступной кнопка <Исключить>. Эта команда позволяет исключить из списка контролируемых объектов набор файлов, предварительно сохраненный в файле .HSH. Такая функция может быть полезной, в случае, когда изменился состав контролируемого ПО в сторону уменьшения числа файлов

11443195.4012-019 97 02

на жестком диске и нужно эти изменения выполнить на нескольких компьютерах. Порядок действий может быть таков:

- на одном компьютере сохраняем резервную копию списка файлов;
- очищаем список;
- включаем в список только те файлы, которые предполагается исключить из процедуры контроля и сохраняем этот список в отдельном файле;
- восстанавливаем полный список с резервной копии и выполняем команду <Исключить>, используя второй сохраненный файл в качестве шаблона;
- скопировав на носитель файл №2, используем его для исключения файлов из списка контроля на других компьютерах.

6.12 Установка опций настройки

В списке пользователей с помощью мыши или клавиатуры выделите пользователя. В поле «Опции» окна «Параметры пользователя» (Рис. 2) отображается информация о том, какие дополнительные опции настройки системы «Аккорд» установлены у активного (выделенного) пользователя. Выберите режим редактирования, нажав на кнопку, расположенную справа в поле «Опции», или клавишу <Enter>. На экран выводится окно «Опции» (Рис. 31). По умолчанию, установлена лишь одна опция «Показывать скрытые файлы».

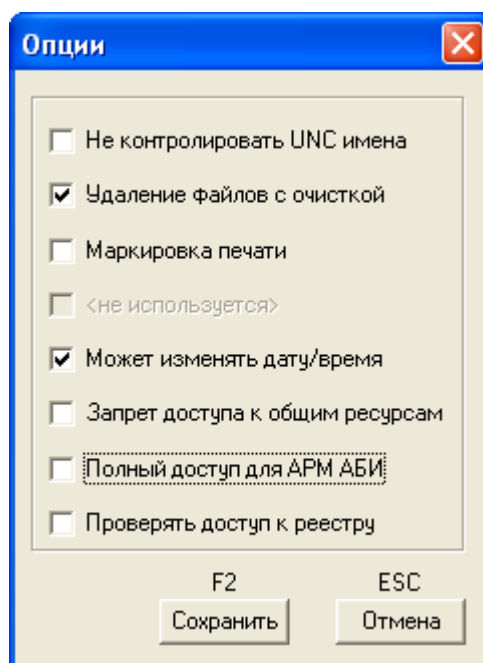


Рис. 31. Опции настройки.

Дополнительные опции работы пользователя в СЗИ «Аккорд-NT/2000»:

- *Не контролировать UNC имена* – контроль уровня секретности информации, помещенной в буфер обмена при использовании мандатного доступа процессов;
- *удаление файлов с очисткой* – в процессе удаления файлов физическое место файла на жестком диске прописывается последовательностью случайных чисел;
- *активировать контроль печати* – включить для данного пользователя процедуру контроля вывода на печать и маркировки документов. Формат и состав параметров, выводимых на печатную копию выполняется в программе «Настройка комплекса Аккорд-NT»;
- *показывать скрытые файлы* - показывать ли файлы с атрибутом Hidden. По умолчанию параметр установлен, т.к. ОС использует при работе файлы с таким атрибутом;
- *может изменять дату/время* - разрешено ли пользователю изменять дату/время;

11443195.4012-019 97 02

- *запрет доступа к общим ресурсам* – установка этого параметра запрещает доступ из сети к ресурсам данного компьютера, даже если они описаны в ОС как общие ресурсы;
- *полный доступ для АРМ АБИ* - при использовании подсистемы распределенного аудита и управления разрешать ли полный доступ к файлам и папкам данного компьютера администратору безопасности информации;
- *проверять доступ к реестру* - использовать ли разграничение доступа к разделам и ключам системного реестра.

Остальные флаги в разделе «Опции настройки» не используются (зарезервированы для дальнейших разработок). Для выхода из режима редактирования с сохранением, нажмите кнопку «Запись» или клавишу <F2>, без сохранения – «Отмена» или <Esc>.

6.13 Установка фиксированных сетевых имен ресурсов общего пользования

В составе комплекса СЗИ «Аккорд NT/2000» реализована дополнительная функция, существенная для функционирования защищенной СВТ в составе ЛВС. Это функция регламентирует процедуру выделения локальных ресурсов данного компьютера в общее пользование для остальных компьютеров локальной сети. Для вызова этой функции можно щелкнуть мышью на иконке с изображением «общего» ресурса на панели задач, или выбрать команду «Имена общих ресурсов» в меню <Команды>. Откроется окно, представленное на Рис. 32.

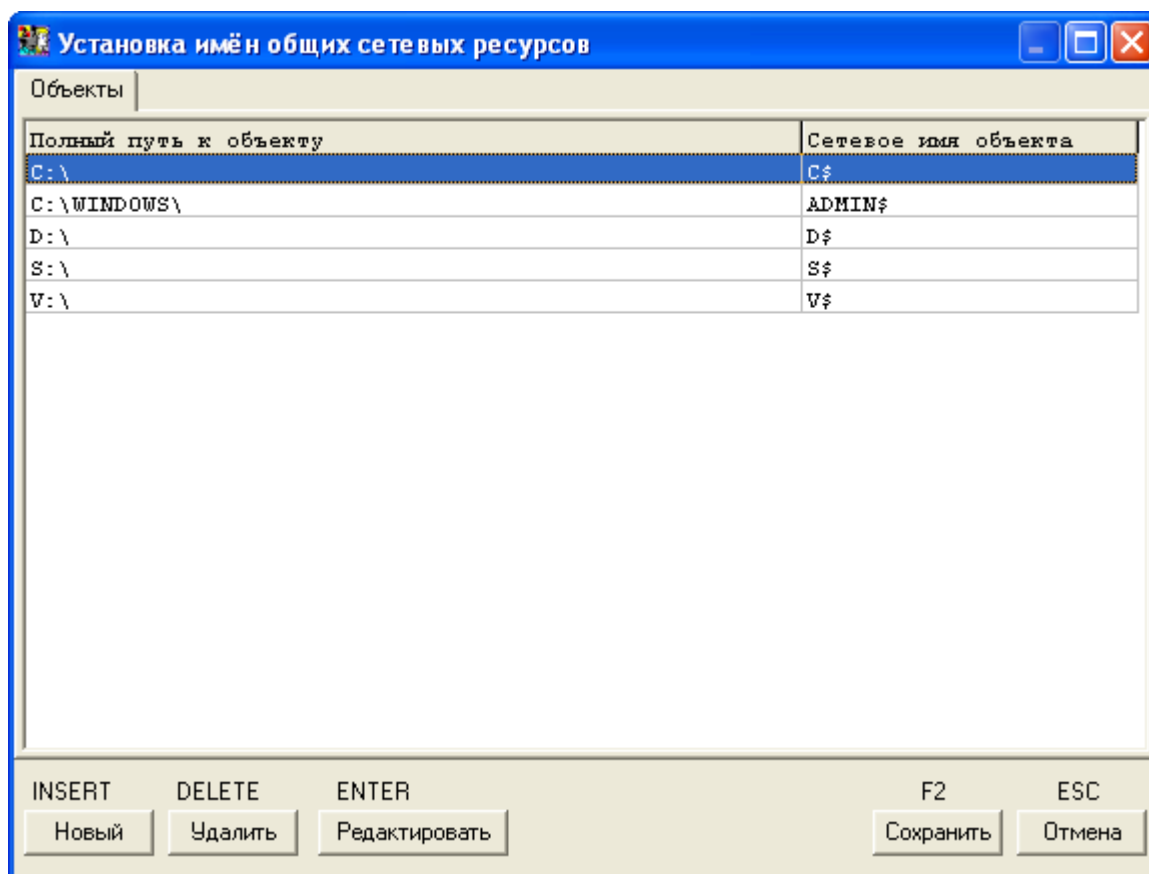


Рис. 32. Список ресурсов, выделяемых для общего доступа.

В этом списке можно описать ресурсы (с полным именем), которые находятся на жестком диске данного компьютера, и задать сетевое имя, под которым ресурс будет доступен другим пользователям в сети. Для изменения сетевого имени объекта нужно выделить соответствующую строку и нажать <Enter>, или щелкнуть мышью на кнопке

11443195.4012-019 97 02

«Редактировать». Для добавления ресурсов в список служит кнопка «Новый». Для чего предназначена данная функция? Во-первых, администратор полностью контролирует ресурсы, которые будут предоставлены для общего доступа, т.е. пользователь не сможет несанкционированно открыть доступ к конфиденциальной информации для других компьютеров в сети, а во-вторых, даже разрешенный ресурс предоставляется с фиксированным сетевым именем. Это важно, если в сети функционируют другие компьютеры с установленной СЗИ «Аккорд», и на этих компьютерах описан доступ к сетевым ресурсам. Поскольку этот доступ проверяется по полному сетевому пути, то администратор получает однозначное выполнение заданной политики безопасности.

6.14 Экспорт/импорт базы данных пользователей и правил разграничения доступа

В программе ACED32.EXE предусмотрены процедуры сохранения и загрузки базы данных пользователей и правил разграничения доступа.

6.14.1 Сохранение/загрузка базы данных пользователей

Для сохранения базы данных пользователей выберите команду «Сохранить как» в меню «Файл» в главном окне программы (см. Рис. 33). На экран выводится окно «Сохранить как» для выбора имени файла, показанное на Рис. 34.

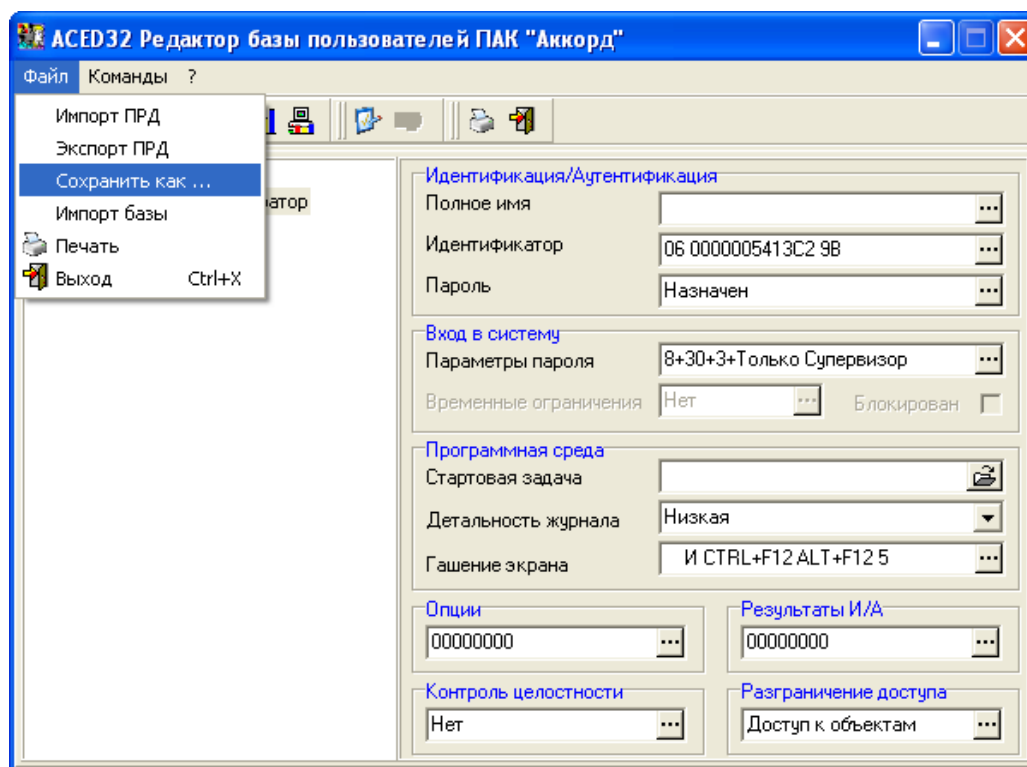


Рис. 33. Команды работы с базой данных пользователей.

11443195.4012-019 97 02

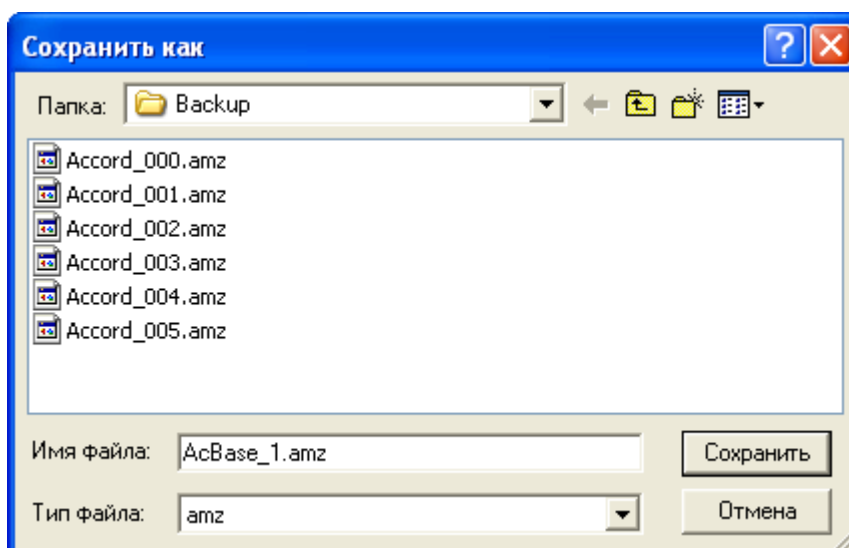


Рис. 34. Выбор имени файла для сохранения.

Расширение файла amz задается по умолчанию, и изменить его нельзя. После задания имени файла нажмите кнопку «Сохранить». Параметры пользователей запишутся в виде файла на жесткий диск. Этот файл можно скопировать на сменный носитель и хранить как средство восстановления данных.

Восстановить настройки пользователей можно, скопировав резервную базу в папку Accord.NT под именем accord.amz. Для синхронизации с контроллером АМДЗ и базой пользователей ОС достаточно после копирования запустить редактор ПРД и сделать любое изменение в настройках любого пользователя, например, изменить время срабатывания Screen Saver. При выходе из программы подтвердить сохранение изменений.

Для корректировки настроек пользователей, или просмотра базы данных в файле, отличном от accord.amz предназначена команда «Импорт базы» в меню «Файл». После вызова этой команды на экран выводится окно выбора имени файла (Рис.35.).

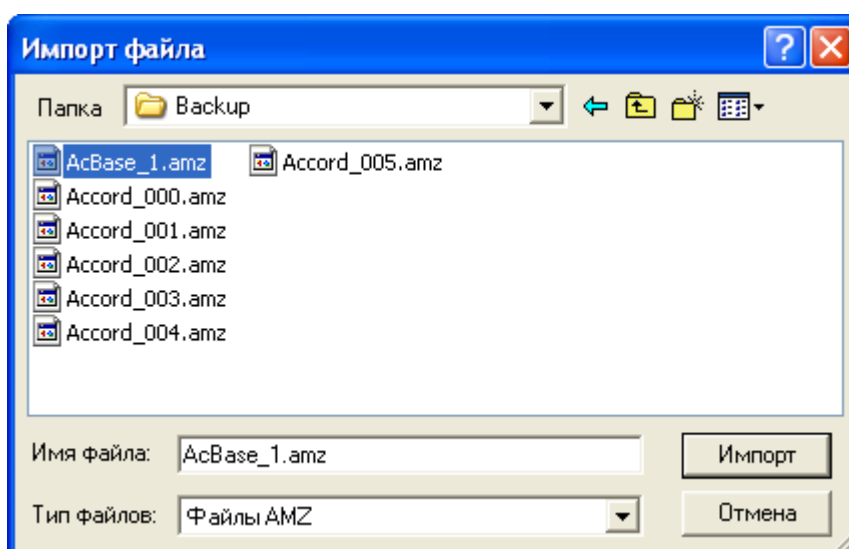


Рис.35. Выбор файла для импорта базы данных пользователей.

После ввода имени файла нажмите кнопку «Импорт».

Внимание! Изменения, которые внесены в импортированную базу, сохраняются по умолчанию в том же файле, из которого были импортированы. Такой режим работы с базой

11443195.4012-019 97 02

ПРД может быть полезен в том случае, когда администратору необходимо скорректировать настройки для удаленного компьютера, но подсистема удаленного аудита и управления не установлена. Администратор на своем компьютере выполняет импорт базы, вносит изменения, сохраняет настройки и отправляет полученный файл по электронной почте, или на дискете. После получения файла пользователь, выполняющий обязанности администратора удаленного компьютера, копирует его на жесткий диск и выполняет синхронизацию. При этом администратору удаленного компьютера достаточно самых простых, базовых знаний по настройке комплекса «Аккорд NT/2000». В этой технологии может возникнуть еще одна проблема, если пользователь зарегистрирован в базе данных .amz, но отсутствует в памяти контроллера АМДЗ. Если в настройках комплекса включена синхронизация с базой АМДЗ, то при старте редактора ПРД АсED32.EXE база первоначально считывается из контроллера, и пользователи, отсутствующие в контроллере не учитываются. Для выхода из такой ситуации предназначена программа Acsync.exe. Запуск этой программы с параметром /1 позволяет считать список пользователей из платы в файл accord.amz. Запустив программу с параметром /2, Вы скопируете данные из файла accord.amz в плату контроллера АМДЗ. После этого можно запускать редактор ПРД и выполнить синхронизацию со списком пользователей в ОС.

6.14.2 Экспорт/импорт правил разграничения доступа

Программа ACED32.EXE позволяет сохранять в отдельных файлах правила разграничения доступа (ПРД) пользователя. Для этого следует выбрать пользователя и команду «Экспорт ПРД» в меню «Файл». На экран выводится окно выбора параметров, которые предполагается сохранить (Рис.36.).

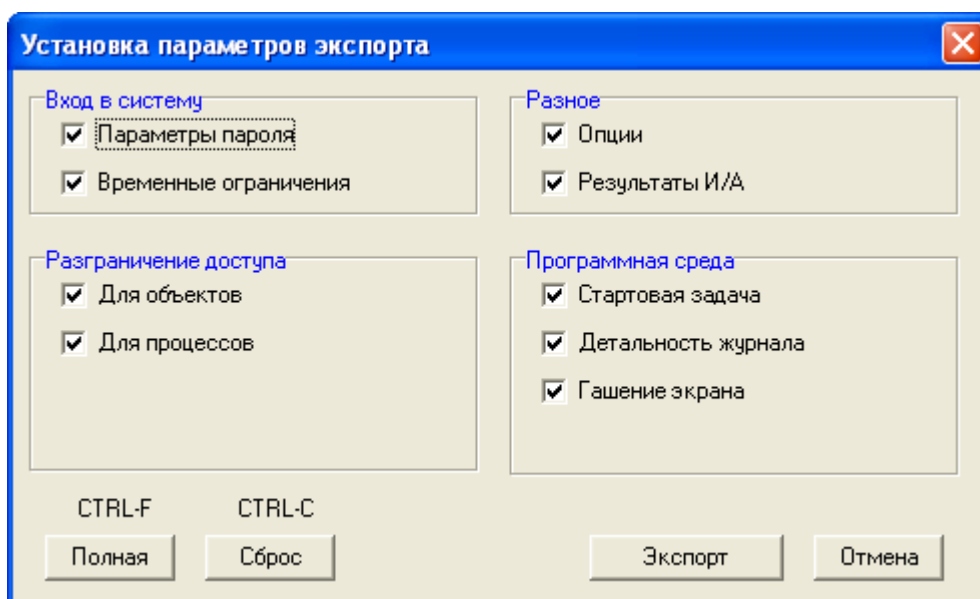


Рис.36. Выбор параметров ПРД для экспорта.

После выбора необходимого перечня экспортируемых параметров нажмите кнопку «Экспорт». Выводится окно ввода имени файла для сохранения (Рис.37.).

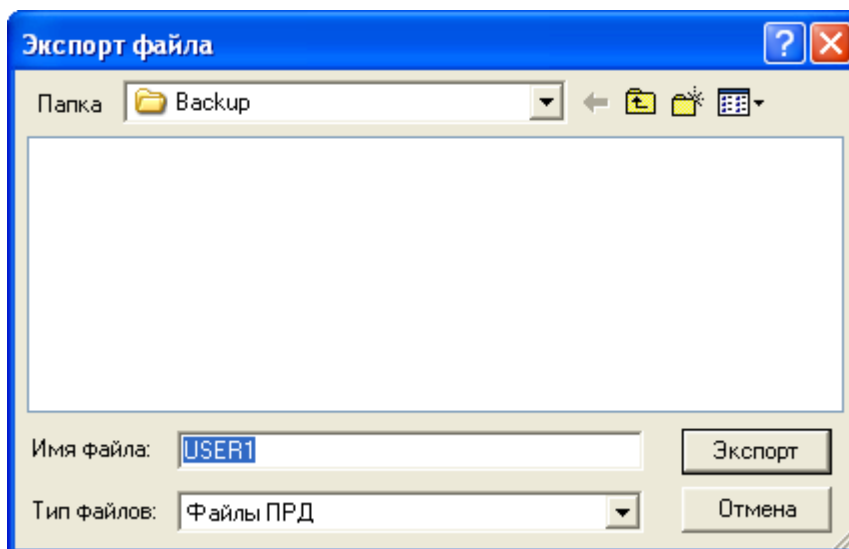


Рис.37. Выбор имени файла для экспорта ПРД.

Программа предлагает для сохранения имя файла, совпадающее с именем пользователя, но это не является обязательным условием, а сделано для удобства администратора безопасности. После ввода имени файла нажмите кнопку «Экспорт». Файл запишется на диск.

Для импорта ПРД из файла следует отметить пользователя и выбрать команду «Импорт ПРД» в меню «Файл». Выводится окно выбора файла для импорта (Рис.38.).

11443195.4012-019 97 02

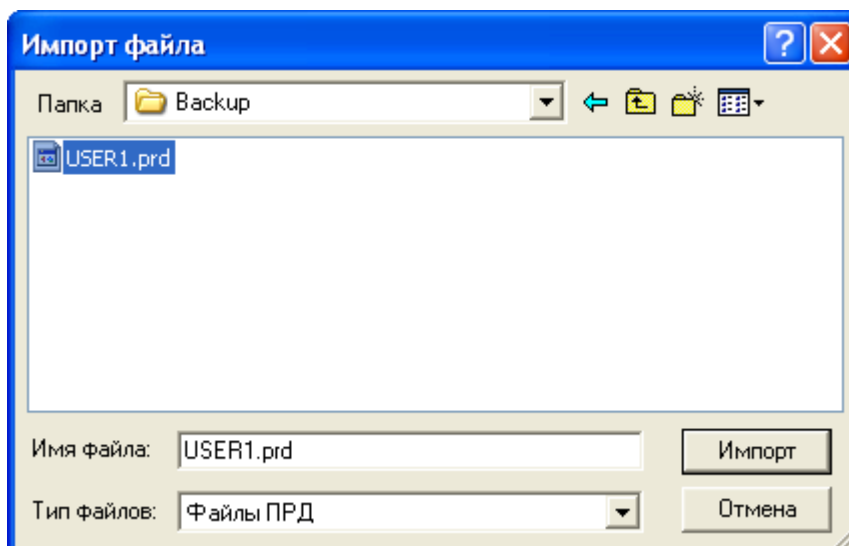


Рис.38. Выбор имени файла для импорта ПРД.

После ввода имени файла нажмите кнопку «Импорт». После этого на экран выводится окно выбора параметров, которые предполагается импортировать данному пользователю (Рис.39).

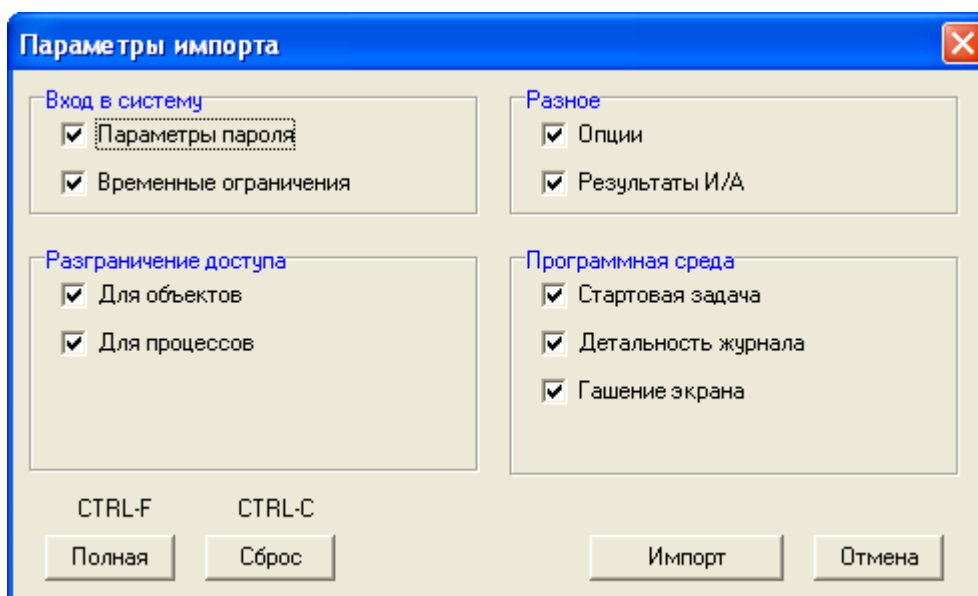


Рис.39. Выбор параметров для импорта.

Мышью следует выбрать параметры и нажать кнопку «Импорт». На экран выводится окно выбора процедуры включения ПРД в настройки пользователя (Рис.40).

11443195.4012-019 97 02

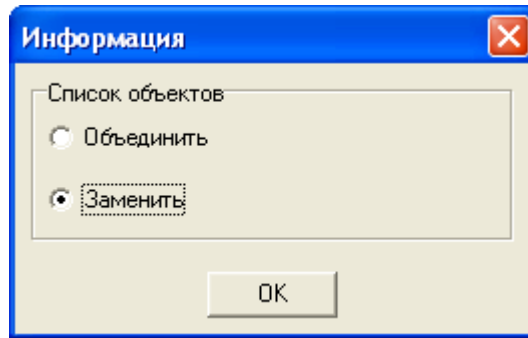


Рис.40. Выбор процедуры формирования нового списка ПРД.

Если выбран параметр «Объединить», то импортируемые ПРД добавляются в настройки пользователя. Если выбран параметр «Заменить», то настройки пользователя очищаются и записываются только новые ПРД из файла.

Аналогично выполняется экспорт/импорт меток мандатного доступа для объектов. Для этого нужно выбрать соответствующие пункты в меню «Команды».

В состав комплекса «Аккорд NT/2000» входят две программы, которые позволяют сформировать файл правил разграничения доступа (файл с расширением .prd) на основе записей в журнале регистрации событий. Программа LogToPRD.exe формирует список объектов, а программа AcProc.exe формирует список процессов. Подробно работа с этими программами описана в документе «Подсистема регистрации. Программа работы с журналами регистрации «LogView». Из полученных в результате работы программ файлов .prd можно импортировать правила доступа отдельному пользователю, или группе пользователей. Такая технология формирования ПРД, избавляет администратора безопасности от необходимости «вручную» вводить список объектов.

6.15 Формирование списка разрешенных USB устройств

Большинство современных компьютеров имеют в своем составе USB шину для работы со сменными устройствами. Программа-редактор ACED32 позволяет администратору безопасности сформировать список USB-устройств, с которыми разрешено работать данному пользователю. Поскольку в некоторых организациях сменные флэш-диски уже заменили привычные дискеты в качестве носителей, подлежащих учету, то такая возможность администрирования доступа становится актуальной. По умолчанию для обычных пользователей в список объектов уже включена запись «USB, Vid=*, Pid=*, Sn=*, -, Allowed all USB devices!». Это означает, что любое USB-устройство разрешено для доступа. Если администратора безопасности не устраивает такая ситуация, то ему необходимо эту строчку из списка объектов доступа удалить и назначить конкретные устройства, к которым доступ будет разрешен. Для выполнения данной операции нужно в окне редактирования правил доступа пользователя (Рис. 17) щелкнуть мышью по клавише <USB>. Открывается окно редактирования списка USB устройств (Рис 41). **ВНИМАНИЕ!** В этот список нужно добавить клавиатуру и мышь, подключенные по USB, для их нормальной работы.

11443195.4012-019 97 02

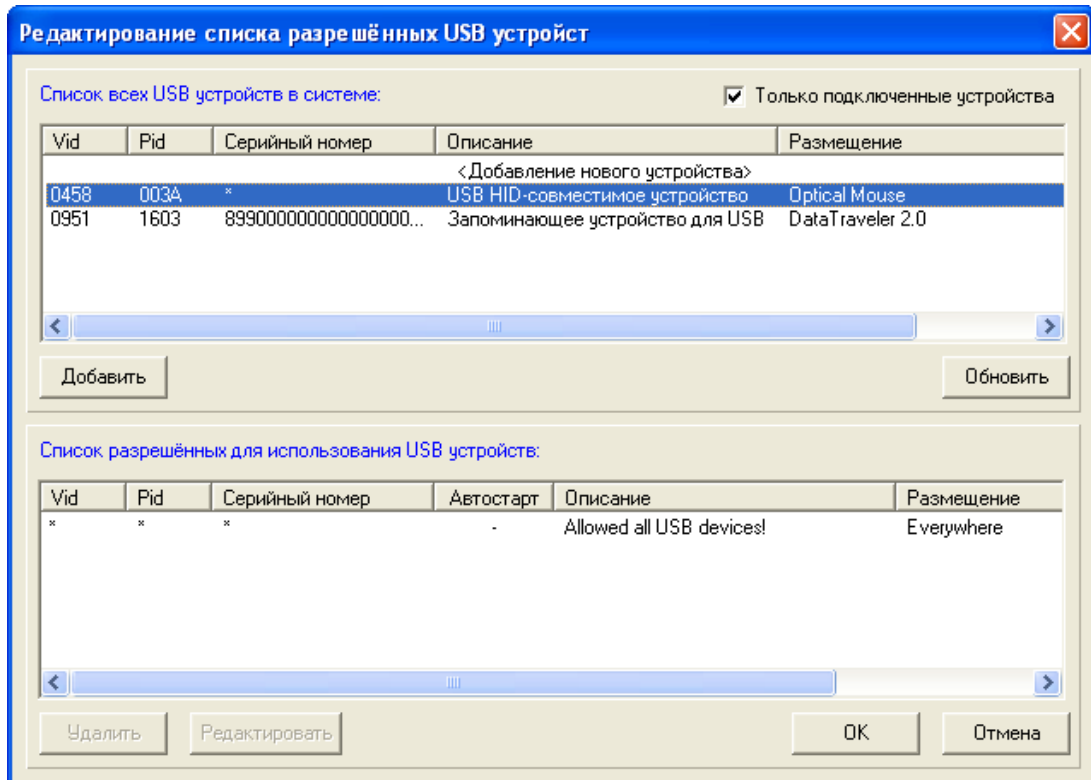


Рис. 41. Окно редактирования списка разрешенных USB устройств.

В верхней части окна по умолчанию включен флаг «Только подключенные устройства». В этом режиме в списке доступных устройств отображаются только те, которые в данный момент подключены к компьютеру. Если в списке нет устройства, щелкните мышью по кнопке «Обновить». По этой команде выполняется поиск подключенных USB устройств и они появляются в верхней половине окна в списке устройств. Установите курсор на то устройство, доступ к которому Вы хотите разрешить данному пользователю. Нажмите кнопку «Добавить» и USB устройство появится в нижней половине окна в списке разрешенных для использования (Рис. 42). Чтобы включить несколько устройств, нужно повторить операцию выбора и добавления устройств. Для завершения процедуры выбора нажмите кнопку «Ок» и выбранные устройства появятся в списке объектов (Рис. 17).

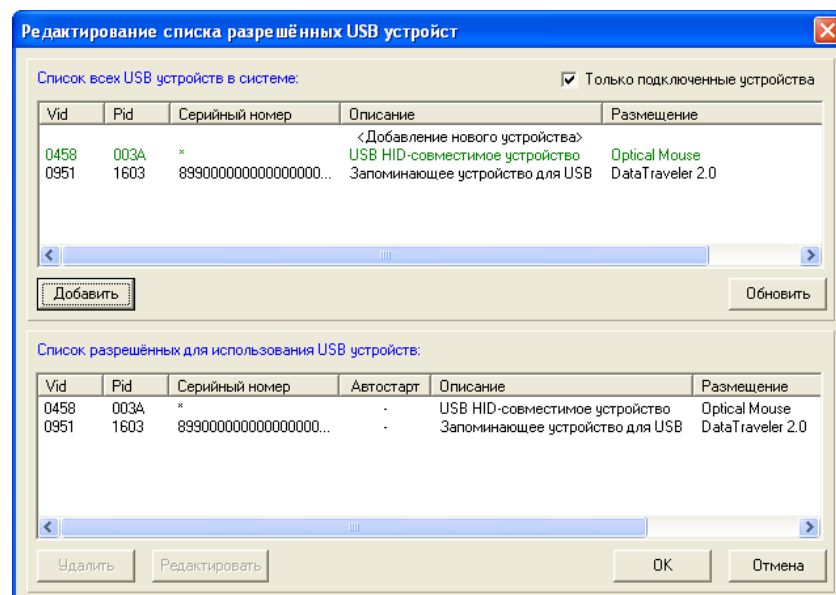


Рис. 42. USB устройство добавлено в список разрешенных.

11443195.4012-019 97 02

Можно использовать другой режим добавления устройств, когда снят флаг «Только подключенные устройства». В этом случае в списке выводятся идентификационные параметры USB устройств, которые подключены к компьютеру в данный момент и подключались ранее - эти сведения сохраняются операционной системой (Рис.43).

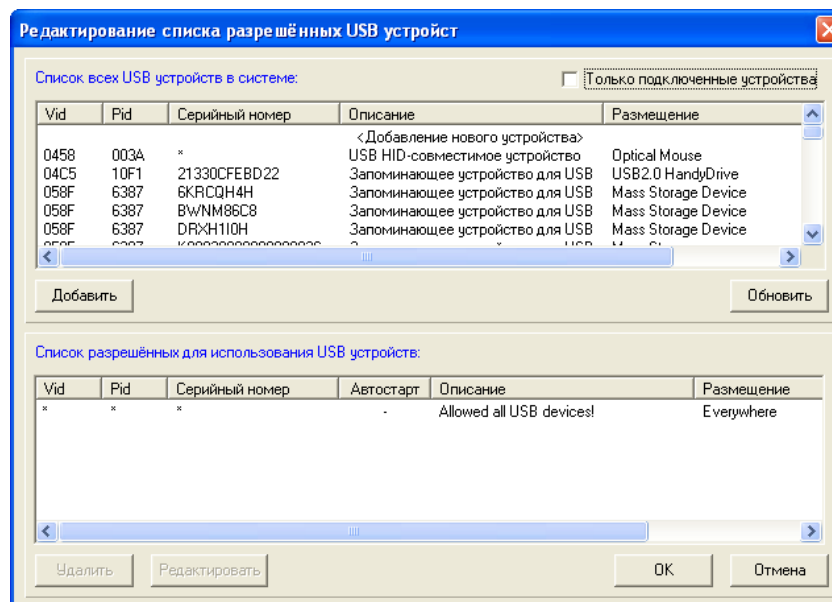


Рис. 43. Выбор разрешенных USB устройств из общего списка.

Пользоваться этим режимом следует с осторожностью, только в том случае, когда Вам точно известен серийный номер того устройства, доступ к которому будет разрешен.

Если USB-устройство – это съемный диск (флорпи, Zip, CD, флэш – не важно), то после включения его в список разрешенных устройств, следует описать правила доступа к тому логическому съемному диску, который монтируется в системе после подключения физического устройства к компьютеру. Если такую операцию не выполнить, то съемный диск останется недоступным после подключения к компьютеру, т.к. все логические диски, не включенные в список ПРД, запрещены. Атрибуты доступа устанавливаются стандартным образом, эта процедура описана в пункте 6.10.1. настоящего руководства.

ВНИМАНИЕ! Процедура описания правил доступа к съемным дискам (USB флэш, Zip, floppy, сменные HDD) выполняется корректно только в том случае, когда сменное устройство подключено к компьютеру ДО запуска программы ACED32.EXE и остается подключенным до завершения процедуры сохранения базы данных пользователей. Только в таком варианте редактор ПРД может точно определить соответствие логического диска, под которым съемное устройство отображается в GUI и физического устройства, например Device\Harddisk1\, к которому обращаются запросы уровня ядра операционной системы.

6.16 Формирование правил доступа для отдельных программ (процессов)

В состав комплекса “Аккорд NT/2000” входит программа, которая позволяет сформировать файл правил разграничения доступа для отдельных программ (файл с расширением .prc). Программа MakePrc.EXE использует тот же набор атрибутов доступа, что и редактор ACED32.EXE, поэтому логично привести ее описание в данном документе. После запуска программы на экран выводится главное окно (Рис.44.).

11443195.4012-019 97 02

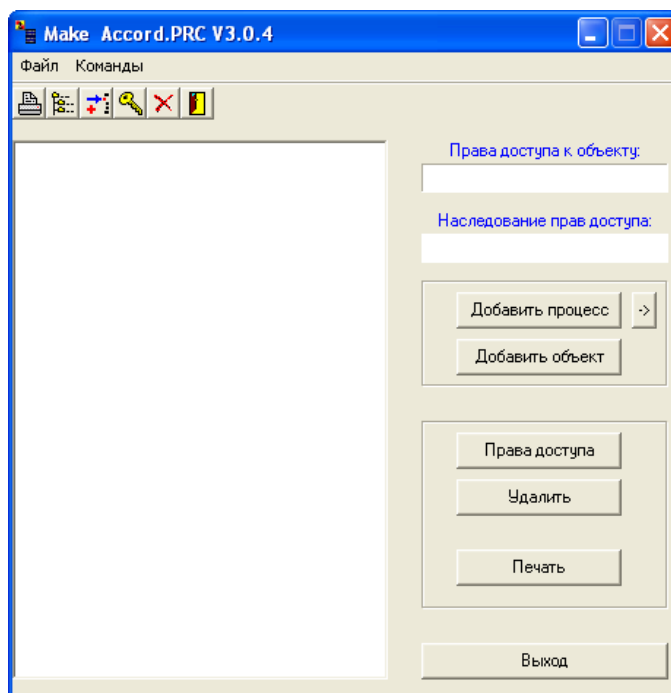


Рис.44. Главное окно программы MakePrc.

Вначале необходимо добавить программу (процесс), для которого будут устанавливаться правила доступа. Для этого на панели инструментов нажмите кнопку с изображением дерева каталогов, или в меню “Команды” выберите команду “Добавить процесс”. На экран выводится окно выбора процесса (Рис. 45.).

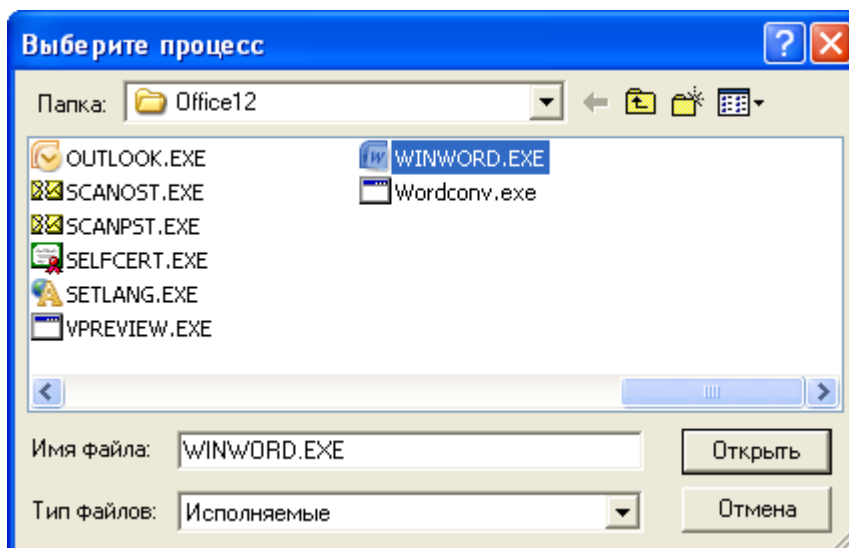


Рис. 45. Выбор процесса, для которого будут устанавливаться ПРД.

Отметьте нужный исполняемый файл (.exe или .dll) и нажмите кнопку “Открыть”. Выбранный файл появится в списке процессов в левой половине главного окна. При необходимости процедуру выбора файла можно повторить, т.е. в системе защиты “Аккорд” можно создать целый список процессов, для которых задаются правила доступа, не зависящие от ПРД текущего сеанса пользователя.

Теперь каждому процессу, включенному в список нужно сопоставить список объектов. Для этого мышью отмечается процесс, после чего становится доступной кнопка

11443195.4012-019 97 02

на панели <Добавить объект>. При нажатии этой кнопки открывается окно выбора файлов и каталогов (Рис.46.).

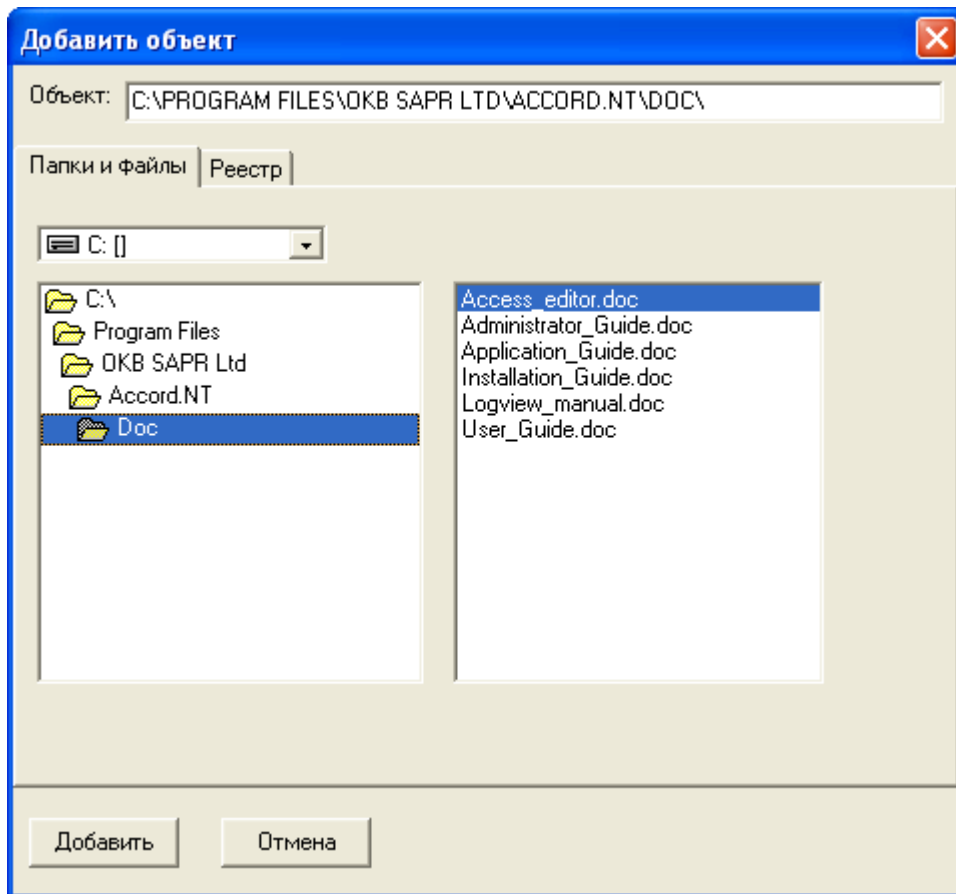


Рис. 46. Окно выбора файлов и каталогов

Отметьте необходимый каталог, нажмите кнопку <Добавить>. Выбранной объект появляется в списке под именем процесса. Для выбора конкретного файла из каталога нужно предварительно два раза щелкнуть мышью на каталоге в левом поле. В правом поле окна появится список файлов. Установите мышью курсор на нужном файле, нажмите кнопку <Добавить>. Если одному процессу необходимо назначить доступ к нескольким объектам, то операцию выбора нужно повторить. Теперь для каждого объекта из списка можно поменять ПРД (по умолчанию установлен полный доступ). Выберите мышью нужный объект. По двойному щелчку мышью, или при нажатии кнопки <Права доступа> открывается окно установки атрибутов доступа. Атрибуты доступа полностью соответствуют дискреционным ПРД, которые устанавливаются с помощью редактора ACED32.EXE.

После того, как установлены ПРД для выбранного объекта, нажмите клавишу "Запись". Повторите операцию для других объектов. После того, как всем объектам назначены правила доступа, следует сохранить настройки в файл на жестком диске. Нажмите кнопку <Выход>, подтвердите сохранение файла (Рис.47.). Запись производится в файл C:\Accord.NT\accord.prc. При старте монитора разграничения доступа AcRun.SYS выполняется проверка наличия файла accord.prc. Если файл обнаруживается, то при запуске процессов, описанных в этом файле, будут выполняться заданные ПРД.

11443195.4012-019 97 02

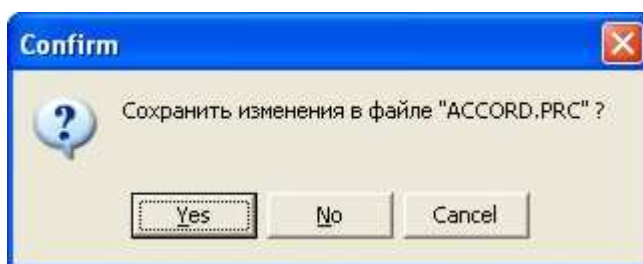


Рис.47. Сохранение файла ПРД для выделенных процессов.

Внимание! ПРД, загружаемые из файла accord.prc действуют только для заданных процессов и не зависят от настроек правил доступа текущего пользователя. Важно понимать, что для выделенного процесса будет предоставлен доступ ТОЛЬКО к тем объектам, которые включены в список объектов в файле accord.prc!

Для каких целей используется данная технология? Предположим, что в составе АРМ имеются ресурсы, доступ к которым должен предоставляться независимо от настроек пользователя и только выделенными процессами. Самому пользователю, как правило, эти ресурсы недоступны. Например, при установке на защищаемый АРМ подсистемы распределенного аудита и управления "Аккорд", программа - клиент запускается из каталога Accord.NT и выполняет запись в файл регистрации событий. В ПРД пользователя по умолчанию запрещен доступ к каталогу Accord.NT, чтобы пользователь не мог нарушить настройки системы защиты. Можно каждому пользователю прописать доступ к некоторым файлам в каталоге Accord.NT, а можно с помощью программы MakePrc назначить программе - клиенту рабочей станции AcWS32.EXE полный доступ к каталогу Accord.NT. Программа AcWS32.EXE запускается монитором разграничения доступа AcRun.sys при старте операционной системы и получает доступ к каталогу Accord.NT. С помощью этой программы администратор безопасности с сетевой консоли может менять настройки СЗИ и правила разграничения доступа пользователей. Пользователь (и все остальные процессы) при этом не имеют доступа к каталогу Accord.NT.

6.17 Групповая политика и особенности установки ПРД на контроллере домена Windows

В данном руководстве уже упоминалось, что при создании новой группы пользователей можно указать группу в составе ОС, в которую будут включаться пользователи СЗИ «Аккорд» при синхронизации баз данных. Для того, чтобы эта технология работала, в настройках комплекса должен быть установлен флаг «Синхронизация с базой пользователей NT». При установке ПО «Аккорд NT/2000» этот флаг включен по умолчанию. Соответствие группы пользователей СЗИ «Аккорд» группам в составе ОС устанавливается нажатием кнопки «NT группы» в главном окне программы после выбора нужной группы. Открывается окно выбора из списка существующих групп в составе ОС (Рис. 48).

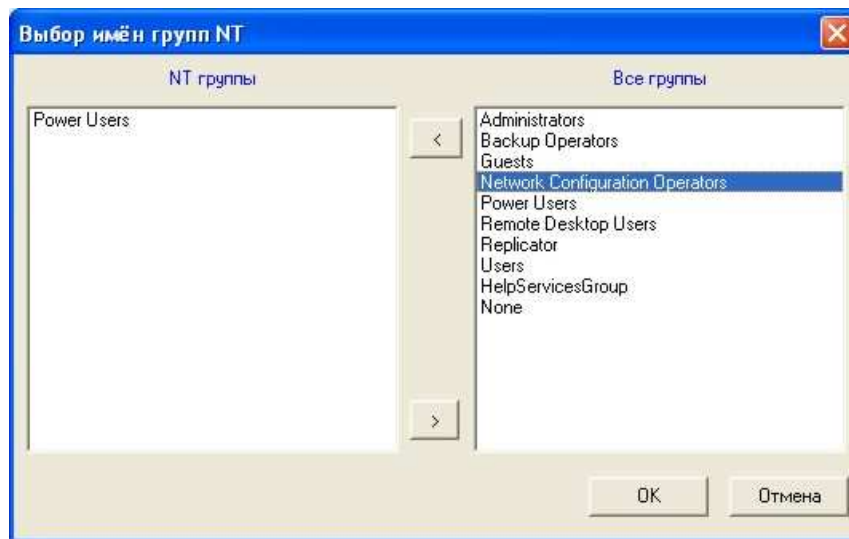


Рис. 48. Окно выбора групп пользователей.

В правой половине окна перечислены все группы, в левую часть можно перенести одну, или несколько групп, к которой должны принадлежать пользователи СЗИ «Аккорд». Такой вариант показан на Рис. 49. Изменить привязку к группам в составе ОС можно и для двух создаваемых по умолчанию групп СЗИ «Аккорд» - «Администраторы» и «Обычные». При установке подсистемы разграничения доступа «Администраторы» соответствуют группе «Administrators/Администраторы», и «Обычные» соответствуют группе «Users/Пользователи» в зависимости от основного языка установленной ОС.

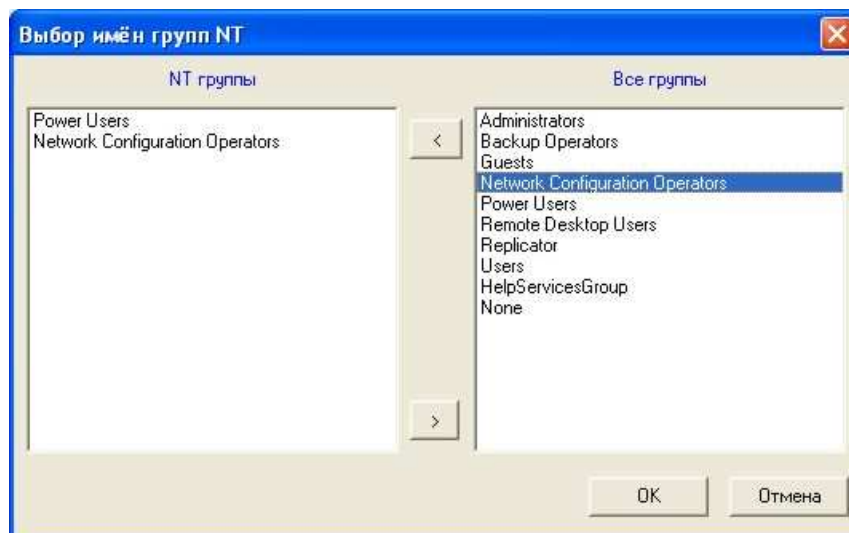


Рис. 49. Синхронизация пользователя СЗИ «Аккорд» с несколькими группами ОС.

Для завершения процедуры с сохранением нажмите <Ок>, выход без сохранения изменений <Отмена>. При завершении программы ACED32.EXE с сохранением изменений пользователи «Аккорда» будут добавляться в базу данных ОС с членством в указанных группах.

Установка комплекса «Аккорд NT/2000» на контроллере домена Windows требует некоторых дополнительных настроек. Вход в систему должен выполняться с правами администратора домена. В список групп NT для пользователей группы «Администраторы» должна быть добавлена запись Domain Administrators, для пользователей группы «Обычные» должна быть добавлена запись Domain Users. Только в этом случае пользователи СЗИ «Аккорд» будут добавляться в базу контроллера домена.

Внимание! Правила разграничения доступа, установленные в системе «Аккорд», будут действовать только в том случае, когда пользователь проходит процедуру идентификации/аутентификации на компьютере, на котором установлен контроллер домена. При удаленном подключении пользователя к домену с другого компьютера действуют настройки политики безопасности домена.

7 ЗАКЛЮЧЕНИЕ

Программа ACED32.EXE является лишь редактором параметров доступа пользователя к объектам доступа СВТ. Разграничение доступа пользователей к ресурсам компьютера реализуется монитором безопасности ACRUN.SYS, который использует матрицу доступа, подготовленную с помощью редактора ACED32.EXE. Подробно процесс настройки и запуска монитора безопасности описан в «Руководстве по установке» (11443195.4012-019 98 02).

8 Приложение 1. Файл ACCORD.INI – файл конфигурации СЗИ НСД «Аккорд»

Описание параметров, задаваемых в файле accord.ini, которые могут быть изменены администратором СЗИ или субъектом с правами администратора:

[COMMON]

TmPageNo=0 – страница идентификатора. В этой и следующей странице памяти идентификатора хранится секретный ключ пользователя. Значение по умолчанию – 0, т.е. данные занимают 0-ю и 1-ю страницы. **Внимание!** Не рекомендуется изменять этот параметр без необходимости. При изменении параметра требуется перерегистрировать ВСЕ ТМ-идентификаторы с генерацией нового секретного ключа. Будьте внимательны при использовании программных средств других производителей, которые используют ТМ для хранения своих данных. Если эта информация будет повреждена, то пользователь не получит доступ к компьютеру с установленным комплексом Аккорд, т.к. в базе данных хранится результирующая функция, в которой используется заводской номер идентификатора, пароль и ключ пользователя.

TmTimeout=20

PasswTimeout=20 – Временной интервал, который отводится для предъявления идентификатора и ввода пароля.

UseLogicalDisksNames=(No по умолчанию) – использование логических имен разделов жесткого диска в матрице описаний правил доступа. Параметр может быть изменен в случае использования дополнительных съемных дисков, или аппаратных RAID массивов, которые меняют порядок физических дисков в системе. После изменения этого параметра обязательно запустить редактор ПРД для создания нового списка контролируемых логических разделов. Если используются логические имена, то невозможно будет разграничить доступ к съемным дискам (флорпи, USB и др.).

UsePPOCheck – Параметр зарезервирован для дальнейшего использования.

[ACRUN]

LockUSB - блокировка USB портов во время работы ScreenSaver. Значения: Yes – блокировать, No – не блокировать (установлено по умолчанию).

ClearSteps=1 – число повторов записи последовательности случайных чисел на диск (при удалении файлов с очисткой).

ClearPagefile – очищать файл подкачки при завершении сеанса пользователя
Значения: Yes – очищать. No – не очищать (установлено по умолчанию).

DisplayNSD – Выводить на экран сообщения об НСД от имени СЗИ. No – не выводить отдельного сообщения (установлено по умолчанию), а все отказы в доступе транслировать на уровень стандартного интерфейса ОС.

WriteNsdOnFind=Yes - (установлено по умолчанию) параметр определяет запись в журнал событий НСД при операциях Find1st/FindNxt и Traverse, т.е. при проверке существования пути. Если =NO, то не будет записи таких событий в журнал. Редактируется флаг только вручную.

WriteWarningToLog=No – Определяет запись в журнал кода результата «Warning». Данный результат фиксируется при применении атрибута O, при очистке файла, а пишется в журнал при установке значения Yes. Редактируется флаг только вручную.

CheckCompOffTime – контроль времени завершения сеанса пользователя
Значения: Yes – контроль времени используется. No – не используется.

11443195.4012-019 97 02

WarningCompOffTime=5 – интервал времени до завершения сеанса, с того момента, когда выводится пользователю предупреждение о предстоящем окончании работы. Задается в минутах.

HardResetCompDeltaTime=2 – интервал времени, через который принудительно перегружается компьютер, если сеанс не удалось завершить корректно (с закрытием всех приложений). Задается в минутах.

DisableSessionLogOff – принудительная перезагрузка по завершению сеанса пользователя (по умолчанию – No, в программе настройки флаг «завершать сессию полной перезагрузкой»).

LoginUseFullName (по умолчанию - No) - использование полного имени пользователя при входе в систему.

FullProcessPath – контроль процессов по полному пути доступа. Значения: Yes – контроль по полному пути. No – контроль только по имени процесса.

WriteLogicalNames – тип записи в журнал регистрации событий имени тома. Значения: Yes – запись логического имени. No – запись в журнал полного пути, например: DEVICE\HardDiskVolum1\...

MarkCaption (по умолчанию Yes) – выводить в заголовке окна текущее значение уровня доступа запущенного процесса.

UseAntivirus - использование антивирусного ядра (по умолчанию - No).

CheckPrint (по умолчанию No) - отвечает за перехват функций печати. Если значение параметра No, то функции печати никогда не будут перехватываться. Этот параметр необходим в некоторых системах, где при перехвате этих функций срабатывает DEP.

DelayStartSpecProcess=0

ExistsAsAttrib (по умолчанию Yes). Если установлен этот параметр, то проверка существования объекта проверяется через ZwQueryFullAttributesFile, т.е. более быстрым алгоритмом. Если вдруг начнут «отваливаться» службы ILO HP, или будет аварийно завершаться Device Lock, то установить значение No.

ClearOnNet - отвечает за удаление с очисткой файлов на сетевых дисках. Эти файлы могут быть в общем доступе, или DFS, поэтому параметр по умолчанию выключен.

CheckDevices (по умолчанию No) - отвечает за контроль доступа к устройствам. Список контролируемых устройств появляется в редакторе ПРД после включения этого параметра. Проверка доступа выполняется на уровне файловых операций ввода-вывода, поэтому мышь на Com-порту будет работать через свой драйвер, даже если в Аккорде запрещен доступ к последовательному порту, а вот модем, или программа обмена файлами с другим компьютером работать не будут.

ChkDsk – параметр определяет возможность старта программы проверки дисков при загрузке ОС. Значение по умолчанию – No.

[ACED]

Flag0100=Не контролировать UNC имена

Flag0200=Удаление файлов с очисткой

Flag0400=Маркировка печати

Flag0800=<не используется>

Flag1000=Может изменять дату/время

Flag2000=Запрет доступа к общим ресурсам

Flag4000=Полный доступ для АРМ АБИ

Flag8000=Проверять доступ к реестру

11443195.4012-019 97 02

English – язык интерфейса программ СЗИ Аккорд (значение No определяет вывод всех заголовков и сообщений на русском языке).

PrdType=New

UseAmdzBase – использование базы пользователей АДЗ в программе ACED32.
Значения: Yes – АДЗ используется. No – АДЗ не используется.

UseNTBase – синхронизация с БД пользователей операционной системы. Значения:
Yes – при создании пользователя в БД СЗИ «Аккорд» он заносится в список пользователей операционной системы. No – синхронизация не выполняется.

DeleteNoAccordUsers – при синхронизации с базой пользователей ОС удалять существующих пользователей, которые не являются пользователями СЗИ «Аккорд». Значения: Yes – удалять. No – не удалять.

DiscreteAccess – использование дискреционного метода разграничения доступа
Значения: Yes – используется. No – не используется.

MandatoryAccess – использование мандатного метода разграничения доступа.
Значения: Yes – используется. No – не используется.

CheckProcess – использование контроля исполняемых файлов как дополнительной подсистемы мандатного метода. Значения: Yes – используется, при этом в сеансе конкретного пользователя допускается выполнение только процессов из «белого» списка. При этом процессу назначается уровень доступа. No – не используется.

NoConvertNetPath (по умолчанию No). Если значение Yes, то при выходе из редактора Aced32 в базу пишутся только длинные имена сетевых файлов (т.е не производится их конвертация в короткие имена) . Параметр необходим в тех случаях, когда в базу ПРД включено много сетевых ресурсов на серверах, не доступных в данный момент времени. Преобразование таких имен при выходе из Aced32 занимает очень много времени, т.к. ОС пытается несколько раз получить доступ к недоступному ресурсу, прежде чем возвращает код ошибки.

Параметры, задаваемые в файле accord.ini изменяются программой настройки комплекса. Не рекомендуется менять их значение вручную без четкого понимания последствий вносимых изменений. Исключение – параметры UseLogicalDisksNames, WriteNsdOnFind, WriteWarningToLog, и NoConvertNetPath, они корректируются только в файле accord.ini любым текстовым редактором.