МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Нижегородский государственный университет им. Н.И. Лобачевского

А.А. Горбунов
Л.Ю. Ротков
А.А. Рябов

ЗАЩИТА ОТ НСД С ПОМОЩЬЮ ПАК «АККОРД»

Учебно-методическое пособие

Рекомендовано методической комиссией радиофизического факультета для студентов ННГУ, обучающихся по специальностям 10.05.02 «Информационная безопасность телекоммуникационных систем», направлению подготовки 02.03.02 «Фундаментальная информатика и информационные технологии» и слушателей курсов послевузовского краткосрочного повышения квалификации специалистов по информационной безопасности

Нижний Новгород
2015

УДК 004.056.53

Горбунов А.А., Ротков Л.Ю., Рябов А.А. ЗАЩИТА ОТ НСД С ПОМОЩЬЮ ПАК «АККОРД»: Учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2015. – 28 с.

Рецензент: начальник 1 отдела Нижегородского государственного университета им. Н.И. Лобачевского, к.т.н., доцент **Казачков А.П.**

Методическая разработка содержит описание к лабораторной работе «Защита от несанкционированного доступа с помощью программно-аппаратного комплекса «АККОРД».

Лабораторная работа предназначена для изучения аппаратных средств защиты информации от несанкционированного доступа (НСД) на примере программно-аппаратного комплекса (ПАК СЗИ НСД) «Аккорд». В описании приведены общие принципы и правила организации работы по обеспечению конфиденциальности информации. Дан обзор архитектуры комплексов семейства «Аккорд». В работе изучаются основные защитные функции комплекса, его возможности, особенности применения.

Пособие предназначено для студентов, обучающихся по специальностям 10.05.02 «Информационная безопасность телекоммуникационных систем», направлению подготовки 02.03.02 «Фундаментальная информатика и информационные технологии» и слушателей курсов послевузовского краткосрочного повышения квалификации специалистов по информационной безопасности.

Ответственный за выпуск:
заместитель председателя методической комиссии
радиофизического факультета ННГУ,
д.ф.-м.н., проф. каф. общей физики Грибова Е.З.

УДК 004.056.53

1. ОБЩИЕ СВЕДЕНИЯ

Актуальность и значимость проблем защиты информации предусмотрены требованиями законодательных и нормативных документов, действующих в Российской Федерации.

Выполнение работ по защите информации, составляющей государственную тайну, осуществляют специально аккредитованные органы и испытательные центры (лаборатории), имеющие лицензии на право проведения работ в области защиты информации. Целями защиты являются предотвращение ущерба и реализация адекватных мер защиты информации, предусмотренных Законами и нормативными документами Российской Федерации.

Защита достигается применением специальных программно-аппаратных средств защиты, организацией системы контроля безопасности информации в автоматизированных системах (АС).

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа (ПАК СЗИ НСД) «Аккорд», далее комплекс «Аккорд», предназначен для применения на персональных компьютерах (ПК) и серверах в целях защиты информационных ресурсов от несанкционированного доступа (НСД).

2. ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ

Защита информации осуществляется путем выполнения комплекса мероприятий.

Мероприятия по защите информации являются составной частью управленческой, научной и производственной деятельности предприятия и осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима конфиденциальности.

Защита информации конкретизируется следующими концептуальными положениями:

- определение охраняемых сведений;
- ценность информации и ее носителей;
- определение источников угроз безопасности информации, демаскирующих признаков, технических каналов утечки и несанкционированного доступа к информации;
- оценка возможностей источников угроз безопасности информации;
- разработка и проведение обоснованных мероприятий по защите информации;
- контроль эффективности принятых мер защиты.

Для эффективного применения комплекса и поддержания необходимого уровня защищенности ПК и информационных ресурсов необходимы:

- физическая охрана ПК, недопущение изъятия контроллера комплекса;
- наличие администратора безопасности информации (БИ).
- использование в ПК сертифицированных технических и программных средств защиты.

Администратор БИ планирует защиту информации, определяет права доступа пользователям, организует установку комплекса в ПК, эксплуатацию и контроль за правильным использованием ПК, осуществляет периодическое тестирование средств защиты комплекса. Применение комплекса «Аккорд» совместно с сертифицированными программными средствами криптографической защиты информации (СКЗИ) и/или программными средствами защиты информации от НСД (СЗИ НСД) позволяет значительно снизить нагрузку на организационные меры защиты информации, определенные условиями применения этих средств.

3. ОСОБЕННОСТИ ЗАЩИТНЫХ ФУНКЦИЙ КОМПЛЕКСА

Защитные функции комплекса реализуются применением:

1. Дисциплины защиты от НСД к ПК, включающей:
   - идентификацию пользователя по уникальному ТМ (touch-memory)-идентификатору;
   - аутентификацию с учетом необходимой длины пароля и времени его жизни;
   - ограничением времени доступа субъекта к компьютеру.
2. Процедур блокирования экрана и клавиатуры.
3. Дисциплины разграничения доступа к ресурсам ПК.
4. Дисциплины применения специальных процедур печати, управления стандартными процедурами печати, процедурами ввода/вывода на отчуждаемые носители информации.
5. Контроля целостности критичных с точки зрения информационной безопасности программ и данных.

Комплекс «Аккорд» может применяться в произвольной и функционально замкнутой программной среде. Предусмотрено подключение подсистемы криптографической защиты информации с использованием индивидуальных ключей, хранящихся в персональном ТМ-идентификаторе.

4. ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ КОМПЛЕКСА

Защита информации с использованием средств комплекса основана на обработке событий, возникающих при обращении прикладных программ или системного ПО к ресурсам ПК. При этом средства комплекса перехватывают соответствующие программные и/или аппаратные прерывания, в случае возникновения контролируемого события (запрос прерывания) анализируют запрос и в зависимости от соответствия полномочий субъекта доступа (его прикладной задачи), установленных администратором БИ, либо разрешают, либо запрещают обработку этих прерываний.

Разграничение прав доступа к данным обеспечивается программно-аппаратным комплексом на базе контроллера «Аккорд-АМДЗ» и специального программного обеспечения.

Комплекс «Аккорд» можно условно представить в виде трех взаимодействующих между собой подсистем защиты информации.

- Подсистема управления доступом.
- Подсистема регистрации и учета.
- Подсистема обеспечения целостности.

4.1. Подсистема управления доступом

Подсистема управления доступом предназначена для защиты ПК от посторонних пользователей, управления доступом к объектам доступа и организации совместного их использования зарегистрированными пользователями в соответствии с установленными правилами разграничения доступа.

Подсистема обеспечивает идентификацию, проверку подлинности и контроль доступа субъектов при:

- входе в систему;
- доступе к внешним устройствам ПК;
- доступе к файлам, каталогам, дискам.

В комплексе «Аккорд» реализованы принципы как избирательного, так и полномочного управления доступом. В настоящей работе рассматриваются только аспекты избирательного управления доступом.

В настоящей работе рассматривается использование комплекса для реализации дисциплины разграничения доступа, основанной на избирательном принципе.

4.2. Подсистема регистрации и учета

Подсистема регистрации и учета предназначена для регистрации в журнале учета следующих событий, происходящих в ПК:

- вход (выход) субъектов доступа в (из) системы;
- запуск (завершение) программ и процессов (заданий, задач);
- доступ программ субъектов к защищаемым файлам, включая их создание и удаление;
- доступ программ субъектов доступа к внешним устройствам ПК;
- изменение полномочий субъектов доступа;
- создание (удаление) защищаемых объектов доступа.

Предусмотрена разная степень детализации журнала учета.

4.3. Подсистема обеспечения целостности

Подсистема обеспечения целостности предназначена для исключения несанкционированных модификаций программной среды, в том числе программных средств комплекса и обрабатываемой информации.

5. СОСТАВ КОМПЛЕКСА

- контроллер «Аккорд-АМДЗ»;
- контактное устройство – считыватель информации;
- интеллектуальные персональные ТМ-идентификаторы;
- специальное программное обеспечение СЗИ НСД, работающее под управлением операционной системы.

6. ПРИНЦИП РАБОТЫ КОМПЛЕКСА

Плата контроллера комплекса «Аккорд» устанавливается в свободный слот материнской платы ПК.

Каждый пользователь ПК должен быть зарегистрирован в комплексе администратором. В процессе регистрации администратор выдает пользователю персональный ТМ-идентификатор, память которого содержит уникальный идентификатор пользователя, о чем делается запись в журнал учета носителей информации. Пользователь обязан хранить свой идентификатор с соблюдением правил, доведенных до него администратором БИ.

Особенностью и преимуществом комплекса «Аккорд» является проведение процедур идентификации, аутентификации и контроля целостности защищаемых файлов до загрузки операционной системы. Это обеспечивает-

ся при помощи ПЗУ, установленного на плате контроллера комплекса, которое получает управление во время так называемой процедуры ROM-SCAN.

При установленном комплексе «Аккорд» загрузка компьютера осуществляется в порядке, предусмотренном процедурой работы автоматизированного модуля доверенной загрузки:

1. BIOS компьютера выполняет стандартную процедуру POST (проверку основного оборудования компьютера) и по ее завершении переходит к процедуре ROM-SCAN, во время которой управление перехватывает контроллер комплекса «Аккорд».
2. Выполняется процедура идентификации и аутентификации пользователя по предъявленному ТМ-идентификатору. Для аутентификации пользователя (в том числе для предотвращения возможности использования утраченного / похищенного идентификатора) предусмотрен режим ввода пароля с клавиатуры после проверки ТМ-идентификатора. При ошибке (неправильный пароль) или при истечении времени по тайм-ауту дальнейшая процедура загрузки системы блокируется.
3. Возможность загрузки с отчуждаемых носителей информации (например, гибких дисков, CD и DVD дисков, внешних USB-накопителей) блокируется.
4. После успешной аутентификации комплекс производит контроль целостности BIOS и отмеченных для проверки системных файлов. Важной функцией комплекса «Аккорд» является возможность проверки целостности данных на дисках ПК. При проверке файлов на целостность вычисляются их текущие контрольные суммы и сравниваются со значениями, записанными в память контроллера. В комплексе «Аккорд» используются стойкие алгоритмы вычисления хэш-функций, практически исключающие факт несанкционированной модификации файла.
5. После успешной проверки целостности системы, если для пользователя задана проверка целостности файлов, производится проверка указанных контролируемых объектов пользователя.
6. При успешном прохождении процедур, описанных в пп. 1–5, производится передача управления штатному загрузчику системы.

7. ПОРЯДОК РАБОТЫ ПОЛЬЗОВАТЕЛЯ С ПК, ОСНАЩЕННЫМ КОМПЛЕКСОМ «АККОРД»

Для того, чтобы приступить к работе на ПК пользователь должен выполнить следующие действия.

Включить компьютер, при этом в процессе загрузки на мониторе на синем фоне появится надпись: *«Прислоните ТМ-идентификатор…»*.

Прикоснуться к считывателю идентификатором, и на запрос *«Введите пароль»* ввести пароль.

Здесь возможно появление сообщения *«Ошибка чтения ТМ-идентификатора»*, сопровождаемое звуковым сигналом. Такое сообщение может появиться по следующим причинам:

- плохой контакт идентификатора со съемником;
- использование незарегистрированного ТМ-идентификатора;
- нарушение содержимого идентификатора, что может свидетельствовать о попытке несанкционированного воздействия на защищаемый ПК.

При появлении указанного сообщения необходимо повторить процедуру доступа к системе и если ситуация окажется устойчивой – обратиться к администратору.

В штатном режиме при корректно введенном пользователем пароле на ПК выполняются действия по загрузке операционной системы. В случае подозрения на нештатный режим работы пользователь обязан прекратить работу и обратиться к администратору БИ.

При осуществлении процедур идентификации, аутентификации пользователя и проверки целостности, комплекс блокирует клавиатуру и загрузку ОС с отчуждаемого носителя информации. При касании съемника информации осуществляется поиск предъявленного ТМ-идентификатора в списке зарегистрированных на ПК идентификаторов. Если предъявленный ТМ-идентификатор обнаружен в списке, то производится контроль целостности защищаемых по перечню данного пользователя файлов. При проверке перечня файлов пользователя на целостность вычисляются значения хэш-функции (контрольных сумм) этих файлов и сравниваются с контрольным значением. Если нарушена целостность защищаемых файлов, загрузка операционной системы не производится. Для продолжения работы потребуется вмешательство администратора БИ. Таким образом, контрольные процедуры (идентификация, аутентификация, проверка целостности системных файлов ОС) осуществляются до загрузки ОС. При этом обеспечивается защита от разрушающих программных воздействий. В процессе работы пользователя программа *«Монитор безопасности»* препятствует любым видам НСД к системным файлам ОС.

В случае санкционированной модификации защищенных файлов осуществляется процедура перезаписи контрольных значений хэш-функции модифицированных файлов.

В процессе функционирования комплекса резидентная часть *«Монитора безопасности»* проверяет файлы всех загруженных драйверов и обеспечивает оперативный контроль целостности исполняемых файлов перед передачей им управления. Тем самым обеспечивается защита от программных вирусов и закладок.

Кроме того, *«Монитор безопасности»* ограничивает доступ к файлам ПО комплекса, запрещая пользователю их переименование, уничтожение, изменение.

8. СОСТАВ УСТАНОВКИ

- Персональный компьютер (ПК) с установленной операционная системой Windows XP SP3.
- Контроллер «Аккорд-5».
- Специальное программное обеспечение разграничения доступа «Аккорд NT/2000».

9. ПРАВИЛА АДМИНИСТРИРОВАНИЯ СУБЪЕКТОВ И УСТАНОВКИ ПРАВ ДОСТУПА

Программа *«Редактор прав доступа»* из набора специального программного обеспечения комплекса «Аккорд» представляет собой редактор параметров (атрибутов) разграничения доступа субъектов (пользователей) к объектам ПК (рис. 1). Программа используется администратором БИ или субъектами, наделенными правами супервизора. Каждый ее запуск требуется подтверждение наличия прав супервизора при помощи соответствующих ТМ-идентификатора и пароля.

Права супервизора рекомендуется назначать администратору БИ. Допускается назначение этого статуса любому уполномоченному пользователю.

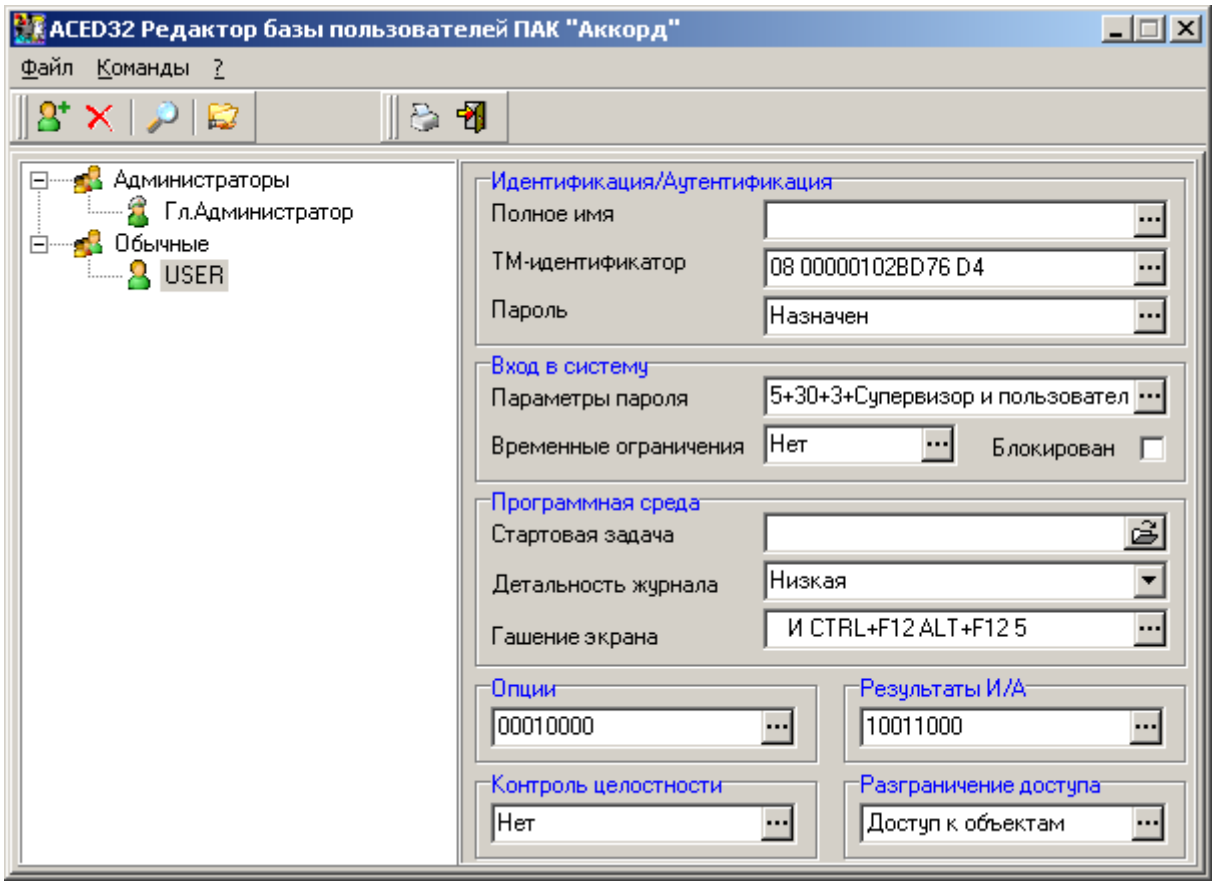

Рис. 1.

Регистрация нового пользователя.

Для регистрации нового пользователя необходимо произвести следующие операции.

Запустить программу *«Редактор прав доступа»*.

В главном окне программы необходимо указать, к какой из групп будет относиться вновь регистрируемый пользователь (например, к группе пользователей «Обычные»). В разделе «Команды» основного меню выбрать пункт «Создать» (или соответствующий значок на панели инструментов) и в появившемся окне ввести имя создаваемого пользователя (рис. 2). Администратор должен присваивать каждому пользователю уникальное в данной вычислительной среде имя.

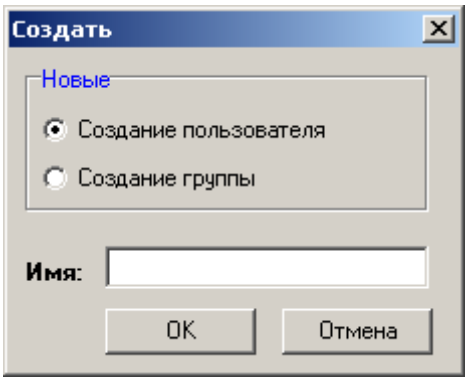

Рис. 2.

Далее в главном окне программы (рис. 1) в соответствии с реализуемой политикой безопасности следует задать параметры вновь созданного пользователя. Для сохранения параметров пользователя и выхода используется значок на панели инструментов «Выход из редактора» (либо сочетание клавиш [Ctrl] + [X]).

Некоторые параметры пользователя являются обязательными, без ввода которых невозможен ввод остальных, например, – «ТМ-идентификатор», «Пароль». Часть параметров является недоступной при различных типах ТМ-идентификаторов (например, «Контроль целостности» недоступен, если ТМ- идентификатор не имеет памяти).

Для назначения вновь созданному пользователю персонального ТМ-идентификатора необходимо нажать кнопку ([...]) напротив пункта «ТМ-идентификатор». В появившемся окне (рис. 3) выбрать пункт «Сгенерировать», после чего прислонить ТМ-идентификатор, выделенный для нового пользователя, к считывателю и нажать кнопку «Далее» ([F2]).

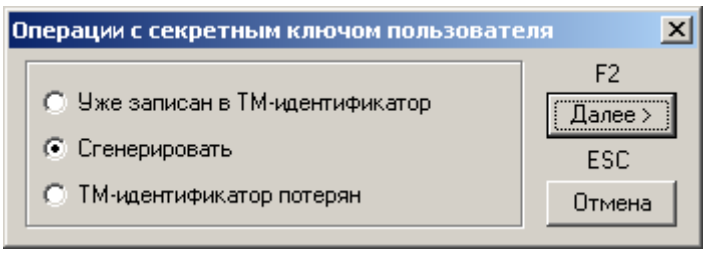

Рис. 3.

Аналогично производится перерегистрация ТМ-идентификатора пользователя.

Программа запрещает разным пользователям регистрировать один и тот же ТМ-идентификатор.

Создание пароля пользователя осуществляется по нажатию кнопки напротив пункта «Пароль» и ввода в появившемся окне (рис. 4) символов пароля с клавиатуры.

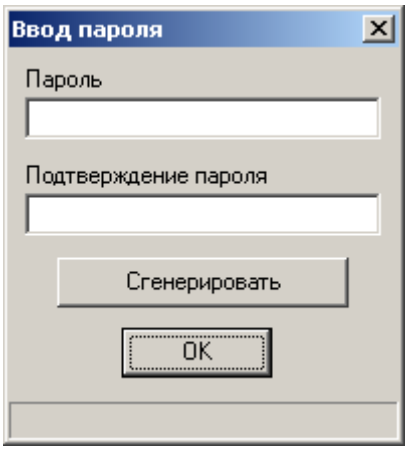

Рис. 4.

Заданный пароль назначается пользователю только после успешной проверки на соответствие параметрам, указанным в пункте «Параметры пароля».

Удаление пользователя из списка зарегистрированных.

В подменю списка пользователей (рис. 1) необходимо выбрать и отметить имя пользователя, предназначенного для удаления из списка. Удаление пользователя осуществляется путем выбора в разделе «Команды» основного меню пункта «Удалить», либо путем нажатия клавиши [Del] на клавиатуре. Для завершения операции требуется подтвердить удаление.

Редактирование параметров пользователей.

В этом режиме администратор производит изменение параметров доступа пользователя к объектам ПК, а также настройку свойств для данного пользователя, обуславливающих особенности его работы с ПК.

Вызов определенного окна настройки свойств пользователя (рис. 5) осуществляется путем нажатия кнопки напротив соответствующего пункта в главном окне программы *«Редактор прав доступа»*.

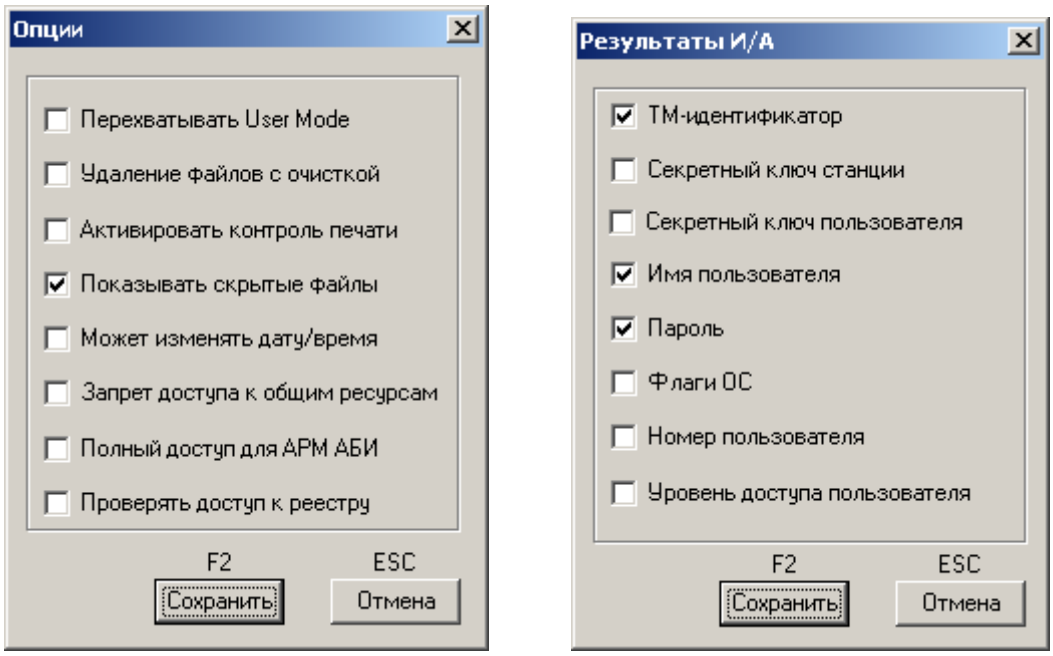

Рис. 5.

Задание запускаемой программы пользователя.

Этот параметр определяет задачу, которая запускается после загрузки компьютера. Стартовая задача может быть из числа файлов `*.EXE`, `*.COM`, `*.BAT`. Стартовая задача у пользователя может не задаваться.

Установка прав доступа к объектам ПК.

Установка прав доступа пользователя к объектам ПК осуществляется в окне «Редактирование правил разграничения доступа» (рис. 6), вызываемого по нажатию кнопки ([...]) в соответствующем разделе главного окна программы *«Редактор прав доступа»*.

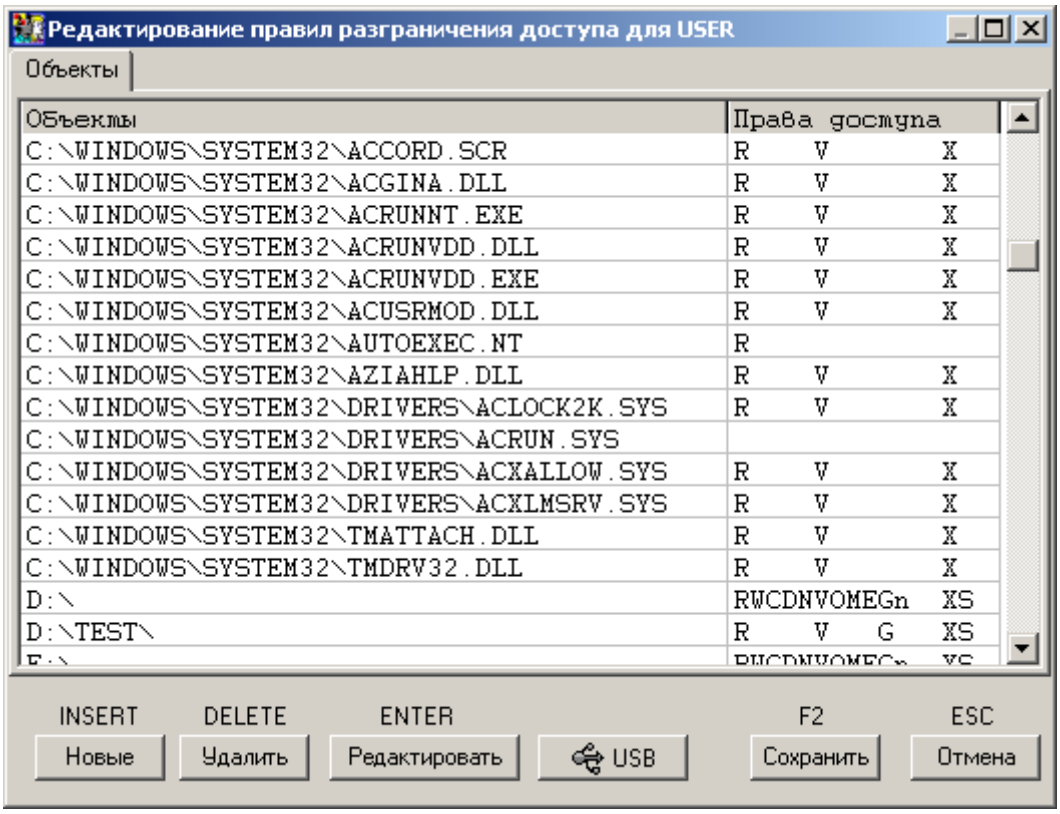

Рис. 6.

По умолчанию выведен перечень всех доступных корневых каталогов дисков, ключей реестра (строки, начинающиеся с «\HKEY_»), сетевых и локальных принтеров (при наличии таковых на ПК).

В этом окне нет деления на диски, каталоги, файлы и т.д., а ведется один общий список объектов ПК. В список объектов для обычных пользователей уже включены правила разграничения доступа (ПРД), которые защищают от модификации программные компоненты комплекса «Аккорд».

После выбора в разделе «Объекты» строки с именем конкретного объекта и нажатия кнопки «Редактировать» (или клавиши [Enter]) – выводится окно определения правил доступа к данному объекту (рис. 7).

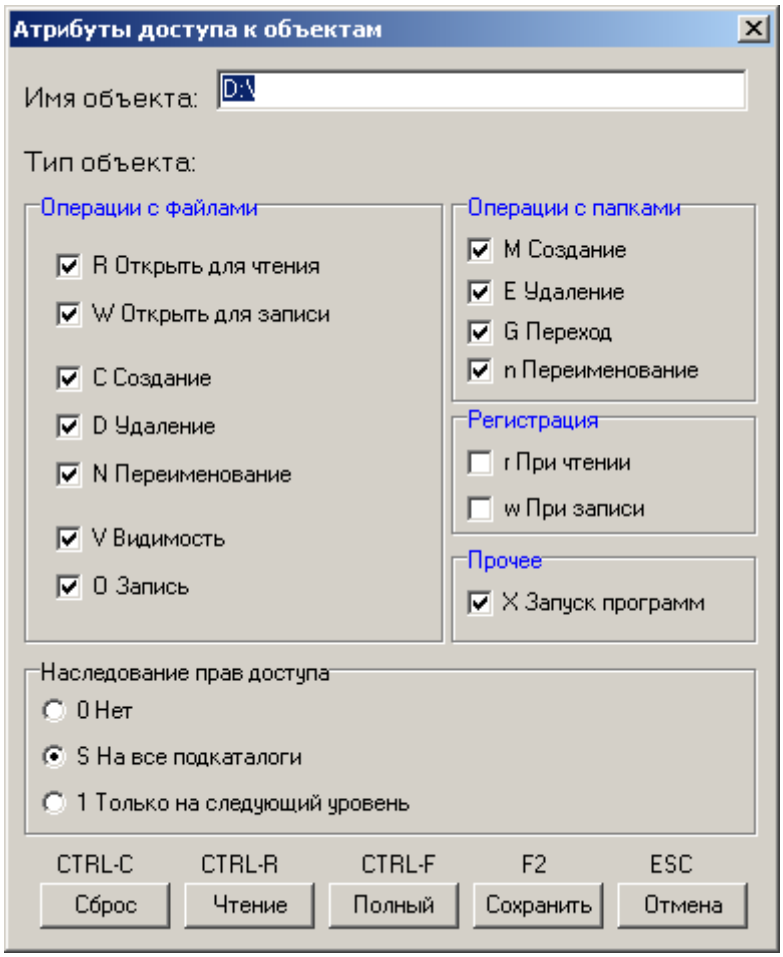

Рис. 7.

При указании ПРД для файлов можно пользоваться простым групповым обозначением имени файла, используя шаблон `*.расширение` (например, `*.bak`, `*.txt` и т.п.)

Если необходимо удалить какой-либо объект и установленные для него ПРД, то следует выбрать строку с названием объекта, нажать кнопку «Удалить» или клавишу [Delete], после чего подтвердить или отменить удаление.

Выход из режима редактирования с сохранением осуществляется нажатием кнопки «Запись» (или клавиши [F2]), без сохранения – кнопки «Закрыть» (или клавиши [Esc]).

Для того, чтобы запретить доступ к логическому диску, достаточно исключить корневой каталог этого диска из списка объектов. 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.

При установке ПРД к объекту могут использоваться следующие атрибуты доступа.

1. 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 пользователю требуется разрешить только просмотр файла.

2. 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 на переход в каталог.
- n – переименование каталога. Например, в ОС Windows, удаление папки в корзину является операцией переименования каталога.

3. Прочее:

- X – разрешение на запуск программ.

4. Регистрация:

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

Для группового манипулирования параметрами доступа используются кнопки «Сброс» (сброс всех параметров), «Чтение» (установка параметров R, V, G, X, S), «Полный» (установка всех параметров, кроме параметров группы «Регистрация») или соответствующие им сочетания клавиш: [Ctrl]+[C], [Ctrl]+[R], [Ctrl]+[F] (рис. 7).

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 наследуется только подкаталогами следующего уровня.
- `0` – параметры доступа текущего каталога не наследуются подкаталогами.

Например, если для корня дерева каталогов диска `D:\` установить атрибут `0`, доступными будут только файлы в корневом каталоге, а остальные каталоги для данного пользователя будут недоступны. Каталог на диске `D:\` будет доступен пользователю (с любой непротиворечивой комбинацией атрибутов) только при явном его описании в списке прав доступа.

Если для корневого каталога `D:\` установить атрибут `S`, то все его файлы, каталоги и подкаталоги будут доступны пользователю, правила доступа к ним будут определяться атрибутами, установленными для `D:\`. В этом случае отдельный каталог можно включить в список ПРД и установить для него персональные атрибуты, отличные от «родительских».

Если какой-либо объект явно прописан в списке доступа, то для него действуют установленные ПРД, независимо от атрибутов наследования объектов вышестоящего уровня.

При отсутствии в списке (рис. 6) необходимого объекта, нажатием кнопки «Новый» (или клавиши [Insert]) на экран выводится расширенное окно «Атрибуты доступа к объектам» (рис. 8).

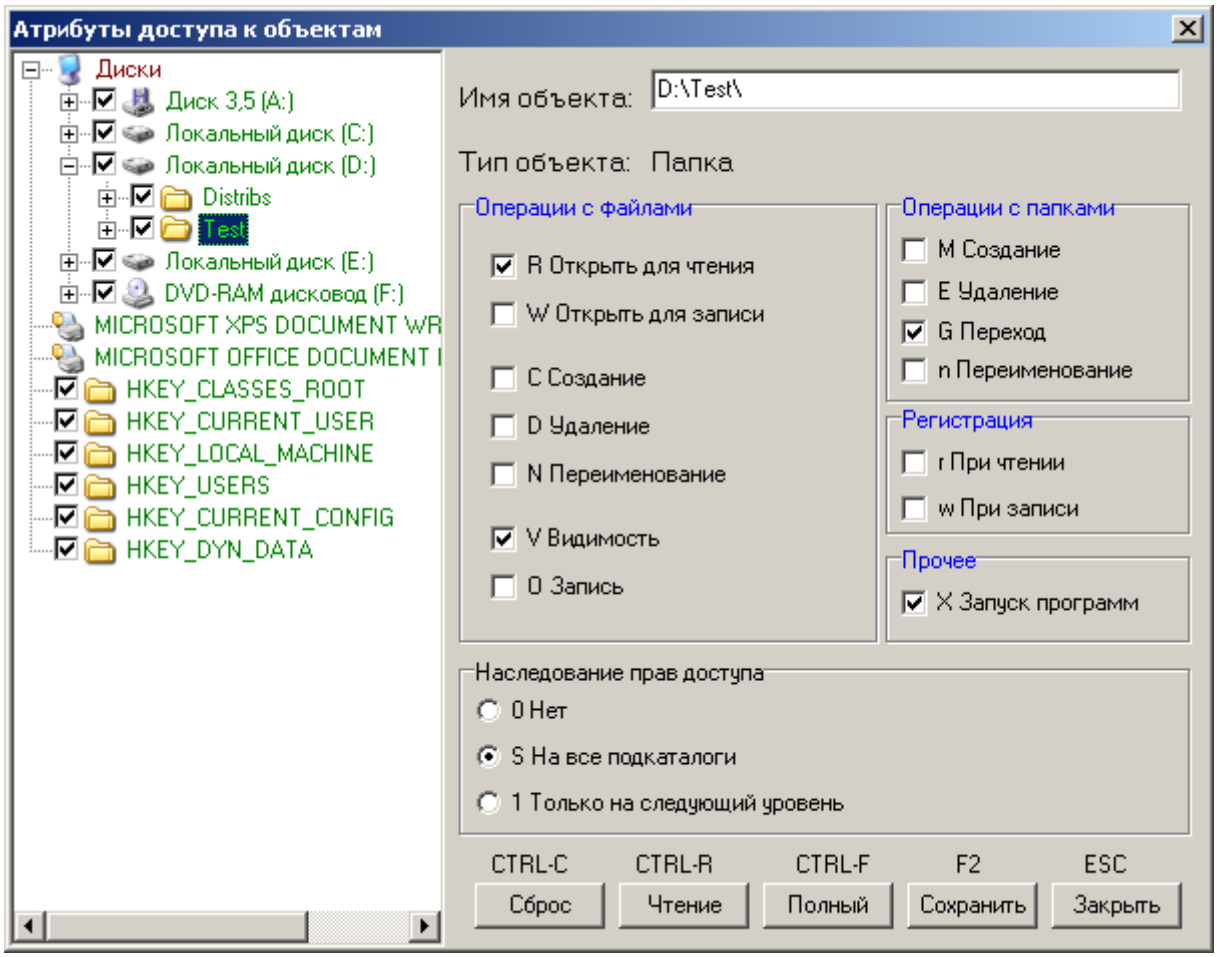

Рис. 8.

Справа в этом окне отображен список всех объектов. В поле «Имя объекта» вводится имя объекта, ниже устанавливаются необходимые для него атрибуты. С помощью мыши также можно выбрать имя объекта, щелкнув левой кнопкой мыши на имени объекта в дереве объектов. В этом случае в поле «Имя объекта» будет отображено 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 описании правил доступа к съемному устройству (USB флэш-диск, USB Zip-диск) необходимо, чтобы это устройство было подключено к компьютеру. В этом случае, после нажатия кнопки «Новый» ([Insert]), необходимо в списке выбрать букву диска, соответствующего устройству типа «Съемный диск». Далее ему устанавливаются ПРД и кнопкой «Запись» (или клавишей [F2]) сохраняются изменения. В дальнейшем при работе пользователя после подключения соответствующего устройства для него будут действовать установленные ПРД.

Процедура описания правил доступа к съемным дискам (USB Flash, Zip, Floppy, сменные HDD) выполняется корректно только в том случае, когда

сменное устройство подключено к компьютеру до запуска программы *«Редактор прав доступа»* и остается подключенным до завершения процедуры сохранения базы данных пользователей. Только в таком варианте редактор ПРД может точно определить соответствие логического диска, под которым отображается съемное устройство 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.

Программа-редактор *«Редактор прав доступа»* позволяет администратору БИ сформировать список USB-устройств, с которыми разрешено работать данному пользователю. По умолчанию для обычных пользователей в список объектов включена запись «`USB Vid=* Pid=* Sn=* – Allowed all USB devices!`». Это означает, что любое USB-устройство разрешено для доступа. Если для пользователя не предусмотрен доступ к произвольному USB-устройству, то эту строчку из списка объектов доступа необходимо удалить и назначить конкретные устройства, к которым будет разрешен доступ. Для выполнения данной операции нужно в окне редактирования правил доступа пользователя (рис. 6) щелкнуть мышью по клавише [USB]. Откроется окно редактирования списка USB устройств (рис 9).

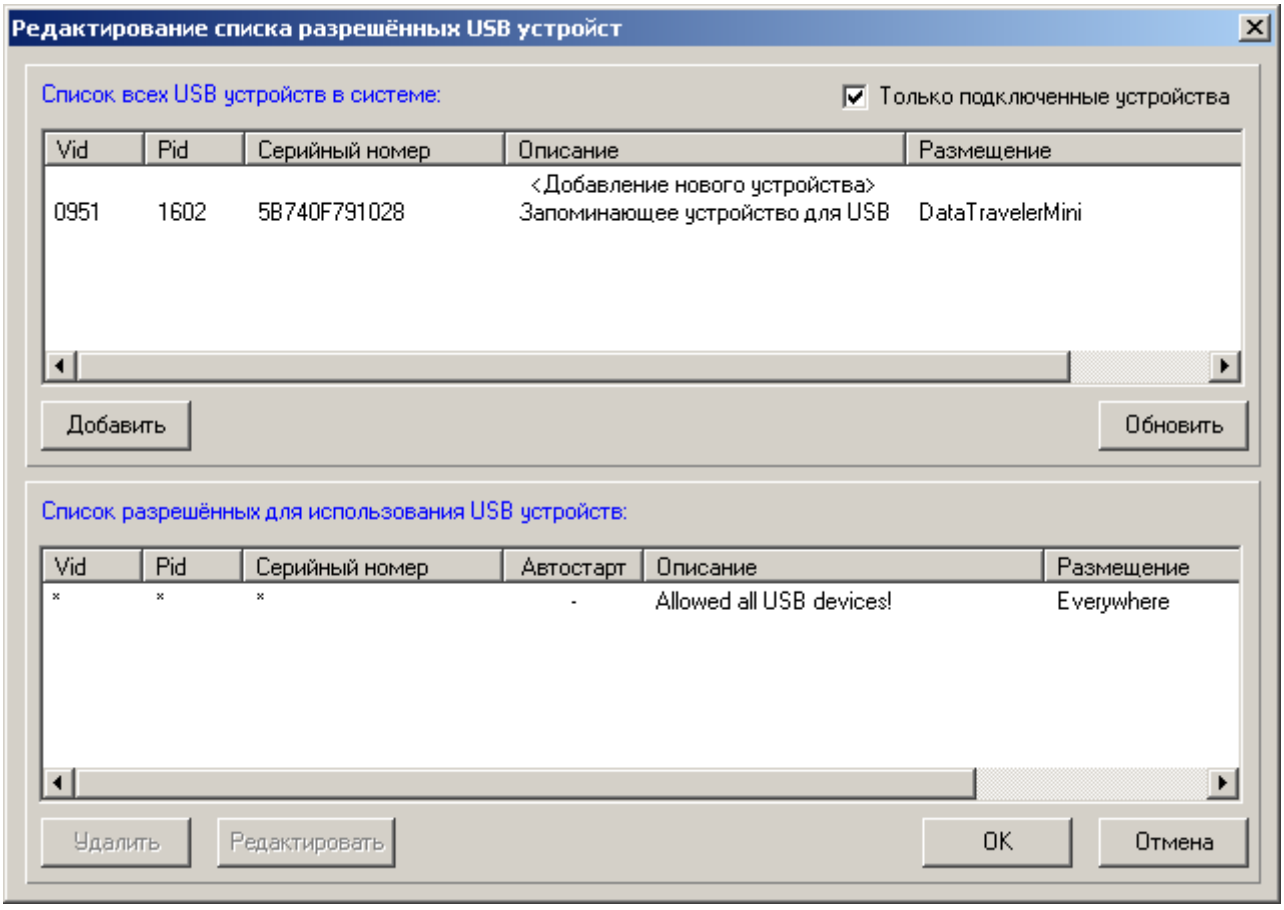

Рис. 9.

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 требующегося устройства, необходимо щелкнуть мышью по кнопке «Обновить». По этой команде выполняется поиск подключенных USB-устройств и они появляются в верхней половине окна в списке устройств.

Для того, чтобы разрешить данному пользователю доступ к устройству, необходимо установить на данное USB-устройство курсор в верхнем списке, нажать кнопку «Добавить», после чего оно появится в нижней половине окна в списке разрешенных для использования. Включение нескольких устройств осуществляется повторением операции выбора и добавления устройств.

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.

Если USB-устройство – это съемный диск (USB Flash, Zip, Floppy, сменный HDD), 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.

При наличии на ПК клавиатуры и мыши, подключенных по USB, для нормальной работы нужно добавить их в список разрешенных USB-устройств.

Установка детальности протокола работ пользователей.

Во время каждого сеанса работы пользователя ведется журнал регистрации событий, в котором отображаются действия пользователя, прикладного и системного программного обеспечения. Администратору БИ 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.

Уровень детальности протокола работы пользователей задается в списке, раскрывающемся по щелчку мыши, который расположен в поле «Детальность журнала» главного окна программы *«Редактор прав доступа»* (рис. 1).

Для выбора доступны следующие уровни детальности:

- «Нет» – регистрируются только вход в систему / выход из системы.
- «Низкая» – регистрируются вход в систему / выход из системы, а также попытки несанкционированного доступа, запуск задач.
- «Средняя» – то же, что и при низкой детальности, а также регистрируются операции доступа к файлам и каталогам.
- «Высокая» – то же, что и при средней детальности, а также регистрируется выполнение функций просмотра каталогов.

Работа с журналами регистрации событий осуществляется при помощи программы *«Просмотр журнала событий»*, входящей в набор специального программного обеспечения комплекса «Аккорд». Доступ к работе с программой предоставляется только администратору БИ, либо субъектам, наделенным правами супервизора.

Для каждого сеанса работы пользователя создается отдельный файл журнала. Имя данного файла генерируется с помощью системной даты, времени и некоторой случайной компоненты (для исключения совпадения имен различных файлов журнала).

Контроль целостности.

Комплекс «Аккорд» позволяет контролировать целостность файлов по индивидуальному списку, созданному администратором БИ для каждого пользователя. Установка контроля целостности возможна только для пользователей, которые имеют ТМ-идентификатор с памятью.

Предусмотрены два режима контроля: «статический» и «динамический». В «статическом» режиме осуществляется контроль целостности файлов, расположенных на жестком диске в момент начала сеанса работы пользователя, а также производится обновление контрольных сумм при завершении сеанса работы пользователя. «Динамический» режим – это контроль исполняемых модулей перед их загрузкой в оперативную память ПК.

Для создания списка контролируемых файлов необходимо нажать кнопку ([...]), расположенную справа в поле «Контроль целостности» главного окна программы *«Редактор прав доступа»* (рис. 1). На экран будет выведено окно «Контроль целостности файлов» для указанного пользователя (рис. 10).

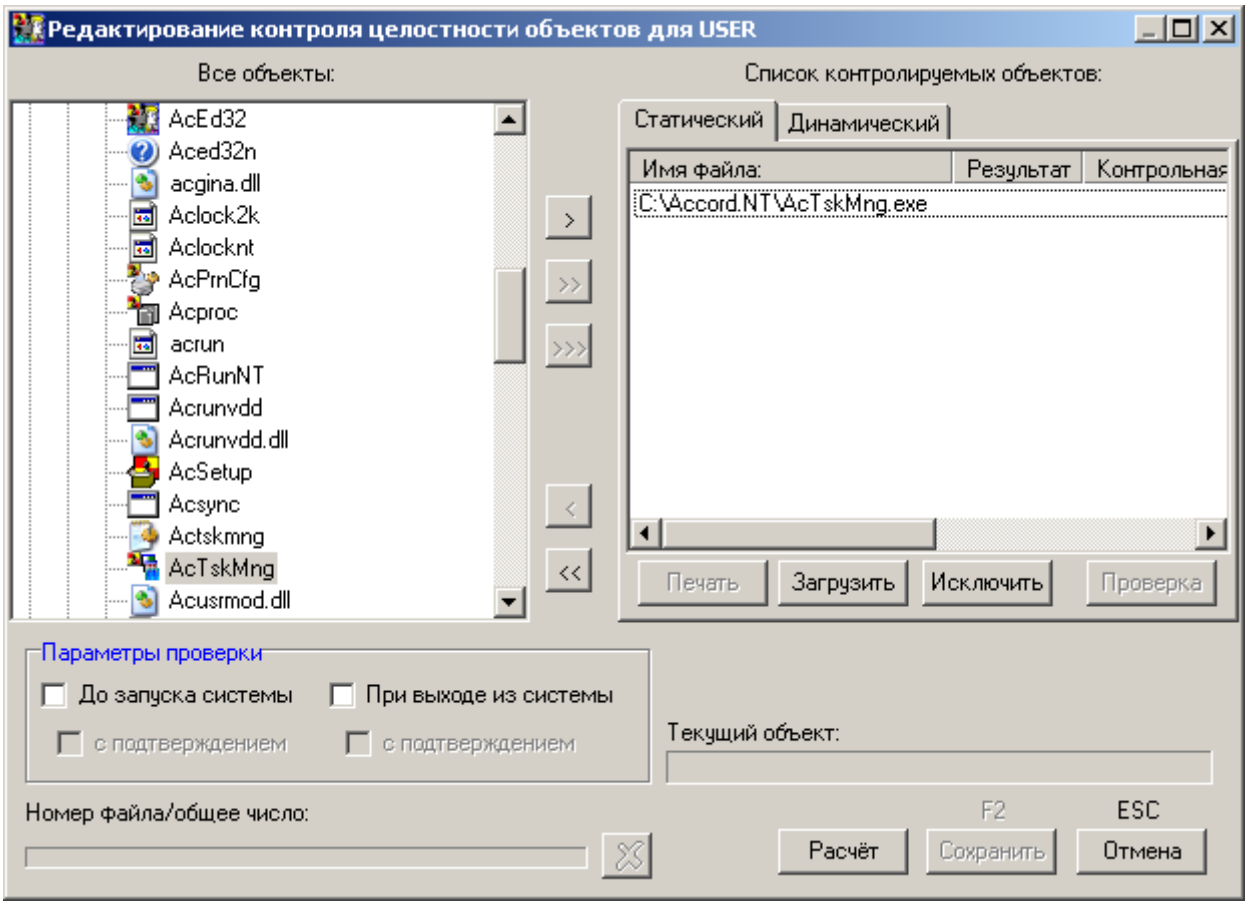

Рис. 10.

При «статическом» контроле целостности файлов необходимо сформировать список тех файлов, для которых будет рассчитана контрольная сумма (хэш-функция). Возможен выбор отдельного файла, или всех файлов из указанного каталога. Далее для выбранных файлов производится установка режимов контроля целостности (осуществляется установкой флагов в нижней панели окна (рис. 10)). Возможны следующие варианты:

- «До запуска системы» – контроль целостности до запуска операционной системы.
- «С подтверждением» – запрос подтверждения контроля целостности до запуска операционной системы (пользователь может отказаться от выполнения процедуры контроля).
- «При выходе из системы» – обновление хэш-функции после завершения сеанса работы пользователя.
- «С подтверждением» – запрос подтверждения обновления хэш-функции после завершения сеанса работы.

Операция формирования списка файлов для «статического» контроля целостности завершается расчетом хэш-функции контролируемых файлов, запуск которого осуществляется при нажатии кнопки «Расчет». В процессе расчета запрашивается ТМ-идентификатор данного пользователя. В алго-

ритме расчета используется секретный ключ, записанный в ТМ-идентификатор при регистрации пользователя. Тем самым исключается возможность подделки результирующей хэш-функции при несанкционированном изменении файлов. Расчет хэш-функции производится только при установленных режимах контроля целостности (должен быть установлен хотя бы один флаг).

«Динамический» контроль целостности файлов выполняется при каждом запуске процесса (исполняемого модуля). Со списком файлов для динамического контроля целостности, который находится в окне «Контроль целостности файлов» (рис. 10), можно работать так же, как и со «статическим», но не требуется задания параметров контроля.

10. ПРИМЕРЫ ПРД И ИХ РЕАЛИЗАЦИИ

Правила разграничения доступа (ПРД), приведенные в настоящем разделе, служат лишь примерами использования атрибутов доступа, а не полным описанием политики безопасности. В каждом конкретном случае администратор БИ должен описывать реальные ресурсы ПК.

Будем считать, что физический жесткий диск компьютера разбит на два логических диска. Программные средства в основном размещены на диске `C:`. На диске `D:` размещены каталоги, доступ к которым могут иметь разные пользователи.

10.1. Пользователю разрешен доступ для работы в каталоге `D:\DOC`

В этом случае ПРД для пользователя должны содержать следующий перечень атрибутов:

Права доступа

```
D:\                    [R     V   GX S ]
D:\DOC\                [RWCDNVMEGX   0]
D:\TEMP\               [RWCDNVMEG    0]
```

Пояснения: при этом весь диск `D:\` доступен только для чтения, каталог `D:\DOC\` доступен полностью.

К каталогу `TEMP` (при его наличии) следует всегда задавать полный доступ, за исключением, разве что, запуска программ – часто он требуется для размещения временных файлов прикладных задач.

10.2. Пользователю на диске будут видны и доступны только явно описанные каталоги

Права доступа

```
D:\                     [RWCDNVMEGX 0]
D:\DOC\                 [RWCDNVMEGX 0]
D:\TEMP\                [RWCDNVMEG S ]
```

Корневой каталог описан без наследования прав доступа. Именно такой вариант ПРД предоставляет пользователю доступ только к явно описанным каталогам и файлам – остальные ресурсы недоступны и невидимы из любых файловых оболочек.

Обратите внимание – при таких атрибутах видны и доступны файлы, размещенные в корневом каталоге диска `D:`. Для того чтобы эти файлы были недоступны пользователю, из описания корневого каталога нужно удалить атрибут "`V`".

10.3. Разрешено работать только с файлами и только в выделенном каталоге

В этом случае пользователю необходимо запретить запуск задач, создание и удаление подкаталогов.

Права доступа

```
D:\                     [RWC  VMEGX 0]
D:\DOC\                 [RWCDNV  G  0]
D:\TEMP\                [RWCDNVMEG S ]
```

Создать каталог можно, но при работе с ними будут возникать трудности – по крайней мере, до тех пор, пока администратор БИ не установит вновь созданным каталогам необходимые атрибуты.

10.4. Применение атрибутов наследования

Для устранения трудностей при работе с подкаталогами для разрешенного каталога устанавливается атрибут наследования прав доступа.

Права доступа

```
D:\                     [RWC  VMEGX 0]
D:\DOC\                 [RWCDNVMEG S ]
D:\TEMP\                [RWCDNVMEG S ]
```

11. ЗАДАНИЯ

Задание 1. Разобрать контрольный пример из раздела 10 (по вариантам).

Задание 2. Реализовать политику разграничения доступа «Конфиденциальное делопроизводство» по следующей схеме.

Создать пользователей `User1` и `User2`. Создать домашние каталоги `D:\U1` и `D:\U2` соответственно для пользователей `User1` и `User2`.

В корневом каталоге диска `D:` пользователям видны только каталоги для работы с документами («домашние» и «обменные»).

Варианты организации документообмена:

1. Пользователь `User1` передает документ(ы) пользователю `User2` через каталог `D:\FROM_U1`. Пользователь `User2` передает документ(ы) пользователю `User1` через каталог `D:\FROM_U2`. При этом пользователи не имеют права создавать и модифицировать файлы в каталоге, через который им поступают документы.
2. Пользователь `User1` получает документ(ы) с USB флэш-диска и передает (возможно, обработав) пользователю `User2` через каталог `D:\FROM_U1`. Пользователь `User2` не имеет права создавать и модифицировать файлы в каталоге `D:\FROM_U1`.
3. Пользователь `User1` готовит документ(ы) и передает их пользователю `User2` через каталог `D:\FROM_U1`. Пользователь `User2` обрабатывает документ(ы) и записывает их на флэш-диск. При этом `User2` не имеет права копировать файлы с данного флэш-диска.

Задание 3. Разработать набор испытаний реализации ПРД из задания 2.

Построить таблицу испытаний следующего вида:

Действия	Проверяемое правило	Результат
Попытка пользователя `User1` создать файл в каталоге `D:\FROM_U2`	Запрет пользователю `User1` создавать и модифицировать файлы в каталоге `D:\FROM_U2`	Файл не создан *Соответствующая запись из журнала сеанса пользователя*

В колонке результат привести записи журнала, регистрирующие произведенные действия.

Задание 4. Исследовать содержимое журналов комплекса «Аккорд». Выделить в них сеансы работы всех пользователей системы. Детально описать один сеанс любого пользователя.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Основы информационной безопасности. Учебное пособие для вузов. / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия - Телеком, 2006.

2. Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». – М.: Радио и связь, 1999.

3. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения». – М.: ГТК РФ, 1992.

4. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». – М.: ГТК РФ, 1992.

5. Руководящий документ Гостехкомиссии России «Средства вычислительной техники защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». – М.: ГТК РФ, 1992.

Александр Александрович **Горбунов**
Леонид Юрьевич **Ротков**
Аркадий Анатольевич **Рябов**

ЗАЩИТА ОТ НСД С ПОМОЩЬЮ ПАК «АККОРД»

Учебно-методическое пособие

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Нижегородский государственный университет им. Н.И. Лобачевского».
603950, Нижний Новгород, пр. Гагарина, 23.