**В.М.ЗИМА, А.А.МОЛДОВЯН**

# ТЕХНОЛОГИЯ ПРАКТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Утверждено в качестве учебного пособия***

***ВОЕННАЯ ИНЖЕНЕРНО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО***
**Санкт-Петербург - 1997**

**ББК 32.973**
**З-40**
**УДК [681.324+681.3.067] (075.8)**

Зима В.М., Молдовян А.А. Технология практического обеспечения информационной безопасности: Учеб. пособие. - Спб, 1997. - 118 с.

Излагаются общие принципы применения системы защиты «Кобра» для обеспечения безопасности обработки и хранения информации в компьютерных системах. Приводится классификация схем и уровней защиты, реализуемых системой. Рассматриваются основные способы разграничения доступа пользователей к компьютерным ресурсам, а также меры противодействия обходу системы защиты. Описываются приемы использования системы защиты по обеспечению эталонного состояния рабочей среды компьютера. Рассматриваются способы регистрации действий пользователей, а также особенности реализации других функций по защите информации.

Для курсантов и слушателей академии, специализирующихся в областях, связанных с защитой информационно-программного обеспечения, а также всех пользователей компьютерных систем, заинтересованных в безопасности хранения и обработки данных.

Рецензент: В.Н.КУСТОВ, доктор технических наук, профессор

# СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Современный этап развития человечества характеризуется появлением большого количества новых угроз, порождаемых интенсивным распространением и совершенствованием компьютерных технологий.

Перед построением любой системы защиты должны быть четко осознаны цели, определяющие что и от чего необходимо защищать для обеспечения безопасности людей.

Действия людей основаны на переработке информации. Вычислительные же системы предназначены для автоматизированной обработки и хранения больших объемов данных. Поэтому становится понятным, что информация, хранящаяся в вычислительных системах, а также процесс ее обработки, реализуемый компьютерными программами, должны быть надежно защищены. Информацию следует защищать от хищения и потери, а программы - от сбоев и отказов.

В соответствии с целями процесс защиты информационно-программного обеспечения вычислительных систем (ИПО ВС) должен обеспечивать поддержку конфиденциальности и целостности информации, а также надежности программ.

**Конфиденциальность данных** предполагает их доступность только для тех лиц, которые имеют на это соответствующие полномочия.

Под **целостностью информации** понимается способность обеспечивать ее неизменность (физическую целостность) и непротиворечивость (логическую целостность) в процессе хранения и обработки данных.

**Надежность программных средств** предполагает точное и своевременное выполнение ими всех своих функций. Для надежной обработки данных необходимо отсутствие ошибок в программных и аппаратных средствах ВС, что достигается в процессе разработки и сопровождения

соответствующих компонентов. Но следует учитывать, что полное отсутствие ошибок гарантировать невозможно. Поэтому для поддержания надежности программ должны быть предусмотрены функции предупреждения сбоев и отказов, а также оперативного восстановления работоспособности ВС после их возникновения. К таким функциям прежде всего относятся функции резервирования информации и поддержания эталонного состояния рабочей среды компьютера.

Построение любой системы защиты в соответствии с установленными целями осуществляется путем выполнения следующих трех базовых этапов.

1. Анализ структуры и принципов функционирования системы, частью которой являются объекты защиты, и выделение на основе анализа уязвимых элементов данной системы, которые влияют на безопасность защищаемых объектов.
2. Определение и анализ возможных угроз выделенным элементам и формирование перечня требований к системе защиты.
3. Разработка системы защиты в соответствии с предъявленными требованиями.

В основу разработки системы защиты должны быть положены следующие принципы [1]:

- учет требований защиты ИПО при построении ВС и разработке технологии автоматизированной обработки информации;
- комплексность использования средств и методов защиты;
- обеспечение непрерывности процесса защиты.

При защите ИПО ВС необходимо учитывать и то, что высокий уровень безопасности определяется не только потенциальными возможностями защитных подсистем, но и качественным сопровождением системы защиты, которое предполагает:

- периодический контроль правильности функционирования всех подсистем защиты;
- постоянный сбор данных о поддерживаемой безопасности обработки и хранения данных;
- анализ накапливаемых данных и разработка, а также осуществление мероприятий по совершенствованию системы защиты;
- внедрение новых технологий по защите ИПО ВС.

Разработка системы защиты ИПО ВС может выполняться с самого начала без использования каких-либо разработанных ранее защитных средств, а также на основе существующих общесистемных или специализированных средств защиты.

Система защиты, построенная на основе общесистемных программных средств, не обеспечивает необходимый уровень безопасности при повышенных требованиях к защите информации и процесса ее обработки. В этом случае для усиленной защиты необходимо использование специализированных систем.

К одной из наиболее эффективных отечественных специализированных систем информационной безопасности относится система «Кобра». Достижение высокого уровня безопасности информационно-программного обеспечения на основе любой специализированной системы защиты возможно только при детальном знании технологии ее применения. Данное пособие посвящено детальному рассмотрению технологии применения системы «Кобра».

# 1. ОБЩИЕ ПРИНЦИПЫ ПРИМЕНЕНИЯ СИСТЕМЫ ЗАЩИТЫ

## 1.1. Назначение и структура специализированного программного комплекса

Система «Кобра» в рассматриваемой версии предназначена для обеспечения безопасности хранения и обработки информации в персональных компьютерах, функционирующих под управлением операционной системы MS-DOS/ Windows 3.XX.

Программная реализация данной системы информационной безопасности основана на технологии прозрачной защиты [7], согласно которой для пользователя не меняется привычная среда его работы и он не испытывает неудобств, вызванных функционированием защитных средств. Другими словами, система защиты при функционировании является для пользователя невидимой.

Базисом технологии прозрачной защиты, реализованной в системе «Кобра», является метод динамического шифрования конфиденциальной информации, с которой работает пользователь. Конфиденциальная информация, записываемая на внешние устройства, подвергается автоматическому зашифровыванию по ключу, зависящему от пароля пользователя. При считывании санкционированным пользователем эта информация автоматически расшифровывается. Такое динамическое шифрование информации, по причине того, что его не замечает пользователь, называют прозрачным шифрованием или прозрачным криптографическим преобразованием.

В системе «Кобра» реализована технология криптозащиты [5, 6], обеспечивающая повышение как скорости шифрования, так и криптостойкости зашифрованных сообщений.

Повышение скорости шифрования достигается за счет двухэтапной организации процесса криптографических преобразований, а повышение криптостойкости - за счет внесения неопределенностей в процесс шифрования.

Суть двухэтапного процесса криптографических преобразований заключается в выделении в виде самостоятельного модуля процедур настройки резидентной части шифра (см. □). Такая организация делает шифр очень гибким. Например, целесообразно воспользоваться схемой, для которой пользователям достаточно выбирать пароли сравнительно малой длины, а подпрограмма настройки независимо от длины первичного ключа будет осуществлять управляемую паролем генерацию ключевой последовательности достаточно большого размера.

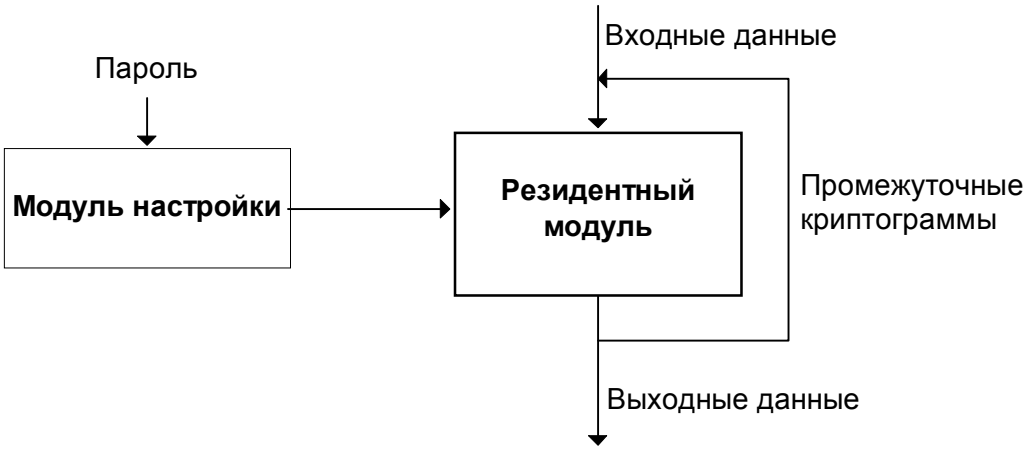


**Рис. 1.1. Обобщенная структура программно-ориентированной криптосистемы**

Идея внесения неопределенностей в процесс шифрования заключается в том, чтобы в подпрограмме настройки предусмотреть управляемые паролем процедуры генерирования алгоритма резидентной подпрограммы. В этом случае криптоаналитику не будет известен конкретный

алгоритм криптографических преобразований, так как для различных паролей алгоритмы шифрования будут отличаться друг от друга.

Комплекс «Кобра» включает в себя семь базовых подсистем защиты, а также вспомогательные подсистемы (см. □).

К вспомогательным относятся следующие подсистемы:

- подсистема затирания, предназначенная для гарантированного уничтожения остаточных данных в областях дисковой памяти;
- подсистема блокировки клавиатуры и монитора, обеспечивающая блокировку устройств доступа к компьютеру по тайм-ауту при оставлении компьютера без присмотра;
- подсистема окончания работы на компьютере, предназначенная для корректного завершения сеанса пользователя, в процессе которого выполняется проверка соответствия состояния операционной среды эталонному и занесение соответствующей записи в журнал учета работ;
- подсистема создания дополнительных логических дисков, позволяющая создать дополнительные логические диски на винчестере с сохранением на нем информации и без его переразбиения утилитой FDISK.


**Рис. 1.2. Структура системы «Кобра» и назначение основных компонентов**

Базовые и вспомогательные подсистемы защиты позволяют установить требуемый режим защищенной обработки данных. Каждому законному пользователю могут быть назначены индивидуальные права дос-

тупа к вычислительным ресурсам и обрабатываемой информации. В рамках предоставленных полномочий пользователи не будут испытывать никаких неудобств. В указанных пределах функционирование системы «Кобра» будет прозрачным, однако все несанкционированные действия будут заблокированы. «Кобра» автоматически контролирует работы, выполняемые на ЭВМ, и ведет их учет.

«Кобра» доступна не только опытному профессионалу, с ней может работать любой пользователь ЭВМ. Даже при сложных нарушениях в работе компьютера данная система защиты поможет пользователю самостоятельно и быстро восстановить исходную рабочую среду. Все широко используемые системы и программы корректно взаимодействуют с системой «Кобра», не приводя к нарушениям в работе. Функционирование системы является прозрачным. При установке всех режимов защиты в полном объеме уменьшение скорости обработки данных не превышает 3%.

## 1.2. Этапы формирования схемы защиты

Основополагающим требованием к реализации защиты информации в вычислительных системах является необходимость комплексного подхода [1], учитывающего всю совокупность требований к защите и влияющих на защиту факторов.

На уровень защиты информации, реализуемый системой “Кобра”, непосредственное влияние оказывают ее используемые компоненты, а также параметры их настройки и режимы функционирования, задаваемые администратором службы безопасности.

Поэтому, основной задачей главного администратора безопасности перед настройкой и использованием системы “Кобра” является определение для каждого компьютера схемы защиты, соответствующей выдвинутым к защите требованиям. Под схемой защиты при этом понимается со-

вокупность используемых компонентов системы “Кобра”, а также параметры их настройки и устанавливаемые режимы функционирования.

Схемы, а также уровни защиты, реализуемые системой “Кобра”, можно классифицировать по следующим базовым признакам:

1) **уровень подтверждения подлинности**, характеризующий стойкость используемого способа аутентификации;
2) **уровень разграничения доступа**, отражающий степень возможной детализации полномочий пользователей;
3) **объем защищаемой информации**, для которого могут определяться наиболее эффективные схемы и уровни защиты;
4) **уровень криптографического закрытия защищаемых данных**, характеризующий криптостойкость используемых способов шифрования;
5) **уровень защиты от обхода системы “Кобра”**, отражающий степень защиты от программных закладок, а также несанкционированного изменения настроек системы защиты и операционной среды;
6) **уровень защиты от компьютерных вирусов**, характеризующий степень защищенности от несанкционированных программ;
7) **уровень защиты от модификации информации**, характеризующий возможности по определению фактов несанкционированной модификации системных и несистемных данных винчестера;
8) **уровень ограничения доступа пользователей к дискетам**, отражающий возможности по ограничению для каждого пользователя числа дискет, которые можно использовать на компьютере;
9) **уровень защиты от несанкционированного доступа к информации при оставлении компьютера без завершения сеанса работы**, отражающий возможности блокировки клавиатуры, мыши и экрана по тайм-ауту;

10) **уровень защиты от доступа к остаточной информации**, характеризующий степень защищенности от хищения остаточной информации на винчестере;

11) **уровень защиты от несанкционированных действий санкционированных пользователей**, отражающий возможности по предотвращению таких несанкционированных действий;

12) **уровень защиты от потери информации**, отражающий возможности по резервированию данных.

В соответствии с каждым из данных признаков могут быть установлены разные схемы защиты. Для формирования конкретной схемы администратор службы безопасности должен выполнить следующие этапы.

1. Изучение положений законодательных актов по защите информации [2 - 4], а также назначения компонентов системы “Кобра”.
2. Определение и уяснение требований к защите на основе выявления и анализа угроз информации в компьютерной системе, для которой приобретена система “Кобра”.
3. Определение требуемых уровней защиты на основе анализа изложенной далее классификации возможностей системы “Кобра” по каждому из выше перечисленных признаков.
4. Систематизация полученной информации и окончательное формирование схемы защиты.

При выполнении третьего и четвертого этапов необходимо учитывать, что эффективная защита должна удовлетворять двум противоречивым требованиям:

- обеспечение надежной защиты информации в компьютерной системе;
- обеспечение удобства работы пользователей на компьютере (отсутствие назойливости со стороны системы защиты, а также других недостатков, мешающих нормальной работе пользователей).

Только в этом случае будет достигнут максимальный эффект от использования компьютерной системы.

После определения схемы защиты администратор службы безопасности может приступить к установке и настройке всех необходимых компонентов системы “Кобра”.

## 1.3. Классификация схем и уровней защиты

### Уровни подтверждения подлинности

Уровень подтверждения подлинности характеризует стойкость используемого способа аутентификации пользователя при его входе в компьютерную систему.

Система “Кобра” для каждого пользователя позволяет реализовать один из следующих уровней подтверждения подлинности:

- ввод пароля с клавиатуры;
- ввод пароля с дискеты;
- вход в систему при условии раздельного ввода независимыми субъектами двух разных паролей.

Каждый следующий уровень из перечисленных является мощнее предыдущего. Первые два реализуются подсистемой санкционирования доступа. Для реализации третьего уровня необходимо использовать еще и подсистему закрытия.

При вводе пароля с клавиатуры его длина может достигать 64 символа, набор которых возможен на трех регистрах, переключаемых с помощью клавиш F1, F2 и F3 (по умолчанию - F1).

Для высокой надежности аутентификации пароли должны быть длинными и нетривиальными. Но чем длиннее и нетривиальнее пароль, тем сложнее его запомнить. Поэтому, при формировании трудно запоминаемого пароля большой длины система “Кобра” позволяет записать его

на дискету и в дальнейшем использовать эту дискету в качестве электронного аутентификатора для подтверждения подлинности пользователя. При использовании такого способа аутентификации администратору службы безопасности необходимо обратить особое внимание на разъяснительную работу среди пользователей о необходимости тщательной сохранности дискет с их паролями от похищения.

Кроме возможности использования электронного аутентификатора “Кобра” с помощью подсистемы закрытия позволяет создать ключевую дискету, без которой загрузка операционной системы на компьютере станет невозможной. В этом случае появляется возможность организации входа в компьютерную систему только при условии раздельного ввода двух разных паролей - пароля, хранящегося на ключевой дискете, и пароля, используемого для подтверждения подлинности.

## Уровни разграничения доступа

Уровень разграничения доступа характеризует степень возможной детализации полномочий пользователей по использованию ресурсов компьютерной системы (областей дисковой памяти, портов ввода-вывода).

Система “Кобра” предоставляет следующие возможности по разграничению доступа пользователей к компьютерным ресурсам:

- ♦ разграничение на уровне логических дисков и портов ввода-вывода, реализуемое подсистемой санкционирования доступа;
- ♦ разграничение на уровне файлов и каталогов, реализуемое подсистемой разграничения доступа к файлам.

Для организации разграничения на уровне логических дисков значительную помощь может оказать подсистема создания дополнительных логических дисков. При наличии свободного пространства на жестком диске данная подсистема позволяет создать дополнительные логические

диски без переразбиения винчестера. Созданные таким образом виртуальные логические диски могут использоваться администраторами для детализации разграничения доступа пользователей к дисковому пространству.

## Влияние объема защищаемой информации

Для достижения высокой эффективности использования системы “Кобра” при определении конкретной схемы защиты необходимо учитывать и объемы защищаемых пользователями данных.

Рассмотрим наиболее удобные возможности системы защиты для малых и больших объемов конфиденциальной информации.

Если объем защищаемых данных конкретного пользователя составляет небольшое количество файлов (например, до 10), или эти файлы легко специфицируются по шаблону (например, *.sec), то для защиты этой информации целесообразно использовать подсистему разграничения доступа к файлам или подсистему файлового шифрования.

При использовании подсистемы разграничения доступа к файлам для защищаемых файлов необходимо установить режим суперзащиты (режим «S»), обеспечивающий прозрачное для пользователя шифрование информации при обращении к этим файлам.

При использовании же подсистемы файлового шифрования пользователю самому следует в начале своего сеанса работы расшифровать, а перед окончанием - зашифровать конфиденциальные данные. Для автоматизации этого процесса можно воспользоваться макроязыком подсистемы файлового шифрования. Перед окончанием сеанса работы необходимо также позаботиться об уничтожении остаточной информации в отведенных пользователю областях жесткого диска с помощью подсистемы затирания.

Если объем защищаемых данных составляет большое количество файлов, размещенных в разных каталогах, то для защиты секретных данных целесообразно использовать возможности подсистемы санкционирования доступа. В этом случае для логического диска с защищаемыми данными необходимо установить режим суперзащиты (режим «S»), обеспечивающий прозрачное для пользователя шифрование информации при обращении к этому диску.

## Уровни криптографического закрытия защищаемых данных

Уровень криптографического закрытия защищаемых данных характеризует криптостойкость используемых способов шифрования.

Система “Кобра” поддерживает **одинарный**, **двойной** и **тройной** уровни криптографического закрытия информации. Каждый следующий из этих уровней дополняет функции предыдущего.

Одинарный уровень криптографического закрытия реализуется одним из следующих способов:

- прозрачным шифрованием информации подсистемой санкционирования доступа или подсистемой разграничения доступа к файлам после задания для логических дисков или файлов с секретными данными режима суперзащиты (режима «S»);
- использованием подсистемы файлового шифрования для шифрования файлов с конфиденциальными данными.

Двойной уровень криптографического закрытия реализуется следующими путями:

- совместным использованием для одних и тех же данных двух перечисленных способов шифрования;
- усилением одинарного уровня использованием подсистемы закрытия для прозрачного шифрования всего пространства жесткого диска.

Тройной уровень криптографической защиты реализуется совместным использованием всех перечисленных способов шифрования.

Необходимо учитывать, что эффективность многоуровневого криптографического закрытия информации будет высокой только в том случае, если для разных уровней заданы разные ключи шифрования (пароли).

Следует также отметить, что в системе “Кобра” поддерживается режим гарантированного шифрования информации при ее записи на дискеты, реализуемый подсистемой санкционирования доступа. Установка такого режима выполняется администратором путем задания в полномочиях пользователя режима суперзащиты для дискет. При установке режима гарантированного шифрования записываемой на дискеты информации администратору следует позаботиться о подготовке требуемого количества дискет для пользователя, так как другими дискетами он воспользоваться уже не сможет.

## Уровни защиты от обхода системы "Кобра"

Уровень защиты от обхода системы "Кобра" отражает степень защиты от программных закладок, а также несанкционированного изменения настроек операционной среды и самой системы защиты, возможных при загрузке с системной дискеты.

Система "Кобра" предоставляет четыре усиливающихся варианта защиты от несанкционированной загрузки с системной дискеты, реализуемые подсистемой закрытия:

**первый вариант** - с прозрачным шифрованием только загрузочного раздела жесткого диска (MBR);

**следующие три варианта** - с прозрачным шифрованием первичного, а при необходимости - расширенного раздела винчестера.

Первый вариант в документации назван защитой **без использования**, а следующие три - **с использованием ключевого диска**.

При установке **защиты без использования ключевого диска** (с шифрованием MBR) после загрузки с системной дискеты жесткий диск будет доступен только в том случае, если загрузка осуществлялась с дискеты, специально подготовленной администратором службы безопасности. Однако, данный вариант не обеспечивает защиту от профессионалов, так как доступ к незашифрованной информации винчестера все-таки возможен, но с помощью низкоуровневых редакторов, и на системном уровне.

Более высокие уровни защиты от несанкционированной загрузки с системной дискеты реализуются **защитой с использованием ключевого диска**, при которой шифруется не только MBR, но и первичный, а при необходимости расширенный разделы винчестера. В этом случае загрузиться с системной дискеты для доступа к винчестеру будет возможно только при наличии сформированного ключа загрузки.

Предусмотрены следующие три усиливающихся варианта защиты с использованием ключевого диска:

- с переносом ключа загрузки с ключевой дискеты на жесткий диск без задания дополнительного пароля загрузки;
- с переносом ключа загрузки с ключевой дискеты на жесткий диск с заданием дополнительного пароля загрузки;
- без переноса ключа загрузки с ключевой дискеты на жесткий диск.

В первом случае для загрузки операционной системы с винчестера, кроме ввода пароля аутентификации, не нужно выполнять каких-либо дополнительных действий, во втором - необходимо ввести дополнительный пароль загрузки, а в третьем - необходимо наличие ключевой дискеты.

При установке последнего варианта защиты загрузиться с винчестера без ключевой дискеты будет невозможно.

## Уровни защиты от компьютерных вирусов

Данный признак классификации схем защиты характеризует степень защищенности компьютерной системы от несанкционированных саморепродуцирующихся программ.

Использование системы "Кобра" совместно с общесистемными программными средствами позволяет реализовать следующие взаимодополняющие уровни защиты от компьютерных вирусов:

**1)** уровень обнаружения факта заражения вирусом и восстановления рабочей среды, реализуемый с помощью подсистемы обеспечения эталонного состояния рабочей среды ПЭВМ;

**2)** уровень анализа на наличие вирусов и восстановления поступающих извне программных средств, реализуемый с помощью доступного детектора-дезинфектора, например, DrWeb или AidsTest;

**3)** уровень защиты от деструктивных действий компьютерных вирусов, реализуемый с помощью доступного фильтра, например, Vsafe, входящего в состав MS-DOS начиная с 6-й версии.

При поддержке первых двух уровней обеспечивается высокая, но не максимальная степень защиты. Максимальной степени защиты от компьютерных вирусов можно достигнуть только при одновременной поддержке всех трех перечисленных уровней.

На **первом уровне** обеспечивается:

- периодическая (при каждой загрузке компьютера и каждом корректном завершении сеанса работы) проверка соответствия текущего состояния рабочей среды эталонному состоянию, сформированному администратором;
- восстановление эталонного состояния рабочей среды при обнаружении несоответствий.

Для данного уровня защиты следует особое внимание обратить на то, чтобы запоминание эталонного состояния рабочей среды выполнялось только после тщательной проверки компьютера детектором-дезинфектором и восстановления его нормального состояния при обнаружении признаков заражения вирусами.

На **втором уровне защиты** администратор должен организовать проверку детектором всех поступающих извне программных средств. Зараженные программы должны быть восстановлены дезинфектором или уничтожены при невозможности восстановления.

В качестве обязательных деструктивных действий, контролируемых фильтром на **третьем уровне защиты**, администратор должен определить следующие:

- низкоуровневое форматирование диска;
- размещение в памяти резидентной программы;
- модификация исполняемого файла (следует учитывать, что некоторые программы могут сами модифицировать содержимое своего исполняемого файла для изменения каких-либо параметров настройки);
- модификация загрузочных секторов винчестера и дискет.

## Уровни защиты от модификации информации

Уровень защиты от модификации информации характеризует возможность по определению фактов несанкционированной модификации системных и несистемных данных винчестера. Этот вид защиты реализуется подсистемой обеспечения эталонного состояния рабочей среды, с помощью которой обеспечивается периодическая (при каждой загрузке компьютера и каждом корректном завершении сеанса работы), а также специально инициируемая проверка заданной текущей информации вин-

честера на соответствие эталонной. Для несистемной информации в качестве эталонных данных используются контрольные суммы.

Предусмотрены следующие функции по определению фактов несанкционированной модификации информации:

- проверка системных данных (содержимого CMOS-памяти, MBR, Config.sys, Autoexec.bat, системных файлов DOS);
- проверка заданных исполняемых файлов;
- проверка заданных файлов данных.

Первые две функции подсистемы обеспечения эталонного состояния рабочей среды используются также для защиты от компьютерных вирусов с целью обнаружения фактов изменения вирусами системных данных и заданных исполняемых файлов.

При организации проверки заданных информационных файлов необходимо учитывать, что после каждого санкционированного изменения этих файлов необходимо обновлять и соответствующую им эталонную информацию (эталонные контрольные суммы).

## Уровни защиты от несанкционированного доступа к информации при оставлении компьютера без завершении сеанса работы

В системе "Кобра" предусмотрена возможность блокировки клавиатуры, мыши и экрана компьютера по тайм-ауту при отсутствии признаков активности пользователя. Кроме того, пользователь может принудительно заблокировать клавиатуру, мышь и экран на время оставления компьютера без присмотра.

После любого способа блокировки вход в систему возможен только после ввода пароля, специально заданного для разблокирования.

Все перечисленные функции реализуются с помощью подсистемы блокировки.

Без использования подсистемы блокировки перед каждым оставлением компьютера необходимо корректно завершить сеанс работы путем активизации подсистемы окончания работ.

## Уровни ограничения доступа пользователей к дискетам

Данный уровень отражает возможности по ограничению для каждого пользователя числа дискет, которые можно использовать на компьютере.

Предусмотрены два варианта по ограничению доступа каждого пользователя к дискетам, реализуемые подсистемой санкционирования доступа:

- ♦ режим ограничения отключен;
- ♦ режим ограничения включен.

Включение режима ограничения осуществляется заданием администратором в полномочиях пользователя режима суперзащиты (режима «S») для накопителей дискет. В этом случае будет осуществляться прозрачное шифрование как системной, так и несистемной информации при обращении к дискетам. В результате станет возможна работа только с теми дискетами, которые специально подготовлены администратором.

## Уровни защиты от доступа к остаточной информации

Уровень защиты от доступа к остаточной информации характеризует степень защищенности от хищения секретной остаточной информации на винчестере.

Общеизвестно, что после удаления файлов средствами MS DOS/Windows обновляется только информация в FAT и соответствующих каталогах. Область данных же на диске остается без изменения до ее затирания другой информацией. Оставшиеся на диске данные после удаления файлов и каталогов называют остаточной информацией.

В системе "Кобра" предусмотрены следующие возможности по защите от доступа к остаточной информации, реализуемые подсистемой затирания:

- полное удаление файловой информации на физическом уровне;
- очистка свободного пространства на диске от остаточной информации.

Администратору службы безопасности необходимо уделить особое внимание на разъяснительную работу среди пользователей о строгом выполнении одного из следующих правил:

- удаление файлов с секретными данными необходимо выполнять только с помощью подсистемы затирания;
- перед окончанием сеанса работы необходимо активизировать подсистему затирания для уничтожения остаточной информации на задействованных в процессе работы логических дисках.

Следует заметить, что если доступ к конфиденциальной информации реализуется в режиме суперзащиты, то открытая остаточная информация не появляется. Поэтому, в этом случае защита от доступа к остаточной информации не нужна.

## Уровни защиты от несанкционированных действий санкционированных пользователей

Данный уровень характеризует возможности системы "Кобра" по недопущению и обнаружению несанкционированных действий санкционированных пользователей. Предоставляются следующие взаимодополняющие функции по поддержке данного уровня защиты:

- регистрация и учет всех заданных действий пользователей различных категорий, реализуемые подсистемой регистрации;

- использование специальной оболочки пользователя, отображающей и предоставляющей пользователям различных категорий только те возможности, которые соответствуют их полномочиям.

Сам факт регистрации является мощным психологическим препятствием для попыток совершения пользователями несанкционированных действий, так как они понимают, что эти действия будут обнаружены. Кроме того, регистрируемые данные значительно облегчают процесс анализа причин случившегося несанкционированного доступа к информации и позволяют оптимизировать используемую политику безопасности, а также схему защиты.

При организации регистрации и учета работ администратор должен обязать всех пользователей корректно завершать свои сеансы работы путем активизации подсистемы окончания работ, так как данная подсистема, кроме запуска процесса проверки текущего состояния рабочей среды компьютера на соответствие эталонному, активизирует процесс отметки в журнале регистрации времени окончания сеанса работы соответствующего пользователя.

Использование специальной оболочки, отображающей и предоставляющей пользователям компьютерные ресурсы, соответствующие пользовательским полномочиям, позволяет скрыть сам факт наличия ресурсов, доступ к которым запрещен, что также оказывает положительное влияние на снижение попыток несанкционированного доступа.

## Уровни защиты от потери информации

Уровень защиты от потери информации отражает возможности по резервированию данных, хранимых и обрабатываемых в компьютере.

Для эффективной защиты от потери информации необходимо обеспечить выполнение следующих функций по резервированию данных:

- ♦ резервирование системной информации (содержимого CMOS-памяти, MBR, Config.sys, Autoexec.bat, системных файлов DOS), реализуемое подсистемой обеспечения эталонного состояния рабочей среды;
- ♦ резервирование несистемных данных (файлов с документами, файлов баз данных, файлов с электронными таблицами и т.д.), реализуемое доступными архиваторами (ARJ, RAR и др.) или встроенными средствами DOS/Windows, например, обычным копированием.

Резервные копии системных данных необходимо сбросить на дискету с помощью подсистемы обеспечения эталонного состояния рабочей среды. С помощью данной подсистемы выполняется и восстановление соответствующей системной информации. На дискете с резервными системными данными обычным копированием необходимо разместить также резервные копии файлов настройки Windows, имеющих расширение .INI, а также .GRP. Файлы Config.sys, Autoexec.bat, *.ini, и *.grp необходимо резервировать после каждого изменения настроек операционной среды с пометкой даты, времени, а также причин их обновления. Старые версии аналогичных файлов в архивах резерва удалять не следует. Такая тактика позволяет значительно ускорить процесс восстановления работоспособности компьютера или ранее используемых параметров его настроек.

Файлы с несистемной информацией можно резервировать как на дискеты, так и на стример.

Администратору службы безопасности необходимо постоянно напоминать пользователям о необходимости резервирования своих данных и обновления архивов после модификации информации перед окончанием сеанса работы. Необходимо также обратить внимание на то, чтобы конфиденциальная информация резервировалась только в закрытом (зашифрованном) виде.

# 2. КОНТРОЛЬ ДОСТУПА К КОМПЬЮТЕРНЫМ РЕСУРСАМ

В системе «Кобра» поддерживаются две модели разграничения доступа к информации:

- ♦ дискреционная;
- ♦ мандатная.

Использование дискреционного принципа позволяет поставить в соответствие каждому субъекту (пользователю) группу объектов (логические диски, элементы файловой структуры и порты ввода-вывода).

Мандатный принцип контроля доступа реализуется применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов. При условиях, сопоставимыми с требованиями, изложенными в руководящих документах ГОСТЕХКОМИССИИ РФ [2-4], субъект может читать объект, осуществлять запись в объект и производить его коррекцию. Для определения санкционированности доступа сопоставляются классификационные метки каждого субъекта (пользователя системы) и каждого объекта (логического устройства), отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам назначаются классификационные уровни (категории конфиденциальности). Система “Кобра” при вводе новых данных в систему запрашивает и получает от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта ему также назначаются в зависимости от уровня доступа классификационные метки.

Основные функции по контролю доступа к компьютерным ресурсам реализуются подсистемами санкционирования доступа, а также разграничения доступа к файлам.

Подсистема санкционирования доступа обеспечивает выполнение функций идентификации и подтверждения подлинности пользователей

при их входе в систему (загрузке операционной системы), а также разграничения доступа пользователей на уровне логических дисков и портов ввода-вывода. Данная подсистема включает следующие компоненты:

- транзитная программа LOGON.EXE, выполняющая функции идентификации и аутентификации пользователей при их входе в компьютерную систему (при инсталляции системы защиты вызов программы LOGON вставляется в начало файла автозапуска AUTOEXEC.BAT);
- драйвер COBRA.SYS, контролирующий доступ к ресурсам и функционирующий в прозрачном для пользователя режиме, за исключением попыток выполнения пользователем несанкционированных действий; при инсталляции системы защиты строка загрузки драйвера COBRA.SYS помещается в файл конфигурации CONFIG.SYS;
- оболочка администратора COBRA.EXE, предназначенная для регистрации пользователей, а также определения и изменения их полномочий.

Подсистема санкционирования доступа поддерживает требуемый режим работы пользователей, разделенных по статусу на четыре группы:

- Суперпользователь, который является главным администратором безопасности;
- Администратор, выполняющий функции администрирования в рамках полномочий, предоставленных Суперпользователем;
- Программист, который в своих полномочиях, определенных администратором, может изменить только пароль для входа в систему;
- Коллега, который не может изменить никакие установки в своих полномочиях.

Общее число пользователей не должно превышать 48. Каждому законному пользователю ЭВМ Суперпользователь или Администратор мо-

жет установить индивидуальные полномочия по доступу к дискам (запрет доступа, только чтение, полный доступ, СуперЗащита (режим «S»)), а также полномочия по доступу к портам ввода-вывода.

Установка режима «S» приводит к включению механизма динамической криптографии. Работа с использованием режима «S» гарантирует секретность информации даже если дискеты, винчестер или сам компьютер будут похищены злоумышленником.

Подсистема разграничения доступа к файлам позволяет детализировать разграничение доступа пользователей к компьютерным ресурсам на уровне файловой структуры. Контроль полномочий пользователей по доступу к файлам и каталогам реализуется резидентным компонентом данной подсистемы - программой LOCK.EXE. Для файлов с секретной информацией, как и для секретных логических дисков, может быть задан режим суперзащиты. У пользователя есть возможность и самостоятельно зашифровать секретные файлы с помощью подсистемы файлового шифрования SAFE.

Результативность разграничения доступа к компьютерным ресурсам в системе «Кобра» значительно повышается при использовании специальной оболочки пользователя US, обеспечивающей интерфейсную поддержку функций разграничения.

## 2.1. Идентификация и подтверждение подлинности пользователей

### *2.1.1. Правила использования паролей*

Пароль применяется для подтверждения подлинности пользователя при входе в компьютерную систему, а также при запуске оболочки администратора безопасности, предназначенной для модификации эталонной информации системы защиты.

Функции идентификации и аутентификации пользователей при их входе в компьютерную систему реализует транзитная программа LOGON.EXE, запускаемая из файла AUTOEXEC.BAT при загрузке операционной системы.

В системе “Кобра” возможно использование следующих вариантов паролей:

- основной пароль;
- основной пароль, перенесенный на дискету.
- дополнительный пароль, сформированный на жестком диске или дискете.

## Основной пароль

Основной пароль используется не только для аутентификации пользователя, но также является ключом для криптографического преобразования информации при установленном режиме прозрачного шифрования (режиме «S»). В этом случае изменение основного пароля приведет к перешифровыванию информации на диске.

Основной пароль может быть длиной от 4 до 64 символов, что соответствует количеству ключей около $10^{100}$.

При вводе пароля можно пользоваться латинским и русским алфавитом, цифрами, специальными символами (!, @, #, ...), клавишами управления курсором, <ESC>, <TAB>, функциональными клавишами F1 - F10. Любая клавиша, нажатие которой приводит к изменениям в окне ввода пароля, будет использована в качестве символа пароля. Клавиши F1, F2, F3 - служат для переключения регистров. По умолчанию установлен F1, что соответствует стандартным клавиатурным кодам. F2 и F3 переключают коды клавиш в другой диапазон и таким образом используются все 256 возможных значений вводимого в данный момент символа па-

роля. С помощью клавиши <BACKSPACE> можно удалять неправильно введенные символы пароля.

Не следует определять тривиальных и коротких паролей. Максимальная длина пароля - 62 символа. Для служебной информации целесообразно использование не менее 9 символов, а для секретной - 15 и более.

Следует учитывать, что при утере пароля данные на диске, для которого установлен режим суперзащиты будут недоступны.

### Основной пароль, перенесенный на дискету

Запись основного пароля на дискету позволяет сформировать электронный аутентификатор. В результате, пользователю для подтверждения подлинности вместо ввода пароля на клавиатуре достаточно будет вставить в накопитель дискету с основным паролем. После формирования электронного аутентификатора необходимо принять особые меры безопасности по обеспечению его сохранности и невозможности несанкционированного копирования файла с паролем.

### Дополнительный пароль

Основное назначение дополнительного пароля - обеспечение группового доступа к диску с Суперзащитой. Для организации группового доступа всем пользователям группы ставится в соответствие единый основной пароль, который будет являться ключом для прозрачного шифрования информации на диске. С целью реализации политики разграничения доступа основной пароль пользователям группы не сообщается, а каждому пользователю группы совместного доступа к диску ставится в соответствие личный дополнительный пароль. Основным паролем владеет только Суперпользователь, распределяющий доступ и устанавливающий режим Суперзащиты.

Суперпользователю необходимо принять особые меры к сохранению в тайне основного пароля группы совместного доступа, так как посредством этого пароля можно получить доступ к информации каждого пользователя группы.

Дополнительный пароль каждого пользователя группы может быть изменен и является действительным только до изменения основного пароля. После изменения основного пароля дополнительный пароль необходимо создать заново.

### *2.1.2. Порядок действий пользователя*

На стадиях идентификации и аутентификации в процессе загрузки операционной системы пользователю необходимо выбрать свой идентификатор из отображаемого списка, нажать клавишу Enter, и далее ввести пароль.

Тип пароля, который запрашивается первоначально, (основной пароль, основной пароль, перенесенный на дискету, или дополнительный) определяется типом пароля, использованного этим пользователем при предыдущем входе в систему. Система автоматически запоминает тип пароля пользователя и использует этот тип при последующем входе. По желанию, после появления окна запроса пароля, нажав клавишу <Esc>, можно перейти в меню для выбора типа пароля или возвращения к стадии идентификации (см. □).

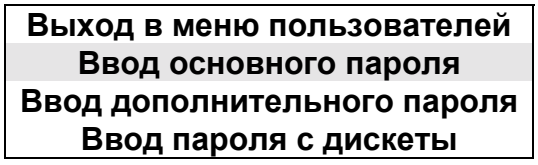


**Рис. 2.1. Меню для выбора типа пароля**

С помощью пункта меню **Выход в меню пользователей** можно вернуться к стадии идентификации, если пользователь по ошибке выбрал

в нем не себя. При необходимости использования электронного аутентификатора (дискеты с основным паролем) следует выбрать пункт меню **Ввод пароля с дискеты**.

Ввод дополнительного пароля возможен только в следующих случаях:

- если ключевая запись о дополнительном пароле создана на одном из логических дисков винчестера;
- если ключевая запись о дополнительном пароле создана на дискете и эта дискета вставлена в дисковод.

Ввод основного пароля с дискеты производится путем выбора пункта меню **Ввод пароля с дискеты**, установки дискеты в соответствующий дисковод и нажатия клавиши <ENTER>.

Следует тщательно оберегать дискеты с зашифрованными файлами дополнительного и основного паролей от несанкционированного копирования, так как эти файлы могут быть легко скопированы даже обычными средствами DOS.

Если при вводе неправильного пароля появится запрос на повторный ввод личного пароля или раздастся звуковой сигнал, свидетельствующий о том, что допустимое число попыток ввода пароля исчерпано, то при появлении запроса необходимо еще раз более внимательно набрать пароль, а при звуковом сигнале сделать перезагрузку машины с помощью кнопки <RESET> и все повторить сначала.

Сразу после инсталляции системы «Кобра» имеется единственный пользователь с идентификатором COBRA и статусом Суперпользователя, для которого в качестве пароля можно просто нажать клавишу <Enter>. После ввода пароля необходимо с помощью оболочки администратора COBRA.EXE, выбрав подменю **Работа со списком,** ввести другое имя Суперпользователя и установить личный пароль. В дальнейшем следует

удалить пользователя COBRA, что избавит от случайного доступа к ЭВМ посторонних лиц.

## 2.2. Управление доступом

Регистрация пользователей и определение их полномочий выполняется администраторами безопасности, имеющими в системе статус Суперпользователя или Администратора. Пользователь, имеющий статус Администратора, может выполнять функции администрирования в рамках полномочий, предоставленных ему Суперпользователем. Для повышения уровня информационной безопасности не рекомендуется определять более одного администратора со статусом Суперпользователя.

Для регистрация пользователей и определения их полномочий предназначена специальная оболочка администратора COBRA.EXE. После запуска данной оболочки необходимо, как и при входе в систему, выбрать свой идентификатор и ввести пароль.

При условии успешной аутентификации появляется главное меню администратора (□).

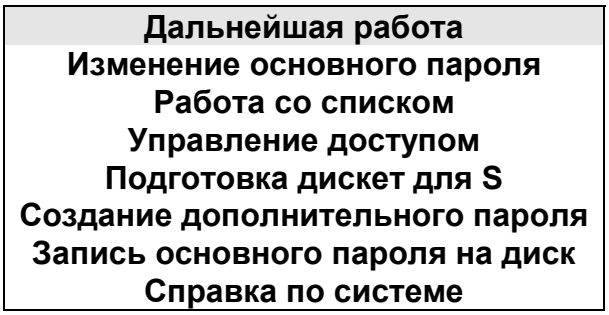


**Рис. 2.2. Главное меню администратора**

При выборе элемента меню **Дальнейшая работа** завершается работа с оболочкой администратора и происходит выход в среду операционной системы с сохранением измененной эталонной информации по разграничению доступа. Пункт меню **Справка по системе** позволяет вос-

пользоваться справочной информацией. Остальные пункты меню рассмотрим более детально.

### *2.2.1. Изменение списка и характеристик пользователей*

Для регистрации новых пользователей, определения и изменения их идентификаторов, статуса, модели контроля доступа, а также удаления эталонных данных пользователей из системы предназначена команда главного меню администратора **Работа со списком**. При вводе этой команды становятся доступными следующие подкоманды (□).

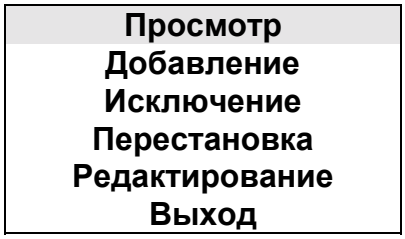


**Рис. 2.3. Меню для работы со списком пользователей**

**Просмотр** - получить список всех пользователей, которые имеют доступ к системе.

**Добавление** - регистрация нового пользователя, при которой определяются следующие характеристики (□):

- ♦ имя (идентификатор) пользователя;
- ♦ статус пользователя (Суперпользователь, Администратор, Программист, Коллега):
  - ⇒ СУПЕРПОЛЬЗОВАТЕЛЮ доступны все действия в системе.
  - ⇒ АДМИНИСТРАТОРУ доступны все возможности в рамках полномочий, определенных суперпользователем;
  - ⇒ ПРОГРАММИСТ может изменить свой личный пароль;
  - ⇒ КОЛЛЕГА имеет право только на доступ к установленным ресурсам ЭВМ;
- ♦ режим мандатного доступа (включен или отключен);
- ♦ режим блокировки комбинации клавиш CTRL+C, CTRL+Break:

⇒ включен - с помощью данных комбинаций клавиш можно прервать выполнение программ;

⇒ выключен - комбинации клавиш блокированы.

**Редактирование пользователя**

**Имя**
**Статус** *(коллега)(программист)(администратор)(суперпользователь)*
**Мандатный доступ** *(выключен)(включен)*
**CTRL/C** *(выключен)(включен)*

**Рис. 2.4. Окно регистрации и изменения характеристик пользователя**

При установке режима “Мандатный доступ - выключен” производится распределение доступа в соответствии с дискреционным принципом.

При установке режима “Мандатный доступ - включен” производится распределение доступа в соответствии с мандатным принципом. Пользователю определяются права доступа (см. □).

**Права доступа пользователя**

**Информация** *(неконфиденциальная)(конфиденциальная)*
**Коррекция доступа** *(нет)(да)*

**Рис. 2.5. Окно определения мандатных прав доступа**

Если пользователю устанавливается “Информация - неконфиденциальная”, то он может работать только с незащищенной информацией (диски, не имеющие режима Суперзащиты). Если устанавливается “Информация - конфиденциальная”, то пользователь получает доступ по чтению ко всем незащищенным дискам, а также полный доступ к тем защищенным дискам, к которым имеет доступ регистрирующий его администратор. Кроме того, в этом случае отсутствует доступ пользователя к портам ввода-вывода. Сформированные правила доступа можно дополнительно ограничить, установив режим “Корректировка доступа - да”.

Команда **Исключение** позволяет удалить лишних пользователей из системы. При выборе этого элемента отображается список идентификаторов всех пользователей. Для удаления пользователя необходимо выбрать его идентификатор и нажать <Enter>. Следует иметь в виду, что нельзя удалить:

- первого в списке пользователя;
- самого себя, т.е. того, кто вошел в систему и работает со списком;
- пользователя с более высоким статусом, чем работающий со списком.

Для удаления первого в списке пользователя необходимо сделать перестановку идентификаторов в списке с помощью команды **Перестановка**.

Следует также учесть, что при удалении пользователя, имеющего диски с режимом суперзащиты, информация на этих дисках станет недоступной для других пользователей. Перед удалением такого пользователя следует с помощью команды главного меню администратора **Управление доступом** (□) снять режим “S” со всех дисков, принадлежащих удаляемому пользователю.

Команда **Перестановка** позволяет менять порядок идентификаторов пользователей в списке. Для этого необходимо после выдачи данной команды выбрать два имени для перестановки, после чего система сама их поменяет.

С помощью команды **Редактирование** можно изменить характеристики пользователей, определяемые при их регистрации с помощью команды Добавление (см. □).

Команда **Выход** позволяет закончить работу со списком пользователей и выйти в главное меню администратора.

### *2.2.2. Формирование и изменение паролей*

Для изменения и формирования своего основного пароля или основного пароля пользователя более низкой категории предназначена команда главного меню администратора **Изменение основного пароля**.

Формирование электронного аутентификатора (дискеты с основным паролем) выполняется с помощью команды **Запись основного пароля на диск**.

Для создания дополнительного пароля необходимо выполнить следующие действия:

**1)** выполнить из главного меню администратора команду **Создание дополнительного пароля**;

**2)** указать диск, на который будет помещен дополнительный пароль (это может быть как жесткий диск, так и дискета);

**3)** ввести на запрос дополнительный пароль.

На указанном диске будет создана зашифрованная ключевая запись в файле COBRA.ALT, определяющая введенный дополнительный пароль. Войти в систему с дополнительным паролем можно будет только при наличии соответствующей ключевой записи в файле COBRA.ALT. При размещении ключевой записи о дополнительном пароле на дискете эта дискета не должна быть защищена режимом суперзащиты.

Если ключевая запись о дополнительном пароле создана на дискете, то при передаче этой дискеты на хранение второму лицу появляется возможность входа в систему только при наличии двух пользователей (“Сейф с двумя ключами”): один пользователь владеет ключевой дискетой и устанавливает ее в накопитель, а второй знает и вводит дополнительный пароль.

### *2.2.3. Определение и изменение полномочий пользователей*

Для определения и изменения прав доступа пользователей к логическим дискам винчестера, дискетам, последовательным и параллельным портам предназначена команда главного меню администратора **Управление доступом** (см. □). После ввода этой команды на экране появляется список идентификаторов всех пользователей компьютера. Для изменения полномочий доступа конкретного пользователя необходимо выбрать его имя и нажать <Enter>. В результате на экране появится окно, представленное на □.

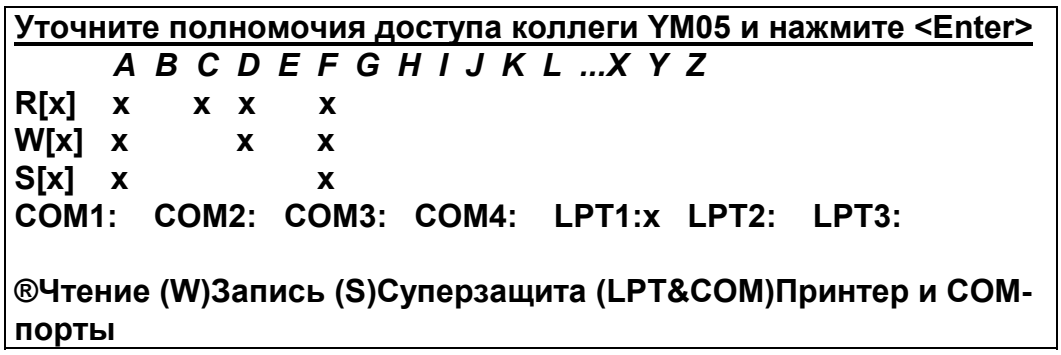


**Рис. 2.6. Окно определения полномочий пользователя**

В верхней строке отображены имена всех возможных приводов для дискет и логических дисков. Отдельными цветами выделены реально существующие приводы, включая приводы для RAM-дисков. Символы “R”, “W”, “S” означают соответственно:

R - чтение с данного диска;

W - запись на данный диск;

S - суперзащита.

Знаком “x” отмечается наличие для рассматриваемого пользователя (в данном случае - коллеги YM05) соответствующих прав доступа к диску или порту. Перемещение указателя от диска к диску и от функции к функции производится с помощью клавиш управления курсором, установка или снятие осуществляется клавишей “Пробел”.

Так, в приведенном выше примере пользователю YM05, имеющему статус “коллега”, разрешен доступ:

- к диску C: - только на чтение;
- к диску D: - на чтение и запись;
- к дискам A: и F: - на чтение и запись с установкой Суперзащиты.

К остальным дискам у данного пользователя доступ отсутствует. Кроме того, ему запрещен доступ к последовательным портам и разрешен доступ только к одному (первому) параллельному порту.

При установке полномочий доступа следует иметь ввиду, что нельзя установить пользователю разрешение на запись на какой-либо диск, не разрешив ему чтение с этого диска (система не даст этого сделать).

Режим “S” требует пояснения.

Каждый пользователь имеет право устанавливать режим Суперзащиты только себе. Исключением здесь является случай, когда Суперпользователем организуется режим совместного доступа к логическому диску, защищенному режимом «S».

При установке режима ”S” производится преобразование информации в соответствии с паролем установленным для данного пользователя. При этом остальные пользователи не будут видеть этот диск. Чтобы другой пользователь мог работать с этим диском, у него также должен быть установлен режим “S” для этого диска и должен совпадать основной пароль. Однако это не означает, что указанные пользователи должны работать с одним паролем. Каждому из пользователей выделяется свой индивидуальный дополнительный пароль, основной пароль знает только Суперпользователь, который распределяет доступ.

Для возможности работы с диском с установленным режим «S» из среды Windows, для данного диска с помощью **Панели управления** должен быть установлен 16-разрядный режим доступа.

Если режим “S” установлен для дискеты, то для работы с информацией на дискете с установленной Суперзащитой необходимо соблюдение одновременно трех условий:

- компьютер, на котором производится считывание информации, оснащен системой “КОБРА”;
- пользователь владеет паролем (знает или имеет дискету с ним), по которому зашифрована информация на дискете;
- пароль входа пользователя в систему должен соответствовать основному паролю, по которому зашифрована информация на дискете.

Установив в окне определения полномочий пользователей режим “S” по доступу к какому-либо логическому диску необходимо будет ответить на запрос системы (см. □).

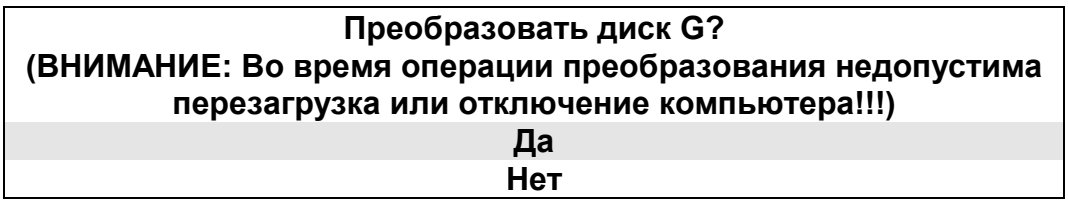


**Рис. 2.7. Окно запроса на зашифровывание информации на диске**

При ответе “Да” будет произведено криптографическое преобразование данных на диске и информация на нем станет доступна только пользователю этого диска. Остальные же пользователи с этого момента доступ по чтению и записи к данному диску потеряют, даже если он раньше у них и был доступен без режима “S”.

При ответе “Нет” пользователь диска, как и остальные, потеряет доступ к информации на диске (если только криптографическое закрытие этого диска и с данным паролем не было произведено ранее). Диск заблокируется. Для того, чтобы разблокировать данный диск необходимо повторно выполнить команду **Управление доступом,** снять для пользо-

вателя этого диска режим “S”, и на запрос системы “Снять защиту с диска ..?” ответить “Нет” (он не был закрыт ). В этом случае информация на диске станет доступна пользователям в обычном режиме (без закрытия) в соответствии с их полномочиями.

Если устанавливается режим “S” на логический диск, который уже защищен для другого пользователя режимом суперзащиты по другому основному паролю, то режим “S” не будет установлен и на экран будет выведено соответствующее сообщение (□).

**Режим S на диске G: уже установлен**
**у пользователя “NNN”**
**Не может быть двух пользователей**
**с разными базовыми паролями и суперзащитой**
**на один и тот же диск**

**Рис. 2.8. Сообщение пользователю**

Если необходимо организовать совместный доступ нескольких пользователей к одному диску, защищенному режимом суперзащиты, то перед установкой этого режима суперпользователю следует для всех пользователей данной группы установить один и тот же основной пароль и разные дополнительные. Основной пароль пользователям не должен сообщаться. Для входа в систему каждым из пользователей группы совместного доступа должен использоваться индивидуальный дополнительный пароль.

Следует отметить, что нельзя устанавливать режим суперзащиты для логического диска, который в себе уже содержит или будет содержать виртуальные логические диски с режимом “S”, сформированные с помощью подсистемы создания дополнительных логических дисков (см. п. 4.3). После установки режима суперзащиты для логического диска, содержащего виртуальные логические диски, эти виртуальные логические диски будут недоступны.

Для снятия Суперзащиты необходимо выполнить команду главного меню администратора **Управление доступом**, выбрать требуемый идентификатор пользователя  и убрать отметку режима “S” для выбранного диска. Если пользователь, для которого снимается Суперзащита, последний, имеющий режим “S” для выбранного диска, то следует ответить на запрос системы (□). Если при установке режима “S” применялось преобразование, то необходимо ответить “Да”. Если не применялось, то “Нет”.

Если случайно был удален пользователь, который в момент удаления имел диск с режимом “S”, то необходимо добавить его снова с тем же паролем, установить в его полномочиях на этот диск режим “S” и на вопрос системы “Преобразовать диск ..?” ответить “нет” (он и так уже был защищен). После этого защищенные данные для случайно удаленного пользователя станут доступны снова.

После изменений полномочий доступа к ресурсам компьютера для их сохранения необходимо завершить работу оболочки администратора командой **Дальнейшая работа**.

При установке режима суперзащиты для накопителя на гибких дисках зашифровывание информации на вставленной в накопитель дискете не выполняется. Дискеты должны быть подготовлены администратором с помощью команды главного меню администратора **Подготовка дискет для S** (см. □). Снятие Суперзащиты с гибких дисков может выполнять только администратор.

### *2.2.4. Подготовка дискет, защищенных режимом суперзащиты*

Суперзащита дискеты имеет тот же смысл, что и для диска: данные и программы на дискете будут видимы только по паролю пользователя, которым защищена эта дискета. Пользователю с другим паролем эти данные будут недоступны, так как пароль является ключом к защищенной

информации. Поскольку в режиме суперзащиты на дискете зашифровывается как системная так и несистемная информация, то если для пользователя установлен данный режим, пользователь сможет пользоваться только дискетами, специально подготовленными для него администратором. Таким образом, установка пользователю режима Суперзащиты для гибких дисков позволяет организовать его работу только на заданном подмножестве дискет. Пользователь сможет использовать только подготовленные администратором дискеты с установленной на них Суперзащитой по паролю пользователя.

Для подготовки администратором дискеты, защищенной режимом суперзащиты, следует ранее отформатированную дискету, на которой может храниться информация, вставить в дисковод и выполнить команду главного меню администратора **Подготовка дискет для S** (см. □). В результате будет выдан запрос на ввод пароля (□□).

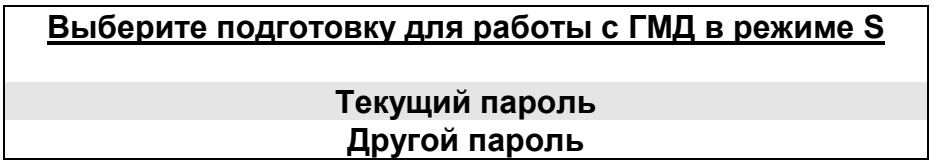


**Рис. 2.9. Запрос на ввод пароля**

После определения пароля необходимо выбрать имя привода для гибких дисков: «A:» или «B:». Далее следует указать требуемое действие (□□).

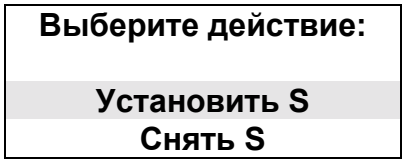


**Рис. 2.10. Запрос на установку или снятие режима суперзащиты**

В результате установки режима «S» вся системная и несистемная информация на дискете будет зашифрована на уровне секторов по указанному ключу (паролю).

## 2.3. Разграничение доступа к файлам

Подсистема разграничения доступа к файлам, названная как подсистема LOCK, предназначена для разграничения доступа пользователей к файлам данных и программ, находящимся на одном компьютере, и для специального назначения действий пользователя, подлежащих регистрации в системном журнале. LOCK поддерживает режим динамического шифрования заданных каталогов и файлов. Подсистема реализована в виде резидентной программы LOKC.EXE, следящей за действиями пользователя и отклоняющей те запросы к операционной системе, которые не соответствуют данным ему правам. Ее предназначение в первую очередь - предотвратить запуск опасных программ неопытными пользователями, так как их неумелое использование может привести к плохим последствиям, вплоть до уничтожения всех данных на жестком диске.

Программа LOCK имеет конфигурационный файл, в котором задаются для всех пользователей права доступа к различным каталогам, файлам, дискам и т. д. В этом файле можно указать имена файлов и директорий, для которых LOCK будет поддерживать режим прозрачного шифрования независимо от места записи в дисковой памяти.

### *2.3.1. Основы реализации разграничения доступа*

Для разграничения доступа пользователей к элементам файловой структуры необходимо включить в AUTOEXEC.BAT строку на вызов программы LOCK.EXE. При этом никакие параметры задавать не следует.

В процессе своей работы программа LOCK перехватывает все запросы по доступу к элементам файловой структуры и разрешает доступ

только в том случае, если характер запроса соответствует полномочиям пользователя, заданным в файле конфигурирования LOCK.CFG.

Для нормальной работы подсистемы разграничения доступа вызов программы LOCK.EXE должен быть вставлен до вызова интерфейсных оболочек MS-DOS, например, Norton Commander, DOS Navigator, Volkov Comander, DOS Shell.

При настройке конфигурации программы LOCK рекомендуется запускать LOCK.EXE с клавиатуры предварительно выгрузив перечисленные выше программы из памяти.

Для выгрузки из памяти программы LOCK.EXE необходимо выдать команду

LOCK.EXE /U

Полномочия пользователей по доступу к элементам файловой структуры задаются в конфигурационном файле LOCK.CFG. Кроме полномочий пользователей, данный конфигурационный файл может содержать параметры настройки, задающие режимы отслеживания действий пользователей.

Конфигурационный файл разделен на несколько разделов. Каждый раздел начинается с описателя раздела, который выглядит как [###], где ### - идентификатор пользователя, которому этот раздел предназначен, или зарезервированное слово COMMON. Раздел COMMON задает права доступа, общие для всех пользователей. Полномочия пользователя внутри соответствующего раздела задаются в виде последовательности строк маски (шаблона).

Формат строки маски:

[path]\FileMask [R][W][D][N][E][S]

Здесь path - путь к файлу или группе файлов. Для сетевых дисков нужно задавать не локальный путь, например, Z:\XYZ, а полное сетевое имя каталога, например, \HOST\UTILITES\DRIVERS\KEYBOARD, иначе

при смене отображения диска сервера с Z: на Y: все права доступа будут утеряны.

Если имя диска не задано (к примеру, \COBRA\), то диск считается всегда совпадающим. Если не задан путь (к примеру, задана строка *.*), то он считается всегда совпадающим.

FileMask - имя и тип файла или маска (шаблон) группы файлов.

Параметры имеют следующие значения:

- R - разрешено чтение файла(-ов);
- W - разрешена запись в файл(-ы);
- D - разрешено удаление файла(-ов);
- N - разрешено переименование файла(-ов);
- E - разрешен запуск файла(-ов);
- S - задать для файла(-ов) режим суперзащиты по текущему паролю.

Режим суперзащиты файла аналогичен одноименному режиму для диска. Информация в файле зашифровывается и расшифровывается в прозрачном для пользователя режиме. Первоначально каталог для размещения файлов, которым определен режим «S», не должен этих файлов содержать. Режим «S» работает только при использовании драйвера COBRA.SYS, являющегося основным резидентным компонентом подсистемы санкционирования доступа, и оболочки комплекса “Кобра”.

Если какой-либо каталог не подходит ни к одной из заданных масок, то этот каталог не будет доступен для поиска файлов (запуск команды DIR не приведет к визуализации каталога). В случае, если заданы глобальные маски без пути все каталоги будут видны, если в этих масках присутствуют символы ‘?’ или ‘*’. Если в глобальной маске нет ни ‘?’ ни ‘*’, то эта маска не будет влиять на видимость каталогов. Например, строка

LPT1 RW

не будет влиять на доступность какого-либо каталога, в то время как

*.* RE

повлечет за собой доступ ко всем без исключения каталогам на всех локальных дисках.

Для сетевых дисков нужно указать, например:

\\SERVER**.* RWDEN

Следует иметь в виду, что сетевое имя может иметь другой формат записи. Для его определения необходимо выдать в командной строке DOS команду TRUENAME.

Недопустимо указывать два пути для файлов или маски в одной строке.

Комментарий в файле конфигурирования LOCK.CFG может размещаться в любой строке, но каждая его строка должна начинаться с символа «;». При этом комментарий может находиться в любом месте строки, например, строка

*c:\dos*.com RWDNE ; Разрешить доступ к MS-DOS файлам*

является правильной, так же как и строки

*; Разрешить доступ к MS-DOS файлам*

*c:\dos*.com RWDNE*

По умолчанию подсистема LOCK исповедует принцип “все, что не разрешено - запрещено”. Однако в некоторых случаях, когда, например, следует разрешить доступ ко всем файлам, кроме некоторых, более удобной может оказаться другая стратегия. В таком случае используется ключевое слово .DEFAULT. Формат команды:

.DEFAULT [R][W][D][N][E][S]

Тем самым устанавливаются те права, которые не подойдут ни к одной из перечисленных масок. По умолчанию работает оператор

.DEFAULT

т.е. не устанавливается ни одного разрешенного действия на те файлы которые не подходят к перечисленным маскам. Никаких ограни-

чений на использование оператора .DEFAULT не налагается - можно использовать его в блоках COMMON, также можно использовать несколько операторов .DEFAULT, при этом каждый новый оператор .DEFAULT полностью отменяет действие предыдущего.

Следует учесть, что в файле конфигурирования особое значение имеет местонахождение раздела COMMON, так как при определении прав доступа к файлу просмотр всех полномочий ведется сверху вниз. Так, например, если в разделе COMMON в начале файла конфигурации определен доступ ко всем файлам на всех дисках только для чтения, то никакие последующие маски уже учитываться не будут, т.к. при определении прав доступа к любому файлу он совпадет с первым же шаблоном (маской).

Поэтому в разделе COMMON в начале файла конфигурации следует избегать неконкретных имен файлов, таких как c:*.*, c:\dos*.com и.т.д. В начале файла конфигурации в блоке COMMON полезно указать права доступа к C:\COMMAND.COM на запуск/чтение, права доступа к интерфейсной оболочке DOS (DN, NC, VC), а все остальное - в разделе COMMON в конце конфигурации. Например, в самом конце можно указать:

*:**.* R

что означает: «Все файлы, не совпавшие ни с одной из вышеперечисленных масок доступны только для чтения».

### *Примечания*

1. Приоритет маски в файле конфигурирования уменьшается по строкам сверху - вниз. Будут работать ограничения для файла по первому подходящему шаблону. Например, если в начале в блоке COMMON указано “C:\FILE1.DAT R”, а в личном блоке - “*:**.* RWDNE”, то FILE1.DAT будет доступен ТОЛЬКО НА ЧТЕНИЕ. Чтобы исключить такие случаи не-

обходимо использовать блоки COMMON в конце конфигурационного файла.

2. Необходимо принять меры, чтобы был соответствующий доступ ко всем требуемым пользователю файлам, например, если будет использоваться NC (Norton Commander), то нужен доступ на чтение/запись/выполнение к C:\NC*.* и т.д.

3. Для использования режима суперзащиты обязательно должен быть загружен драйвер COBRA.SYS. В этом случае реализуется режим прозрачного шифрования для указанного шаблона файлов, за исключением файлов с расширениями EXE и COM.

4. Для шаблонов с режимом суперзащиты не следует разрешать переименование файлов, т.к. с файлов не будет правильно снята защита после смены имени.

5. В блоке COMMON в начале конфигурационного файла следует указать все стандартные потоки DOS (например CON, LPT, AUX и т.д.) с указанием соответствующих прав, иначе эти устройства будут трактоваться как файлы в текущем каталоге с вытекающими правами доступа к ним. Например, если не указан доступ к PRN и находитесь в каталоге с запретом на запись, то файл не удастся распечатать с помощью, скажем, команды COPY <FILE> PRN.

6. В шаблонах доступны стандартные символы для масок файлов - «*» и «?». В качестве диска также можно указывать, как «*», так и «?». Если в пути встречается значок «*», то все символы пути после него игнорируются. Если в имени файла встречается «*», то все символы до точки игнорируются.

7. В одной строке могут встречаться имена более чем одного пользователя. Например, можно указать общий блок для нескольких пользователей начав блок со строки

[User][Administrator][Superuser]

8. При использовании команд APPEND, SUBST, JOIN программа LOCK всегда анализирует настоящее имя файла (т.е. если диск U: является каталогом C:\DN\, то на файлы U:*.* будут те же права доступа что и на C:\DN*.*).

### *2.3.2. Редактирование файла с полномочиями пользователей*

Для редактирования файла LOCK.CFG можно использовать любой доступный текстовый редактор. Для более наглядного редактирования этого файла предназначена программа SETRIGHT.EXE, поставляемая в комплекте с подсистемой разграничения доступа к файлам.

После запуска программы SETRIGHT.EXE на экране появится меню, содержащее названия всех блоков прав доступа в файле LOCK.CFG. Можно прямо здесь добавить новый блок. Для этого внизу меню всегда имеется пустая строка. Кроме того, можно изменить заголовок уже существующего блока.

SETRIGHT может работать максимум с 40 блоками. Для редактирования содержимого блока необходимо выбрать требуемый заголовок и нажать клавишу Enter. На экране появится окно, содержащее имена файлов в текущем каталоге и права доступа к ним.

Для более детального объяснения букв, обозначающих права доступа, следует нажать клавишу F1. Для выделения текущего файла используется горизонтальная полоса отличного от основного цвета, на ней можно заметить область выделенную другим цветом.

Если длинная полоса выделения перемещается с помощью клавиш <↑> и <↓>, то вторая область выделения перемещается с помощью клавиш <→> и <←>. Второй областью выбираются характеристики файла, нуждающиеся в изменении. Если нажать клавишу <Пробел>, то соответствующий атрибут файла инвертируется. Наличие отметки между знаками

«[« и «]» означает, что доступ к данному файлу разрешен. Например, если в столбце R все файлы имеют установленным этот атрибут, это значит что все файлы доступны по чтению.

Все атрибуты файлов разделены на два раздела. В первый раздел входят атрибуты файлов для программы LOCK, а во второй - стандартные атрибуты, используемые операционной системой. Ниже приведен список атрибутов файлов MS-DOS и их назначения.

- ARC - не архивирован. Если этот атрибут установлен это означает, что данный файл подвергался изменениям со времени последнего резервного копирования системной утилитой Backup и некоторыми другими архиваторами. После резервного копирования этот атрибут сбрасывается, однако при первом же изменении файла этот атрибут устанавливается операционной системой.
- R/O - только чтение. Означает что данный файл предназначен только для чтения и в него не может быть произведена запись, а также этот файл не может быть удален. Norton Commander при удалении такого файла дополнительно спрашивает подтверждения на его удаление.
- HDN - скрытый. Файл не будет отображаться на экране при вызове списка файлов командой DIR без ключа /A (в MS-DOS версии 5 и выше).
- SYS - данный атрибут означает что этот файл является системным файлом, используемым операционной системы. Эти файлы также не отображаются на экране командой DIR.
- SHA - SHAREABLE (разделяемый). Этот атрибут имеет смысл только при использовании локальной сети (в частности Novell NetWare) для того чтобы придать этому файлу статус разделяемого ресурса. Это означает что данный файл может одновременно использоваться несколькими пользователями. В частности,

это относится к базам данных. Если же этот атрибут не установлен то этот файл может одновременно использоваться только одним пользователем.

При редактировании масок прав доступа имеются следующие функции.

- <F1> - вызов помощи. На экран выводится список доступных функциональных клавиш и разъяснения атрибутов файлов.
- <F2> - записать измененные маски доступа. Все изменения сбрасываются в файл LOCK.CFG и программа переходит в меню выбора блока масок прав доступа, т.е. туда же где она оказывается после запуска.
- <F3> - просмотреть файл. На экран выводится содержимое файла, отмеченного курсором.
- <F4> - редактирование масок доступа. Можно вручную ввести маски доступа к файлам, а также изменить их порядок. Для этого доступны те же клавиши, что и в меню выбора блока масок. Для изменения порядка следования масок следует выделить маску, которую необходимо передвинуть, и нажать <F6>. После этого, с помощью стрелок вверх/вниз необходимо передвинуть маску на новое место и снова нажать <F6>.
- <F9> - добавить маску в текущий список. При изменении права доступа к некоторым файлам в текущем каталоге, программа setRight пытается подобрать под них подходящую маску и формирует подходящую строку для добавления к уже действующим. Та же функция вызывается автоматически при переходе в другой каталог. Если на предложение отредактировать строку, добавляемую к блоку масок, нажать <Esc>, то строка добавлена не будет.
- <Ins> - выделить/снять выделение с файла.
- <+> - выделить все файлы с тем же расширением, что и текущий.

- <-> - снять выделение со всех файлов, имеющими то же расширение, что и текущий.
- <*> - инвертировать выделение всех файлов в текущем каталоге.

### 2.3.3. Достижение максимальной глубины защиты

Отдельное использование программы LOCK имеет довольно низкую стойкость против опытного пользователя из-за открытой архитектуры системы MS-DOS. Для обеспечения максимальной стойкости системы нужно использовать весь комплекс программ входящих в систему COBRA.

1. Использовать подсистему закрытия (программу MBRinst) для закрытия загрузочного раздела жесткого диска. При этом обеспечивается защита от проникновения в систему в обход CONFIG.SYS и AUTOEXEC.BAT с диска C:

2. Использовать систему LOCK для разграничения доступа пользователей к файлам. При этом пользователям не следует давать доступа к средствам трассировки, отладки и низкоуровневого редактирования (например DiskEdit, Afd, Td, Soft-Ice, Periscope, Debug, Peekpoke), т.е. к программам позволяющим просматривать и изменять содержимое памяти компьютера и системных областей дисков.

3. Защитить необходимо все диски.

4. Для ограничения списка действий, которые может выполнить пользователь, не следует ему позволять работать с командной строкой DOS или оболочкой типа Norton Commander. Необходимо использование специальной оболочки пользователя (US), поставляемой вместе с системой «Кобра».

***Пример файла конфигурации***

```
[COMMON]
.LOG EDNS
```

```
NUL RW
PRN RW
CON RW
AUX RW
LpT1 RW
LpT2 RW

 [Andy]
.LOG
k:\myown\*\*.* RWDES
\\server\bp\*\*.* RWDNE

[User1] [User2]
c:\command.com RE
c:\dos\chkdsk.exe RE
c:\util\q.exe RE
c:\cobra\us\*.* RWE
h:\*\*.* RWDNE
*.t* RWD
*.b* R

 [COMMON]
c:\command.com RE
c:\dos\*.com E
c:\cobra\*.* RWE
c:\dn\*.* RWDE
*:\*\*.* R
```

## 2.4. Принудительное шифрование фрагментов файловой структуры

### *2.4.1. Работа с подсистемой файлового шифрования*

Система «Кобра» обеспечивает как прозрачное, так и принудительное шифрование элементов файловой структуры, реализуемое подсистемой файлового шифрования.

Подсистема файлового шифрования SAFE представляет собой автоматизированное рабочее место (например шифровальщика, администратора или оператора компьютерной сети, администратора или оператора базы данных, криптографа, да и вообще любого пользователя компью-

тера, нуждающегося в надежном засекречивании своей информации) и служит мощным и удобным инструментом для надежного и быстрого зашифровывания и расшифровывания компьютерной информации, начиная с уровня файла и выше (т.е. файл, любая заданная группа файлов, группа файлов в соответствии с заданными масками, каталог, каталог с подкаталогами любого допускаемого DOS уровня вложенности, группа каталогов с подкаталогами, логический раздел диска или дискета).

Подсистема имеет простой, наглядный и удобный интерфейс, не доставляющий трудностей в общении с ней даже начинающему пользователю и легко изучаемый за один сеанс работы. Пользователю же, знакомому с работой оболочки Norton Commander и ей аналогичных, система будет близка и понятна уже с первых минут общения.

Для начала работы с подсистемой файлового шифрования необходимо запустить на выполнение файл SAFE.EXE из каталога COBRA.

После запуска программы SAFE на экран выводятся две файловые панели, подобные файловым панелям оболочки Norton Commander. Первая панель предназначена для отображения зашифрованных файлов, а вторая - для отображения исходных (незашифрованных). Переход между панелями выполняется нажатияем клавиши Tab. Для вызова краткой справки следует нажать клавишу F1. Как и в оболочке Norton Commander, для смены отображаемых дисков в левой и правой панелях используются комбинации клавиш Alt+F1 и Alt+F2. Для смены текущего диска в активной панели можно использовать также комбинацию клавиш Alt+C.

Перед шифрованием (зашифровыванием или расшифровыванием) необходимо задать пароль (ключ шифрования), нажав клавишу F2, и далее выделить требуемые файлы и каталоги. Используемый пароль никаким образом не связан с другими паролями. Он задается сугубо индивидуально для файла или группы файлов, с которыми предстоит работа.

Выделение, а также отмена выделения файлов и каталогов в активной панели выполняется, как и в оболочке Norton Commander, с помощью клавиши INS. Для выделения и снятия выделения по маске предназначены клавиши <+> и <-> в цифровом блоке клавиатуры.

Активизация процесса шифрования выполняется нажатием клавиши F5. При зашифровывании выделенные файлы и каталоги из каталога на правой файловой панели после зашифровывания перемещаются в каталог на левой панели. В процессе расшифровки - наоборот.

Выход из среды программы SAFE выполняется нажатием клавиши F10.

При работе с подсистемой SAFE используются следующие клавиши:

- F1 - помощь;
- F2 - установка текущего пароля для шифрования;
- F3 - просмотр указанного курсором файла;
- F4 - определить маски нешифруемых файлов;
- F5 - активизация шифрования файлов;
- F6 - смена текущего диска;
- F7 - создание нового каталога;
- F8 - удаление указанных файлов и каталогов;
- F9 - измерение скорости шифрования по введенному паролю;
- F10 - выход из программы;
- Alt+F - переключение между полным и сжатым форматом файловых панелей;
- Alt+B - выбор режима сортировки файлов;
- Alt+C - смена диска на текущей файловой панели;
- Alt+R - обновление содержимого файловых панелей.

### *2.4.2. Использование встроенного интерпретатора команд*

Подсистема SAFE имеет встроенный интерпретатор команд, который позволяет автоматизировать часто выполняемые действия пользователя. Встроенный интерпретатор команд представляет собой простой макроязык программирования, дающий доступ ко всем возможностям системы файлового шифрования. Файл для размещения программы на макроязыке встроенного интерпретатора подсистемы SAFE должен быть обычным текстовым файлом с любым расширением. Для запуска на выполнение такого файла следует указать его спецификацию в качестве параметра запуска программы SAFE, например,

SAFE D:\RAB04.SF

Структура командного файла для подсистемы файлового шифрования следующая:

**[заголовок процедуры 1]**

**....**

**....**

**[заголовок процедуры 2]**

**....**

**....**

**[заголовок процедуры N]**

**....**

**....**

Заголовок - это произвольная строка идентификации какого-либо участка программы (название процедуры) для подсистемы SAFE. Из этих заголовков подсистема SAFE при запуске командного файла формирует для пользователя меню с перечнем названий процедур (задач), из которых пользователь может выбрать и запустить нужную. Выбор процедур

осуществляется клавишами управления курсором или нажатием “горячих” клавиш, которые в заголовках помечаются знаком ~ (см. ниже примеры).

Одна программа может иметь много процедур. Пользователю предоставляется право выбрать одну из них для выполнения. Например, файл обеспечивающий конфиденциальность базы данных, может иметь одну процедуру для снятия защищенной страховочной копии на стример, другую - для восстановления базы со стримера, третью - для того чтобы зашифровать эту базу данных прямо на винчестере и т.д. Каждая процедура заканчивается либо началом другой, либо признаком конца файла.

При успешном завершении процедуры подсистема SAFE возвращает управление операционной системе и устанавливает код выхода (errorlevel) в 0. Если же в процессе выполнения процедуры произошла фатальная ошибка, или процесс не выполнился, код ошибки не нулевой. Это позволяет выполнять программу Safe как часть командных файлов (.BAT) операционной системы и, в зависимости от успешного или неуспешного выполнения процедуры, производить те или иные действия.

Каждая процедура состоит из макрокоманд, функция каждой из которых доступна пользователю и посредством диалогового режима подсистемы SAFE.

Между макрокомандами могут располагаться комментарии, ограниченные фигурными скобками ‘{’ и ‘}’. Некоторые макрокоманды имеют аргументы. Аргумент макрокоманды задается в круглых скобках. В качестве аргументов, как правило, используются текстовые строки. Макрокоманды должны быть отделены друг от друга точкой с запятой ‘;’.

Рассмотрим основные макрокоманды встроенного интерпретатора подсистемы SAFE.

**Directory(...);**

Команда служит для выбора каталогов в двух панелях программы SAFE. Аргументами служат одна или две строки, каждая из которых за-

дает путь, по которому будут извлекаться имена файлов для работы. Одна из строк может иметь в начале знак подчеркивания '_'. Это означает, что панель с этим каталогом будет активной (в ней появится курсор).

***Примеры***

*Directory(\ _e:\work\garbage);*

В данном примере левая панель защищенных файлов будет отображать содержимое корневого каталога текущего диска, а правая панель незащищенных файлов, являющаяся активной, - каталог E:\WORK\GARBAGE.

*Directory(e:\);*

Левая панель будет отображать корневой каталог диска E:.

*Directory( _);*

Устанавливает правую панель активной. Здесь аргумент для левой панели пропущен, но разделитель между аргументами (знак пробела) присутствует, иначе аргумент будет воспринят как команда для левой, а не правой панели.

**MkDir(...);**

Команда MkDir аналогична команде MkDir (md) операционной системы MS-DOS, но если при попытке сформировать каталог произошла ошибка (кроме ошибки: "каталог уже существует"), то управление будет передано операционной системе и код выхода будет установлен в 1.

Пример: MkDir(j:\tempdir);

**RmDir(...);**

Данная команда аналогична одноименной команде MS-DOS, за исключением того факта, что, в отличие от команды RmDir операционной системы, команда RmDir подсистемы SAFE уничтожает без запроса подтверждения каталог вместе со всем содержимым, включая вложенные каталоги.

Пример; RmDir(j:\tempdir);

**Select(...);**

Отметить файлы в активном окне. В качестве аргументов могут быть заданы одна или несколько масок файлов которые будут отмечены, например, для шифрования. По умолчанию маски действуют только на файлы. Если же маска предназначена для каталогов, то в ее конце должен стоять символ '\', например, Select(mydir\)

Пример: Select(*.pas left\ right\);

**Unselect(...);**

Аналогична команде Select с точностью до наоборот.

Пример: Unselect(*.* *.*\);

**SetExceptions(...);**

Установить маски файлов-исключений, т.е. тех файлов, которые не будут шифроваться, если они окажутся в отмеченном каталоге или в каталоге еще более глубокого уровня вложенности при шифровании целых каталогов.

Пример: SetExceptions(*.bak; *.exe; *.sys; *.com; *.ovr; *.ovl);

**EnterExceptions;**

Позволяет отредактировать текущую маску исключений. То же самое, что и клавиша F2 в диалоговом режиме.

**InputPassword;**

Запрашивает с клавиатуры пароль для шифрования. Шифрование будет невозможно, пока длина пароля не будет отличной от нуля. Если пароль не был введен, то при команде EncryptFiles (см. ниже) будет запрашиваться пароль до тех пор пока его длина не станет больше нуля.

**EncryptFiles;**

Запускает процесс зашифровывания отмеченных файлов. Зашифровываются файлы из каталога на правой панели в каталог на левой панели. Если директории совпадают, то при зашифровывании файл будет

закрываться непосредственно, т.е. не будет создано архивной копии. Это может оказаться полезным, например, при защите 20-мегабайтной базы данных в случае отсутствия свободного места на диске. Но следует учитывать, что если в процессе зашифровывания процесс будет прерван, например, из-за скачка напряжения в сети, то данные будут навсегда утеряны. Поэтому данным режимом при отсутствии устройства бесперебойного питания следует пользоваться только в крайних случаях.

**DecryptFiles;**

Аналогична команде EncryptFiles, но выполняет обратное преобразование. Если ключ зашифровывания не соответствует введенному ключу расшифровывания, будет выведено предупреждающее сообщение.

**DosCommand(...);**

Запускает на выполнение произвольную программу. Если программа вернет ненулевой код завершения, то процесс будет прерван. Перед запуском программы целесообразно с помощью макрокоманды ChDir (см. ниже) установить текущим каталог, из которого должна запускаться программа.

Пример: DosCommand(arj m -r e:\mywork);

**ChDir(...);**

Устанавливает текущий каталог для запуска программ или команд MS-DOS.

Пример: ChDir(i:\tempdir);

**DeleteFiles;**

Удаляет без запроса подтверждения все отмеченные файлы в активной панели. Подтверждение будет выводится лишь в случае, если отмечены один или несколько каталогов перед удалением каждого из них.

**Message(####);**

где #### - произвольный текст

Выводит сообщение пользователю. Используется, если в процессе выполнения командного файла системы SAFE необходимо вывести какие-либо сообщения оператору (например об установке магнитных носителей).

Пример:

Message(вставьте дискету в дисковод A: и нажмите <Enter>);

**Exit;**

Прекращает выполнение командного файла. Можно использовать эту функцию для отладки командных файлов, когда необходимо временно отключить некоторые команды. Так как все команды после Exit игнорируются, то их можно даже не заключать в скобки комментария ‘{‘ и ‘}’.

## Пример использования встроенного интерпретатора команд

С помощью встроенного интерпретатора команд можно настраивать подсистему “SAFE” на выполнение определенных функций, как показано в приведенном ниже примере.

Пусть необходимо составить программу из макрокоманд подсистемы SAFE для выполнения следующих заданий.

*Задание 1*

а) Заархивировать группу текстовых файлов с расширениями *.TXT, *.DOC из каталога PLAN диска E: в архив на виртуальный диск H:.

б) Зашифровать полученный архив на диске H:.

в) Скопировать защищенный архив с диска H: на дискету.

*Задание 2*

в) Скопировать защищенный архив с дискеты на виртуальный диск H:.

б) Расшифровать архив на диске H:.

а) Извлечь файлы с расширениями *.TXT, *.DOC из архива и поместить их в каталог PLAN на диска E:.

*Задание 3* - завершить работу без выполнения каких-либо функций.

Используя любой текстовый редактор, не создающий служебных символов при формировании текстового файла, опишем эти три задания на языке интерпретатора.

```
[Задание ~1. С оздать архив. Защитить. Скопировать.]
{ В фигурных скобках можно размещать комментарии }
MkDir(H:\tmp);      {Создать временный каталог   }
ChDir(H:\tmp);      {Перейти во временный каталог}
DosCommand(arj a ARHIV E:\PLAN\*.TXT E:\PLAN\*.DOC);      {Запустить архиватор}
Directory(H:\tmp _H:\tmp);      {Установить панели  }
Select(*.*);  {Отметить все файлы }
InputPassword;      {Запросить пароль   }
EncryptFiles;       {Запустить процесс защиты}
Message(установите дискету в дисковод A: и нажми <Enter>);
DosCommand(copyH:\tmp\ARHIV.arj a:\)      {Скопировать архив на диск}
RmDir(H:\tmp);      {Удалить временный каталог   }
{ После выполнения Задания 1  на дискете будет находится защищенный архив с данными каталога PLAN диска E    }
```

```
[Задание ~2. Взять архив. Снять защиту. Восстановить данные.]
MkDir(H:\tmp);      {Создать временный каталог   }
ChDir(H:\tmp);      {Перейти во временный каталог}
Message(установите дискету в дисковод A: и нажми <Enter>);
DosCommand(copya:\ARHIV.arjH:\tmp);       {Скопировать архив с дискеты}
Directory(_H:\tmp H:\tmp);       { Установить панели}
Select(ARHIV.arj); { Отметить файл}
InputPassword;      { Запросить пароль}
DecryptFiles        { Снять защиту}
DosCommand(arj x  ARHIV );    { Восстановить из архива}
{После выполнения Задания 2 данные каталога PLAN диска E будут восстановлены из защищенного архива, хранящегося на дискете A }
```

**[Задание ~3. Выход.]**

Exit; { завершить работу без выполнения каких-либо функций}

Набранный текст запишем в файл под именем, например, D:\RAB04.SFG и тогда для выполнения любого из этих трех заданий нужно выполнить команду

SAFE D:\RAB04.SFG

В результате на экране появится меню из трех пунктов:

*Задание **1**. Создать архив. Защитить. Скопировать.*

*Задание **2**. Взять архив. Снять защиту. Восстановить данные.*

*Задание **3**. Выход.*

Активизация любого пункта приведет к выполнению подсистемой SAFE соответствующей процедуры из файла D:\RAB04.SF. Цифры 1, 2 и 3 в пунктах меню будут выделены другим цветом. Это говорит о том, что активизировать любой пункт меню можно не только нажатием клавиши Enter после его выбора, но и нажатием клавиши с соответствующей цифрой (1, 2 или 3). Эта возможность появилась в связи с тем, что в каждом заголовке процедуры перед цифрой стоит знак «~», определяющий «горячую» клавишу.

## 2.5. Интерфейсная поддержка разграничения доступа

Интерфейсная поддержка разграничения доступа в системе «Кобра» реализуется специальной оболочкой пользователя US (user`s shell). Данная подсистема является простым и надежным средством отображения состояния файловой системы MS-DOS и выполнения необходимых задач по обработке информации на компьютере. Главное отличие настоящей оболочки от хорошо известных (Norton Commander, Dos Navigator, PC Shell) состоит в том, что она предоставляет пользователю только те возможности по манипулированию командами операционной

системы и запуску программ, и показывает только те каталоги и файлы, которые соответствуют полномочиям пользователя.

US позволяет разграничивать доступ к следующим категориям ресурсов:

- функциональные клавиши US (F1..F10);
- файлы;
- каталоги;

Кроме того, оболочка US запрещает доступ к командной строке, что предотвращает возможность запуска несанкционированных программ.

Подсистема US обладает встроенной системой многоуровневых меню, которая позволяет автоматизировать часто реализуемые последовательности действий по выполнению задач обработки информации, оформляя их в виде отдельных поименованных заданий, которые будут отображаться в виде меню для их выбора и запуска. Учитывая, что доступ к командной строке из оболочки US заблокирован, для предоставления пользователю возможности запуска каких-либо программ с передачей им параметров, администратору следует командные строки запуска этих программ включить в меню данного пользователя (см. п. 2.5.1 и 2.5.2) или установить соответствующую связь с требуемыми пользователю расширениями файлов (см. п. 2.5.3).

Для активизации оболочки следует запустить на выполнение файл US.COM. Строку вызова данного программного файла необходимо вставить в конец файла автозапуска AUTOEXEC.BAT.

Основные приемы манипулирования и управления отображением элементов файловой структуры в среде оболочки US те же, что и в оболочке Norton Commander. Например, переход между панелями выполняется нажатием клавиши Tab. Для вызова краткой справки следует нажать клавишу F1, а для смены отображаемых дисков в левой и правой панелях используются соответственно комбинации клавиш Alt+F1 и Alt+F2. Выде-

ление, а также отмена выделения файлов и каталогов в активной панели выполняется с помощью клавиши INS. Для выделения и снятия выделения по маске предназначены клавиши <+> и <-> в цифровом блоке клавиатуры.

Для эффективной интерфейсной поддержки разграничения доступа пользователей к ресурсам компьютера следует выполнить правильную настройку параметров функционирования оболочки US.

### *2.5.1. Настройка интерфейсной поддержки*

Параметры настройка подсистемы US находятся в конфигурационном файле US.CFG. Данный файл представляет собой обыкновенный текстовый файл и его можно создать и редактировать в любом доступном редакторе. Для составления конфигурационного файла программы US в качестве исходной заготовки может послужить, входящий в комплект поставки файл US.CFG. При этом необходимо четко уяснить какие права доступа к ресурсам машины, а также функциям оболочки следует давать разным пользователям.

Комментарии в файле настройки берутся в фигурные скобки ‘{‘ и ‘}’, все остальное, что вне фигурных скобок, учитывается при интерпретации конфигурационного файла.

Для каждого пользователя необходимо создать раздел, в котором должны быть описаны права доступа пользователя ресурсам компьютера. Раздел должен начинаться с заголовка. Заголовок представляет собой идентификатор пользователя, заключенный в квадратные скобки и располагаемый в отдельной строке. Разделы нескольких пользователей могут быть объединены. В этом случае в строке заголовка объединенного раздела следует указать идентификаторы соответствующих пользователей. Каждый из этих идентификаторов должен быть заключен в квадратные скобки.

Например, раздел предназначенный пользователю Alex может начинаться со строки

[Alex],

а раздел, предназначенный пользователям Andy и Dendy - со строки

[Andy] [Dendy]

Если в строке заданы несколько пользователей, то между ними не может быть комментария, т.е. вместо строки

[Andy] {это я} [Dendy] {это он}

следует писать

[Andy] [Dendy] {первым иду я а потом он}

Раздел, задающий права, общие для всех пользователей, должен начинаться с заголовка [COMMON].

Внутри каждого раздела файла US.CFG описываются права доступа соответствующего пользователя (пользователей) к различным ресурсам. Каждое такое описание должно располагаться в отдельной строке и начинаться с ключевого слова (названия параметра настройки), после которого могут следовать какие-либо аргументы. Если должно быть указано несколько аргументов, то между аргументами, разделенными запятыми, не должно быть пробелов.

Доступны следующие параметры настройки.

**Menu Arg1,Arg2**

Arg1 задает спецификацию файла пользовательского меню (см. подр. 2.5.2), вызываемого по клавише F2. Arg2 определяет признак автозапуска пользовательского меню из данного файла. Если Arg2 = Yes, то пользовательское меню автоматически выводится при каждом запуске US.

Пример: Menu us.mnu,No

**Extensions Arg1**

Определяет имя файла реагирования на различные расширения. Когда пользователь устанавливает курсор на какой-либо файл с расширением отличным от .COM, .EXE, .BAT, .BTM и нажимает <Enter>, оболочка US автоматически ищет в заданном файле реагирования запись, соответствующую расширению выбранного файла (см. подр. 2.5.3). К примеру, нажатию <Enter> на файле с расширением .TXT можно присвоить вызов LEXICON`a со спецификацией выбранного файла в качестве параметра. В Arg1 задается только имя файла реагирования. Файл всегда ищется в каталоге, откуда запускается US.

Пример: Extensions us.ext

**Keys Arg1,Arg2,...**

Устанавливает доступные пользователю клавиши US. В качестве аргументов нужно задавать названия функциональных клавиш, доступных пользователю.

Пример: Keys F1,F2,F3,F4,F5,F6,F7,F8,F9,F10

**Files Arg1,Arg2,Arg3,...**

Устанавливает маски файлов, которые видны пользователю. Например , если пользователю должны быть доступны только текстовые файлы, следует задать

Files *.txt,*.doc

Директивы Files могут быть аддитивными, т.е. вторая директива Files может не заменять, а дополнять предыдущую. Для этого первым символом аргумента следует указать ‘+’, например:

Files +lo*.*,ma*.*,be*.who

Суммарная длина масок файлов не может превышать 255 символов.

Пример: Files *.bat,*.com,*.exe,*.btm,*.txt,*.doc

**Paths Arg1,Arg2,Arg3,...**

Устанавливает маски доступных данному пользователю каталогов. Имена каталогов могут содержать знаки шаблонов ‘*’ и ‘?’. Например, чтобы дать пользователю доступ ко всем каталогам на диске D: следует указать: paths d:*.*

Пример: paths c:\dos,c:\4dos,d:*.*,e:\work.txt

**Editor Arg1**

Устанавливает редактор, вызываемый по клавише F4. Если установить курсор на какой-либо файл и нажать F4 (если, конечно, эта клавиша доступна пользователю), то вызывается указанная программа, которой в качестве параметра передается имя файла, на который указывает курсор.

Примеры:

Editor d:\lexicon\lexicon.exe

Editor c:\NC\ncedit.exe

**Copyprompt Arg1**

Разрешает или запрещает US спрашивать пользователя о каталоге назначения при активизации процесса копирования или перемещения файлов. По умолчанию выделенные файлы копируются или перемещаются в каталог, отображаемый на противоположной панели. Если установить **Arg1** в Yes, то диалог при нажатии клавиш F5 или F6 будет примерно таким же, как и в Norton Commander’e. Если же Arg1 = No то оболочка US будет без запроса копировать (перемещать) выделенные файлы с каталога активной панели в каталог неактивной.

Пример: Copyprompt No

**EnableCTRL Arg1**

Разрешает или запрещает пользователю пользоваться клавишей CTRL. Если Arg1 = No то клавиша CTRL будет полностью заблокирована, и, к примеру, нажатие CTRL+Break или CTRL+C не приведет ни к какому результату.

Пример: EnableCTRL Yes

**EraseDirs Arg1**

Разрешает или запрещает пользователю удалять каталоги целиком. Если Arg1 = Yes и клавиша F8 доступна пользователю то он может, выбрав каталог, удалить его целиком по клавише F8. В этом случае удаление произойдет и при условии, что внутри каталога есть файлы, которые пользователю недоступны (см. выше ключевое слово Files). Если же Arg1 = No то каталог сможет быть удален только пошагово (сначала файлы каталога, потом пустой каталог - как в NC 3.0)

Пример: EraseDirs No

**TempDir Arg1**

Устанавливает каталог для временных файлов US. Когда происходит запуск какой-либо программы, US временно сохраняет свою конфигурацию в файл US.DSK в указанном каталоге. Эта опция полезна в случае, если диск на котором установлен US защищен от записи (по умолчанию US.DSK записывается в тот же каталог, где расположен US.COM).

Пример: TempDir c:\temp

**ReplaceCommand Arg1**

Установить заменитель COMMAND.COM. Когда из US запущена какая-либо внешняя программа, то при временном выходе из этой программы в окружение DOS может быть потерян контроль над действиями пользователя. Учитывая, что обычно программы ищут командный процессор по переменной окружения COMSPEC, то становится возможным «обмануть» их, указав вместо COMMAND.COM другую программу. Лучше всего подставить вместо COMMAND.COM US.COM с тем, чтобы пользователь имел возможность в окружении DOS выполнить требуемые ему функции, оставаясь при этом в границах выделенных ему полномочий. Для более жесткого контроля рекомендуется подстановка программы LOCK.EXE, входящей в подсистему разграничения доступа к файлам.

Пример: ReplaceCommand c:\cobra\us\us.com

## Пример файла конфигурации US.CFG

```
[COMMON]
Menu us.mnu,Yes
Extensions us.ext
Keys F1,F2,F3
Files *.t*
paths c:\us*,c:\do*,d:\*,h:\*,e:\t*
Editor d:\lexicon\lexicon.exe
Copyprompt No
EnableCtrl Yes
EraseDirs No
TempDir g:\temp
ReplaceCommand c:\cobra\us\us.com

[ОБРАЗЕЦ]                    {имя (имена) пользователей}
Menu  us1.mnu,No             {меню пользователя и его автозапуск}
Extensions  us.ext           {Файл с реакцией на расширения}
Keys  F1,F2,F3,F4,F5,F7,F9   {доступные функциональные клавиши}
Files  rt*.*,*.t*,*.bat      { видимые файлы }
paths  *.*                   { видимые директории  }
Editor  c:\te.com            { запускаемый по F4 редактор файлов}
TempDir h:\                  { Каталог для временных файлов US}
ReplaceCommand c:\cobra\us\us.com  {Замена COMSpEC (для DOS-shell)}
Copyprompt Yes               { подтверждение при копировании}
EraseDirs Yes                { Разрешено ли удаление подкаталогов}
EnableCtrl Yes               { доступность клавиши Ctrl}

[Alex] [Andy]
Menu us.mnu,Yes
```

```
Keys F1,F2,F3,F4,F5,F6,F7,F8,F9,F10
Files *.*
paths *.*
Copyprompt  Yes
EnableCtrl Yes
EraseDirs Yes
Editor c:\qe\q.exe
ReplaceCommand  c:\dos\command.com

[User]
Keys F1,F2,F3,F4
Files  *.bat;*.doc
paths  c:\us;e:\work.txt;d:\*;h:\*
Menu  us.mnu,No
TempDir h:\
```

### *2.5.2. Создание пользовательского меню*

Как и в оболочке Norton Commander, вызов меню из US выполняется нажатием клавиши F2. Оболочка US предоставляет очень мощную поддержку пользовательских меню. Девять возможных уровней вложенности, а также возможность вставки команд между уровнями покрывают требования практически любых пользователей. Файл меню содержит обычные команды MS-DOS, а также команды оболочки US, группирующие команды MS-DOS по пунктам меню.

Рассмотрим простейший файл меню:

```
>1 Запуск ~TURBO PASCAL
     d:
     cd\bp\bin
     turbo
>1 Запуск ~Foxpro
     e:
```

```
    cd\fox
    foxpro
>1 Закончить работу
    call c:\cobra\e.bat
```

Строки, начинающиеся с знака ‘>’ задают строки пользовательского меню. Знак ‘~’ перед «TURBO» и перед «Foxpro» задают «горячие» клавиши, т.е. первый пункт меню можно запустить нажав клавишу с буквой «T», а второй - клавишу с буквой «F». При визуализации меню, эти буквы будут выделены желтым цветом. Число после знака «>», обозначает уровень вложенности меню. Например первый пункт меню можно разнообразить:

```
>1 Запуск ~TURBO PASCAL
    >2 Из каталога \bp\work
        d:
        cd\bp\work
        \bp\bin\turbo
    >2 Из каталога \bp\examples
        d:
        cd\bp\examples
        \bp\bin\turbo
```

В данном случае при выборе первого пункта меню первого уровня вложенности перед появится меню второго уровня, в котором можно уточнить некоторые параметры запуска Turbo pascal. Заметьте, что в последнем примере в обоих пунктах меню повторяется команда «d:» и «\bp\bin\turbo». В этом случае можно переписать фрагмент файла меню следующим образом:

```
>1 Запуск ~TURBO PASCAL
    d:
>2 Из каталога \bp\work
    cd\bp\work
>2 Из каталога \bp\examples
    cd\bp\examples
<1 \bp\bin\turbo
```

Это меню функционально абсолютно эквивалентно описанному выше. Строка ‘<1’ означает «Вернуться к уровню 1». Таким образом, при выборе пункта меню «Запуск ~TURBO PASCAL» и далее «Из каталога \bp\examples» US выберет для запуска во всем меню те строки которые находятся «по пути» к выбранному пункту меню (и обратно) на всех уровнях вложенности. Можно вернуться и на нулевой уровень вложенности - команды в строках возврата на этот уровень будут выполняться для всех пунктов меню, независимо от их вложенности.

При запуске какого-либо пункта меню, оболочка US создает временный командный файл US_TEMP.BAT, в который записывает из файла US.MNU все относящиеся к выбранному пункту меню команды MS-DOS, и запускает созданный командный файл на выполнение.

Если при запуске любого пункта меню одновременно удерживается нажатой клавиша Shift то US попросит отредактировать строку параметров, с которыми будет запущен файл US_TEMP.BAT. В этом случае если перед вызовом меню на активной панели был выбран каталог, то по умолчанию .BAT-файлу передается один параметр - путь выбранного каталога.

Если же перед вызовом меню на активной панели был выбран файл, то по умолчанию при запуске любого пункта меню .BAT-файлу передается три параметра: первый из них - это путь выбранного файла, второй - его имя без ‘.’, и третий - расширение выбранного файла без ‘.’.

## Пример файла US.MNU

```
>1 Запуск ~CheckDisk
    echo Процедура проверки диска ...
        >2 проверка диска ~C
            c:\dos\chkdsk c:
        >2 проверка диска ~D
            c:\dos\chkdsk d:
        >2 проверка диска ~E
            c:\dos\chkdsk e:
```

```
<1
    echo Это была программа ChkDsk!
 >1 Запуск программы ~SAFE
        >2 Запуск ~без параметров
            c:\cobra\safe.exe
         >2 Запуск с пакетным файлом указанным курсором
             c:\cobra\safe.exe %1%2 %3
>1 Запуск программы ~TETRIS
     d:
     cd games\tetris
     tetris
<0
     echo ... для возврата в US нажмите любую клавишу ...
     pause >NUL
```

### *2.5.3. Установка связи с расширениями файлов*

Система US имеет довольно гибкую систему обработки файлов в зависимости от их расширений, превосходя в этом, скажем, Norton Commander. При нажатии клавиши <Enter> на выбранном файле с определенным расширением оболочка US может выполнить операцию любой степени сложности, так как позволяет присвоить каждому расширению содержимое целого командного файла MS-DOS, описываемого в файле US.EXT.

Файл US.EXT может содержать сколь угодно записей - по одной на каждое расширение. Каждая запись может занимать любое количество строк и имеет следующую структуру:

EXT{.....

.....

.....}

где, EXT означает расширение. Внутри фигурных скобок размещается содержимое BAT-файла произвольной сложности с циклами, условиями, метками и т.д. При нажатии <ENTER> на выбранном файле с расширением EXT содержимое файла US.MNU между фигурными скобками, соответствующее данному расширению, будет записано во временный

файл US_TEMP.BAT, который затем будет запущен на выполнение. Если нажатие <ENTER> выполнялось при нажатой клавише Shift, то оболочка US предоставит возможность отредактировать строку параметров, с которыми будет запущен файл US_TEMP.BAT. По умолчанию .BAT-файлу передаются три параметра. Первый из них - это путь выбранного файла, второй - имя выбранного файла без ‘.’, и третий - расширение выбранного файла без ‘.’.

## Пример файла US.EXT

```
pas{@echo off turbo %2}
lzh{lha x %2.%3}
arj{arj x %2.%3}
zip{pkunzip -d %2.%3}
ha{ha x %2.%3}
bak{del *.bak /y /q}
stm{player %2.%3}
mod{player %2.%3}
bpm{player %2.%3}
cdm{player %2.%3}
asm{@echo off
cls
echo ____________________________________________
echo _ Assembling and linking COM file... _
echo ____________________________________________
tasm %2 /z /m4
if errorlevel 1 goto end
tlink /t /x /3 %2.obj
del %2.obj /q
:End}
```

# 3. ПРОТИВОДЕЙСТВИЕ ОБХОДУ СИСТЕМЫ ЗАЩИТЫ

Для выполнения основных функций противодействия обходу системы «Кобра» предназначена подсистема закрытия, обеспечивающая гарантированную защиту от программных закладок и несанкционированной загрузки с системной дискеты.

Повышения степени защиты от обхода системы «Кобра» можно добиться лишь при использовании подсистемы закрытия совместно с подсистемой обеспечения эталонного состояния рабочей среды и подсистемой регистрации действий пользователей.

Подсистема обеспечения эталонного состояния рабочей среды позволяет своевременно обнаружить изменения в системных программах и файлах настройки, которые могут быть следствиями программных закладок.

Регистрация, учет и анализ действий пользователей не только позволяет своевременно обнаружить попытки обхода защитных уровней со стороны санкционированных пользователей, но и оказывает значительную помощь в выявлении и устранении недостатков системы защиты.

## 3.1. Защита от программных закладок и несанкционированной загрузки с системной дискеты

Основные функции защиты от программных закладок и несанкционированной загрузки с системной дискеты в системе «Кобра» реализуются подсистемой закрытия (программой MBRINST.EXE). Данная подсистема доступна только администратору безопасности со статусом Суперпользователя.

Смысл установки режима гарантированной защиты от программных закладок и несанкционированной загрузки с дискеты заключается в прозрачном шифровании всех областей диска C:, включая главную загрузоч-

ную запись (MBR), загрузочный сектор (BR), корневой каталог (RDir), таблицу размещения файлов (FAT) и сами каталоги и файлы. Во время установки такого режима подготавливается специальная ключевая дискета, с помощью которой в дальнейшем осуществляется загрузка компьютера. Со стороны санкционированных пользователей должна быть обеспечена тщательная защита данной дискеты от похищения и несанкционированного копирования.

При знании пароля, по которому была установлена защита от программных закладок, ключевая дискета может быть создана на другой ЭВМ с установленной системой «Кобра». Без наличия ключевой дискеты в дисководе А: загрузка с жесткого диска будет невозможна, а при загрузке с обычной системной дискеты жесткий диск будет недоступен. При физическом чтении жесткого диска злоумышленнику доступна только криптограмма. Программная закладка в этом случае теоретически может быть установлена только при условии раскрытия злоумышленником шифра, что практически нереализуемо ввиду высокой криптостойкости использованных алгоритмов.

Предусмотрена возможность перенесения ключа на жесткий диск. В этом случае диск С: останется зашифрованным и в то же время с него можно будет загрузиться без использования ключевой дискеты, но при условии знания пароля начала загрузки (общего для всех зарегистрированных пользователей). Таким образом, при этом каждый зарегистрированный пользователь должен для входа в систему знать и вводить два пароля: пароль загрузки (общий для всех пользователей) и свой личный (основной или дополнительный) пароль.

Следует отметить, что при невысоких требованиях к информационной безопасности подсистема закрытия обеспечивает и наиболее простой вариант защиты от программных закладок и несанкционированной загрузки с системной дискеты - защиту без использования ключевого диска. В

этом случае производится прозрачное шифрование только главной загрузочной записи жесткого диска (MBR). При установке такого режима после загрузки с системной дискеты жесткий диск будет доступен только в том случае, если загрузка осуществлялась со специальной дискеты, подготовленной администратором службы безопасности.

Независимо от того, какой режим защиты от программных закладок и несанкционированной загрузки с системной дискеты установлен, сразу после установки данного режима необходимо с помощью программы COBRAINS.EXE обновить эталонную информацию о состоянии рабочей среды компьютера.

### *3.1.1. Защита с использованием ключевого диска*

#### Установка защиты

Для установки защиты с использованием ключевого диска необходимо после запуска программы MBRINST.EXE в ее главном меню (□) выбрать команду **Установить защиту от загрузки с дискеты** и далее **Защита с использованием ключевого диска**.

| **Установить защиту от загрузки с дискеты** |
|---|
| **Снять защиту от загрузки с дискеты** |
| **Восстановить ключевую дискету** |
| **Выйти в операционную систему** |

**Рис. 3.1. Главное меню программы MBRINST**

В результате на экран будет выдан запрос (□), в ответ на который следует дважды ввести пароль (ключ) длиной от 4-х до 63-х символов, по которому будет шифроваться информация на жестком диске.

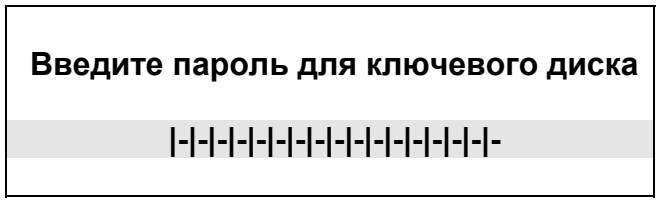


**Рис. 3.2. Запрос на ввод ключа шифрования (пароля)**

Затем в появившемся диалоговом окне (□) необходимо выбрать область жесткого диска, которая зашифруется и далее будет использоваться в режиме прозрачного шифрования.

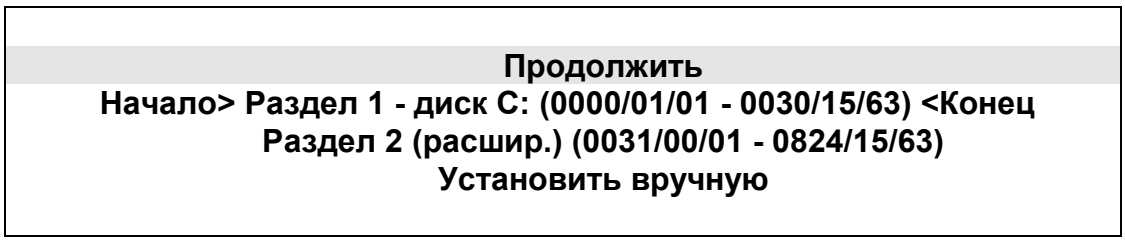


**Рис. 3.3. Запрос на криптографическое преобразование разделов жесткого диска**

По умолчанию предлагается зашифровать только первый раздел винчестера - диск C:. Для добавления расширенного раздела следует перейти на строку **Раздел 2**, нажать клавишу Enter и определить в следующем окне, что данный раздел будет концом преобразуемого участка. Для ручного задания физических адресов начала и конца шифруемой области винчестера следует выбрать команду **Установить вручную**. Данная команда требует от Суперпользователя знания структуры жесткого диска. При этом желательно записать и сохранить информацию о начале и окончании шифруемой области.

Определив область преобразования винчестера следует ввести команду **Продолжить**. До ввода данной команды можно отказаться от процесса шифрования, нажав клавишу Esc.

После ввода команды **Продолжить** ответными действиями на соответствующий запрос необходимо будет вставить чистую дискету в диско-

вод A: для создания ключевой дискеты. Далее автоматически будет активизирован процесс зашифровывания указанной области жесткого диска. Процесс зашифровывания может занять несколько минут и прерывать его нельзя ни в коем случае, так как при прерывании этого процесса данные на диске могут быть безвозвратно утеряны. Для предотвращения случайной потери напряжения в электрической сети на время установки защиты от программных закладок и несанкционированной загрузки с системной дискеты целесообразно использование источника бесперебойного питания.

По завершении шифрования винчестера без наличия ключевой дискеты в дисководе A: загрузиться с жесткого диска будет невозможно. Жесткий диск будет доступен только в случае загрузки операционной системы с винчестера при наличии в дисководе ключевой дискеты или в случае загрузки с самой ключевой дискеты. Загрузка операционной системы с ключевой дискеты выполняется при нажатой клавише <Alt>. При загрузке с обычной системной дискеты жесткий диск будет недоступен.

## Копирование и восстановление ключевой дискеты

Подготовить ключевые дискеты для всех санкционированных пользователей компьютера можно обычным копированием исходной ключевой дискеты с помощью команды MS-DOS DISKCOPY.

Всем пользователям необходимо обратить особое внимание на защиту их ключевых дискет от похищения и несанкционированного копирования.

Если ключевая дискета была одна, то в случае ее утраты загрузка с жесткого диска на компьютере, для которого она была подготовлена, будет возможна только после создания новой ключевой дискеты на другом компьютере с установленной системой "КОБРА". Для создания новой ключевой дискеты необходимо на другом компьютере установить защиту

от программных закладок и несанкционированной загрузки с тем же самым паролем, который использовался для установки этой же защиты на компьютере, от которого утеряна ключевая дискета. После создания новой дискеты целесообразно переустановить защиту от программных закладок и несанкционированной загрузки, изменив пароль шифрования жесткого диска.

В случае, если ключевая дискета повреждена, например, на ней случайно изменена загрузочная запись командой SYS, то данную дискету можно восстановить с помощью программы MBRINST.EXE. Для этого следует из главного меню данной программы выбрать команду **Восстановить ключевую дискету**, после чего программа MBRINST затребует вставить ключевую дискету в дисковод и восстановит ее работоспособность. Данная функция программы MBRINST будет выполнена только для ключевой, а не какой-либо другой дискеты.

### Перенос ключа на жесткий диск

Когда установлена защита от программных закладок и несанкционированной загрузки с использованием ключевого диска, для удобства работы с “Коброй” существует возможность переноса ключа с дискеты на жесткий диск. При этом можно задать специальный дополнительный пароль загрузки, единый для всех пользователей. Использовать эту возможность может только Суперпользователь. После переноса ключа на жесткий диск при загрузке операционной системы больше не нужно будет вставлять ключевую дискету в дисковод. В этом случае степень защиты снижается, но удобство работы пользователей увеличивается.

Для переноса ключа на жесткий диск необходимо запустить программу MBRINST.EXE. Главное меню данной программы (□) при установленной защите с использованием ключевого диска отличается от исходного (см. □), когда этот вид защиты не установлен.

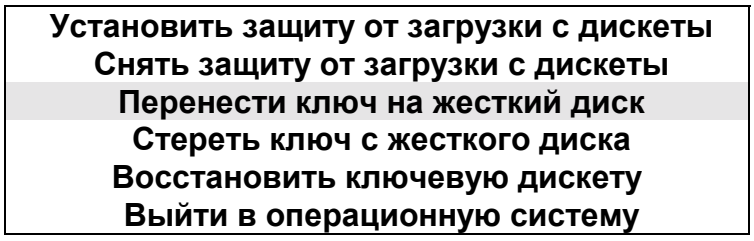


**Рис. 3.4. Главное меню программы MBRINST при установленной защите с использованием ключевого диска**

Затем следует выполнить команду **Перенести ключ на жесткий диск**, после чего появятся запросы на вставку ключевой дискеты и ввод дополнительного пароля загрузки. Если дополнительный пароль устанавливать не нужно, то в ответ на запрос о вводе данного пароля следует просто нажать клавишу Enter.

После завершения ввода пароля на экране появится сообщение о переносе ключа и предупреждение о мерах безопасности (□).

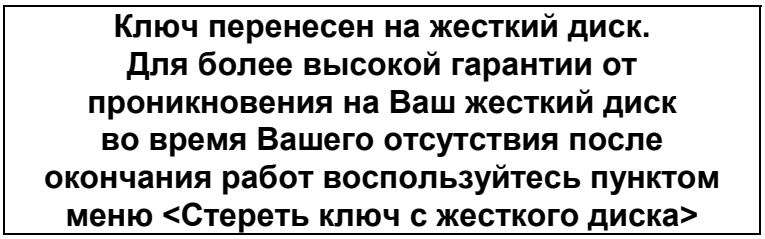


**Рис. 3.5. Сообщение о завершении переноса ключа на жесткий диск**

Выполнение команды главного меню программы MBRINST **Стереть ключ с жесткого диска** отменяет действие команды **Перенести ключ на жесткий диск**.

Если в процессе переноса ключа на жесткий диск был установлен дополнительный пароль загрузки, то в дальнейшем до стирания ключа с жесткого диска все пользователи при входе в систему, кроме своего пароля, должны будут вводить дополнительный пароль загрузки. Если этот

пароль не будет введен, то операционная система с жесткого диска или ключевой дискеты загружена не будет.

Следует учитывать, что после переноса ключа на жесткий диск ключевую дискету следует сохранить, так как она понадобится не только в случае необходимости загрузки операционной системы с ключевой дискеты, но и при откате (снятии) защиты от программных закладок и несанкционированной загрузки.

### *3.1.2. Защита без использования ключевого диска*

В случае установленной защиты без использования ключевого диска производится прозрачное шифрование только главной загрузочной записи (MBR) винчестера, а остальное пространство жесткого диска остается незашифрованным. В данном режиме несанкционированная загрузка с обычной системной дискеты будет невозможна. Для санкционированной загрузки с дискеты должна быть использована специальная системная дискета, подготовленная администратором.

Перед непосредственной установкой защиты без использования ключевого диска следует подготовить стандартную системную дискету. Эта дискета понадобится в процессе установки защиты для создания специальной загрузочной дискеты, которая будет использоваться далее в случае необходимости санкционированной загрузки с дискеты.

Для установки защиты без использования ключевого диска следует в главном меню программы MBRINST (см. □) выбрать команду **Установить защиту от загрузки с дискеты** и далее **Защита без использованием ключевого диска**.

В результате появится запрос (□), согласно которому для создания специальной загрузочной дискеты следует вставить в дисковод подготовленную стандартную загрузочную дискету и нажать клавишу Enter. Специальную загрузочную дискету следует создать обязательно, так как в

случае ее отсутствия загрузиться с дискеты при возникновении ошибок загрузки с винчестера будет невозможно.

**Когда Ваш хард-диск будет закрыт программой MBRINST
Вы не сможете загрузиться ни с одной стандартной
системной дискеты. Вы можете сейчас подготовить
загрузочную дискету на тот случай если Вы не сможете
загрузиться с хард-диска по какой-либо причине.
Вставьте обработанную командой SYS дискету в A:
и нажмите <ENTER> для подтверждения
или <ESC> для пропуска этой части**

**Рис. 3.6. Запрос на подготовку специальной загрузочной дискеты**

После создания ключевой дискеты по окончании установки защиты будет выдано соответствующее сообщение (□).

**Защита от загрузки с флоппи-дисков установлена
После перезагрузки не забудьте запомнить командой
CobraINS текущее состояние главной загрузочной записи**

**Рис. 3.7. Сообщение о завершении установки защиты**

Ответным действием на это сообщение администратор должен, запустив программу COBRAINS.EXE, обновить эталонную информацию о состоянии рабочей среды компьютера.

Следует учитывать, что специальная системная дискета должна храниться только у администратора. При этом, как и для ключевой дискеты, необходимо обратить особое внимание на защиту данной дискеты от копирования и похищения.

### *3.1.3. Откат защиты*

Правом снятия защиты от программных закладок и несанкционированной загрузки с системной дискеты, как и правом ее установки обладает только администратор со статусом суперпользователя.

Для снятия защиты от программных закладок и несанкционированной загрузки с системной дискеты необходимо запустить программу MBRINST и в ее главном меню выбрать команду **Снять защиту от загрузки с дискеты**.

Если защита была установлена без использования ключевой дискеты, то снятие производится автоматически в течении нескольких секунд.

Если же была установлена защита с использованием ключевой дискеты, то после выдачи команды **Снять защиту от загрузки с дискеты** программа MBRINST потребует вставить ключевую дискету, без которой откат защиты невозможен. После обращения к ключевой дискете автоматически будет активизирован процесс расшифровывания области жесткого диска, зашифрованной при установке защиты. Процесс расшифровывания может занять несколько минут и прерывать его нельзя ни в коем случае, так как в случае прерывании этого процесса данные на диске могут быть безвозвратно утеряны. Для предотвращения случайной потери напряжения в электрической сети на время снятия защиты с применением ключевой дискеты целесообразно использование источника бесперебойного питания.

## 3.2. Обеспечение эталонного состояния рабочей среды

К функциям обеспечения эталонного состояния рабочей среды, реализуемых системой «Кобра», относятся следующие:

- обнаружение несанкционированных изменений в рабочей среде компьютера со стороны лиц, получивших доступ к ПЭВМ;
- обнаружение несанкционированных изменений, вызванных компьютерными вирусами и программами-вредителями;
- обнаружение искажений в программах и ключевой информации, возникших в результате машинных сбоев или износа магнитного носителя.

Подсистема обеспечения эталонного состояния рабочей среды реагирует на появление разных типов существующих компьютерных вирусов, а также предусматривает возможность появления их новых модификаций и типов. Кроме того, данная подсистема выполняет автоматическое восстановление основных компонентов рабочей среды ПЭВМ, а в случае невозможности автоматического восстановления сигнализирует об этом пользователю, выдавая данные о поврежденных областях рабочей среды для проведения ручного восстановления. Подсистема контролирует состояние оперативной памяти ЭВМ, содержание главной загрузочной записи (MBR) и загрузочного сектора (BR) диска, состояние батарейной памяти CMOS, файлы конфигурирования и автозапуска CONFIG.SYS и AUTOEXEC.BAT, системные и прикладные программы, а также заданные информационные файлы.

### *3.2.1. Создание эталонных характеристик*

Перед периодической проверкой характеристик текущей рабочей среды на соответствие эталонным необходимо эти эталонные характеристики создать. Для этого предназначена программа COBRAINS.EXE.

Функции программы COBRAINS.EXE доступны только для пользователей, имеющих статус Администратора или Суперпользователя. При попытке выполнить программу пользователем, не обладающим таким статусом, программа завершает свою работу выдачей соответствующего сообщения.

Перед непосредственным формированием эталонных характеристик рабочей среды с помощью программы COBRAINS необходимо выполнить следующие действия:

1) тщательная проверка компьютера на наличие вирусов и их обезвреживание с помощью доступных сканеров (детекторов-дезинфекторов), например, DrWeb или AidsTest;

2) тщательный анализ файлов конфигурирования и автозапуска на отсутствие вызовов программных закладок и удаление программных закладок при их обнаружении.

Если же перед формированием эталонных характеристик перечисленные действия реализованы не будут, то при создании эталонных характеристик будут сформированы характеристики зараженной среды, и в дальнейшем зараженная среда будет считаться как безопасная.

Для формирования эталонных характеристик следует запустить программу COBRAINS.EXE, задать параметры ее работы и далее нажать клавишу Enter. Формируемые эталонные характеристики программа COBRAINS зашифровывает и записывает в специальные файлы, располагаемые в каталоге, куда была инсталлирована система «Кобра». Если была задана соответствующая опция в параметрах настройки программы, то файлы с эталонными характеристиками будут записаны не только на винчестер, но и на дискету.

Параметры работы программы COBRAINS определяют режим формирования эталонных характеристик и их количество. Задание параметров выполняется с помощью окна настроек (□□), появляющегося сразу после запуска программы .

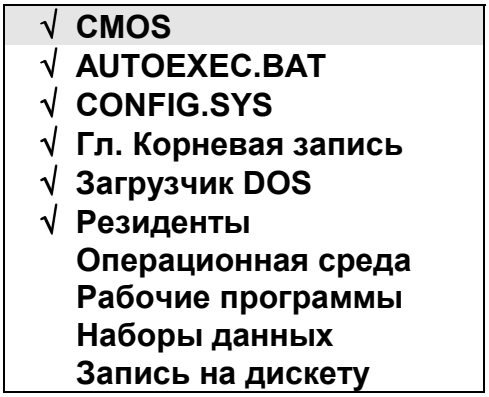


**Рис. 3.8. Окно настроек программы COBRAINS**

Каждая строка окна настроек является командой-переключателем, включенное состояние которой определяет выполнение соответствующей функции после активизации процесса формирования эталонных характеристик нажатием клавиши Enter. При выключенном состоянии команды-переключателя соответствующая ей функция выполняться не будет. Для настройки параметров в окне настроек необходимо нажатием клавиши пробела включить или отключить команды-переключатели. Выбор команды выполняется клавишами с вертикальными стрелками. Включенное состояние команды-переключателя помечается «птичкой».

Все команды, за исключением последней, задают функцию формирования соответствующих им эталонных характеристик:

1) **CMOS** - содержимого CMOS-памяти;
2) **AUTOEXEC.BAT** - содержимого файла автозапуска;
3) **CONFIG.SYS** - содержимого файла конфигурирования CONFIG.SYS;
4) **Гл. Корневая запись** - главной загрузочной записи (MBR) винчестера;
5) **Загрузчик DOS** - системного загрузчика (BR) активного раздела DOS;
6) **Резиденты** - контрольных сумм резидентных программ;
7) **Операционная среда** - контрольных сумм системных программ MS-DOS;
8) **Рабочие программы** - контрольных сумм любых программ;
9) **Наборы данных** - контрольных сумм любых файлов данных.

Если необходима запись всех сформированных эталонных характеристик не только в каталог расположения системы «Кобра», но и на дискету, то в окне настроек необходимо включить команду-переключатель **Запись на дискету**. Дискету с эталонными характеристиками следует формировать обязательно, так как эта дискета понадобиться для восста-

новления эталонных характеристик рабочей среды, когда автоматическое восстановление с винчестера окажется невозможным.

Формирование эталонных характеристик содержимого CMOS-памяти, файлов автозапуска и конфигурирования, главной загрузочной записи и системного загрузчика винчестера, а также резидентных программ после нажатия клавиши Enter выполняется автоматически.

Если же при активизации процесса формирования эталонных характеристик (нажатии клавиши Enter) были включены такие команды-переключатели как **Операционная среда**, **Рабочие программы** и **Наборы данных**, то для вычисления контрольных сумм по каждой из данных команд будет произведен запрос (□□).

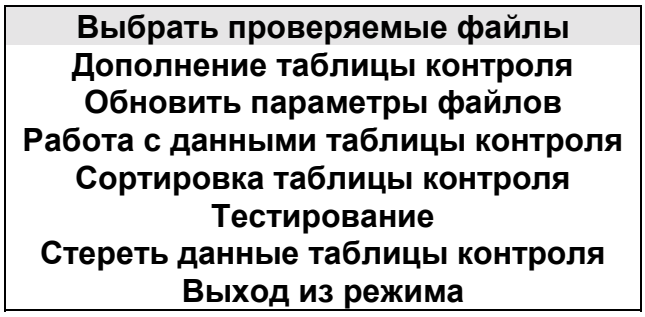


**Рис. 3.9. Запрос на выполнение действий с файлами**

Перед непосредственным вычислением контрольных сумм необходимо сформировать таблицу с обрабатываемыми файлами, называемую таблицей контроля. Для формирования или дополнения такой таблицы требуется выполнить следующие этапы:

1) с помощью команды **Выбрать проверяемые файлы** указать файлы, из которых необходимо сформировать, или которыми следует дополнить таблицу контроля;
2) выполнить команду **Дополнить таблицу контроля**, которая создаст таблицу контроля или дополнит существующую.

Формирование контрольных сумм файлов из таблицы контроля выполняется по команде **Обновить параметры файлов**. Если при следующих запусках программы COBRAINS дополнять таблицу контроля не нужно, то для обновления контрольных сумм файлов из ранее сформированной таблицы достаточно будет ввести команду **Обновить параметры файлов**.

Команда **Работа с данными таблицы контроля** предназначена для просмотра таблицы обрабатываемых файлов и удаления из нее файлов, для которых контрольные суммы проверять не нужно. С помощью команды **Сортировка таблицы контроля** можно задать критерий сортировки файлов в таблице.

По команде **Тестирование** будет выполнена проверка всех файлов из таблицы контроля на соответствие их эталонным характеристикам, если эти эталонные характеристики были созданы по команде **Обновить параметры файлов**.

Для удаления из таблицы контроля всех файлов предназначена команда **Стереть данные таблицы контроля**.

После выполнения всех необходимых действий по формированию контрольных сумм файлов следует выполнить команду **Выход из режима**.

### *3.2.2. Поддержание эталонного состояния рабочей среды*

Проверка соответствия текущих характеристик рабочей среды компьютера эталонным осуществляется запуском тестовой программы COBRATST.EXE.

Список всех ключей программа выводит на экран при ее запуске с параметром /?:

COBRATST.EXE /?

Для автоматического восстановления измененных файлов необходимо программу COBRATST запустить с параметром /a:

COBRATST.EXE /a

В процессе инсталляции системы «Кобра» вызов программы COBRATST.EXE добавляется в файл автозапуска AUTOEXEC.BAT, что обеспечивает автоматический контроль соответствия текущих характеристик рабочей среды эталонным в процессе загрузки операционной системы.

Если при проверке очередного компонента компьютерной системы устанавливается соответствие его характеристик эталонным, то на экран дисплея выводится сообщение, в котором против имени соответствующего компонента указывается «ОК». При несоответствии текущих характеристик эталонным, в сообщении указывается об обнаруженном факте несоответствия. В этом случае, если для программы COBRATST не был задан режим автоматического восстановления, то следует запустить данную программу повторно, но уже с ключом /a, устанавливающим данный режим. В результате будут автоматически восстановлены: содержимое CMOS-памяти, главная загрузочная запись, загрузчик DOS, CONFIG.SYS, AUTOEXEC.BAT. Также будет предпринята попытка восстановления взятых под контроль и измененных после этого файлов с расширением EXE, причем по каждому из таких файлов будет выведено сообщение об итогах такой попытки (удачном восстановлении или же, напротив, о невозможности восстановления).

В случае, если в режиме автоматического восстановления появится сообщение об отсутствии или повреждении файлов с эталонными характеристиками на винчестере или загрузка с винчестера окажется невозможной, то необходимо восстановить эталонные характеристики с дискеты, на которую они должны были быть записаны при их формировании. Для этого требуется выполнить следующие действия:

**1)** загрузиться с системной дискеты;

**2)** вставить в дисковод дискету с эталонной средой, запустить с нее программу COBRATST.EXE с ключом /a, и затем ответить соответствующим образом на вопросы программы.

## 3.3. Регистрация и учет действий пользователей

Подсистема регистрации и учета действий пользователей обеспечивает выполнение следующих функций:

- регистрация обобщенных данных по каждому пользователю;
- регистрация детальных операций каждого пользователя;
- выдача по запросу (только Суперпользователя или Администратора) справки о работе пользователей за текущий период.

### *3.3.1. Регистрация обобщенных данных*

В системе «Кобра» обеспечивается автоматическая регистрация таких обобщенных данных как:

**1)** данных о работе пользователей;

**2)** данных об изменениях администраторами пользовательских полномочий.

Регистрация обобщенных сведений выполняется драйвером COBRA.SYS, вызов которого автоматически вставляется в файл CONFIG.SYS при инсталляции системы защиты. Данный драйвер является основным программным компонентом и подсистемы санкционирования доступа. Вся информация в журнал регистрации заносится только в зашифрованном виде. Журнал регистрации обобщенных ведется в файле COBRA.USR, располагаемом в каталоге системы «Кобра».

К регистрируемым данным о работе каждого пользователя относятся следующие сведения:

- дата и время регистрации пользователя администратором;

- дата и время начала и окончания последнего сеанса работы пользователя;
- время работы пользователя на компьютере;
- количество сеансов работы пользователя;
- количество нарушений пользователем правил работы с системой «Кобра».

Учет времени работы пользователей на компьютере производится по показаниям встроенных часов. Поэтому, в случае необходимости изменения показаний часов командами MS-DOS DATE и TIME или аналогичными действиями эти изменения следует вносить перед непосредственным окончанием сеанса работы. В противном случае фиксируется нарушение правил работы с системой “КОБРА”.

К нарушению правил работы относится также завершение пользователем сеанса работы обычным выключением питания компьютера или перезагрузкой операционной системы. Для правильного завершения своего сеанса работы пользователь должен выполнить команду **E**, т.е. запустить на выполнение командный файл **E.BAT**, располагаемый в каталоге системы «Кобра». Данный командный файл содержит вызов программы COBRATST.EXE, проверяющей состояние рабочей среды на соответствие эталонным характеристикам, а также вызов программы LOGOFF.EXE, отмечающей в журнале регистрации время окончания сеанса работы пользователя и выполняющей перезагрузку системы.

Под сеансом работы пользователя на компьютере при формировании системой защиты записей в журнале регистрации понимается время между вводом пользователем своего пароля при входе в систему и корректным завершением сеанса работы (выполнением команды **E)**.

К регистрируемой информации об изменениях администраторами пользовательских полномочий относятся следующие сведения:

- дата и время изменений пользовательских полномочий;

- ♦ имя и статус пользователя;
- ♦ наличие мандатного доступа;
- ♦ изменение прав доступа.

Например, в журнал регистрации могут быть занесены следующие записи:

**27/03/95 09:50:10 Adm1 добавил нового пользователя**
**Имя** Иванов А.
**Статус** Суперпользователь
**Мандатный доступ** нет
**Доступ к дискам** A:RW B:RW C:RW D:RW E:RW F:RW G:RW H:RW
**Доступ к портам** LPT1[x] LPT2[x] LPT3[x] LPT4[x] COM1[x] COM2[x] COM3[x] COM4 [x]
**Комбинация CTRL/C** разрешена

**27/03/95 09:50:46 Adm2 добавил нового пользователя**
**Имя** Петров Б.
**Статус** Коллега
**Мандатный доступ** нет
**Доступ к дискам** A:R B:R C:R D:RW H:RW
**Доступ к портам** LPT1[x] LPT2[ ] LPT3[ ] LPT4[ ] COM1[x] COM2[ ] COM3[ ] COM4 [ ]
**Комбинация CTRL/C** запрещена

Здесь Adm1 и Adm2 - идентификаторы администраторов.

Для просмотра журнала регистрации обобщенных данных предназначена программа COBRA_L.EXE. Функции данной программы доступны только для лиц, имеющих статус Администратора или Суперпользователя. При попытке получить информационную справку лицом, не обладающим таким статусом, программа завершает свою работу с выдачей соответствующего сообщения.

После запуска программы COBRA_L.EXE пользователем со статусом Администратора или Суперпользователя на экране появляется ее главное меню (□□).

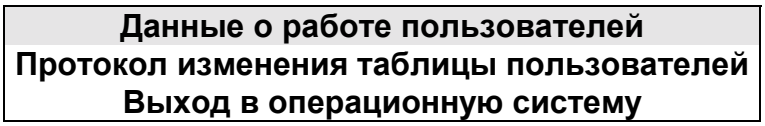


**Рис. 3.10. Главное меню программы COBRA_L.EXE**

Первая команда позволяет осуществить доступ к данным о работе пользователей, а вторая - к данным об изменениях администраторами пользовательских полномочий. При выборе третьей команды или при нажатии клавиши Esc производится возврат в операционную систему.

После выбора одной из первых двух команд появляется подменю (□□) для манипулирования содержимым журнала регистрации.

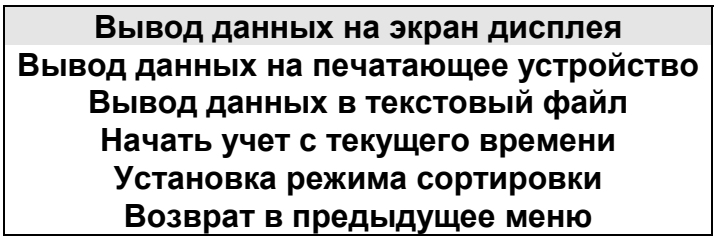


**Рис. 3.11. Команды для работы с журналом регистрации**

Для просмотра журнала регистрации можно пользоваться первыми тремя командами. Для очистки журнала необходимо выбрать команду **Начать учет с текущего времени**.

При необходимости изменения режима сортировки записей в журнале необходимо выбрать команду **Установка режима сортировки**, после чего можно задать следующие критерии сортировки:

- по имени;
- по количеству нарушений;
- по дате регистрации;
- по суммарному времени работы.

## *3.3.2. Регистрация детальных операций*

### Настройка параметров регистрации

К детальным операциям, которые могут регистрироваться системой «Кобра» для заданных пользователей, относятся следующие:

- ♦ запуск исполняемых файлов;
- ♦ открытие и закрытие файлов;
- ♦ выполнение операций чтения из файлов и записи в файлы;
- ♦ удаление и переименование файлов;
- ♦ выполнение таких действий с каталогами, как изменение текущего каталога, создание, переименование и удаление подкаталогов.

Выполнение функций регистрации детальных операций возложено на резидентную программу LOG.EXE, вызов которой должен быть вставлен в файл автозапуска AUTOEXEC.BAT до вызова программы LOCK.EXE, являющейся основой подсистемы разграничения доступа к файлам. Журнал регистрации детальных операций ведется в зашифрованном виде в файле COBRA.LOG каталога системы «Кобра».

Строка запуска программы LOG имеет следующий формат:

LOG [/D] [/F] [/L<спецификация файла журнала регистрации>]

Если задан ключ /F, то системный журнал не будет буферизироваться и запись на диск будет происходить после каждого регистрируемого события. Иначе (по умолчанию) системный журнал буферизируется и записи регистрации сбрасываются на диск при корректном завершении сеанса работы и в том случае, если внутренний буфер журнала регистрации размером в 192 байта переполняется.

При необходимости записи системного журнала в файл, отличный от COBRA.LOG, следует задать ключ /L<спецификация файла журнала регистрации>, например /Lc:\system.log.

При ведении учета операций файлового чтения-записи часто получается такая ситуация, когда программа открывает файл, а затем читает из него множество раз. По умолчанию утилита LOG запишет все эти операции в системный журнал. Если нет необходимости повторения в журнале регистрации записей об одних и тех же действиях, то следует в строке запуска программы LOG указать ключ /D.

Программа LOG использует тот же конфигурационный файл, что и программа LOCK (см. подр. 2.3), а именно - файл LOCK.CFG, располагаемый в каталоге размещения системы «Кобра».

Для того, чтобы задать для какого-либо пользователя список действий, подлежащих запоминанию, необходимо в раздел файла LOCK.CFG, заголовок которого содержит имя данного пользователя, вставить команду .LOG следующего формата:

.LOG [E][O][R][W][D][N][S]

Каждая буква после ключевого слова .LOG означает регистрацию какого-либо класса событий. Для регистрации доступны следующие классы событий:

- E - запуск исполняемых файлов, имеющих расширения .COM и .EXE;
- O - открытие и закрытие файлов; при открытии файла в журнале регистрации этому файлу присваивается уникальный номер, используемый далее до закрытия файла;
- R - выполнение операций чтения из файлов;
- W - выполнение операций записи в файлы;
- D - удаление файлов;
- N - переименование файлов;
- S - выполнение операций по манипулированию каталогами (изменение текущего каталога, создание, переименование и удаление подкаталогов).

Например, если в файле конфигурации для какого-либо пользователя записать

.LOG EDNS

- это означает регистрацию для данного пользователя всех запусков программ, удалений и переименований файлов, а также всех действий с каталогами.

Независимо от установок регистрации, заданных в файле LOCK.CFG, обязательной регистрации подлежат все неразрешенные действия пользователей, отклоненные системой "Кобра".

Каждая новая директива .LOG для одного и того же раздела файла LOCK.CFG полностью перекрывает действие предыдущей директивы. Кроме того, если директива .LOG указана в разделе COMMON, общем для всех пользователей и располагаемом в начале файла LOCK.CFG, то директивы, указанные в следующих разделах пользователей переопределят действие директивы .LOG раздела COMMON.

## Просмотр журнала регистрации

Для просмотра журнала регистрации детальных операций, который ведется в замаскированном виде, предназначена утилита LogView.exe, формат командной строки запуска которой имеет следующий вид:

LogView[.EXE] [<Спецификация файла системного журнала>]

Если спецификация файла не указана, то журнал регистрации ведется в файле COBRA.LOG, расположенном в каталоге системы «Кобра».

Доступ к краткой справке в среде программы LogView выполняется путем нажатия клавиши <F1>. При просмотре содержимого журнала регистрации с помощью утилиты LogView, различные классы событий выделяются различным цветом. Текущая запись журнала выделяется маркером, который можно перемещать по записям журнала с помощью клавиш <↑>, <↓>, <PgUp> и <PgDn>. Для автоматического перехода к записи о

следующем событии из того же класса, что и событие, описанное в текущей записи, необходимо нажать клавишу <Tab>. Если такой записи не существует, то маркер останется на месте. Чтобы перейти к предыдущей записи о событии того же класса следует использовать комбинацию клавиш <Shift>+<Tab>.

В процессе функционирования утилиты LOG при создании или открытии каждого файла ему в журнале регистрации присваивается уникальный идентификационный номер (handle). После открытия или создания файла его идентификационный номер используется вместо спецификации данного файла при регистрации всех действий, связанных с этим файлом. Например, в журнал регистрации могут быть занесены следующие записи:

```
22:56:02 Открытие файла C:\DN\DN.CFG; handle = 0005
22:56:02 Чтение из handle 0005
22:56:02 Закрытие handle 0005
```

Данный фрагмент журнала регистрации описывает, что программа открыла для чтения файл DN.CFG, которому присвоен идентификатор 0005. После этого программа прочитала информацию из файла с идентификационным номером 0005 (т.е. из файла DN.CFG) и далее закрыла этот файл.

При функционировании резидентной утилиты LOG в журнале регистрации может создаваться множество повторяющихся записей. Например, программа открывает некий файл, а потом читает из него информацию мелкими порциями. При этом фрагмент системного журнала может выглядеть примерно так:

```
23:17:09 Открытие файла C:\COBRA\DOC\LOCK.DOC;handle = 0009
23:17:09 Чтение из handle 0009
23:17:09 Чтение из handle 0009
23:17:09 Чтение из handle 0009
.....
23:17:10 Чтение из handle 0009
23:17:10 Чтение из handle 0009
```

23:17:10 Чтение из handle 0009
23:17:10 Закрытие handle 0009

Для удаления повторяющихся записей из журнала, находясь в среде программы LogView, следует нажать клавишу <F9>. Программа просмотрит и удалит все последовательные записи, в которых совпадает все, кроме времени, оставив лишь одну из них. Почти того же эффекта можно добиться при условии запуска программы LOG с ключом /D. Отличие будет заключаться лишь в том, что опция /D исключает только повторяющиеся записи о чтении из файлов и записи в файлы, а функция программы LogView, доступная при нажатии клавиши <F9>, исключает вообще все повторяющиеся записи.

Кроме того, программа LogView позволяет удалять записи выборочно и по классам.

Для ненужных записей выборочно следует их выделить, нажав на них клавишу <Пробел> (повторное нажатие отменяет выделение), и далее нажать клавишу <Del>. Все отмеченные записи при этом из системного журнала будут удалены.

Для удаления записей по классам необходимо выполнить следующие действия:

**1)** нажать клавишу <F4>;

**2)** в появившемся диалоговом окне нажатием клавиши <Пробел> в соответствующих строках указать классы записей, которые следует удалить;

**3)** нажать клавишу <Enter>.

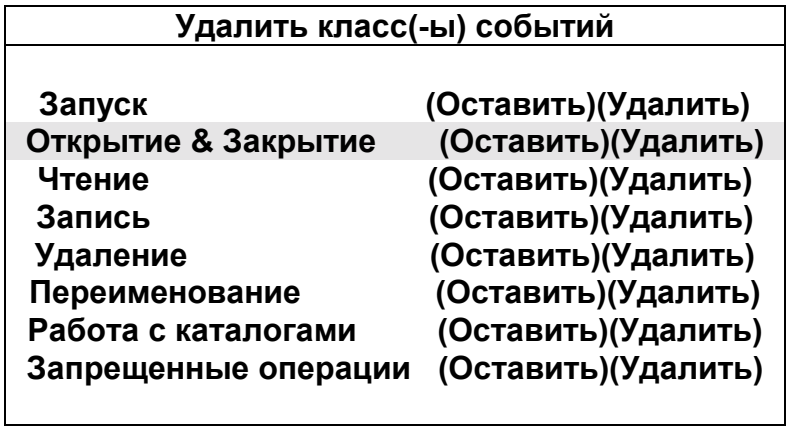


**Рис. 3.12. Окно запроса на удаление классов записей**

Еще одной из функций программы LOGVIEW является удаление части системного журнала. Если нужно удалить все записи с начала системного журнала до определенного места, следует перейти к последней удаляемой записи и нажать <F7>. Если же нужно удалить записи от какого-либо места до конца системного журнала, следует перейти к первой удаляемой записи и нажать <F8>.

Для вывода системного журнала в текстовый файл можно воспользоваться клавишей F2. При этом будет предложено ввести спецификацию файла для вывода (по умолчанию syslog.txt). Если такой файл уже существует, то будет выдан запрос, в ответ на который пользователь может переписать существующий файл либо добавить журнал к его концу.

# 4. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ ЗАЩИТЫ

## 4.1. Защита от доступа к дисковой остаточной информации

При удалении какого-либо файла средствами MS-DOS происходит только замена первого символа имени файла в его каталоге на служебный символ и изменение элементов таблицы размещения файлов (FAT), где описатели кластеров, принадлежащие файлу помечаются как свободные. Само же содержимое файла в области данных диска остается без изменений и может быть похищено злоумышленником с помощью средств низкоуровневого редактирования или утилит восстановления удаленных файлов, например, с помощью утилиты Нортона DiskEdit или - UnErase.

Для удаления дисковой остаточной информации предназначена подсистема затирания, состоящая из двух утилит:

- WIPE.EXE, ориентированной на полное удаление файлов;
- CLEANDSK.EXE, позволяющей выполнить очистку свободного пространства на диске от остаточной информации.

### Полное удаление файлов

При удалении файлов утилита WIPE в соответствии со специальным алгоритмом формирует наборы кодов, которые записываются на место удаленного файла, после чего восстановление информации, принадлежащей файлу становится невозможным.

Формат командной строки для запуска утилиты следующий:

WIPE[.EXE] <File1> [<File2>] ... [/P#] [/Y]

Здесь:

<File1>, <File2> ... - спецификации удаляемых файлов, которые могут содержать и символы шаблона «*» и «?»;

/P# - количество проходов для перезаписи, #=1..8; по умолчанию выполняется три прохода, что является достаточным для предотвращения возможности восстановления стертой информации с помощью специализированных средств;

/Y - не спрашивать подтверждения.

Пример:

WIPE d:*.bak /Y /P4

Для гарантированного удаления пользователем остаточной информации администратору необходимо обеспечить обязательное использование утилиты WIPE. Это можно сделать с помощью специальной оболочки пользователя US (см. п. 2.5). В файле настройки данной оболочки US.CFG следует лишить пользователей возможности использования функциональной клавиши F8, предназначенной для обычного удаления файлов, а в файл настройки пользовательского меню следует вставить строки:

```
>1 Удаление файла
   C:\COBRA\WIPE.EXE %2.%3
```

Здесь предполагается, что система «Кобра» размещена в каталоге C:\COBRA.

В результате вставки данных строк в файл настройки пользовательского меню, для полного удаления файла из оболочки US пользователю необходимо будет перейти к данному файлу (установить на нем маркер), нажать клавишу <F2> и выполнить пункт меню **Удаление файла**.

## Удаление остаточной информации в свободном пространстве диска

Для гарантированного удаления остаточной информации в свободном пространстве дисковой памяти пользователю следует после окончания работы запустить на выполнение утилиту CLEANDSK.EXE. Эта утилита затирает в соответствии с алгоритмом используемым в утилите WIPE все свободное пространство на диске, включая пустые области внутри частично используемых последних файловых кластеров.

Командная строка для запуска утилиты CLEANDSK имеет следующий формат:

CLENDSK[.EXE] [<Путь1>] [<Путь2>] ... [/I[e][f]] [/P#]

Здесь:

<Путь1>, <Путь2>, ... пути каталогов, внутри которых будут очищены все неиспользуемые области последних файловых кластеров;

/I[e][f] - определение областей для очистки (по умолчанию /Ief):

e - очистка неиспользуемых областей последних файловых кластеров;

f - очистка всех незанятых кластеров диска;

/P# - Установить количество проходов (по умолчанию #=1): # = 1...8.

Если определен режим очистки всех незанятых кластеров диска, то для этой очистки будут обработаны диски, имена которых указаны в заданных путях.

Пример:

CleanDsk c:\Work /P2 /Ief

По этой команде очистка неиспользуемых областей последних файловых кластеров будет выполнена для содержимого каталога c:\Work, а очистка всех незанятых кластеров будет выполнена для диска C:.

По усмотрению Администратора вызов утилиты CLEANDSK может быть включен в командный файл E.BAT, предназначенный для корректно-

го завершения сеанса работы пользователем, или в файл настройки пользовательского меню.

## 4.2. Защита от несанкционированного доступа к информации при оставлении компьютера без завершении сеанса работы

Для выполнения функций принудительного и автоматического блокирования устройств ввода-вывода на время оставления компьютера без присмотра предназначена подсистема блокировки. Автоматическое блокирование предполагает блокировку клавиатуры, экрана и мыши по истечении заданного времени бездействия пользователя (времени, в течении которого отсутствуют нажатия клавиш клавиатуры и кнопок мыши). Для разблокирования устройств ввода-вывода пользователю необходимо ввести специально установленный пароль.

Подсистема блокировки состоит из двух программ:

- резидентной программы KBDLOCK.EXE, предназначенной для непосредственного выполнения принудительного и автоматического блокирования устройств ввода-вывода, а также их разблокировки;
- транзитной программы SETPASSW.EXE, выполняющей функции настройки параметров работы подсистемы блокировки (пароля разблокирования и времени бездействия пользователя, по истечении которого будет выполнено блокирование).

Для настройки параметров блокировки пользователю следует запустить программу SETPASSW и в появившемся списке выбрать свой идентификатор, нажав после этого клавишу <Enter>. В результате появится диалоговое окно (□), в котором необходимо с помощью клавиш со стрелками указать пароль разблокирования, задать время бездействия пользователя, по истечении которого будет осуществляться автоматическая блокировка, и далее нажать клавишу <Enter>. В качестве пароля

разблокирования пользователь может определить свой пароль аутентификации или ввести другой пароль. Если в окне запроса пользователь указал на необходимость изменения пароля аутентификации, то после нажатия клавиши <Enter>, пользователю будет выдан запрос на ввод пароля разблокирования. При вводе этого пароля допустимо использование любых клавиш, включая клавиши <Shift>, <Ctrl>, <ScrollLock>, <CapsLock> и т.д.

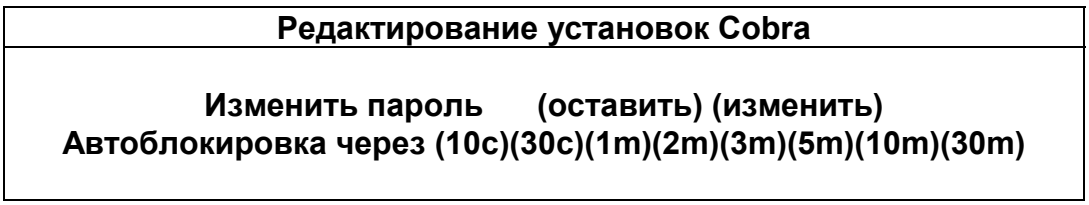


**Рис. 4.1. Запрос на установку параметров блокировки**

Строку вызова программы KBDLOCK необходимо вставить в файл автозапуска AUTOEXEC.BAT перед вызовом командной оболочки.

Принудительное блокирование устройств ввода-вывода перед оставлением компьютера без присмотра выполняется нажатием комбинации клавиш <Ctrl>+<Alt>+<CapsLock>. Если перед оставлением компьютера пользователь забудет выполнить принудительную блокировку, то по истечении заданного времени бездействия программа KBDLOCK заблокирует клавиатуру, экран и мышь самостоятельно.

Для разблокировки следует ввести установленный пароль. Если при наборе пароля произошла ошибка, необходимо нажать <Enter> для сброса всех введенных до этого символов и повторить попытку снова.

## 4.3. Создание дополнительных логических дисков без переразбиения винчестера

Для организации разграничения доступа на уровне логических дисков значительную помощь может оказать подсистема создания дополнительных логических дисков. При наличии свободного пространства на же-

стком диске данная подсистема позволяет создать дополнительные логические диски без переразбиения винчестера. Созданные таким образом виртуальные логические диски могут использоваться администраторами для детализации разграничения доступа пользователей к дисковому пространству с помощью подсистемы санкционирования доступа (см. п. 2.2).

Подсистема создания дополнительных логических дисков включает следующие компоненты:

- транзитную программу SDINST.EXE, предназначенную для непосредственного создания виртуальных логических дисков ;
- драйвер SPLITDRV.SYS, эмулирующий функционирование созданных виртуальных логических дисков.

Каждый виртуальный логический диск может быть создан только при выполнении следующих условий:

- на винчестере достаточно свободного места;
- свободная область винчестера, необходимая для создания виртуального диска, может быть дефрагментирована, т. е. в этой области отсутствуют дефектные или неперемещаемые кластеры.

Для непосредственного создания каждого виртуального логического диска необходимо выполнить следующие действия.

1. Запустить программу SDINST.EXE. В результате на экране появится перечень доступных логических дисков с указанием свободного места на каждом из них.
2. Выбрать с помощью клавиш управления положением курсора необходимый диск и нажать клавишу <Enter>, после чего осуществится автоматический запуск утилиты дефрагментации диска Defrag.exe, входящей в состав MS-DOS, с передачей ей необходимых параметров.
3. Дождаться окончания дефрагментации и на появившийся запрос ввести имя каталога, в котором будет создан файл

NEWDRIVE.SDx для эмуляции создаваемого виртуального диска. По умолчанию этот файл создается в корневом каталоге.

4. В ответ на соответствующий запрос ввести в килобайтах размер создаваемого виртуального диска (по умолчанию устанавливается размер в 32494 килобайта).
5. Дождавшись сообщения о завершении процесса создания виртуального диска, перезагрузить компьютер.

В результате выполнения перечисленных действий в каталоге, указанном пользователем, будет создан файл эмуляции виртуального логического NEWDRIVE.SDx, где x - номер по порядку созданного виртуального диска, начиная с нуля. Кроме того, в конец файла конфигурации CONFIG.SYS будет добавлена строка загрузки драйвера SPLITDRV.SYS с указанием спецификации файла NEWDRIVE.SDx, эмулирующего виртуальный диск. После перезагрузки компьютера, т.е. выполнения пятого пункта перечисленной последовательности действий созданному виртуальному диску в качестве имени будет присвоена следующая по алфавиту латинская буква после имени логического привода, который до создания виртуального диска был последним, например, если до создания виртуального диска последним логическим диском был диск D:, то созданному виртуальному диску будет присвоено имя E:.

Попытка создания дополнительного логического диска может быть неудачной в случае, если по каким-либо причинам не была вызвана утилита Defrag для дефрагментации свободной области винчестера или после дефрагментации полученная свободная область винчестера из-за наличия дефектных или неперемещаемых кластеров осталась фрагментированной. Для выхода из данной ситуации необходимо перенести неперемещаемые кластеры, вызвав утилиту Defrag с ключом /H, или при создании логического диска указать его меньший размер.

При необходимости удаления созданного виртуального диска требуется выполнить следующую последовательность действий:

1) все необходимые данные, хранящиеся на удаляемом виртуальном диске переписать на другой носитель информации;
2) из файла CONFIG.SYS удалить строку, инициирующую загрузку драйвера SPLITDRV.SYS, в которой в качестве параметра указана спецификация файла NEWDRIVE.SDx, эмулирующего удаляемый виртуальный диск (здесь x соответствует n-1, где n - номер по порядку имени удаляемого диска среди имен всех виртуальных дисков);
3) перезагрузить компьютер;
4) удалить сам файл NEWDRIVE.SDx, который эмулировал удаляемый виртуальный диск.

## 4.4. Индивидуальная настройка рабочей среды и рекомендации по обеспечению максимальной безопасности

### *4.4.1. Индивидуальная настройка рабочей среды*

В процессе инсталляции системы «Кобра» в начало файла AUTOEXEC.BAT вставляется вызов программы идентификации-аутентификации пользователя LOGON:

C:\COBRA\LOGON.EXE /f

Здесь предполагается, что система «Кобра» инсталлирована в каталог C:\COBRA. Ключ /f определяет загрузку встроенного шрифта кириллицы.

Программа LOGON.EXE при завершении формирует код завершения, равный номеру вошедшего в систему пользователя из списка доступа и переменную окружения USER, содержащую его идентификатор. Анализируя код завершения или переменную окружения в файле

AUTOEXEC.BAT, можно обеспечить для каждого пользователя выполнение индивидуальной части командного файла.

## Анализ кода завершения

При анализе кода завершения программы LOGON все конструкции «if errorlevel» должны указываться, начиная с проверки наибольшего номера пользователя в списке доступа, и далее - по убыванию. Номерами пользователей являются номера строк их идентификаторов в списке, появляющемся в процессе идентификации при входе в компьютерную систему. Этот же список можно просмотреть из оболочки администратора COBRA.EXE (см. п. 2.2.1). Для трех пользователей файл AUTUEXEC.BAT может иметь следующий вид:

```
@echo off
prompt=$p$g
path=c:\;c:\dos;c:\util;
c:\cobra\logon /f
rem Если номер польз.= 3 или >3, то переход к метке 3
    if errorlevel == 3 goto 3
rem Если номер польз.= 2 или >2, то переход к метке 2
    if errorlevel == 2 goto 2
rem Команды для первого пользователя
    d:
    cd \nom1
    goto COMMON
rem Команды для второго пользователя
:2
    d:
    cd \nom2
    goto COMMON
rem Команды для третьего пользователя
:3
    d:
    cd \nom3
rem Команды для всех пользователей
:COMMON
c:\cobra\cobratst.exe
c:\cobra\us\us.com
```

## Анализ переменной окружения

Анализ переменной окружения USER предоставляет аналогичные возможности по выполнению для каждого пользователя индивидуальной части командного файла. Следующие два примера файла AUTOEXEC.BAT эквивалентны предыдущему примеру.

***Пример 1***

```
@echo off
prompt=$p$g
path=c:\;c:\dos;c:\util;
c:\cobra\logon /f
rem Если USER=Ivanov, то переход к метке Ivanov
if %user%==Ivanov goto Ivanov
rem Если USER=Sidorov, то переход к метке Sidorov
if %user%==Sidorov goto Sidorov
rem Команды для пользователя Petrov
    d:
    cd \nom1
    goto COMMON
rem Команды для пользователя Sidorov
:Sidorov
    d:
    cd \nom2
    goto COMMON
rem Команды для пользователя Ivanov
:Ivanov
    d:
    cd \nom3
rem Команды для всех пользователей
:COMMON
c:\cobra\cobratst.exe
c:\cobra\us\us.com
```

***Пример 2***

```
@echo off
prompt=$p$g
path=c:\;c:\dos;c:\util;
c:\cobra\logon /f
goto %user%
rem Команды для пользователя Petrov
:Petrov
    d:
```

```
    cd \nom1
    goto COMMON
rem Команды для пользователя Sidorov
:Sidorov
    d:
    cd \nom2
    goto COMMON
rem Команды для пользователя Ivanov
:Ivanov
    d:
    cd \nom3
rem Команды для всех пользователей
:COMMON
c:\cobra\cobratst.exe
c:\cobra\us\us.com
```

### *4.4.2. Рекомендации по обеспечению максимальной безопасности*

Система «Кобра» предоставляет разнообразные возможности для выбора конкретного варианта защиты конфиденциальной информации (см. п. 1.3). При планировании вариантов защиты следует иметь ввиду, что максимально возможная защита от несанкционированного доступа реализуется только при следующих основных условиях:

- программой MBRINST (см. п. 3.1) защищен весь жесткий диск и загрузка компьютера осуществляется с помощью созданной ключевой дискеты;
- на всех логических дисках (кроме диска C, на котором должны содержаться только общесистемные программы, обеспечивающие загрузку компьютера) включен режим суперзащиты (см. п. 2.2.3);
- длина основных паролей выбирается в диапазоне 12 и более символов, а сами пароли не должны быть тривиальными.

При этих условиях гарантированная стойкость защиты обеспечивается сохранением в тайне используемых пользователями паролей и ключей.

Для обеспечения тайны паролей и ключей необходимо периодически выполнять соответствующий важности информации комплекс организационно-технических мероприятий с целью реализации следующих требований:

- технические средства должны быть чисты от электронных закладок (радиомаяков, «жучков» и др.);
- должна предусматриваться защита от электромагнитного, акустического и других видов излучений;
- используемые программы должны быть чистыми от программных закладок и других участков кода, направленного на перехват элементов паролей и ключей системы защиты;
- перед установкой ключевой дискеты для инициирования загрузки обязательно нажать кнопку “RESET”, а в случае ее отсутствия выключить и через 30 секунд включить компьютер, что предотвратит сохранение в оперативной памяти несанкционированной программы;
- на компьютере всегда должен быть установлен и поддерживаться режим первичной загрузки с устройства считывания ключевой дискеты для предотвращения считывания несанкционированного загрузчика с жесткого диска;
- выполнять в полном объеме при каждой загрузке операционной системы и завершении сеанса работы контроль соответствия текущих характеристик рабочей среды эталонным.

В случае, если модель нарушителя не предполагает злоумышленника среди штатного персонала, выполнение перечисленных требований оставит только единственный путь получения конфиденциальной информации - через барьер задачи математического анализа.

При предположении нарушителя среди штатного персонала, допущенного к работе на защищенной ЭВМ, необходимо настроить и исполь-

зовать дополнительную подсистему защиты LOCK (см. п. 2.3) и специальную оболочку US (см. п. 2.5), не дающие пользователю выйти за рамки штатных действий. Кроме того, следует ввести дополнительные ограничения:

- штатный персонал защищенной ЭВМ не должен иметь статуса администратора и выше;
- средства разработки и отладки программ должны быть недоступны штатному персоналу;
- начало работы и смена персонала должны производиться только в присутствии уполномоченного службы безопасности с выполнением установленных действий по завершению и началу сеанса работы на ЭВМ (в зависимости от установленного варианта защиты).

## Литература


**1.** Герасименко В.А. Защита информации в автоматизированных системах обработки данных.- В 2-х кн.- М.: Энергоатомиздат. - 1994.

**2.** Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от НСД к информации. - М.: Военное издательство. - 1992.

**3.** Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации. - М.: Военное издательство. - 1992.

**4.** Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. - М.: Военное издательство. - 1992.

**5.** Молдовян А.А., Молдовян Н.А., Молдовян П.А. Принципы построения программно-ориентированных криптосистем с неопределенным алгоритмом// УСиМ. - 1995, N 1/2. С.49 - 56.

**6.** Молдовян А.А., Молдовян Н.А. Новый принцип построения криптографических модулей в системах защиты ЭВМ// Кибернетика и системный анализ. - 1993, N 5. С.42 - 50.

**7.** Молдовян А.А. Некоторые вопросы защиты программной среды ПЭВМ// Безопасность информационных технологий. -М., МИФИ, -1995, N2. С.22-28.